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	
Configurazione WI-FI	17
NAT	
Collegamento Internet	
ETHERNET, ISDN, ADSL, HDSL, SHDSL, UMTS	
Connessione Ethernet	
Connessione ISDN	
Connessione ADSL	
Connessione UMTS tramite PCMCIA	57
Connessione UMTS tramite chiavetta USB	59
Connessione HDSL	
Tunnel Privati Virtuali (VPN)	72
IPSec e PPTP	72
Premessa	73
Configurazione di un tunnel IPSEC	74
Configurazione di un tunnel PPTP	
Configurazione DynDNS	
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 <u>reti informatiche</u> un **router**, in inglese letteralmente *instradatore*, è un <u>dispositivo di rete</u> che si occupa di instradare <u>pacchetti</u> tra reti diverse ed eterogenee. Un Router lavora al livello 3 (<u>rete</u>) del modello <u>OSI</u>, ed è quindi in grado di interconnettere reti di livello 2 eterogenee, come ad esempio una <u>LAN ethernet</u> con un collegamento geografico in tecnologia <u>frame relay</u> o <u>ATM</u>.

La funzione di <u>instradamento</u> è basata sugli indirizzi di livello 3 (rete) del modello OSI, a differenza dello <u>switch</u> 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 crescite 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 <u>broadcast</u> e razionalizza meglio le connessioni tra <u>host</u> posti su segmenti diversi.

Per fare questo sono stati messi a punto dei <u>protocolli di routing</u> appositi, come l'<u>OSPF</u> e il <u>BGP</u>, attraverso i quali i router si scambiano informazioni sulle reti raggiungibili.

Alcuni router possiedono anche un <u>firewall</u> 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 <u>access point</u> per <u>reti</u> <u>wireless</u>.

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 <u>wire speed</u>, 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: <u>www.wikipedia.org</u>]

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 riassemblaggio 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'<u>ADSL</u>).

La schermata iniziale si presenta così:

ROOT> SETUP> 🛅 192.168.177.1 - SecureCRT File Edit View Options Transfer Script Tools Help R230aw Setup Tool Funkwerk Enterprise Communications GmbH ~ r230aw System External Systems Licenses LAN : XEY-100SW, Fast Ethernet WLAN : CM-WLAN, Wireless LAN ×DSL : CM-ADSL, ADSL WAN Partner Security IPSEC IP PPP CREDITS 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 Telnet 24, 80 24 Rows, 80 Cols VT100 NUM Ready

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.

i 192.1	68.17	77.1 - Se	ecureCRT	ſ							X
<u>F</u> ile <u>E</u> dit	⊻iew	Options	<u>T</u> ransfer	Script	Tools	<u>H</u> elp					
R230aw ESWITCH	Setup]: Fas	Tool st Ether	rnet Con	figura	ation	Funkwerk	Enterpris	e Comr	nunicatio	ons GmbH r230aw	^
	Fas	st Ethei	rnet/en1	-0 >							
	Fas	st Ether	rnet/en1	1 >							
	Swj	itch Cor	nfigurat	ion >							
			EXIT								
											~
Ready				Τe	elnet	24, 80) 24 Rows, 8	30 Cols	VT100	NUM	

i	2.168.17	7.1 - Se	cureCR	Г							-		×
<u>File E</u> o	dit <u>V</u> iew	Options	<u>T</u> ransfer	<u>S</u> cript	Too <u>l</u> s	<u>H</u> elp							
R230au ESWIT(W Setup CHIESLOT	Tool 1 UNIT	O ETHI	l: Conf	igure	Funl Ethe	kwerk E rnet In 	nterpri: terface	se Comi	municati	ions r2	GmbH 30aw 	~
Int	terface	Mode	•	MAC	-Addr	ess	For	mat	VLAN	-ID			
en:	1-0	Rout	ing	00a	a0f90d	afff	Unt	agged	—				
	ADD		DE	LETE		:	SAVE		EXI	Т			Ξ
Press	<ctrl-n< td=""><td>>, ≺Ctr</td><td>`l−p> to</td><td>) scrol</td><td>.1, <s< td=""><td>pace></td><td>tag/un</td><td>tag DELB</td><td>ETE, <</td><td>Return></td><td>to e</td><td>dit</td><td>~</td></s<></td></ctrl-n<>	>, ≺Ctr	`l−p> to) scrol	.1, <s< td=""><td>pace></td><td>tag/un</td><td>tag DELB</td><td>ETE, <</td><td>Return></td><td>to e</td><td>dit</td><td>~</td></s<>	pace>	tag/un	tag DELB	ETE, <	Return>	to e	dit	~
Ready				Τe	Inet		24, 80	24 Rows,	80 Cols	VT100		NUM	

Selezionando *Add* è possibile creare altre interfacce virtuali per applicazioni avanzate. ROOT> SETUP>LAN>

🕞 192.168.177.1 - SecureCRT	
<u> Eile E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Tools	Help
R3000 Setup Tool [SWITCH][SLOT 1 UNIT 0 ETH][EDIT]: Com	Funkwerk Enterprise Communications GmbH 🔨 nfigure Interface Channel 0 r3000
Interface Mode	Routing
IP-Configuration Local IP-Number Local Netmask Second Local IP-Number Second Local Netmask Encapsulation	Manual 192.168.177.1 255.255.255.0 81.174.35.161 255.255.255.248 Ethernet II
MAC Address Frame Format	Untagged
Advanced Settings >	
SAVE	CANCEL
Use <space> to select</space>	

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	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Tools	Help
R3000 Setup Tool [SWITCH]: Fast Ethernet Configuration	Funkwerk Enterprise Communications GmbH 🔨 r3000
Fast Ethernet/en1-0 >	
Fast Ethernet/en1-1 $>$	
Fast Ethernet/en1-4 >	
Switch Configuration $>$	
EXIT	

📠 192.168.177.1 - SecureC	RT	
<u>File Edit View O</u> ptions <u>T</u> ransfe	er <u>S</u> cript Too <u>l</u> s <u>H</u> elp	
R3000 Setup Tool [SWITCH][ASSIGN]: Switch] 	Funkwer Interface Assignment	k Enterprise Communications GmbH 🟊 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	CAI	NCEL
Use <space> to select</space>		

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.

🕞 192.168.177.1 - SecureCRT	
<u>File Edit View O</u> ptions <u>T</u> ransfer <u>S</u> cript Tools	Help
R3000 Setup Tool [SWITCH][SLOT 1 UNIT 0 ETH][EDIT]: Cor	Funkwerk Enterprise Communications GmbH 🔨 nfigure Interface Channel 0 r3000
Interface Mode	Routing
IP-Configuration Local IP-Number Local Netmask Second Local IP-Number Second Local Netmask Encapsulation	Manual 192.168.177.1 255.255.255.0 81.174.35.161 255.255.255.248 Ethernet II
MAC Address Frame Format	Untagged
Advanced Settings >	
SAVE	CANCEL
Use <space> to select</space>	

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*

🕞 192.168.177.1 - SecureCRT	
<u>File Edit View Options Transfer Script Tools</u>	Help
R3000 Setup Tool	Funkwerk Enterprise Communications GmbH 🔨 r3000
Licenses System	External Systems
Physical Interfaces: AUX: Console LAN: Ethernet Switch ISDN: BRI2-0 BRI2-1 DSL: ADSL	
WAN Partner Security PPTP IPSEC IP PPP X.25 FR BRRP CREDITS CAPI	ATM QoS VOIP GRE L2TP VLAN
Configuration Management Monitoring and Debugging Exit	
Press (Ctrl-n), (Ctrl-p) to scroll thr	ough menu items, <return> to enter</return>

📠 192.168.177.1 - Secure	CRT 📃 🗖 🔀								
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> rans	fer <u>S</u> cript Tools <u>H</u> elp								
R3000 Setup Tool [IP]: IP Configuration 	Funkwerk Enterprise Communications GmbH 🛧 r3000								
Routing Static Settings Network Address Translation UPnP Bandwidth Management (TDRC / Load Balancing / BOD) IP Address Pools BOOTP Relay BOOTP Relay SNMP Remote Authentication (RADIUS/TACACS+) DNS DynDNS Routing Protocols Multicast									
	EATI								
Press (Ctrl-n), (Ctrl-p)	to scroll through menu items, <return> to enter</return>								

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



	192.1	168.17	77.1 - Se	cureCRT	Г							×
File	<u>E</u> dit	⊻iew	Options	<u>T</u> ransfer	Script	Tools	<u>H</u> elp					
R30 EIF	00 S 900 S 900Y	etup 1 NAMIC: 	[ool][POOL]; 	: Dynami	c IP ƙ	Addres	Funk s Pool	werk Ent s 	erprise	Communicatio	ns GmbH r3000	^
	Id	Desci	ription	IP Add	ress		Range	Primary	DNS	Secondary	DNS	
	<u>90</u>	0		DE	LETE			EXIT				*

🖬 192.168.177.1 - SecureCRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Tools <u>H</u> elp	
R3000 Setup Tool	werk Enterprise Communications GmbH 🟊 P Addresses r3000
Identifier Description IP Address Number of Consecutive Addresses Primary Domain Name Server Secondary Domain Name Server	0 LAN 192.168.177.50 10 192.168.177.1 0.0.0.0
SAVE	CANCEL
Enter integer value	

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

	192.1	168.17	77.1 - Se	ecureCRT	Г							×
File	<u>E</u> dit	⊻iew	Options	Transfer	Script	Tools	<u>H</u> elp					
R30 EIF 	00 S JEDY	etup 1 NAMIC: 	[ool][POOL]: 	: Dynami	с IР (Addres	Funk s Pool	werk Ent s 	erprise	Communicatio	ns GmbH r3000	+ <mark>~</mark> }
	Id 0	Desci LAN	ription	IP Add 192,16	ress 8,177	.50	Range 10	Primary 192,168	DNS .177.1	Secondary 0.0.0.0	DNS	
	<u>90</u>	•		DE	LETE			EXIT				



🖬 192.168.177.1 - SecureCRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Tools <u>H</u> elp	
R3000 Setup Tool Funk [IP][DYNAMIC][DHCP][ADD]: Define DHCP Pool U: 	werk Enterprise Communications GmbH 🟊 sage r3000
Interface Pool Assignment Mode Lease Time (minutes, O=disabled) Gateway First TFTP Server Second TFTP Server Radius Accounting Radius Group Id Alive Check Alive Test Period (seconds, O=disabled) Admin State	en1-0 LAN local 120 0.0.0.0 0.0.0.0 disabled 0 disabled 0 enabled
SAVE	CANCEL

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.

E 192 168 0 254 - SecureCPT
File Edit View Options Transfer Script Tools Help
R230aw Setup Iool Europe Toop Europe Functions SmbH
r230aw
Licenses System External Systems
LAN : XEY-100SW, Fast Ethernet
WLAN : <u>DM-WLAN, Wireless LAN</u> xDSL : CM-ADSL, ADSL
WAN Partner Security IPSEC IP PPP CREDITS ATM QoS VoIP L2TP VLAN
Configuration Management Monitoring and Debugging Exit
Press 〈Ctrl-n〉, 〈Ctrl-p〉 to scroll through menu items, 〈Return〉 to enter
🖬 192.168.177.1 - SecureCRT
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp
R230aw Setup Tool Funkwerk Enterprise Communications GmbH A [WLAN-1]: Configure WLAN Interface r230aw
Operation Mode Access Point >
Location Italy
Radio Band 2,4 GHz

1

Telnet

Channel

Advanced >

Ready

VSS Configuration >

SAVE

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

Sel. Channel

6

CANCEL

NUM

24, 80 | 24 Rows, 80 Cols | VT100

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

🖬 192.168.0.254 - SecureCRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript	Tools Help
R230aw Setup Tool [WLAN-1][MODE]: Select Operation	Funkwerk Enterprise Communications GmbH 🔼 Mode r230aw
Operation Mode	Access Point
SAVE	CANCEL
File Edit View Options Transfer Script	Tools Help
R230aw Setup Tool [WLAN-1]: Configure WLAN Interfac 	Funkwerk Enterprise Communications GmbH 📩 e r230aw
Operation Mode	Access Point >
Location	Italy
Radio Band	2.4 GHz
Channel	11
VSS Configuration $>$	
havanceu /	
SAVE	CANCEL

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 - SecureCR	ľ		×
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer	Script Tools Help		
R230aw Setup Tool [WLAN-1][WIRELESS]: Interfa	Funkwerk Enterprise Communicatio ace List	ns GmbH r230aw	^
Network Name	Status Security ACL-Filter interface		
*Funkwerk-ec	enable NONE disable vss1-0		
ADD DE	ELETE EXIT		
Press (Ctrl-n), (Ctrl-p) to	o scroll, <space> tag/untag DELETE, <return> t</return></space>	o edit	*

🕞 192.168.0.254 - SecureCRT		
<u>File Edit View Options Transfer Script</u>	Tools Help	
R230aw Setup Tool [WLAN-1][WIRELESS][EDIT]: Wireles: 	Funkwerk Enterprise Communications GmbH 🖪 s Interface (Funkwerk-ec) r230aw	J
AdminStatus Network Name Name is visible Local Communication	enable Funkwerk-ec yes enabled	
Security Mode	NONE	
IP and Bridging > ACL Filter > SAVE	CANCEL	
Use <space> to select</space>		

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.

