

## IP ACCESS ROUTER



# Professional Gigabit Ethernet Router **bintec RS120**

- 5 x Gigabit Ethernet
- USB and SFP port
- Web-based configuration / assistants
- IPSec - 5 tunnels, HW acceleration
- Stateful Inspection Firewall
- SIP Application Level Gateway

ETHERNET

5	4	3	2	1	
●	●	●	●	●	LNK/ACT
●	●	●	●	●	SPEED

**bintec RS120**

**funkwerk**

**Disponibilité : 01/03/2010****Routeur professionnel Gigabit Ethernet**

## RS120

Le produit bintec RS120 est un routeur puissant, et flexible car il est équipé de nombreux ports. Conçu dans un boîtier métallique robuste, il convient parfaitement aux PME/PMI, agences ainsi qu'aux travailleurs à domicile. L'équipement possède 5 ports Ethernet Gigabit, qui peuvent être configurés en LAN, WAN ou DMZ. Le routeur RS120 possède également un slot SFP pour gérer un module destiné à la fibre optique. Un modem intégré UMTS connecté au port USB peut être utilisé pour un accès de configuration à distance ou comme interface de secours (backup).

L'équipement est livré en sortie d'usine avec une licence supportant 5 tunnels IPSec avec accélérateur matériel.

### Utilisation des fonctionnalités en souplesse

Seules quelques fonctions sont nécessaires pour transmettre les paquets de données entre deux réseaux. Le routeur bintec RS120 possède les caractéristiques qui vont bien au-delà du routage et peut s'intégrer dans des infrastructures IT complexes. Les fonctionnalités telles que le Routage Étendu et le NAT permettent de gérer les paquets entrants et sortants en fonction de critères pré-définis : protocole IP (Couche 4), adresse IP source ou destination, port source ou destination, TOS / DSCP, interface source ou destination et état de l'interface source ou destination. En outre, il est possible d'utiliser le NAT pour transférer le trafic des données en appel entrant et sortant et pour chaque interface, suivant de nombreux critères.

Grâce au support "multicast", le produit bintec RS120 est idéal pour les applications qui utilisent les techniques de multimédia ou de streaming.

La fonctionnalité Stateful Inspection Firewall (SIF) offre une protection efficace contre les attaques en provenance d'Internet en filtrant dynamiquement les paquets. La gestion du pare-feu est facilitée grâce à de nombreux services pré-configurés. Le filtrage d'URL est une option\* payante. Dans ce cas, toutes les requêtes sortantes Internet sont classées, et permettent que les contenus non souhaités soient filtrés de manière fiable.

L'équipement de base de la Série RS fournit également un niveau SIP Gateway (ALG) pour la connexion directe des téléphones IP au sein du réseau ou l'enregistrement auprès d'un fournisseur de VoIP, sans que la connexion WAN soit affectée au niveau de la sécurité. Les correspondances NAT et le Stateful Inspection Firewall interne sont contrôlés automatiquement par ALG durant la communication.

La QoS (qualité de service) est plus qu'un slogan dans les équipements FEC. Grâce à la convergence croissante entre voix et données, la classification des flux de données gagne en importance. Nos routeurs fournissent les mécanismes QoS pour hiérarchiser le trafic VoIP par rapport au trafic Internet normal, par exemple, et garantissent ainsi une bande passante suffisante.

Vous pouvez de ce fait décider de donner la priorité à votre trafic de données plutôt qu'au trafic lié à la messagerie (e-mail). La mise en oeuvre de la QoS bintec, permet de laisser passer en priorité la voix, par rapport au flux de messagerie dans le tunnel VPN

La fonction DNS proxy prend en charge le réseau local pour la mise en oeuvre d'adresses et la configuration automatique des adresses IP est réalisée via le serveur intégré DHCP.

### Implémentation IPSec

IPSec, intégré au routeur bintec RS120 travaille soit avec des clés pré-partagées soit avec des certificats, ce qui assure un maximum de sécurité. L'Office Fédéral de la Sécurité de l'Information recommande l'utilisation de certificats.