To 192.168.177.1 - SecureCRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Tools	Help
R230aw Setup Tool [SWITCH][SLOT 1 UNIT 2 ETH][EDIT]: Co 	Funkwerk Enterprise Communications GmbH 🔼 nfigure Interface Channel 0 r230aw
Interface Mode Bridge Interface	Bridging br0
IP-Configuration Local IP-Number Local Netmask Second Local IP-Number Second Local Netmask	Manual 172.16.1.1 255.255.0.0
Advanced Settings >	
SAVE	CANCEL
Use <space> to select</space>	
Ready Telnet	24 80 24 Rows 80 Cols VT100 NUM .:
	21, 00 211003, 00 003 11100 1001
🖬 192.168.177.1 - SecureCRT	
ia 192.168.177.1 - SecureCRT File Edit <u>V</u> iew Options <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s	
Image: Secure CRT File Edit View Options Iransfer Script Tools R230aw Setup Tool Image: Script CONFIGURA CWLAN-13EWIRELESSSIEDITJEIP CONFIGURA Image: Script Constraints	Help Funkwerk Enterprise Communications GmbH
Image: Secure CRT Eile Edit Yiew Options Iransfer Script Tools R230aw Setup Tool Image: Script CONFIGURA CWLAN-13EWIRELESSSIEDITJEIP CONFIGURA Image: Script CONFIGURA Interface Mode Bridge Interface	Help Help Funkwerk Enterprise Communications GmbH TION]: Interface <200000> r230aw Bridging br0
Image: Second Control File Edit View Options Iransfer Script Tools R230aw Setup Tool [WLAN-1][WIRELESS][EDIT][IP CONFIGURA Interface Mode Bridge Interface IP-Configuration Local IP-Number Local Netmask Second Local IP-Number Second Local Netmask	Help Funkwerk Enterprise Communications GmbH TION]: Interface <200000> r230aw Bridging br0 Manual 172.16.1.1 255.255.0.0
Image: Second Control File Edit View Options Iransfer Script Tools R230aw Setup Tool IWLAN-1JEWIRELESSJEEDITJEIP CONFIGURA	Help Funkwerk Enterprise Communications GmbH IION]: Interface <200000> r230aw Bridging br0 Manual 172.16.1.1 255.255.0.0
Image: Second Control File Edit View Options Transfer Script Tools R230aw Setup Tool CWLAN-1JEWIRELESSJEEDITJEIP CONFIGURA	Help Funkwerk Enterprise Communications GmbH IION]: Interface <200000> r230aw Bridging br0 Manual 172.16.1.1 255.255.0.0 CANCEL
Image: Second Control File Edit View Options Transfer Script Tools R230aw Setup Tool CWLAN-1JEWIRELESSJEEDITJEIP CONFIGURA	Help Funkwerk Enterprise Communications GmbH IION]: Interface <200000> r230aw Bridging br0 Manual 172.16.1.1 255.255.0.0 CANCEL

🖬 192.168.0.254 - SecureCRT		
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript	Tools <u>H</u> elp	
R230aw Setup Tool [WLAN-1][WIRELESS][EDIT]: Wireles	Funkwerk Enterprise Communications (s Interface (Funkwerk-ec) r2	GmbH 🔼 30aw
AdminStatus Network Name Name is visible Local Communication	disable Funkwerk-ec yes enabled	
Security Mode Default Key	WEP 40/64 Key 1	
Key 1 Key 2 Key 3 Key 4		
IP and Bridging > ACL Filter > SAVE	CANCEL	
Use 〈Space〉 to select		

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*.

🖻 192.168.0.254 - SecureCRT		
<u> Edit View Options Transfer Script</u>	Tools Help	
R230aw Setup Tool [WLAN-1][WIRELESS][EDIT][ACCESS L 	Funkwerk Enterprise Communications IST]: Interface <funkwerk-ec> r</funkwerk-ec>	s GmbH 🔼 ~230aw
AdminStatus	disable	
Accept Address	ADD	
ACCEPT	DENIED	
Press 'a' to move selected R	eject Address to Accept List.	
SAVE REMOVE	EXIT REFRESH	
Enter string, max length = 12 cha	ins	•

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.

🖬 192.168.0.254 - SecureCRT						
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript	Tools Help					
R230aw Setup Tool [WLAN-1]: Configure WLAN Interface	Funkwerk Enterprise Communications GmbH 🔥 e r230aw					
Operation Mode	Access Point >					
Location	Germany					
Radio Band	2,4 GHz					
Channel	11					
VSS Configuration >						
Advanced >						
SAVE	CANCEL					
	· · · · · · · · · · · · · · · · · · ·					

1	92.1	68.0.	254 - S	ecureCRT	Г								×
Eile	<u>E</u> dit	⊻iew	Options	Transfer	<u>S</u> cript	Tools	Help						
R230 EWLA)aw (N-1)	Setup JEADVA	Tool WCEDJ:	WLAN Sp	ecific	: Sett	Funkwe ings 	erk	Enterpr.	ise	Communicati	ons GmbH r230aw	~
		Wir	reless	Mode		802.	11 mixeo	1					
		Ma>	kimum B	itrate		AUTO							
		FOL	JR-X Bu	rst		on							
		ТΧ	Power	(dBm)		15							
				SAVE					Ci	ANCE	EL		
Üse	<spa< td=""><td>ace> t</td><td>o sele</td><td> ct</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>~</td></spa<>	ace> t	o sele	 ct									~

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>

1	92.16	58.17	7.1	Sec	ureCRT							
File	Edit	⊻iew	Optio	ns <u>T</u> i	ransfer	<u>S</u> cript	Tools	<u>H</u> elp				
R30 EIP	00 Set JENAT:	tup T]: NA	iool NT Co	nfigu	uratio	٦		Funkwe	ərk	Enterprise Commur	nicati(ons GmbH 🔨 r3000
S	elect	IP I	inter	face	to be	confi	igured	d for NA	Г			
N	ame				Nat	St	atic	mapping: Dutside	S	Static mappings		
ei ei ei ei	n1-0 n1-0-s n1-4 n1-4-s thoa5(thoa5(gi	snap snap)-0)-0-s	nap		off off off off off off	+	0 0 0 0 0 0 25	Jutside		from Inside 0 0 0 0 0 0 0 2		_
E	XIT											
Pre	ss <ct< td=""><td>trl-n</td><td>n>, <</td><td>Ctrl</td><td>-p> to</td><td>scrol</td><td>ll, <r< td=""><td>Return> 1</td><td>lo s</td><td>elect/edit</td><td></td><td>v</td></r<></td></ct<>	trl-n	n>, <	Ctrl	-p> to	scrol	ll, <r< td=""><td>Return> 1</td><td>lo s</td><td>elect/edit</td><td></td><td>v</td></r<>	Return> 1	lo s	elect/edit		v

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 remoro, 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>

i 192.168.177.1 - SecureCR	ſ		
<u>File Edit View Options Transfer</u>	<u>Script</u> Too <u>l</u> s	ls <u>H</u> elp	
R3000 Setup Tool [IP][NAT][EDIT]: NAT Config 	uration (n	Funkwerk Enterprise Communications ngi) r 	GmbH 🔨 3000
Network Address Translati Silent Deny PPTP Passthrough	on	on no no	
Enter configuration for s	essions :	requested from OUTSIDE requested from INSIDE	
SAVE CA	INCEL		
			~

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.

192.168.17	7.1 - SecureCRT	3
<u>F</u> ile <u>E</u> dit ⊻iew	<u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Tools <u>H</u> elp	
R230aw Setup [IP][NAT][ED]	Tool Funkwerk Enterprise Communications GmbH TICOUTSIDE]: NAT - sessions from OUTSIDE (ngi) r230aw	•
Abbreviation	ns : r(remote) i(internal) e(external) a(address) p(port)	
Service	Conditions	
900		
	DELETE EXIT	
		111
		•
Ready	Telnet 24, 80 24 Rows, 80 Cols VT100 NUM	.:

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.

🖬 192.168.177.1 - SecureCRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> e	cript Too <u>l</u> s <u>H</u> elp
R3000 Setup Tool [IP][NAT][EDIT][OUTSIDE][ADD] 	Funkwerk Enterprise Communications GmbH 🔨 : NAT - sessions from OUTSIDE (ngi) r3000
Description Service	http
Remote Address Remote Mask	
External Address External Mask	81,174,35,162 255,255,255,255
Internal Address Internal Mask Internal Port	192.168.177.50 255.255.255.255 any
SAVE	CANCEL

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.

<u>Suggerimento</u>: 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 <u>ping</u> (per controllare da remoto se la connessione ADSL è attiva) e il <u>telnet</u> (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.

🖬 192.168.177.1 - SecureCRT		
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> o	cript Tools <u>H</u> elp	
R3000 Setup Tool [IP][NAT][EDIT][OUTSIDE][EDIT 	Funkwerk Enterprise Communications]: NAT - sessions from OUTSIDE (ngi) r	GmbH 🔼 -3000
Description Service Protocol	ping user defined icmp	
Remote Address Remote Mask		
External Address External Mask External Port	any	
Internal Address Internal Mask Internal Port	127.0.0.1 255.255.255.255 any	
SAVE	CANCEL	
Enter string, max length = 35	chars	~

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

🖬 192.168.177.1 - SecureCRT	
<u> Eile Edit View O</u> ptions <u>T</u> ransfer S	cript Tools Help
R3000 Setup Tool [IP][NAT][EDIT][OUTSIDE][EDI]	Funkwerk Enterprise Communications GmbH 🔨 []: NAT - sessions from OUTSIDE (ngi) r3000
Description Service	telnet telnet
Remote Address Remote Mask	
External Address External Mask	
Internal Address Internal Mask Internal Port	127.0.0.1 255.255.255.255 any
SAVE	CANCEL
Enter string, max length = 3	j chars

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*"

🖬 192.168.177.1 - SecureCRT	X
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp	
R230aw Setup Tool Funkwerk Enterprise Communications GmbH [IP][NAT][EDIT]: NAT Configuration (ngi) r230au	Η 🔼 υ -
Network Address Translation on Silent Deny no PPTP Passthrough no	
Enter configuration for sessions : requested from OUTSIDE requested from INSIDE	
SAVE CANCEL	
	~
Ready Telnet 24, 80 24 Rows, 80 Cols VT100 NU	M

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 servizion SMTP (invio di posta elettronica)

a 192.168.177.1 - SecureCRT		
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u>	cript Too <u>l</u> s <u>H</u> elp	
R230aw Setup Tool [IP][NAT][EDIT][EDIT]: NAT 	Funkwerk Enterprise Communication Configuration - sessions from INSIDE (ngi) 	ns GmbH 📩 r230aw
Service	smtp	
Remote Address Remote Mask		
External Address External Mask External Port	81.174.35.166 255.255.255.255 any	
Internal Address Internal Mask Internal Port	192.168.177.105 255.255.255.255 any	
SAVE	CANCEL	
Use <space> to select</space>		~
Ready	Telnet 24, 80 24 Rows, 80 Cols VT100	NUM:

<u>Suggerimento</u>: 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.

192.168.177.1 - SecureC	RT		
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransf	er <u>S</u> cript Too <u>l</u> s <u>H</u> elp		
R230aw Setup Tool [SWITCH][ASSIGN]: Switch 	Funkwer Interface Assignment 	k Enterprise Communications r2	GmbH 🔼 230aw
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	CA	NCEL	
Use <space> to select</space>			~
Ready	Telnet 24, 8	0 24 Rows, 80 Cols VT100	NUM 📑

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

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

🖬 192.168.177.1 - SecureCRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s	Help
R230aw Setup Tool [SWITCH][SLOT 1 UNIT 1 ETH][EDIT]: Cor	Funkwerk Enterprise Communications GmbH 🔼 nfigure Interface Channel 0 r230aw
Interface Mode	Routing
IP-Configuration Local IP-Number Local Netmask Second Local IP-Number Second Local Netmask	Manual 192.168.1.1 255.255.255.0
Encapsulation	Ethernet II
MAC Address Frame Format	Untagged
Advanced Settings >	
SAVE	CANCEL
Use <space> to select</space>	
Ready Telnet	24, 80 24 Rows, 80 Cols VT100 NUM 🛒

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 defaul gateway è rappresentato dal modem ADSL o del ponte radio al quale abbiamo collegato il router Bintec.

🖬 192.168.177.1 - SecureCRT
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp
R230aw Setup Tool Funkwerk Enterprise Communications GmbH 🔼 r230aw
Licenses System External Systems
LAN : XEY-100SW, Fast Ethernet
WLAN : CM-WLAN, Wireless LAN ×DSL : CM-ADSL, ADSL
WAN Partner Security IPSEC IP PPP CREDITS 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</return></ctrl-p></ctrl-n>
Ready Telnet 24, 80 24 Rows, 80 Cols VT100 NUM

🗖 192.168.177.1 - Secure	CRT 📃 🗖	×
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> rans	sfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp	
R230aw Setup Tool [IP]: IP Configuration 	Funkwerk Enterprise Communications GmbH 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></ctrl-p></ctrl-n>	to scroll through menu items, <return> to enter</return>	~
Ready	Telnet 24, 80 24 Rows, 80 Cols VT100 NUM	1.33

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

📠 192.168.177.1 - SecureCR	Г	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer	<u>S</u> cript Too <u>l</u> s	Help
R230aw Setup Tool [IP][ROUTING][ADD]		Funkwerk Enterprise Communications GmbH / r230aw
Route Type Network	Default LAN	route
Gateway IP-Address Metric	192.168. 1	.1.254
5AVE		CANCEL
l Ready	Telnet	24, 80 24 Rows, 80 Cols VT100 NUM

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

🗖 192.168.177.1 - Secure	crt 📃 🗖 🔀
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ran	sfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp
R230aw Setup Tool [IP]: IP Configuration 	Funkwerk Enterprise Communications GmbH 🙍 r230aw
	Routing Static Settings Network Address Translation UPnP Bandwidth Management (TDRC / Load Balancing / BOD) IP Address Pools BODTP 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</return>
Ready	Telnet 24, 80 24 Rows, 80 Cols VT100 NUM

1	92.16	8.17	7.1 - Se	ecureCRT	ſ						×
<u>F</u> ile	<u>E</u> dit <u>V</u>	jew	Options	<u>T</u> ransfer	<u>S</u> cript	Too <u>l</u> s	<u>H</u> elp				
R230 [IP]	aw Se [NAT] 	tup : NA	Tool T Confi 	iguratio	n		Funkwerk	Enterprise	Communicatio	ons GmbH r230aw	~
Se	lect 3	IP I	nterfa	ce to be	confi	.gured	l for NAT				
Na	me			Nat	St	atic	mappings Nutaida	Static map	opings		
en	1-0			off	т	0	Jucside	100 INS: 0	Lae	=	
en	1-0-si	nap		off		0		0			
en an	1-1 1-1-s	nap		off		Ö		0			
et	hoa50	-0		off		Ó		Ó		i	
et	hoa50 [.]	-0-s	nap	off		0		୍			
ng ve	1 rso_r:	izzu	ti	on off		0		0		v	
EX	IT										
 Pres	s <ct< td=""><td>rl-n</td><td>>, <cti< td=""><td>rl-p> to</td><td>scrol</td><td>1, <r< td=""><td>Return> to s</td><td>select/edit</td><td></td><td></td><td>~</td></r<></td></cti<></td></ct<>	rl-n	>, <cti< td=""><td>rl-p> to</td><td>scrol</td><td>1, <r< td=""><td>Return> to s</td><td>select/edit</td><td></td><td></td><td>~</td></r<></td></cti<>	rl-p> to	scrol	1, <r< td=""><td>Return> to s</td><td>select/edit</td><td></td><td></td><td>~</td></r<>	Return> to s	select/edit			~
Ready					Τe	Inet	24, 80	24 Rows, 80	Cols VT100	NUM	1.1

192.168.177.1 -	SecureCRT							×
<u>File E</u> dit <u>V</u> iew <u>O</u> ption	s <u>T</u> ransfer <u>S</u> cript	Too <u>l</u> s <u>H</u> elp	I					
R230aw Setup Tool [IP][NAT][EDIT]: N 	AT Configuratio	Fu on (en1-1)	unkwerk E	Enterpris	se Comm	unicatio	ons GmbH r230aw	~
Network Address Silent Deny PPTP Passthrough	Translation	an na	1 D D					
Enter configurat	ion for session	ns: re re	equested equested	from OUT from INS	SIDE SIDE			
SAVE	CANCEL							
Use <space> to sel</space>	ect							-
Ready	Τe	elnet	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 $IP \rightarrow Static Settings$

🗖 192.168.177.1 - Secure	CRT 📃	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> rans	sfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp	
R230aw Setup Tool [IP]: IP Configuration 	Funkwerk Enterprise Communications G r23	imbH 🔼 30aw
	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</return>	~
Ready	Telnet 24, 80 24 Rows, 80 Cols VT100	NUM 📑

To 192.168.177.1 - SecureCRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>F</u>	<u>H</u> elp
R230aw Setup Tool [IP][STATIC]: IP Static Settings 	Funkwerk Enterprise Communications GmbH 🔼 r230aw
Domain Name Primary Domain Name Server Secondary Domain Name Server Primary WINS Secondary WINS	nextmedia.local 151.99.125.3 151.99.125.1 192.168.177.105 192.168.177.106
Remote CAPI Server TCP port Remote TRACE Server TCP port RIP UDP port	2662 7000 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.