La mise en oeuvre d'IPSec procure une aide réelle lors de la création des connexions VPN avec des adresses IP dynamiques : même si les deux terminaux distants VPN ont une connexion Internet avec des adresses IP dynamiques. Si les deux noeuds VPN possèdent des adresses dynamiques, les informations confidentielles sont assurées.

L'échange d'adresses IP est effectué par le fournisseur DNS.

### Répartition de charge/secours

Les équipements offrent un niveau unique de flexibilité car ils sont pourvu d'un large panel d'interfaces. Le routeur bintec peut être configuré avec deux interfaces WAN. En conséquence, il y a non seulement davantage de bande passante, mais également possibilité de véhiculer le trafic sur des connexions WAN personnalisées, en fonction de la charge ou du type de données. De même, vous pouvez utiliser une liaison (ex. SDSL) pour la connexion VPN du siège et un port WAN en second pour une connexion ADSL à moindre coût garantissant le flux des autres données de l'entreprise. Si une liaison tombe en panne, l'autre prend immédiatement en charge la totalité des données. Dans le cas où les deux lignes ne fonctionneraient plus, le trafic peut être automatiquement dirigé via un modem UMTS connecté sur le port USB.

## Configuration et maintenance aisées

---

Le routeur est configuré via l'interface FCI, qui utilise l'assistant de configuration intégré. Ce configurateur FCI est basé sur le web graphique, et accessible à partir de n'importe quel micro-ordinateur doté d'un navigateur, soit via HTTP, soit via un cryptage en HTTPS. Il offre également la possibilité de gérer, en local ou à distance, les équipements via Telnet, SSH et GSM dialin (seulement dans le cas où un modem USB UMTS est connecté).

DIME Manager de Funkwerk Enterprise Communications (FEC) est un outil gratuit de gestion d'équipements FEC. Il est destiné aux administrateurs qui gèrent des réseaux comportant jusqu'à 50 appareils. Ce logiciel simplifie la gestion et la configuration de routeurs et des points d'accès, soit individuellement, soit par groupe. Lors de sa conception, l'objectif premier de cet outil, était sa simplicité. En effet, il autorise les mises à jour logicielles ou les configurations par simple "drag and drop". Il reconnaît et gère les nouveaux dispositifs du réseau grâce à la multidiffusion utilisée par le SNMP : en d'autres termes, indépendamment de leur adresse actuelle.

\* Le Filtrage d'URL est un service payant. Il existe une version test de 30 jours.