- 192.168.177.1 - SecureCRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Tools	Help
R3000 Setup Tool	Funkwerk Enterprise Communications GmbH 🔨 r3000
Licenses System	External Systems
Physical Interfaces: AUX: Console LAN: Ethernet Switch ISDN: BRI2-0 BRI2-1 DSL: ADSL	
<mark>MAN Partner</mark> Security PPTP IPSEC IP PPP X.25 FR BRRP CREDITS CAPI	ATM QoS VoIP GRE L2TP VLAN
Configuration Management Monitoring and Debugging Exit	
Press (Ctrl-n), (Ctrl-p) to scroll thro	ough menu items, <return> to enter</return>

Nella sezione WAN Partner andiamo ad aggiungere una voce

🖬 192.168.177.1 - SecureCRT	
<u>File Edit View Options Iransfer Script</u>	Tools <u>H</u> elp
R3000 Setup Tool [WAN][ADD]: Configure WAN Partner 	Funkwerk Enterprise Communications GmbH 🔨 r3000
Partner Name	ISDN_prova
Encapsulation Encryption Compression Calling Line Identification	PPP none none no
PPP > Advanced Settings > WAN Numbers >	
IP > Bridge >	
SAVE	CANCEL
Enter string, max length = 25 cham	rs

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.
🖬 192.168.177.1 - SecureCRT	
<u>File Edit View Options Transfer Script</u> To	ols <u>H</u> elp
R3000 Setup Tool [WAN][ADD][PPP]: PPP Settings (ISDN 	Funkwerk Enterprise Communications GmbH
Authentication C Partner PPP ID Local PPP ID 1 PPP Password 8	HAP + PAP ughino@libero.it ******
Keepalives o Link Quality Monitoring o	ff ff
ок	CANCEL
Change password, max length = 40 ch	ars

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

🖬 192.168.177.1 - SecureCRT		K
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript	Tools Help	
R3000 Setup Tool [WAN][ADD][WAN NUMBERS][ADD]: Ad 	Funkwerk Enterprise Communications GmbH or Change WAN Numbers (ISDN_prova) r3000	~
Number Direction	7027020000 outgoing	
Advanced Settings >		
SOVE	CONCEL	
Enter string, max length = 40 ch	ars	×

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

🗖 192.168.177.1 - SecureCRT	×
<u>File Edit View Options Transfer Script Tools Help</u>	
R3000 Setup Tool Funkwerk Enterprise Communications GmbH [WAN][ADD][IP]: IP Settings (ISDN_prova) r3000	^
Basic IP-Settings >	
Advanced Settings >	
EVIT	
EXII	
	~

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).

🖬 192.168.177.1 - SecureCRT	
<u>File Edit View Options Transfer Script Tools</u>	Help
R3000 Setup Tool [WAN][ADD][IP][BASIC]: IP-Settings (IS 	Funkwerk Enterprise Communications GmbH 🛧 DN_prova) r3000
IP Transit Network	dynamic client
Enable NAT Default Route	yes yes
59VE	

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							×
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer	<u>S</u> cript Too <u>l</u> s (<u>H</u> elp					
R230aw Setup Tool [MONITOR]: Monitoring and De 	bugging	Funkwer	rk Enterpr	ise Com	municati	lons GmbH r230aw	^
	ISDN Monit ISDN Credi xDSL Credi	or ts ts	ATM/OA ADSL	М			
	<mark>Interfaces</mark> Messages Email Aler TCP/IP IPSec	t	IP QoS SSHD				
	EXIT						
							~
Ready	Telnet	24, 8	80 24 Row:	s, 80 Cols	VT100	NUM	1:

🗖 192.168.177.1 - Secure	CRT					×
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> rans	;fer <u>S</u> cript Too	<u>l</u> s <u>H</u> elp				
R230aw Setup Tool [MONITOR][INTERFACE]: In 	terface Moni	Funkw toring	erk Enterpr	rise Communi	cations GmbH r230aw 	^
Interface Name Operational Status	en1-0 up		ngi up			
	total	per seco	nd tota	al per	second	
Received Packets Received Octets Received Errors	1005087 716910750 0	3 192	7748 4593 0	307 1 329586 102		
Transmit Packets Transmit Octets Transmit Errors	875351 491948540 0	2 231	9010 6707 0)18 0 754345 0		
Active Connections Duration	N/A N/A		1 5025	53		
EXIT	EXTENDED		EXTE	INDED		
Use <space> to select</space>						~
Ready	Telnet	24,	80 24 Row	s, 80 Cols VT1	.00 NUM	1

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 "*Phisical Connection*" sia "yes" (significa che il doppino è collegato e c'è la portante della linea ADSL).

ROOT> SE	ETUP>

🕞 192.168.177.1 - SecureCRT	
<u> Eile E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Tools	Help
R3000 Setup Tool	Funkwerk Enterprise Communications GmbH 🔨 r3000
Licenses System	External Systems
Physical Interfaces: AUX: Console LAN: Ethernet Switch ISDN: BRI2-0 BRI2-1 DSL: 205	
WAN Partner Security PPTP IPSEC IP PPP X.25 FR BRRP CREDITS CAPI	ATM QoS VoIP GRE L2TP VLAN
Configuration Management Monitoring and Debugging Exit	
Press (Ctrl-n>, (Ctrl-p> to scroll thro	ough menu items, <return> to enter</return>

ROOT> SETUP>xDSL>

192.168.177.1 - SecureCRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp	
R3000 Setup Tool Funkwerk Enterprise [ADSL]: ADSL settings 	Communications GmbH 🔨 r3000
Physical connection established: yes ADSL Trained Mode: ADSL1	
ADSL Configured Mode: <u>Multimode</u> Annex Type: Annex A Verify ATM Configuration >	
Transmit shaping: disabled	
SAVE CANCE	Ľ
Use <space> to select</space>	

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 <u>è indispensabile</u> <u>configurare anche un WAN Partner</u>.

RPoA: altrimenti detta **IPoA** o **RFC1483** non prevede autenticazione ed è legata al doppino físico 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 <u>non prevede la configurazione di un WAN Partner</u>.

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>

🖬 192.168.177.1 - SecureCRT	
<u>Eile E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>F</u>	<u>t</u> elp
R3000 Setup Tool	Funkwerk Enterprise Communications GmbH 🔨 r3000
Licenses System	External Systems
Physical Interfaces: AUX: Console LAN: Ethernet Switch ISDN: BRI2-0 BRI2-1 DSL: ADSL	
WAN Partner Security PPTP IPSEC IP PPP X.25 FR BRRP CREDITS CAPI	ATM QOS VOIP GRE L2TP VLAN
Configuration Management Monitoring and Debugging Exit	
Press <ctrl-n>, <ctrl-p> to scroll thro</ctrl-p></ctrl-n>	ugh menu items, <return> to enter</return>

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>

🕞 192.168.177.1 - SecureCRT	
<u>File Edit View Options Transfer Script Tool</u> s	Help
R3000 Setup Tool [ATM][PPPOA][EDIT] 	Funkwerk Enterprise Communications GmbH 🔨 r3000
Description	ngi
ATM Interface	fcca-3-0
Virtual path identifier (VPI) Virtual channel identifier (VCI)	8 00 35
Encapsulation	VC Multiplexing
Client Type	On Demand (Dialup)
SAVE	CANCEL
Enter integer range 0255	

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 <u>sempre</u> "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.

🖬 192.168.177.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R3000 Setup Tool Funkwerk Enterprise Communications GmbH A r3000
icenses System External Systems
Physical Interfaces: AUX: Console LAN: Ethernet Switch ISDN: BRI2-0 BRI2-1 DSL: ADSL
W <mark>AN Partner</mark> Security PPTP IPSEC IP PPP X.25 FR BRRP 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 🗾 🚽

ROOT> SETUP>WAN Partner>ADD>

🖬 192.168.177.1 - SecureCRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript	Tools Help
R3000 Setup Tool [WAN][EDIT]: Configure WAN Partne	Funkwerk Enterprise Communications GmbH < er r3000
Partner Name	ngi
Encapsulation Encryption Compression	PPP none none
PPP > Advanced Settings >	
IP > Bridge >	
SAVE	CANCEL

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

ROOT> SETUP>WAN Partner>ADD>PPP>

📠 192.168.177.1 - SecureCRT		
<u> Edit View Options Transfer Script</u>	t Tools <u>H</u> elp	
R3000 Setup Tool [WAN][EDIT][PPP]: PPP Settings (Funkwerk Enterprise Communicati (ngi) 	ons GmbH 🔨 r3000
Authentication Partner PPP ID Local PPP ID PPP Password Keepalives Link Quality Monitoring	CHAP + PAP 1466552008 ******** off on	
ОК	CANCEL	
Use <space> to select</space>		*

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>

🖬 192.168.177.1 - SecureCRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s I	<u>H</u> elp
R3000 Setup Tool [WAN][EDIT][ADVANCED]: Advanced Setting	Funkwerk Enterprise Communications GmbH 🛧 s (ngi) r3000
Callback Static Short Hold (sec) Idle for Dynamic Short Hold (%) Delay after Connection Failure (sec) Layer 1 Protocol	no -1 0 10 PPP over ATM (PPPoA)
Extended Interface Settings >	
Special Interface Types	none
ОК	CANCEL
Use <space> to select</space>	

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: <u>indichiamo il tipo di ADSL precedentemente impostato nella sezione ATM.</u> 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>

🖬 192.168.177.1 - SecureCRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript	Tools <u>H</u> elp
R3000 Setup Tool [WAN][EDIT]: Configure WAN Partne	Funkwerk Enterprise Communications GmbH 🔨 er r3000
Partner Name	ngi
Encapsulation Encryption Compression	PPP none none
PPP > Advanced Settings >	
IP > Bridge >	
SAVE	CANCEL

ROOT> SETUP>WAN Partner>ADD>IP>

Te 192.168.177.1 - SecureCRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp	
R3000 Setup Tool Funkwerk Enterprise Communicat [WAN][EDIT][IP]: IP Settings (ngi)	tions GmbH 🔨 r3000
Basic IP-Settings >	
More Routing >	
Advanced Settings >	
EXIT	
	 *

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

🗖 192.168.177.1 - SecureCRT	
<u>File Edit View Options Transfer Script Tools I</u>	Help
R3000 Setup Tool [WAN][EDIT][IP][BASIC]: IP-Settings (ng	Funkwerk Enterprise Communications GmbH < i) r3000
IP Transit Network	dynamic client
Enable NAT Default Route	yes yes
SAVE	CANCEL
Use <space> to select</space>	▼

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:

192.168.177.1	- SecureCRT								
<u>File E</u> dit <u>V</u> iew <u>O</u> ptio	ns <u>T</u> ransfer <u>S</u> cript	Tools <u>H</u> elp							
R3000 Setup Tool [IP][ROUTING]: IP	'Routing	Funkwerk Enter	prise Communicatio	ns GmbH 🔨 r3000					
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 81.174.0.1 81.174.35.160 192.168.177.0 default	Gateway 78.134.13.157 81.174.35.161 192.168.177.1	Mask Flag 255,255,255,255 UH 255,255,255,248 US 255,255,255,0 U 0,0,0,0 UI	s Met, Interface 0 ngi 0 en1-0 0 en1-0 1 ngi	Pro oth loc loc loc					
<u>900</u>	ADDEXT	DELETE	EXIT						
				~					

La <u>prima</u> 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 <u>seconda</u> riga è un indirizzo pubblico aggiuntivo (comprato dal Provider) ed è stato impostato come secondo indirizzo (fisico) della LAN.

La <u>terza</u> 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'<u>quarta</u> 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>

i 192	2.16	8.177.	1 - Se	ecureCRT	-							
<u>File</u>	dit <u>V</u>	jew <u>O</u> p	otions	Transfer	Script	Tools	Help					
R3000 [IP]:	Set IP	up Too Config	l urati 	ion			Funkwer	k Enterpr	rise	Communica	tions	: GmbH 🔼 r3000
				Ro Ne UP BA IP BO SNe IV RO N RO N RO NO	uting atic S twork nP ndwidt Addre OTP Re MP s nDNS uting lticas	ettin Addre h Mar ss Po lay uther uther t	nagement (hagement (hols ntication hocols	ation TDRC / Lo (RADIUS/T	oad B	alancing S+)	/ BOI))
				EX	IT							
Press	<ct< td=""><td>rl−n>,</td><td><ct:< td=""><td>rl-p> to</td><td>scrol</td><td>l thr</td><th>ough menu</th><td>items, <</td><td>Retu</td><td>rn> to en</td><th>ter</th><th>•</th></ct:<></td></ct<>	rl−n>,	<ct:< td=""><td>rl-p> to</td><td>scrol</td><td>l thr</td><th>ough menu</th><td>items, <</td><td>Retu</td><td>rn> to en</td><th>ter</th><th>•</th></ct:<>	rl-p> to	scrol	l thr	ough menu	items, <	Retu	rn> to en	ter	•

ROOT> SETUP>IP>IP Static Settings>

📠 192.168.177.1 - SecureCRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Tools	Help
R3000 Setup Tool [IP][STATIC]: IP Static Settings	Funkwerk Enterprise Communications GmbH 🔥 r3000
Domain Name Primary Domain Name Server Secondary Domain Name Server Primary WINS Secondary WINS	nextmedia.local 192.168.177.105 151.99.125.3 192.168.177.105 192.168.177.106
Remote CAPI Server TCP port Remote TRACE Server TCP port RIP UDP port	2662 7000 520
Unique Source IP Address HTTP TCP port	80
SAVE	CANCEL
Enter string, max length = 35 chars	

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 <u>solamente</u> 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>

🖬 192.168.177.1 - SecureCRT	
<u>File Edit View Options Transfer Script Tools</u>	Help
R3000 Setup Tool [ATM][RP0A][ADD]	Funkwerk Enterprise Communications GmbH 🛧 r3000
Description	Click
ATM Interface	fcca-3-0
Virtual path identifier (VPI) Virtual channel identifier (VCI)	8 35
Encapsulation	non-ISO
IP >	
SAVE	CANCEL
Use <space> to select</space>	

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

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. <u>Gli indirizzi</u> 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 <u>non</u> ci siano voci nell'elenco. Come detto in precedenza la configurazione RPoA (o IPoA) NON prevede la configurazione di un WAN Partner.

ROOT> SETUP>

🖬 192.168.177.1 - SecureCRT	
<u> Edit View Options Iransfer Script Tools H</u> e	əlp
R3000 Setup Tool	Funkwerk Enterprise Communications GmbH 🛧 r3000
Licenses System	External Systems
Physical Interfaces: AUX: Console LAN: Ethernet Switch ISDN: BRI2-0 BRI2-1 DSL: ADSL	
<mark>MAN Partner</mark> Security PPTP IPSEC IP PPP X.25 FR BRRP CREDITS CAPI	ATM QoS VoIP GRE L2TP VLAN
Configuration Management Monitoring and Debugging Exit	
Press (Ctrl-n), (Ctrl-p) to scroll throu	gh menu items, <return> to enter</return>

ROOT> SETUP>WAN Partner>

1	92.1	68.0.	254 - Se	cureCRT	Ē								×
Eile	<u>E</u> dit	⊻iew	Options	Transfer	Script	Tools	<u>H</u> elp						
R230 EWAN)aw 9 13: 0	Setup NAN Pa	Tool artners				Fur	nkwerk	Enterprise	Communic	ations r	: GmbH `230aw	^
	Cur	rrent	WAN Par	rtner Co	nfigur	ation	I						
	F	Partne	ername			Prot	ocol		State				
	<u>901</u>	0		DE	LETE			EXII	Γ				
													~

A questo punto si entra nella sezione IP \rightarrow Routing:

🖬 192.168.177.1 - SecureCRT	
<u>File Edit View Options Transfer Script Tools H</u> elp	
R3000 Setup Tool Funkwerk Enterprise Communi	cations GmbH 🔨 r3000
Licenses System External Systems	
Physical Interfaces: AUX: Console LAN: Ethernet Switch ISDN: BRI2-0 BRI2-1 DSL: ADSL	
WAN Partner Security PPTP IPSEC IP PPP X.25 FR BRRP 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 🚽

ROOT> SETUP>IP>

🖬 192.168.177.1 - Secure	CRT 📃 🗖 🛽	<
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> rans	fer <u>S</u> cript Too <u>l</u> s <u>H</u> elp	
R3000 Setup Tool [IP]: IP Configuration	Funkwerk Enterprise Communications GmbH - 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</return>	~

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

🖬 192.168.177.1 - SecureCRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer	<u>Script Tools H</u> elp
R3000 Setup Tool [IP][ROUTING][ADD]	Funkwerk Enterprise Communications GmbH 🔨 r3000
Route Type Network	Default route WAN without transit network
Partner / Interface	rpoa0
Metric	1
SAVE	CANCEL
Use <space> to select</space>	

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>

🖬 192.168.177.1 - SecureCRT
<u>File Edit View Options Iransfer Script Tools Help</u>
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>

🖬 192.168.177.1 - SecureCRT	
<u>File Edit View Options Transfer Script Tools</u>	Help
R3000 Setup Tool [IP][STATIC]: IP Static Settings	Funkwerk Enterprise Communications GmbH A r3000
Domain Name Primary Domain Name Server Secondary Domain Name Server Primary WINS Secondary WINS	n <mark>extmedia.local</mark> 192.168.177.105 151.99.125.3 192.168.177.105 192.168.177.106
Remote CAPI Server TCP port Remote TRACE Server TCP port RIP UDP port	2662 7000 520
Unique Source IP Address HTTP TCP port	80
SAVE	CANCEL
Enter string, max length = 35 chars	

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

ROOT> SETUP>IP>IP Network Address Translatic
--

🖻 192.168.177.1 - SecureCRT	
<u> Eile E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too	s <u>H</u> elp
R3000 Setup Tool [IP][NAT][EDIT]: NAT Configuration (Funkwerk Enterprise Communications GmbH 🛧 rpoa0) r3000
Network Address Translation Silent Deny PPTP Passthrough	on no no
Enter configuration for sessions :	requested from OUTSIDE requested from INSIDE
SAVE CANCEL	
Use <space> to select</space>	 •

Nel caso in cui ci venga fornito un pool di <u>indirizzi pubblici aggiuntivi</u> 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.

<u>File Edit View Options Transfer Script Tools</u>	Help
R3000 Setup Tool [SWITCH][SLOT 1 UNIT 0 ETH][EDIT]: Com	Funkwerk Enterprise Communications GmbH 🔨 nfigure Interface Channel 0 r3000
Interface Mode	Routing
IP-Configuration Local IP-Number Local Netmask Second Local IP-Number Second Local Netmask Encapsulation	Manual 192.168.177.1 255.255.255.0 8 <mark>1.174.35.161</mark> 255.255.255.248 Ethernet II
MAC Address Frame Format	Untagged
Advanced Settings >	
SAVE	CANCEL
Enter IP address (a.b.c.d or resolvab	le hostname)

A questo punto occorre tornare sulle impostazione 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"

🖬 192.168.177.1 - SecureCRT	
<u>File Edit View Options Transfer Sc</u>	ript Too <u>l</u> s <u>H</u> elp
R3000 Setup Tool [IP][NAT][EDIT][EDIT]: NAT (Funkwerk Enterprise Communications GmbH 🟊 Configuration - sessions from INSIDE (ngi) r3000
Service Protocol	user defined any
Remote Address Remote Mask Remote Port	any
External Address External Mask External Port	81,174,35,161 255,255,255,255 any
Internal Address Internal Mask Internal Port	any
SAVE	CANCEL
Enter IP netmask (a.b.c.d or m	number of bits)

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: <u>http://www.funkwerk-ec.com/prod_bintec_r1200wu_cards_en,75538,837.html</u> (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).

<u>Suggerimento</u>: 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
                             : 0K
        Last Modem Answer
          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 paramerto *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)

 R1200 Setup Tool
 Funkwerk Enterprise Communications GmbH

 [WAN] [EDIT] [ADVANCED]: Advanced Settings (UMTSTest)
 r1200

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 Settings (optional) > Special Interface Settings (optional) > 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	M lang	
RS120 Setup Tool [UMTS]: Settings		Funkwerk Enterprise Communications GmbH 🛌 rs120 🔤
		E
UMTS Admin UMTS PIN SIM card u	status : ses PUK :	enabled
Additional Access Poi Incoming c	Initstring : nt Name (APN): all action :	ibox.tim.it ISDN Login
Current Mo UMTS Netwo UMTS Signa Last Modem Last Modem	dem Status : rk Provider : l Quality : Command : Answer :	up Telecom Italia M (AcT = UMTS) -79 dB (ok) AT+CSQ 17,99
SAVE		CANCEL
Use <space> to sel</space>	ect	▼

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:

G	Telnet 192.168.177.180			_		_ 🗆 🗙	
R	S120 Setup Tool WAN][EDIT]: Configure WAN Partner		Funkwerk	Enterprise	Communicati	ions GmbH rs120	•
	Partner Name TI	M					
l	Encapsulation PP Encryption no	'P ine					
	<mark>PPP ></mark> Advanced Settings >						
	IP > Bridge >						
	SAUE			CANC	EL		
L						-	Ŧ

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

Con Telnet 192.168.177.180				
RS120 Setup Tool [WAN][EDIT][PPP]: PPP Settings	(TIM)	Funkwerk Enterprise	Communications GmbH rs120	
Authentication	DODE			
	nono			
Keepalives Link Quality Monitoring	off off			
ок		CANC	EL	
Use <space> to select</space>				
				-

Clicchiamo su Ok e entriamo poi sulla voce Advanced Settings.

Telnet 192.168.177.180	
RS120 Setup Tool [WAN][EDIT][ADVANCED]: Advanced Setting	Funkwerk Enterprise Communications GmbH _ s (TIM)rs120
Callback Static Short Hold (sec)	no 19
Idle for Dynamic Short Hold (%) Delay after Connection Failure (sec)	0 10
Layer 1 Protocol GPRS/UMTS Interface	GPRS/UMTS Slot 6 Unit Ø E169
Extended Interface Settings >	
Special Interface Types	none
ок	CANCEL
Use <space> to select</space>	
	· ·

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:

Telnet 192.168.177.180	
RS120 Setup Tool [WAN][EDIT][IP][BASIC]: IP-Settings	Funkwerk Enterprise Communications GmbH <tim>rs120</tim>
IP Transit Network	dynamic client
Enable NAT Default Route	yes yes
SAUE	CANCEL
use (space) to select	-

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:

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-Ø BRI2-1 Serial: SBR4-Ø SER4-1	
WAN Partner Security PPTP IPSEC IP PPP FR BRRP CREDITS CAPI QoS Configuration Management Monitoring and Debugging Exit	VoIP GRE L2TP ULAN
Press <ctrl-n>, <ctrl-p> to scroll thre</ctrl-p></ctrl-n>	ough menu items, <return> to enter</return>

	Telnet 62.94.134.113
	300 Setup Tool Funkwerk Enterprise Communications GmbH LOT 4 SERIAL]: Configure Serial Interface - Unit 0 r4300
1	Cable Detection interface & connector type
-	Interface Type V.35 (autodetected) Connector dte (autodetected)
	Layer 2 Mode dte
-	Interface Leads disabled
	SAVE CANCEL
-	~

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

Telnet 62.94.1	34.113		x
R4300 Setup	Tool	Funkwerk Enterprise Communications	GmbH •4300
Licenses	System	External Systems	
Physical Int AUX: LAN: ISDN: Serial:	erfaces: Console Ethernet Switch BRI2-0 BRI2-1 SER4-0 SER4-1		
WAN Partner IP PPP FR	Security PPTP IPSEC BRRP CREDITS CAPI QoS	S VOIP GRE L2TP VLAN	
Configuratic Monitoring a Exit	n Management Ind Debugging		
Press <ctrl-< td=""><td>n>, <ctrl-p> to scroll tł</ctrl-p></td><td>hrough menu items, <return> to enter</return></td><td></td></ctrl-<>	n>, <ctrl-p> to scroll tł</ctrl-p>	hrough menu items, <return> to enter</return>	

Telnet 62.94.134.113			-		- 0 ×	
R4300 Setup Tool [WAN]: WAN Partners	F	unkwerk Entei	rprise C	ommunicati	ons GmbH r4300	
Current WAN Partner	Configuration					
Partnername	Protoco	1	State			
S14-0	f rame_r	relay	սք			
ADD	DELETE	EXIT				
Press (Ctrl-n). (Ctrl-p)	to scroll. <spac< td=""><td>e> tag/untag</td><td>DELETE.</td><td><return></return></td><td>to edit</td><td></td></spac<>	e> tag/untag	DELETE.	<return></return>	to edit	
	topas				_	-

Telnet 62.94.134.113			
R4300 Setup Tool [WAN][EDIT]: Configure Sy	H Inchronous Serial	³ unkwerk Enterprise L Leased Line	Communications GmbH r4300
Partner Name	si4-0		
Encapsulation	Frame F	Relay	
	SAUE	CANCI	ar,
Enter string, max length	= 25 chars		
,			-

Ora impostiamo i parametri relativi al 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-Ø BRI2-1 Serial: SER4-Ø SER4-1	
WAN Partner Security PPTP IPSE IP PPP 📴 BRRP CREDITS CAPI	EC QoS VoIP GRE L2TP VLAN
Configuration Management Monitoring and Debugging Exit	
Press <ctrl-n>, <ctrl-p> to scrol</ctrl-p></ctrl-n>	ll through menu items, <return> to enter</return>



Telnet 62.94.134.113	
R4300 Setup Tool Funkwerk Enterprise [FRAME RELAY][LINK]: Frame Relay Link Configuration	Communications GmbH r4300
Select link to configure	
si4-0	
EXIT	
Press <ctrl-n>, <ctrl-p> to scroll, <return> to select/edit</return></ctrl-p></ctrl-n>	
	T



Telnet 62.94.134.113	
R4300 Setup Tool F [FRAME RELAY][LINK][ADVANCED]: Advanced	unkwerk Enterprise Communications GmbH 🗾 Frame Relay Link Configuration r4300 📑
Supported Virtual Channels Polling Interval Full Enquiry Interval Error Threshold Monitored Events	250 10 6 3 4
ок	CANCEL
Enter integer range 1250	T

Torniamo alla schermata principale di FR...



Verifichiamo che il menù Switching sia vuoto.

Telnet 62.94.134.	113			-				• ×	
R4300 Setup To [FRAME RELAY][ol Switchii	NG]: Frame Re]	Fu Lay Swit	unkwerk En ching	terprise	Communic	ations	GmbH r4300	1
									=
Source		Destinati	ion	_	_				
Interface	DLCI	Interface	DLCI	Вс	Be	CIR			
າກກ		NELETE		FXIT					
1120		PEALIL		20111					
									-

Torniamo ancora alla schermata principale di FR...