## VPN

Feature	Description
PPTP (PAC/PNS)	Point to Point Tunneling Protocol for establishing Virtual Private Networks, inclusive strong encryption methods with 128 Bit (MPPE) up to 168 Bit (DES/3DES, Blowfish)
GRE v.0	Generic Routing Encapsulation V.0 according RFC 2784 for common encapsulation
L2TP	Layer 2 tunnelling protocol inclusive PPP user authentication
Number of VPN tunnels	Inclusive 5 active VPN tunnels with the protocols IPSec, PPTP, L2TP and GRE v.0 (also in combination possible)
IPSec	Internet Protocol Security establishing of VPN connections
Number of IPSec tunnels	Inclusive 5 active IPSec tunnels
IPSec Algorithms	DES (64 Bit), 3DES (192 Bit), AES (128,192,256 Bit), CAST (128 Bit), Blowfish (128-448 Bit), Twofish (256 Bit); MD-5, SHA-1, RipeMD160, Tiger192 Hashes
IPSec hardware acceleration	Integrated hardware acceleration for IPSec encryption algorithms DES, 3DES, AES
IPSec IKE	IPSec key exchange via preshared keys or certificates
IPSec IKE Config Mode	IKE Config Mode server enables dynamic assignment of IP addresses from the address pool of the company. IKE Config Mode client enables the router, to get assigned dynamically an IP address.
IPSec IKE XAUTH (Client/Server)	Internet Key Exchange protocol Extended Authentication client for login to XAUTH server and XAUTH server for logging of XAUTH clients
IPSec IKE XAUTH (Client/Server)	Inclusive the forwarding to a RADIUS-OTP (One Time Password) server (supported OTP solutions see <a href="http://www.funkwerk-ec.com">www.funkwerk-ec.com</a> ).
IPSec NAT-T	Support of NAT-Traversal (Nat-T) for the application at VPN lines with NAT
IPSec IPComp	IPSec IPComp data compression for higher data throughput via LZS
IPSec certificates (PKI)	Support of X.509 multi-level certificates compatible to Microsoft and Open SSL CA server; upload of PKCS#7/8/10/12 files via TFTP, HTTP, HTTPS, LDAP, file upload and manual via FCI
IPSec SCEP	Certificates management via SCEP (Simple Certificate Enrollment Protocol)
IPSec Certificate Revocation Lists	Support of remote CRLs on a server via LDAP or local CRLs
IPSec Dead Peer Detection (DPD)	Continuous control of IPSec connection
IPSec dynamic DNS	Enables the registering of dynamic IP addresses by a dynamic DNS provider for establishing a IPSec connection.
IPSec RADIUS	Authentication of IPSec connections at a RADIUS server. Additionally the IPSec peers, which were configured on a RADIUS server, can be loaded into the gateway (RADIUS dialout).
IPSec Multi User	Enables the Dial-in of several IPSec clients via a single IPSec peer configuration entry
IPSec QoS	The possibility to operate Quality of Service (traffic shaping) inside of an IPSec tunnel
IPSec NAT	By activating of NAT on an IPSec connection it is possible, to implement several remote locations with identical local IP address networks in different IP nets for the VPN connection

## Sécurité

Feature	Description
NAT/PAT	Symmetric Network and Port Address Translation (NAT/PAT) with random generated ports inclusive Multi NAT (1:1 translation of whole networks)
Policy based NAT/PAT	Network and Port Address Translation via different criteria like IP protocols, source/destination IP Address, source/destination port
Policy based NAT/PAT	For incoming and outgoing connections and for each interface variable configurable
Content Filtering	Optional ISS/Cobion Content filter (30 day test license inclusive)
Stateful Inspection Firewall	Packet filtering depending on the direction with controlling and interpretation of each single connection status
Packet Filter	Filtering of IP packets according to different criteria like IP protocols, source/destination IP address, source/destination port, TOS/DSCP, layer 2 priority for each interface variable configurable

## Routeage

Feature	Description
Policy based Routing	Extended routing (Policy Based Routing) depending of diffent criteria like IP protocols (Layer4), source/destination IP address, source/destination port, TOS/DSCP, source/destination interface and destination interface status
Multicast IGMP	Support of Internet Group Management Protocol (IGMP v1, v2, v3) for the simultaneous distribution of IP packets to several stations
Multicast IGMP Proxy	For easy forwarding of multicast packets via dedicated interfaces
Multicast inside IPsec tunnel	Enables the transmission of multicast packets via an IPsec tunnel
RIP	Support of RIPv1 and RIPv2, separated configurable for each interface
Extended RIP	Triggered RIP updates according RFC 2091 and 2453, Poisoned Reverse for a better distribution of the routes; furthermore the possibility to define RIP filters for each interface.

## Protocoles/Encapsulation

Feature	Description
PPP/MLPPP	Support of Point to Point Protocol (PPP) for establishing of standard PPP connections, inclusive the Multilink extension MLPPP for the bundeling of several connections
PPPoE (Server/Client)	Point-to-Point Protocol over Ethernet (Client and Server) for establishing of PPP connections via Ethernet/DSL (RFC 2516)
MLPPPoE (Server/Client)	Multilink extension MLPPPoE for bundeling several PPPoE connections (only if both sides support MLPPPoE)
DNS	DNS client, DSN server, DNS relay and DNS proxy
DYN DNS	Enables the registering of dynamic assigned IP addresses at adynamic DNS provider, e.g. for establishing of VPN connections
DNS Forwarding	Enables the forwarding of DNS requests of free configurable domains to assigned DNS server.
DHCP	DHCP Client, Server, Proxy and Relay for simplified TCP/IP configuration
Packet size controlling	Adaption of PMTU or automatic packet size controlling via fragmentation