Telnet 62.94.134.113	_		ł	- 0 X
R4300 Setup Tool [FRAME RELAY][MPR]: Frame Relay Mult	Funkwerk Entery iprotocol Routing	prise Communicat	ions GmbH r4300
Interface Name	Type point to point			
ADD	DELETE	EXIT		
Press (Ctrl-n), (Ctrl-p> to scroll,	<space> tag/untag]</space>	DELETE, <return></return>	to edit
				-

Telnet 62.94.134.113				
R4300 Setup Tool [FRAME RELAY][MPR][EDIT]:	Funkwerk Configure Frame Relay	k Enterprise Communications GmbH 🗾 MPR Partner r4300 🛁		
		E		
Partner Name	mpfr1			
Interface Type Inverse Arp	point to point disabled	t		
Virtual Circuits >				
IP > Bridge >				
	SAVE	CANCEL		
		-		

Telnet 62.94.134.113	_		
R4300 Setup Tool [FRAME RELAY][MPF	R][SWITCHING]: Config	Funkwerk Enterpri gure Frame Relay Vi	se Communications GmbH 🔽 rtual Circuits r4300 🚽
Courses	Destination		
Interface DI si4-0 20	CI Interface DL	CI Bc Be 2048000 0	GIR 2048000
ADD	DELETE	EXIT	
	$(Ctul_n)$ to coupl (8)	Deco tag (uptag DEL	ETE (Potume) to odit
Tress (CCPI-07, (Corrept to scroll, (S)	paces taysuntay DEL	

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

Telnet 62.94.134.113	
R4300 Setup Tool Fu [FRAME RELAY][MPR][EDIT][SWITCHING][EDIT]	nkwerk Enterprise Communications GmbH
Source Interface Source DLCI	si4-0 20
Pupet committed (Po)	2849888
Burst committee (Bc) Burst excess (Be) Committed Information Rate (CIR)	0 2048000
ок	CANCEL
Use <space> to select</space>	

Telnet 62.94.134.113		
R4300 Setup Tool [FRAME RELAY][MPR][EDIT]: C	Funkwerk Ent onfigure Frame Relay MPR	erprise Communications GmbH 🔽 Partner r4300 📄
Partner Name	mpfr1	
Interface Type Inverse Arp	point to point disabled	
Virtual Circuits >		
Bridge >		
SA	VE	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)

Telnet 62.94.134.113	
R4300 Setup Tool [FRAME RELAY][MPR][EDIT][IP][BASIC]:	Funkwerk Enterprise Communications GmbH IP-Settings (mpfr1) r4300
IP Transit Network	ye s
Local IP Address Partner IP Address	62.94.150.186 62.94.150.185
Default Route	yes
SAUE	CANCEL
Use <space> to select</space>	
	· · · · · · · · · · · · · · · · · · ·

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





	Telnet 62.94.134.113		_		- 0 ×
ľ	4300 Setup Tool IPJ[NAT]: NAT Conf	iguration	Funkwerk	Enterprise Communic	ations GmbH 🛓 r4300 📥
-					=
	Select IP Interfa	ce to be c	onfigured for NAT		
	Name	Nat	Static mappings	Static_mappings	
			from Outside	from_Inside	
	en1-0	off	5	ទ	
	en1-0-snap	off	Ø	Ø	
	en1-4	off	0	0	
	en1-4-snap	off	Ø	Ø	
	mpfr1	on	6	1	
	TUIT				
	EALI				
P	Press ⟨Ctrl−n⟩, ⟨Ct:	rl-p> to s	croll, <return> to</return>	select/edit	
					-
<u> </u>					



Se abbiamo anche degli indirizzo IP aggiuntivi possiamo impostarli sull'interfaccia en1-0 come Second Local IP Number. Qui sotto un esempio:

Telnet 62.94.134.113				
R4300 Setup Tool [SWITCH][SLOT 1 UNIT 0 ETH][EDIT]: Con	300 Setup Tool Funkwerk Enterprise Communications GmbH /ITCH][SLOT 1 UNIT 0 ETH][EDIT]: Configure Interface Channel 0 r4300			
Interface Mode	Routing			
IP-Configuration Local IP-Number Local Netmask Second Local IP-Number Second Local Netmask Encapsulation	Manual 192.168.10.252 255.255.255.0 62.94.134.113 255.255.255.248 Ethernet II			
MAC Address Frame Format	Untagged			
Advanced Settings >				
SAVE	CANCEL			
Use <space> to select</space>				

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.

💼 192.168.177.1 - SecureCRT	
<u>File Edit View Options Transfer Script Tools</u>	Help
R3000 Setup Tool	Funkwerk Enterprise Communications GmbH 🔨 r3000
Licenses System	External Systems
Physical Interfaces: AUX: Console LAN: Ethernet Switch ISDN: BRI2-0 BRI2-1 DSL: ADSL	
WAN Partner Security PPTP IRSEC IP PPP X.25 FR BRRP CREDITS CAPI	ATM QoS VoIP GRE L2TP VLAN
Configuration Management Monitoring and Debugging Exit	
Press (Ctrl-n>, (Ctrl-p> to scroll thr	ough menu items, <return> to enter</return>

Se è la prima volta che si configura una VPN sarà <u>necessario</u> 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:

a 192	168.17	78.1 - Se	cureCR	Г								X
<u>File E</u> di	t <u>V</u> iew	Options	<u>T</u> ransfer	<u>S</u> cript	Too <u>l</u> s	<u>H</u> elp						
R232aw LIPSEC	Setup]: IPse 	Tool ec Confi	iguratic	:ome pr	in Me	Fur nu 	werk 	Enterpri 	se Comm	to do.	ons GmbH r232aw	
	Do	you war	nt to us	e the Yes	wizar 9							
Ready				Te	Inet		24, 80	24 Rows.	80 Cols	VT100	NUN	1



🖬 192.168.178.1 - SecureCRT		×							
<u>File Edit V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp									
32aw Setup Tool Funkwerk Enterprise Communications GmbH PSEC][WIZARD]: IPsec Configuration - Wizard Menu r232aw									
IPsec 1st step configurations wizard Configuration History:									
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 ? c <mark>urrent: PSK</mark> (<space> to choose) (<return> to select</return></space>									
Exit		~							
Ready Telnet 18, 56 24 Rows, 80 Cols VT100	NUM								

C 192.168.178.1 - SecureCRT		×
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp		
R232aw Setup Tool	ns GmbH r232aw	^
<pre>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 ? K1200 II_test (<space> to choce (<space> to choce</space></space></pre>	^ 	
Exit	:007	
		~
Ready Telnet 18, 69 24 Rows, 80 Cols VT100	NUM	

🖬 192.168.178.1 - SecureCRT	×						
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp							
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.							
+ Check for Peer I IPSEC enabled =							
Configure Peer ? <u>start</u> (<space> to choose) (<return> to select)</return></space>							
Exit							
	~						
Ready Telnet 18, 56 24 Rows, 80 Cols VT100 NUM							

🗖 192.168.178.1 - Secur	eCRT		
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> rai	nsfer <u>S</u> cript Too <u>l</u> s <u>H</u>	elp	
R232aw Setup Tool [IPSEC][WIZARD][PEER]: 	IPsec Wizard - Co	Funkwerk Enterprise Com onfigure Peer	munications GmbH 🔼 r232aw
Description: Admin Status: Peer Address: Peer IDs: Pre Shared Key: IPSec Callback:	verso_sede_2 up test2.dyndns.org vpn25_test **** no	\$	
Virtual Interface:	yes		
	SAVE	CANCEL	
Ready	Telnet	24, 80 24 Rows, 80 Cols	VT100 NUM ,;;

🖬 192.168.178.1 - SecureCRT	×									
<u>File Edit V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp										
232aw Setup Tool Funkwerk Enterprise Communications Gmbl [IPSEC][WIZARD]: IPsec Configuration - Wizard Menu r232a 										
IPsec 1st step configurations wizard										
Configuration History:										
Brick now prepared for IPsec enabled standard router. I Further configuration is required for an IPsec only router! I + Check for Peer I IPSEC enabled I Pre Shared Key now set I IPSEC already enabled I + Check for ISDN Callback configuration I + Check for Peer Virtual interface I Configure Virtual interface ? Stant (<space> to choose) (<return> to select)</return></space>										
Exit										
Use <space> to select</space>	~									
Ready Telnet 24, 80 24 Rows, 80 Cols VT100 NUM	1									

💼 192.168.178.1 - SecureCR	Т	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer	<u>Script Tools H</u> elp	
R232aw Setup Tool [IPSEC][WIZARD][PEER][IP]: 	Funkwerk Enterprise Communicatio IP Settings (verso_sede_2)	ns GmbH 🔼 r232aw
	Basic IP-Settings >	
	More Routing >	
	Advanced Settings >	
	EXIT	
		~
Ready	Telnet 24, 80 24 Rows, 80 Cols VT100	NUM;

i	2.168	8.17	8.1 - Se	ecureCRT	r								X
<u>File</u>	<u>i</u> dit ⊻i	iew	Options	<u>T</u> ransfer	<u>S</u> cript	Tools	Help						
R232a EIPSE	w Set CJCWI	:up [ZAR	Tool DJCPEEF	RJCIPJCB	ASIC]:	: IP-S	Fui iettii	nkwerk E ngs (vei	Enterpri: rso_sede	se Comm _2)	unicati	ons GmbH r232au	^
IP	Trans	sit	Networł	<			no						
Loc	al IF	° Ad	ldress				19	2,168,10	00.1				
Def	`ault	Rou	ıte				no						
Rem Rem	ote I ote M	IP A Netm	iddress iask				19) 25!	2.168.20 5.255.29	00.0 55.0				
				SAVE					CAI	NCEL			
Ready		_			Τe	elnet		24, 80	24 Rows,	80 Cols	VT100	NU	1

🖬 192.168.178.1 - SecureCR	ſ	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer	<u>S</u> cript Too <u>l</u> s	Help
R232aw Setup Tool [IPSEC][WIZARD][PEER][IP]: 	IP Settings	Funkwerk Enterprise Communications GmbH 🔺 s (verso_sede_2) r232aw
	Basic IP	P-Settings >
	More Rou	uting >
	Advanced	d Settings >
		· · · · · · · · · · · · · · · · · · ·
Ready	Telnet	24, 80 24 Rows, 80 Cols VT100 NUM 🛒

🖬 192.168.178.1 - SecureCRT		×
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp		
R232aw Setup Tool Funkwerk Enterprise Communications Gm [IPSEC][WIZARD]: IPsec Configuration - Wizard Menu r232 	ibH 2aw	^
IPsec 1st step configurations wizard		
Lonfiguration 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</return></space>		~
Ready Telnet 24, 80 24 Rows, 80 Cols VT100 M	NUM	:

🖬 192.168.178.1 - SecureCRT
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp
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
Ready Telnet 24, 80 24 Rows, 80 Cols VT100 NUM

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

🖬 192.168.177.1 - SecureCRT
<u>File Edit View Options Transfer Script Tools H</u> elp
R3000 Setup Tool Funkwerk Enterprise Communications GmbH A [IPSEC]: IPsec Configuration - Main Menu r3000
Enable IPSec : yes
Configure Peers >
IKE (Phase 1) Defaults *autogenerated* edit > IPsec (Phase 2) Defaults *autogenerated* edit > Certificate and Key Management > Advanced Settings >
Wizard >
SAVE CANCEL
Use <space> to select</space>

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.

🖬 192.168.177.1 - SecureCRT
<u>File Edit View Options Transfer Script Tools H</u> elp
R3000 Setup Tool Funkwerk Enterprise Communications GmbH 🔨 [IPSEC]: IPsec Configuration - Main Menu r3000
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

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
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>Transfer</u> <u>Script</u> Too <u>l</u> s <u>H</u> elp
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.or d 1 0
APPEND DELETE REORG EXIT
Press <ctrl-n>, <ctrl-p> to scroll, <space> tag/untag DELETE, <return> to edit</return></space></ctrl-p></ctrl-n>
Ready Telnet 24, 80 24 Rows, 80 Cols VT100 NUM

🖬 192.168.178.1 - Sec	ureCRT		
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions	<u>T</u> ransfer <u>S</u> cript Too <u>l</u> s	: <u>H</u> elp	
R232aw Setup Tool [PEERS][EDIT]: Config 	gure Peer	Funkwerk Enterprise Communicatio	ns GmbH 🔼 r232aw
Description: Admin Status:	verso_sede_2 up		
Peer Address: Peer IDs: Pre Shared Key:	test2.dyndns.d vpn25_test *	org	
IPSec Callback . Peer specific Se	> ettings >		
Virtual Interfac Interface IP Set	ce: yes ttings >		
	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'algoritmo 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.

192.168.178.1 - SecureCRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp	
R232aw Setup Tool	s GmbH 🔼 r232aw
Special settings for peer No. 1 : verso_sede_2	
IKE (Phase 1) Profile: default	
IPsec (Phase 2) Profile: default edit >	
Special Peer Type: None Start Mode: On Demand	
SAVE CANCEL	
	 >
Ready Telnet 24, 80 24 Rows, 80 Cols VT100	NUM 📑

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.

🗖 192.168.178.1 - Secure	CRT		
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ran	sfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp		
R232aw Setup Tool [PEERS][EDIT][SPECIAL][F 	Funkw PHASE1]: IPsec Configu	erk Enterprise Communicat ration - Phase 1 Profiles 	ions GmbH 📐 : r232aw
AC: Alive Check Auth: Authentication Mode: Phase 1 Mode	N: None A: Auto P(I HS/HE/HB: Heartbeats PSK: Pre Shared Keys DSS: DSS ID-Pr: ID Protect): DPD (Idle Mode) D: De Send/Expect/Both RSA-S: RSA Signatures RSA-E: RSA Encryption Aggr: Aggressive	fault
Description Propo *autogenerated* Blowf	osal ish/MD5	Lifetime Group AC Auth default 2 A PSK	Mode ID-Pr
ADD	DELETE	EXIT	
Press (Ctrl-n), (Ctrl-p)	> to scroll, <space> t</space>	ag/untag DELETE, <return></return>	to edit 🚽
Ready	Telnet 24	, 80 24 Rows, 80 Cols VT100	NUM;

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:



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'autority 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.

19	9 <mark>2.168.1</mark>	78.1 - Se	ecureCRT						×
<u>F</u> ile §	<u>E</u> dit <u>V</u> iew	Options	<u>T</u> ransfer	<u>S</u> cript Too <u>l</u> s <u>H</u> e	lp				
R232a CPEEF	aw Setup RSJEEDIT:	Tool JESPECI6	AL]: Spec	F ial Settings 	Funkwerk (verso_s	Enterprise Comm ede_2)	nunicatio	ons GmbH r232aw	^
	Special	setting	gs for pe	er No. 1 :	verso_se	de_2			
	IKE (Pha	ase 1) F	Profile:	default		edit >			
	IPsec (Phase 2) Profile	: default		edit >			
	Special Peer Type: None Start Mode: On Demand								
			SA	VE		CANCEL			
									-
Ready				Telnet	24, 80	24 Rows, 80 Cols	VT100	NUM	

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

🖬 192.168.178.1 - SecureCRT	\mathbf{X}
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp	
R232aw Setup Tool Funkwerk Enterprise Communications GmbH [PEERS][EDIT][SPECIAL][PHASE2]: IPsec Configuration - Phase 2 Profiles r232aw	+ 🔼
H: Heartbeat Setting N: None S: Send E: Expect B: Both D: Default P: Propagate PMTU Y: Yes N: No D: Default	
Description Proposal Lifetime Group H P	
autogenerated ESP(Blowfish/MDS) no default -1 H N	
ADD DELETE EXIT	
Press <ctrl-n>, <ctrl-p> to scroll, <space> tag/untag DELETE, <return> to edit</return></space></ctrl-p></ctrl-n>	~
Ready Telnet 24, 80 24 Rows, 80 Cols VT100 NUT	м 🔡

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'integrita 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.

📠 192.168.178.1 - Secure(rt 🗖 🗖 🔀
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransf	ier <u>S</u> cript Tools <u>H</u> elp
R232aw Setup Tool [PEERS][EDIT][SPECIAL][P+ 	Funkwerk Enterprise Communications GmbH 🔨 HASE2][EDIT] r232aw
Description (Idx 1) :	*autogenerated*
Proposal Lifetime Policy	: 1 (ESP(Blowfish/MD5) no Comp) : Use default lifetime settings
Use PFS Alive Check Propagate PMTU	: none : autodetect : no
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 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.

192.1	68.178.1 - S	ecureCRT							×
<u>File E</u> dit	<u>V</u> iew <u>O</u> ptions	<u>T</u> ransfer <u>S</u>	cript Too <u>l</u> s	<u>H</u> elp					
R232aw 9 [PEERS][etup Tool EDITJESPECI	AL]: Speci	al Settin	Fur ngs (v	nkwerk E Verso_se	nterprise Com de_2)	omunicatio	ons GmbH r232aw	^
Spe	cial setting	gs for pee	r No. 1	: ve	erso_sec	le_2			
IKE	(Phase 1)	Profile:	default			edit >			
IPs	ec (Phase 2	> Profile:	default			edit >			
Spe Sta	ecial Peer Ty art Mode:	ype:	None On Deman	nd		I			
		SAV	E			CANCEL			
use topa	ace/ to sele	CL							~
Ready			Telnet		24, 80	24 Rows, 80 Cols	; VT100	NUM	

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 \rightarrow 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.

19	92.16	8.17	78.1 - Se	ecureCR	Г										×
Eile	<u>E</u> dit <u>V</u>	<u>/</u> iew	Options	<u>T</u> ransfer	<u>S</u> cript	Tools	<u>H</u> elp								
R232/ [PEE]	aw Se RSJEE	tup DIT:	Tool 1: Conf:	igure Pe	er		Fu	nkwer	rk (Enterpri:	se Comr	nunicat.	ions G r23	mbH 2aw 	^
	Desc Admi	ript n St	ion: atus:	ver up	`so_se	de_2									
	Peer Peer Pre	Ado IDs Shar	hress: ∷ red Key	tes vpr : *	:t2,dyr 125_te:	ndns.c st	org								
	IPSe Peer	c Ca Ispe	allback cific (> Settings	: >										
	Virt Inte	ual rfao	Interfa e IP Se	ace: yes ettings	2										
	SAVE									Ci	ANCEL				
Doodu					Te	Jack		24	00	24 Dours	20 Colo	UT100		NH 164	V
	Inte	rfac		ettings	à AVE 	elnet		24, 1	80	Ci 	ANCEL	VT100			

i 192	.168.17	78.1 - Se	cureCRT	Ē								X
<u>File E</u> d	it <u>V</u> iew	Options	<u>T</u> ransfer	<u>S</u> cript	Too <u>l</u> s	<u>H</u> elp						
R232au CPEERS	Setup JEEDIT:	Tool JESPECIA	ALJEIPJ:	IP Se	tting	Fur s (ve	kwerk E rso_sec	Interpri: We_2)	se Comm	unicatio	ons GmbH r232aw	^
				Bas	ic IP	-Sett	.ings >					
				Mor	e Rou	ting	>					
				Adv	anced	Sett	ings >					
						FYTT						
												_
												~
Ready				Τe	Inet		24, 80	24 Rows,	80 Cols	VT100	NUM	1

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

📠 192.168.178.1 - SecureCR	Г		
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer	<u>S</u> cript Too <u>l</u> s	Help	
R232aw Setup Tool [PEERS][EDIT][SPECIAL][IP][BASIC]: IP-	Funkwerk Enterprise Communication -Settings (verso_sede_2)	ons GmbH 📩 r232aw
IP Transit Network			
Local IP Address		192.168.100.1	
Default Route		no	
Remote IP Address Remote Netmask		192.168.200.0 255.255.255.0	
SAVE		CANCEL	
Use <space> to select</space>			 ~
Ready	Telnet	24, 80 24 Rows, 80 Cols VT100	NUM 💥

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). <u>E' importante che le due reti private abbiano classi di indirizzamento diverse</u> (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*.

ev Telnet 192.168.177.1	_ 🗆 ×
R3000 Setup Tool [PPTP][EDIT]	Funkwerk Enterprise Communications GmbH - r3000
Partner Name	րթէթ
Encapsulation Encryption Compression	PPP MPPE V2 40 (RFC 3078) none
PPP > Advanced Settings >	
IP >	
SAVE	CANCEL
Enter string, max length = 25 cha:	24

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

🔤 Telnet 192.168.177.1	_ 🗆 ×
R3000 Setup Tool [PPTP][EDIT][PPP]: PPP Settings	Funkwerk Enterprise Communications GmbH (pptp) r3000
Authentication Partner PPP ID Local PPP ID PPP Password MS Domain Keepalives Link Quality Monitoring	NS-CHAP V2 prova_pptp prova_pptp **** off off
ок	CANCEL
Use <space> to select</space>	

Autentication: 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:

ex Telnet 62.123.203.199	_ 🗆 ×
R3000 Setup Tool [PPTP][EDIT][ADVANCED]: Advanced Setti 	Funkwerk Enterprise Communications GmbH ngs (Nord_Est 9000 PPTP) r3000
Callback Static Short Hold (sec)	no —1
Delay after Connection Failure (sec) PPTP Mode	10 PPTP PNS
Extended Interface Settings (optional	1>>
Special Interface Types	none
ок	CANCEL
Use <space> to select</space>	

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:

🕰 Telnet 62.123.203.199		- 🗆 X
R3000 Setup Tool [PPTP][EDIT][IP][BASIC]: IP-Settings	Funkwerk Enterprise Communications (Nord_Est 9000 PPTP) r	GmbH 3000
Dynamic PPTP VPN Identification by IP Address PPTP VPN Partner's IP Address	no no	
IP Address Negotiation	dynamic server	
SAVE	CANCEL	
Use <space> to select</space>		-

Dynanic PPTP VPN: no *IP Address Negotiation*: dynamic server

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

Telnet 192.168.177.1	- 🗆 >
R3000 Setup Tool [IP][DYNAMIC][POOL][EDIT]: Define Rang	Funkwerk Enterprise Communications GmbH e of IP Addresses r3000
Identifier Description IP Address Number of Consecutive Addresses Primary Domain Name Server Secondary Domain Name Server	9 WAN 10.10.10.10 3 0.0.0.0 0.0.0.0
SAUE	CANCEL
Enter integer value	

Pool ID: identificativo del pool di indirizzi

IP Address: indirizzo IP di partenza da assegnare dinamicamente (<u>Importante</u>: 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).

🗠 Telnet 192.168.177.1		- 🗆 ×
R3000 Setup Tool [IP][DYNAMIC][DYNAMIC][ADD]:	Funkwerk Enterprise Define Range of IP Addresses	Communications GmbH A
Pool ID	3	
AdminStatus	enabled	
SAVE	CANC	61.
Enter integer value		

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)

🛤 Telnet 62.123.203.199						- 🗆 ×
R3000 Setup Tool [IP][NAT][EDIT][EDIT]: NAT	— sessions	Funkwe from O	rk Ente UTSIDE	erprise Commu (WIZ_XDSL_IM	unication HT_RPoA>	s GmbH r3000
Service	user defin	ied				
Protocol	tcp					
Remote Address Remote Mask						
External Address External Mask External Port	specify		Port	1723		
Internal Address Internal Mask Internal Port	127.0.0.1 255.255.25 any	5.255				
SAUE				CANCEL		
Use <space> to select</space>						•

abilitare il protocollo GRE (protocollo per l'incapsulamento)

🔤 Telnet 62.123.203.199	- 🗆 >	<
R3000 Setup Tool [IP][NAT][EDIT][EDIT]: NA]	Funkwerk Enterprise Communications GmbH [- sessions from OUTSIDE (WIZ_XDSL_INT_RPoA) r3000	
Service Protocol	user defined gre	-
Remote Address Remote Mask		
External Address External Mask External Port	any	
Internal Address Internal Mask Internal Port	127.0.0.1 255.255.255.255 any	
SAVE	CANCEL	
Use <space> to select</space>		•

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*

Creazione guidata nuova connessione	
S	Creazione guidata nuova connessione
	Questa procedura guidata consente di:
	 Connettere il computer a Internet.
	 Connettere il computer a una rete privata, come una rete aziendale.
	Per continuare, scegliere Avanti.
	< Indietro

Selezionare connessione alla rete aziendale

Creazione guidata nuova connessione		
Tipo di connessione di rete Scegliere l'operazione da effettuare.		
O <u>C</u> onnessione a Internet		
Consente di connettere il computer a Internet e di esplorare il Web e leggere la posta elettronica.		
Connessione alla rete aziendale		
Consente di connettere il computer a una rete aziendale, mediante connessione remota o VPN e di lavorare da casa, da una filiale o da un'altra ubicazione.		
Installazione di una connessione avanzata		
Consente di connettere il computer direttamente a un altro computer mediante la porta seriale, parallela o a infrarossi o di impostarlo per consentire la connessione di altri computer.		
< <u>I</u> ndietro <u>Avanti</u> > Annulla		

Selezionare Connessione VPN

Creazione guidata nuova connessione	
Connessione di rete Scegliere la modalità di connessione alla rete aziendale.	
Crea la seguente connessione:	
O <u>C</u> onnessione remota	
Consente di connettere il computer alla rete mediante un modem e una normale linea telefonica oppure mediante una linea ISDN.	
Connessione VPN	
Consente di connettere il computer alla rete mediante una connessione VPN (Virtual Private Network) su Internet.	
< <u>I</u> ndietro <u>Avanti</u> > Annulla	

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. <u>N</u> ome società
Connessione_PPTP
Ad esempio, è possibile immettere il nome della rete aziendale o del server a cui si effettuerà la connessione.
< <u>I</u> ndietro <u>Avanti</u> > 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 <u>h</u> ost o indirizzo IP (ad esempio microsoft.com o 157.54.0.1):
88.26.35.154
< <u>I</u> ndietro <u>A</u> vanti> Annulla

Disponibilità connessione È possibile consentire l'accesso alla nuova connessionea tutti gli utenti o solo a se stessi.
Una connessione creata per uso personale viene salvata nell'account utente e non è disponibile se non si è effettuato l'accesso a proprio nome. Crea questa connessione per: O L'uso da parte di tutti O Solo uso personale
< <u>Indietro</u> Avanti > Annulla

Creazione guidata nuova connessione					
S)	Completamento della Creazione guidata nuova connessione				
	Sono state eseguite le operazioni necessarie per la creazione della seguente connessione:				
	Connessione_PPTP				
	La connessione verrà salvata nella cartella Connessioni di				
	rete.				
	Aggiungi collegamento a questa connessione sul desktopi				
	Per creare la connessione e terminare la procedura guidata, scegliere Fine.				
	< Indietro Fine Annulla				

Specificare User Name e Password indicati nel router.

Connessione	a Connessione_PPTP	? 🗙
<u>N</u> ome utente:	prova_pptp	
Pass <u>w</u> ord:	•••••	
<mark>⊘</mark> <u>S</u> alva nom	e utente e password per gli utenti seguenti:	
⊙ Solo <u>u</u> t ⊖ Qualsia	ente corrente si utente	
<u>C</u> onnetti	Annulla <u>P</u> roprietà	2

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

🗢 Proprietà - Connessione_PPTP 🛛 💽 🔀
Generale Opzioni Protezione Rete Avanzate
Opzioni di protezione
Ipiche (impostazioni consigliate)
Convalida l'identità come descritto di seguito:
✓
Utilizza automaticamente nome utente e password di <u>W</u> indows (e dominio se presente)
Ric <u>h</u> iedi crittografia dati (disconnetti se non disponibile)
 Avanzate (impostazioni personalizzate)
Per utilizzare queste impostazioni è necessario conoscere i protocolli di protezione.
I <u>m</u> postazioni IPSec
OK Annulla

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. Penserà poi il router ad aggiornare il nome di dominio con l'indirizzo IP pubblico acquisito durante il collegamento ADSL.

🖻 192.168.177.1 - SecureCRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s	Help
R3000 Setup Tool	Funkwerk Enterprise Communications GmbH 🔨 r3000
Licenses System	External Systems
Physical Interfaces: AUX: Console LAN: Ethernet Switch ISDN: BRI2-0 BRI2-1 DSL: ADSL	
WAN Partner Security PPTP IPSEC PPP X.25 FR BRRP CREDITS CAPI	ATM QoS VoIP GRE L2TP VLAN
Configuration Management Monitoring and Debugging Exit	
Press (Ctrl-n), (Ctrl-p) to scroll thro	pugh menu items, <return> to enter 🚽</return>

🖬 192.168.177.1 - SecureCRT
<u>File Edit View Options Transfer Script Tools Help</u>
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

1	92.1	68.17	77.1 - Se	ecureCRT	Г					
<u>F</u> ile	<u>E</u> dit	⊻iew	Options	Transfer	Script	Too <u>l</u> s	Help			
R300 EIP:)0 S€]EDYN	tup 1 DNS][[ool EDIT]				Funkwerk	Enterprise	Communication	is GmbH 🔼 r3000
		Hos Int Use Pas Pro MX Wil Per	st Name cerface er ssword ovider Ldcard rmission	n		r 1 * c c	hextmedia.dy hgi Lughino ****** dyndns off enabled	µndns.info		-
				SAVE				CANCE	EL	
Ente	er st	ring,	. max le	ength =	40 cha	irs				~

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	8.177.1 - S	ecureCRT	Г										<
<u>Eile E</u> dit <u>V</u> i	ew <u>O</u> ptions	Transfer	<u>S</u> cript	Too <u>l</u> s	<u>H</u> elp								
R3000 Setu CIPJCDYNDN	ıp Tool (S]: Dynam	ic DNS S	ervice	, 	Funl	kwerk	Enter	prise	Commur	nicati	ons (r	GmbH 3000	~
DynDNS	Services:												
Host Na	me		Int	erfac	e	F	ermis:	sion	State				
nextmed	lia.dyndns	₊info	ngi			E	enable	d	up-to	-date		-	
DynDNS Pr	ovider Li	st>											
ADD		DE	LETE			EXIT							
Press (Ctr	·l−n>, <ct< td=""><td>rl-p> to</td><td>scrol</td><td>1, <9</td><td>ipace></td><td>tag/u</td><td>untag i</td><td>DELETE</td><td>E, KRet</td><td>urn></td><td>to e</td><td>dit</td><td>•</td></ct<>	rl-p> to	scrol	1, <9	ipace>	tag/u	untag i	DELETE	E, KRet	urn>	to e	dit	•

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.