## Qualité de Service (QoS)

Feature	Description
Policy based Traffic Shapping	Dynamic bandwidth management via IP traffic shaping
Bandwidth rreservation	Dynamic reservation of bandwidth, allocation of guaranteed and maximum bandwidths
DiffServ	Priority Queuing of packets on the basis of the DiffServ/TOS field
Layer2/3 tagging	Conversion of 802.1p layer 2 prioritisation information to layer 3 diffserv attributes
TCP Download Rate Control	For reservation of bandwidth for VoIP connections



## Répartition de charge

Feature	Description
BoD	Bandwidth on Demand: dynamic bandwidth to suit data traffic load
Load Balancing	Static and dynamic load balancing to several WAN connections on IP layer
VPN backup	Simple VPN backup via different media. Additional enables the Funkwerk interface based VPN concept the application of routing protocols for VPN connections.

## Fonctionnalité Couche 2

Feature	Description
Bridging	Support of layer 2 bridging with the possibility of separation of network segment via the configuration of bridge groups
VLAN	Support of up to 32 VLAN (Virtual LAN) for segmentation of the network in independent virtual segments (workgroups)
Proxy ARP	Enables the router to answer ARP requests for hosts, which are accessible via the router. That enables the remote clients to use an IP address from the local net.

## Logging / Monitoring / Reporting

Feature	Description
Internal system logging	Syslog storage in RAM, display via web-based configuration user interface (http/https), filter for subsystem, level, message
External system logging	Syslog, several syslog server with different syslog level configurable
E-Mail alert	Automatic E-Mail alert by definable events
SNMP traps	SNMP traps (v1, v2, v3) configurable
Activity Monitor	Sending of information to a PC on which Brickware is installed
IPSec monitoring	Display of IPSec tunnel and IPSec statistic; output via web-based configuration user interface (http/https)
Interfaces monitoring	Statistic information of all physical and logical interfaces (ETH0, ETH1, SSIDx, ...), output via web-based configuration user interface (http/https)
IP accounting	Detailed IP accounting, source, destination, port, interface and packet/bytes counter, transmission also via syslog protocol to syslog server
RADIUS accounting	RADIUS accounting for PPP, PPTP, PPPoE and ISDN dialup connections
Keep Alive Monitoring	Control of hosts/connections via ICMP polling
Tracing	Detailed traces can be done for different protocols e.g. ISDN, PPPoE, ... generation local on the device and remote via DIME manager
Tracing	Traces can be stored in PCAP format, so that import to different open source trace tools (e.g. Wireshark) is possible.

## Administration/Gestion

Feature	Description
RADIUS	Central check of access authorization at one or several RADIUS server, RADIUS (PPP, IPSec inclusive X-Auth and login authentication)
RADIUS dialout	On a RADIUS server configured PPP und IPSec connection can be loaded into the gateway (RADIUS dialout).
TACACS+	Support of TACACS+ server for login authentication and for shell comando authorization
Time synchronization	The device system time can be obtained via ISDN and from a SNTP server (up to 3 time server configurable). The obtained time can also be transmitted per SNTP to SNTP clients.
Automatic Time Settings	Time zone profiles are configurable. That enables an automatic change from summer to winter time.
Supported management systems	DIME Manager, XAdmin
Configurable scheduler	Configuring of time and event controlled tasks, e.g. reboot device, activate/deactivate interface, activate/deactivate WLAN, trigger SW update and configuration backup
Funkwerk Configuration Interface (FCI)	Integrated web server for web-based configuration via HTTP or HTTPS. This user interface is by most of Funkwerk EC products identical.
Software update	Software updates are free of charge; update via local files, HTTP, TFTP or via direct access to the FEC web server
Remote maintenance	Remote maintenance via telnet, SSL, SSH, HTTP, HTTPS and SNMP (V1,V2,V3)
Configuration via serial interface	Serial configuriton interface is available
GSM remote maintenance	Remote maintenance via GSM login (external USB UMTS (3G) modem required)
Device discovery function	Device discovery via SNMP multicast.
On The Fly configuration	No reboot after reconfiguration required
SNMP	SNMP (v1, v2, v3), USM model, VACM views, SNMP traps (v1, v2, v3) configurable, SNMP IP access list configurable
SNMP configuration	Complete management with MIB-II, MIB 802.11, Enterprise MIB
Configuration export and import	Load and save configurations, optional encrypted; optional automatic control via scheduler
SSH login	Supports SSH V1.5 and SSH V2.0 for secure connections of terminal applications
HP OpenView	Integration into Network Node Manager