🖬 192.168.177.1 - SecureCRT	
<u>File Edit V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp	
R230aw Setup Tool Funkwerk Ente [QOSJ[FILTER]: Configure IP Classification Filter	erprise Communications GmbH 🔨 r230aw
Abbreviations: sa (source IP address) sp (s da (destination IP address) dp (d it (icmp type) estab	source port) destination port) o (TCP established)
Index Descr Conditions	
DELETE EXIT	
Ready Telnet 24, 80 24	Rows, 80 Cols VT100 NUM 📑

🗖 192.168.177.1 - Secur	eCRT		
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> rai	nsfer <u>S</u> cript Too <u>l</u> s	Help	
R230aw Setup Tool [QOS][FILTER][][ADD] 		Funkwerk Enterprise (Communications GmbH 🔼 r230aw
Description Index	VoIP		
Protocol	any		
Source Address	192,168,177,9	Source Mask	255,255,255,255
Destination Address		Destination Mask	
TOS/DSCP Level 2 Priority	00000000 000	TOS/DSCP Mask L2 Priority Mask	00000000
SAV	12	CANCEL	
			 ×
Ready	Telnet	24, 80 24 Rows, 80 C	ols VT100 NUM

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

🖻 192.168.177.1 - Se	cureCRT		
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions	<u>T</u> ransfer <u>S</u> cript	Too <u>l</u> s	Help
R230aw Setup Tool [QOS][FILTER][][ADD]]		Funkwerk Enterprise Communications GmbH 🛃 r230aw
Description Index	all		
Protocol	any		
Source Address			Source Mask
Destination Addres	35		Destination Mask
TOS/DSCP Level 2 Priority	00000000 000		TOS/DSCP Mask 00000000 L2 Priority Mask 000
	SAVE		CANCEL
Ready	Τe	Inet	24, 80 24 Rows, 80 Cols VT100 NUM

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

192.168.177.1 -	SecureCRT					×
<u>File E</u> dit <u>V</u> iew Option:	s <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>H</u> e	elp				
R230aw Setup Tool [QOS][FILTER]: Con 	figure IP Classificati	Funkwerk E on Filter 	Interprise Comm	unicatior	ıs GmbH r230aw	^
Abbreviations: s d i	a (source IP address) a (destination IP addr t (icmp type)	sk ess) dk es	o (source port) o (destination stab (TCP estab	port) port)		
Index Descr 1 VoIP 2 all	Conditions sa 192.168.177.9	/32				
<u>900</u>	DELETE	EXIT				
	Talaat	24 90	24 Down - 20 Colo	VT100	DU IM	

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

i 192	.168.17	7.1 - Se	ecureCR	Г						×
<u>File E</u> d	lit <u>V</u> iew	Options	<u>T</u> ransfer	<u>S</u> cript	Tools	Help				
R230aw [QOS]: 	Setup QoS Co	Tool nfigura	ation			Funkwerk	Enterprise	Communicatio	ons GmbH r230aw	^
			IF D	⁹ Filte 9 Class	r ifica	ation and S	ignalling			
			Ir	nterfac	es ar	nd Policies	:			
			Ε>	IT						
Press	<ctrl-r< td=""><td>n>, ≺Cti</td><td>rl-p> to</td><td>) scrol</td><td>l thr</td><td>rough menu</td><td>items, <ret< td=""><td>urn> to enter</td><td></td><td>~</td></ret<></td></ctrl-r<>	n>, ≺Cti	rl-p> to) scrol	l thr	rough menu	items, <ret< td=""><td>urn> to enter</td><td></td><td>~</td></ret<>	urn> to enter		~
Ready				Te	Inet	24, 80	24 Rows, 80	D Cols VT100	NUM	1.33

192.168.177.1	- SecureCRT	
<u>File E</u> dit <u>V</u> iew Opt	ions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp	p
R230aw Setup Too [QOS][CLASS]: Co 	l Fo nfigure IP QoS Classifica	unkwerk Enterprise Communications GmbH 🔼 tion and Signalling r230aw
Abbreviations:	RI (Rule Index) M FI (Filter Index) !! NRI (Next Rule Index) I C (Classify) O	(Action if filter matches) M (Action if filter does not match) (Incoming) (Outgoing)
RI FI NRI	Action Class Filter	Conditions
<u>300</u>	DELETE REORG	EXIT
Ready	Telnet	24, 80 24 Rows, 80 Cols VT100 NUM

Creiamo quindi una catena composta da due regole:

1	92.168	177	7.1 - Se	cureCRT	-							×
Eile	<u>E</u> dit <u>V</u> ie	w <u>(</u>	Options	<u>T</u> ransfer	<u>S</u> cript	Too <u>l</u> s	Help					
R230 EQOS	aw Set: JECLAS	41 qu 1306	001 1003				Funkwerk	Enterpris	e Comm	unicatio	ns GmbH r230aw	^
	Filter Direct	- Lior	ı				VoIP (1) outgoing					
	Action	٦					classify	м				
	<u>Class</u> Signal	ific llir	ation ng (TOS	≥ S/DSCP -	Level	2) >						
				SAVE				CAN	CEL			
												~
Ready					Те	Inet	24, 80	24 Rows, 8	30 Cols	VT100	NUM	1

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

🕞 192.168.177.1 - SecureCRT	
<u>File Edit View Options Transfer Script Tools</u>	Help
R3000 Setup Tool [QOSJ[CLASS][ADD][CLASS]: Configure IP 	Funkwerk Enterprise Communications GmbH 🔨 QoS Classification r3000
Class Type high	priority
<u>IK</u>	CANCEL
	~

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

i	2.168.1	77.1 - Se	ecureCRT	Г		
<u>F</u> ile <u>E</u>	<u>E</u> dit <u>V</u> iew	Options	<u>T</u> ransfer	<u>S</u> cript	Too <u>l</u> s	Help
R230a EQOS:	aw Setup][CLASS]	Tool [ADD]				Funkwerk Enterprise Communications GmbH 🔼 r230aw
	Filter Directio	on				all (2) outgoing
	Action					classify M
	<u>Classif</u> Signall	ication ing (TOS	≥ S/DSCP -	Level	. 2> >	
	Insert	oehind f	Rule			RI 1 FI 1 (VoIP)
			SAVE			
Ready				Τe	Inet	24, 80 24 Rows, 80 Cols VT100 NUM

📠 192.168.177.1 - Secure	CRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ran	sfer <u>S</u> cript Too <u>l</u> s <u>H</u> ei	۰
R230aw Setup Tool [QOS][CLASS][ADD][CLASS] 	F l: Configure IP Qc	Funkwerk Enterprise Communications GmbH 🛧 oS Classification r230aw
Class Type	normal	
Class ID	1	
	ΠK	CANCEL
Deada	Talaak	24 90 24 Dawa 90 Cala LUT100 ANIM

To 192.168.177.1 - SecureCRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp	
R230aw Setup Tool Fu [QOS][CLASS]: Configure IP QoS Classificat	nkwerk Enterprise Communications GmbH < ion and Signalling r230aw
Abbreviations: RI (Rule Index) M FI (Filter Index) !M NRI (Next Rule Index) I C (Classify) O	(Action if filter matches) 1 (Action if filter does not match) (Incoming) (Outgoing)
RI FI NRI Action Class Filter 1 1 2 set M HP VoIP 2 2 0 set M N 1 all	Conditions O sa 192.168.177.9/32 O
DELETE REORG	EXIT
Ready Telnet	24, 80 24 Rows, 80 Cols VT100 NUM 🛒

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


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

🖬 192.168.177.1 - Sec	ureCRT		×
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>I</u>	jransfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp		
R230aw Setup Tool [QOS][INTERFACES]: En	Funkwerk Enterprise Communicatio able IP QoS Classification and Policies	ns GmbH r230aw	^
Interface Fir	st Rule First Filter Scheduler TxRate	e Limit	
en1-0 en1-0-snap en1-1	no IP QoS classification no IP QoS classification no IP QoS classification		
eni-i-snap ethoa50-0 ethoa50-0-snap	no IP Wos classification no IP Wos classification no IP Wos classification		
ngi	no IP QoS classification		
verso_casa verso_rizzuti	no IP QoS classification no IP QoS classification		
vss1-0 vss1-0-snap	no IP QoS classification no IP QoS classification		
EXIT			
Press (Ctrl-n), (Ctrl	-p> to scroll, <return> to select/edit</return>	 I	~
Ready	Telnet 24, 80 24 Rows, 80 Cols VT100	NUM	:

i	2.168.1	77.1 - Se	ecureCRT	Г			×
<u>F</u> ile <u>E</u>	<u>dit V</u> iew	Options	<u>T</u> ransfer	<u>S</u> cript	Too <u>l</u> s	Help	
R230a [QOS]	w Setup ICINTERFA	Tool ACESJEEJ	DITJ			Funkwerk Enterprise Communications GmbH r230aw	^
	Interfa	ce				ngi	
	IP QoS (Classif:	ication	via		RI 1 FI 1 (VoIP)	
	QoS Sche Class-Ba	eduling ased QoS	and Sha 3 Polici	ping) es 〉	>		
	MLPPP In	nterleav	ve Mode			no	
			SAVE			CANCEL	•
Ready				Te	Inet	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 UPload della linea ADSL (quella massima concordata col provider) e indichiamo l'algoritmo di accodamento.

li 19	92.168	177.1 - S	ecureCRT	ſ								×
<u>F</u> ile	<u>E</u> dit <u>V</u> ie	w <u>O</u> ptions	<u>T</u> ransfer	<u>S</u> cript	Too <u>l</u> s	<u>H</u> elp						
R230. EQOS	aw Seti JEINTE	up Tool RFACESIEE	DITJESCH	IEDULEF	R]: Co	Funkw nfigure	erk B QoS	Enterprise Scheduling	Communic g and Sha	ations ping r2 	GmbH 30aw	^
	Queue:	ing and S	chedulin	g Algo	orithm	prior	ity (queueing (f	PQ)			
	Speci	fy Traffi	c Shapin	g		yes						
	Maxim	um Transm	it Rate	(Bits	per S	iecond)		512000				
			OK					CANCE	EL			
Use	<space< td=""><td>> to sele</td><td>ct</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>~</td></space<>	> to sele	ct									~
Ready				Te	elnet	24	, 80	24 Rows, 80	Cols VT10	0	NUM	

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

🖬 192.168.177.1 - SecureCRT	
<u>File Edit View Options Transfer Script Tools</u>	Help
R3000 Setup Tool [QOS][INTERFACES][EDIT]	Funkwerk Enterprise Communications GmbH 🛧 r3000
Interface	ngi
IP QoS Classification via	RI 1 FI 1 (VoIP)
QoS Scheduling and Shaping > Class-Based QoS Policies >	
MLPPP Interleave Mode	no
SAVE	CANCEL
	~

i	92.1	68.17	7.1 - Se	cureCRT	ſ							×
<u>F</u> ile	<u>E</u> dit	⊻iew	Options	<u>T</u> ransfer	<u>S</u> cript	Too <u>l</u> s	Help					
R23(EQO:	0aw 9 5301M	ietup ITERFF	Tool ACESICEI	DITJEPOL	ICYJ:	Confi	Funkwerk E .gure QoS Pol 	Interpri: licies	se Comm	unicati	ons GmbH r230aw	^
	Conf	igure	e QoS Pa	olicies								
	Туре	•		ID	T× Ra	ate	Limitation					
	defa	ault			0		not bounded	k				
	<u>90</u>	0		DE	LETE		EXIT					<
Read	y				Te	elnet	24, 80	24 Rows,	80 Cols	VT100	NUM	1.3

192.1	68.177.1	- Se	cureCRT	ſ					. 0	×
<u>File E</u> dit	<u>V</u> iew <u>O</u> pt	tions	<u>T</u> ransfer	<u>S</u> cript	Tools	<u>H</u> elp				
R230aw S EQOSJEIN	etup Too ITERFACES	51 63CED	ITJCPOL	ICYJEA	כססי	Funkwerk	Enterprise	Communicati	ions GmbH r230aw	~
Cla	iss						high prior	rity		
Мах	imum Tra	ansmi	t Rate	(Bits	per S	iecond)	160000			
Wei Pri	.ght .ority						1 0			
Sha Con Dro Low Upp	aping Alg agestion apping Al ar Queue ar Queue	gorit Avoi lgori e Thr e Thr	hm dance A thm eshold eshold	lgorit (Bytes (Bytes	.hm ;) ;)		token-buck none tail-drop 0 16384	et		
			OK				CANCE	EL		
Enter in	iteger ra	ange	01000	00000						~
Ready				Te	Inet	8, 51	24 Rows, 80	Cols VT100	NUM	

🖻 192.168.177.1 - SecureCRT	
<u> Eile E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s	Help
R230aw Setup Tool [QOS][INTERFACES][EDIT][POLICY][EDIT]	Funkwerk Enterprise Communications GmbH 🛃 r230aw
Class	default
Transmit Rate (Bits per Second) Bound Transmit Rate (Shaping) Transmit Rate Burst	<mark>352000</mark> no 0
Weight Priority	1 255
Shaping Algorithm Congestion Avoidance Algorithm Dropping Algorithm Lower Queue Threshold (Bytes) Upper Queue Threshold (Bytes)	token-bucket none tail-drop 0 16384
ок	CANCEL
Enter integer range 0.,100000000	
Ready Telnet	8, 51 24 Rows, 80 Cols VT100 NUM 🛒

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 - S	ecureCRT	ſ							×
<u>File E</u> dit <u>V</u> ie	w <u>O</u> ptions	<u>T</u> ransfer	<u>S</u> cript	Too <u>l</u> s	<u>H</u> elp					
R230aw Set [QOS][INTE 	up Tool RFACESIEE	DITJCPOL	ICYJ:	Confi	Funkwerf gure QoS F	Enter Olicie	prise Co s	ommunicati	ons GmbH. r230aw	^
Config	ure QoS P	olicies								
Туре		ID	T× Ra	ate	Limitatio	n				
defaul high p	t riority		35200 16000	00 00	not bound bounded	led				
<u></u>		DE	LETE		EX3	.T				
Ready			Τe	elnet	24, 80) 24 Ro	ws, 80 Co	ls 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 <u>due</u> 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 \rightarrow Routing

🖬 192.168.178.1 - SecureCRT	×
<u>File Edit View Options Transfer Script Tools H</u> elp	
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 ×DSL : 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</return></ctrl-p></ctrl-n>	~

🖬 192.168.178.1 - SecureCRT	×
File Edit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Tools <u>H</u> elp	
R232aw Setup Tool Funkwerk Enterprise Communications GmbH [IP]: IP Configuration r232aw	^
RoutingStatic SettingsNetwork Address TranslationUPnPBandwidth Management (TDRC / Load Balancing / BOD)IP Address PoolsBOOTP RelaySNMPRemote Authentication (RADIUS/TACACS+)DNSDynDNSRouting ProtocolsMulticastEXIT	
Press <ctrl-n>, <ctrl-p> to scroll through menu items, <return> to enter</return></ctrl-p></ctrl-n>	~

192.168.178.1	SecureCRT			[K
<u>File E</u> dit <u>V</u> iew <u>O</u> ptio	ns <u>T</u> ransfer <u>S</u> cript	Too <u>l</u> s <u>H</u> elp				
R232aw Setup Tool [IP][ROUTING]: IP 	Routing	Funkwerk B	Interprise Co	mmunications ז	s GmbH 🛃 r232aw	~
The flags are:	U (Up), D (Dorma G (Gateway Route S (Subnet Route)	ant), B (Blocked e), I (Interface), H (Host Route), Route),), E (Extende	d Route)		
Destination 10.0.0.0 192.168.177.0 192.168.178.0 192.168.185.0 213.205.24.20 default default	Gateway 192.168.178.250 192.168.185.2 192.168.178.1 192.168.185.1 217.133.35.252	Mask 255,255,255,0 255,255,255,0 255,255,255,0 255,255,255,0 255,255,255,255,0 0,0,0,0 0,0,0,0	Flags Met. UGS 1 UG 0 U 0 U 0 UH 0 UH 0 UI 1 DI 1	Interface en1-0 en1-1 en1-0 en1-1 Tiscali Tiscali ISON	Pro loc loc loc oth loc loc	
ADD	ADDEXT	DELET	Έ	EXIT		
Press (Ctrl-n), (Ctrl-p> to scroll	l, <space> tag/ur</space>	ntag DELETE,	<return> to</return>	edit	~

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

📠 192.168.178.1 - SecureCRT		
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer	<u>S</u> cript Tools <u>H</u> elp	
R232aw Setup Tool [IP][ROUTING][EDIT]	Funkwerk Enterprise Communications GmbH / r232aw	•
Route Type Network	Default route WAN without transit network	
Partner / Interface	ISDN	
Metric	2	
SAVE	CANCEL	

192.168.178.1	- SecureCRT			
<u>File E</u> dit <u>V</u> iew <u>O</u> ptio	ns <u>T</u> ransfer <u>S</u> cript	Tools <u>H</u> elp		
R232aw Setup Tool [IP][ROUTING]: IP 	'Routing	Funkwerk E	Interprise Commu	nications GmbH 🔼 r232aw
The flags are:	U (Up), D (Dorma G (Gateway Route S (Subnet Route	ant), B (Blocked) e), I (Interface), H (Host Route)), Route),), E (Extended R	oute)
Destination 10.0.0.0 192.168.177.0 192.168.178.0 192.168.185.0 213.205.24.20 default default	Gateway 192.168.178.250 192.168.185.2 192.168.178.1 192.168.185.1 217.133.35.252	Mask 255,255,255,0 255,255,255,0 255,255,255,0 255,255,255,0 255,255,255,255,0 0,0,0,0 0,0,0,0	Flags Met. Int UGS 1 en1 UG 0 en1 U 0 en1 U 0 en1 UH 0 Tis UI 1 Tis DI 2 ISD	erface Pro -0 loc -1 loc -0 loc -1 loc cali oth cali loc N loc
ADD	ADDEXT	DELET	E	EXIT
Press (Ctrl-n), (Ctrl-p> to scrol.	l, <space> tag/ur</space>	ntag DELETE, <re< td=""><td>turn> to edit</td></re<>	turn> to edit

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 \rightarrow Schedule and Monitor \rightarrow Keepalive Monitoring

To 192.168.178.1 - SecureCRT	
<u> Eile Edit View Options Transfer Script Tools H</u>	lelp
R232aw Setup Tool	Funkwerk Enterprise Communications GmbH 🔨 r232aw
Licenses <mark>System</mark>	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	
IP PPP CREDITS CAPI ATM QoS VoIP	GRE L2TP VLAN
Configuration Management Monitoring and Debugging Exit	
Press (Ctrl-n>, (Ctrl-p> to scroll throu	ugh menu items, <return> to enter</return>

🛅 192.168.178.1 - SecureCRT File Edit View Options Transfer Script Tools Help Funkwerk Enterprise Communications GmbH 🔥 R232aw Setup Tool [SYSTEM]: Change System Parameters r232aw System Name Local PPP ID (default) r232aw r232aw_Tiscali Location BINTEC Contact Syslog output on serial console Message level for the syslog table Maximum Number of Syslog Entries no debug 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	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too	s <u>H</u> elp
R232aw Setup Tool [SYSTEM][KEEPALIVE MONITORING][ADD]: 	Funkwerk Enterprise Communications GmbH 🛃 Host Monitoring r232aw
Group IPAddress Interval Trials Source IP DownAction FirstIfIndex Range	0 151.1.1.1 10 3 127.0.0.1 down 10001 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) - Secure	CRT						x
File Edit View Optior	ns Transfer Sc	ript Tools	Help				
🏭 🔀 💭 🏭 🗶 🗈	12 👫 🛛 😼 😼	🕘 🖻 🕯	X 🕈 🛛	0			Ŧ
❤ 192.168.0.254 (1)							4 ⊳
Login: admin Password: Password not change r230aw:> ifstat	d. Call "set	tup" for	quick (configuratio	n.	PhyAddr/ChaTime	
000000 REFUSE 000001 LOCAL 000002 IGNORE 001000 en1-0 001001 en1-0-11c 001002 en1-0-snap 200000 vss1-0 200001 vss1-0-11c 200002 vss1-0-snap 001100 en1-1 001101 en1-1-11c 001102 en1-1-snap 010001 Alice total: 13 r230aw:>■	othr 8192 othr 8192 othr 8192 eth 1500 eth 1496 eth 1492 eth 1496 eth 1492 eth 1500 eth 1492 eth 1492 ppp 1500	0 up 0 up 0 up 100M up 100M up 54M dn 54M dn 54M dn 100M dn 100M dn 100M dn 64K bk	0 0 82 0 0 0 0 327 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 00:00:00 0 00:00:00 0 00:00:00 00:a0:f9:20:e4:: 00:a0:f9:20:e4:: 00:00:00:00:00:00 00:00:00:00:00:00:0	43 43 ≡ 43 00 00 00 43 43 43 43
Ready	Telnet		24, 10	24 Rows, 80 Cols	VT100	CAP NU	JM a

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 conseguenze il router compierà l'azione contraria a quella impostata sul parametro "DownAcrion", 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 .

<u>Suggerimento:</u> 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 - HyperTermi	inal			
File Modifica Visualizza Chiama (<u>T</u> rasferimento <u>?</u>			
				1
R230aw Setup Tool [IP][ROUTING]: IP	Routing	Funkwerk Enterg	orise Communication	r230aw
The flags are:	U (Up), D (Dor G (Gateway Rou S (Subnet Rout	mant), B (Blocked), ite), I (Interface Route e), H (Host Route), E (e), (Extended Route)	
Destination 10.0.0.0 192.168.0.0 default default	Gateway 10.0.0.1 192.168.0.254 10.0.0.2	Mask Flags 255.255.255.252 S 255.255.255.0 0.0.0.0 G 0.0.0.0 BI	s Met. Interface Ø en1-1 Ø en1-0 2 en1-1 1 Alice	Pro loc loc loc loc
	ADDEXT	DELETE	EXIT	
Connesso a 0.35.18 Rile	ev. aut. 9600 8-N-1	SCORR MAIUSC NUM Acquisisci	Eco stampante	_

Se si fa bene attenzione alle metrica 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 \rightarrow Schedule and Monitor \rightarrow Keepalive Monitoring

🕼 192.168.178.1 - SecureCRT	
<u>File E</u> dit <u>V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Tools <u>H</u> elp	
R232aw Setup Tool Funk	werk Enterprise Communications GmbH 🔼 r232aw
Licenses <mark>System</mark>	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 w	nenu items, <return> to enter</return>
I 197.168.178.1 - SecureCR1	
<u>File Edit View Options Transfer Script Tools H</u> elp	werk Enterprise Communications GmbH
File Edit View Options Iransfer Script Tools Help R232aw Setup Tool Funk [SYSTEM]: Change System Parameters	werk Enterprise Communications GmbH 🔼 r232aw
File Edit View Options Iransfer Script Tools Help R232aw Setup Tool Funk [SYSTEM]: Change System Parameters 	werk Enterprise Communications GmbH r232aw
<u>File Edit View Options Iransfer Script Tools H</u> elp R232aw Setup Tool Funk [SYSTEM]: Change System Parameters 	werk Enterprise Communications GmbH r232aw 232aw 232aw_Tiscali
Eile Edit View Options Iransfer Script Tools Help R232aw Setup Tool Funk [SYSTEM]: Change System Parameters	werk Enterprise Communications GmbH r232aw ^232aw ~232aw_Tiscali 3INTEC
Edit View Options Transfer Script Tools Help R232aw Setup Tool Funk ISYSTEM]: Change System Parameters Funk System Name r Local PPP ID (default) r Location r Syslog output on serial console r Message level for the syslog table r Maximum Number of Syslog Entries S Maximum Number of Acctlog Entries S External Activity Monitor > External System Logging > Schedule & Monitor Rassword settings > Time and Date > Time State	kwerk Enterprise Communications GmbH r232aw r232aw r232aw_ r232aw_Tiscali BINTEC
Elle Edit Yiew Options Transfer Script Tools Help R232aw Setup Tool Funk ISYSTEM]: Change System Parameters System Name r Local PPP ID (default) r Location Contact F Syslog output on serial console r Message level for the syslog table o Maximum Number of Syslog E Maximum Number of Acctlog Entries S Maximum Number of Acctlog Entries S External Activity Monitor > External S Password settings > Time and Date > SAVE	Kwerk Enterprise Communications GmbH r232aw 232aw 232aw_Tiscali BINTEC No Bebug 50 20



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.

Router Bintec - HyperTerminal				
Eile Modifica Visualizza Chiama Irasferimento ?				
R230aw Setup Tool Funkwerk Enterprise Communications GmbH [SYSTEM][KEEPALIVE MONITORING][ADD]: Host Monitoring r230aw				
Group 0 IPAddress 151.1.1.1 Interval 10 Trials 3 Source IP 10.0.0.1 DownAction up FirstIfIndex 10001 Range 0				
CANCEL				
	_			
Connesso a 0.46.29 Rilev. aut. 9600 8-N-1 SCORR MAIUSC NUM Acquisisci Eco stampante				

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	
<u>File Edit V</u> iew <u>O</u> ptions <u>T</u> ransfer <u>S</u> cript Too <u>l</u> s <u>H</u> elp	
r230aw:> update http: retrieve current version from: http://www.funkwerk-ec.com/static/files/M	230

r230aw:> update ht retrieve current v Daw/R2 30aw-s_current List of files in this update (len 5778128): Version Length Name .6.1.106 4254565 Boss .6.1.106 798198 webpages.ez 7.6.1.106 7.6.1.106 7.6.1.106 433470 text_ger.ez 64812 CountryProfiles 130952 german.rey 96122 french.rey 7.6.1.106 7.6.1.106 7.6.1.106 *** 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	
<u> Edit View Options Transfer Script Tools H</u> elp	
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 Vr1-f 7.1.1 374902 2006/12/11 14:11:40 XEY-ADSLp.xey Vr1-f 7.6.1.102 433470 2008/07/04 23:53:28 text_ger.ez Vr1-f 7.6.1.102 798158 2008/07/16 13:08:38 webpages.ez Vr1-1 7.6.1.102 96122 2008/07/05 0:00:44 french.rey Vr1-7 7.6.1.102 130952 2008/07/05 0:00:44 german.rey Vr1-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	
<u>File Edit View Options Transfer Script Tools H</u> elp	
r230aw:> update -i	<u>^</u>
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 Vr1-f 7.6.1.102 433470 2006/12/11 14:11:40 XEY-ADSLp.xey Vr1-f 7.6.1.102 433470 2008/07/04 23:53:28 text_ger.ez Vr1-f 7.6.1.102 798158 2008/07/16 13:08:38 webpages.ez Vr1-1 7.6.1.102 96122 2008/07/05 0:00:44 french.rey Vr1-1 7.6.1.102 130952 2008/07/05 0:00:44 german.rey Vr1-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* $\langle y o n \rangle$? 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* $\langle IP del pc che contiene il fw \rangle \langle nome file fw \rangle$

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.

a 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-ROMOK Verify Flash-ROMOK 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 \rightarrow Software & Configuration". Se il router è collegato ad internet è possible scaricare direttamente l'ultima release sul sito del fornitore, altrimenti è possibile specificare il file locale precedentemente scaricato.

🗿 bintec R230aw: Software & Configuration - Options - Microsoft Internet Explorer 🛛 🔲 🗖 🔀					
File Modifica Visualizza Preferiti Strumenti ?					
🔇 Indietro 👻 🕥 🕤 😫	😋 Indietro 🔹 💿 - 🖹 🗟 🏠 🔎 Cerca 📌 Preferiti 🚱 🔗 - 🌺 🕋 - 🛄 🎇 🖄 Collegamenti 🎽				
Indirizzo 🕘 http://192.168.177.1/esi/78	25/esi.cgi?page=status-index.xml&session]	ID=3629612115 💽 🔽 Vai			
bintec R230aw	Language English 🔽 🛛 Online	e Help Express Setup Wizard Logout funkwerki)			
Save configuration		Options			
System Management 🛛 👻					
Physical Interfaces 🔹 👻	Currently Installed Software				
LAN 🔻	BOSS	V.7.8 Rev. 2 (Beta 5) IPSec from 2008/11/14 00:00:00			
Wireless LAN 🔹	System Logic	12			
Routing 🔹	ADEL Logic 621				
WAN -	Software and Configuration Options				
VPN 🔻	Action				
Firewall 🔹	Action				
VoIP 👻	Source Location	Local File			
Local Services 👻 👻	Filename	Local File Stoglia			
Maintenance 🔺	Current Software from Funkwerk Server				
Diagnostics	Go				
External Reporting 🗸 🗸					
Monitoring -					
<					
Cperazione completata		🥑 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 gatway 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.