## Interfaces

Feature	Description
Ethernet	5 x 10/100/1000 Mbps Ethernet Twisted Pair, autosensing, Auto MDI/MDI-X, up to 4 ports can be switches as additional WAN ports incl. load balancing, all Ethernet ports can be configured as LAN or WAN.
SFP slot	SFP slot for conventional optical 10/100/1000 Mbps Ethernet SFP module
USB 2.0 host	USB 2.0 full speed host port for connecting UMTS (3G) USB modem sticks (supported sticks: see <a href="http://www.funkwerk-ec.com">www.funkwerk-ec.com</a> )
Serial console	Serial console interface / COM port (mini USB)

## Caractéristiques matérielles

Feature	Description
Realtime clock	System time persists even at power failure for some hours.
Wall mounting	Integrated in housing
Environment	Temperature range: Operational 0°C to 40°C; storage -10°C to 70°C; Max. rel. humidity 10 - 95% (non condensing)
Power supply	External wall power supply 110-240V / 12 V DC, 1.5 A, with energy efficient switching controller; complies with EuP directive 2008/28/EC
Power consumption	Less than 5 Watt
housing	Metal case, opening for Kensington lock, connectors at back side, prepared for wall mounting
Dimension	Ca. 235 mm x 31.5 mm x 146,5 mm (W x H x D)
Weight	Ca. 1000g
Fan	Fanless design therefor high MTBF
Reset button	Restart or reset to manufacturing preset possible
Status LEDs	Power, Status, 10 * Ethernet, SFP, USB
Standards and certifications	R&TTE directive 1999/5/EG; EN 55022; EN 55024 + EN 55024/A1; EN61000-3-2; EN 61000-3-3; EN 61000-4-4; EN 60950-1; EN 300 328

## Pack de livraison

Feature	Description
Manual	Quick Installation Guide in German and English
DVD	DVD with system software, management software and documentation
Ethernet cable	1 Ethernet cable, 3m
Power supply	Wall power supply 110-240V / 12 V DC, 1.5 A, with high efficient switching controller

## Service

Feature	Description
Warranty	2 year manufacturer warranty inclusive 24h advanced replacement
Software Update	Free-of-charge software updates (system software (BOSS) and management software (DIME manager)

## N° article

Feature	Description
bintec RS120; art. no. 5510000219	IP Access Router; incl. IPSec (5 tunnels), certificates, HW encryption; 4+1 Gigabit Eth. switch; USB port; SFP module slot; german and intern. version.
bintec RS120 - UK; art. no. 5510000256	IP Access Router; incl. IPSec (5 tunnels), certificates, HW encryption; 4+1 Gigabit Eth. switch; USB port; SFP module slot; UK version.

## Options

Feature	Description
Cobion Content Filter Small	License for one year Cobion content filter (small); art. no. 80551
MPPC and Stac compression	Free-of-charge license for Stac and MPPC compression; registration under <a href="http://www.funkwerk-ec.com">www.funkwerk-ec.com</a> required
Service package 'small'	Warranty extension of 3 years to a total of 5 years, including advanced replacement for FEC products of the category "small". (Please find a ) detailed description as well as an overview of the categories on <a href="http://www.funkwerk-ec.com/servicepackages">www.funkwerk-ec.com/servicepackages</a> .
Advanced Replacement	Optional (with costs) advanced replacement outside of warranty time