SpeedStream®

SpeedStream® 5930/5935 ADSL Business Routers

Enabling managed services

Built for Business

Service providers can seize a new ADSL service opportunity: offering high-speed Internet access and managed services to two emerging markets, small and medium businesses (SMBs) and teleworkers. These customers typically need the same service features as larger enterprises—that is, secure access, high availability, and simple management. Yet many of them still have not made the transition from dial-up to high-speed Internet access. This makes them prime candidates for ADSL Internet access—and ultimately, for managed service offerings.

Now, service providers can quickly and cost-effectively provision ADSL services for SMBs and teleworkers, with the SpeedStream® 5930 and 5935 ADSL Business Gateways. What's more, the service provider can add value by offering managed services, such as firewalls, Virtual Private Networks (VPNs), and differentiated classes of service.

Enterprise-grade features for small and medium businesses
To gain maximum value from their DSL infrastructures, service providers need

to deliver more than just Internet access. With 5930/5935 ADSL Business Gateways, service providers can offer managed services at the time of initial service introduction or later, depending on their business model. Potential managed services include:

> **Security**—The service provider can deploy VPNs and firewalls for SMBs that don't have an IT staff, or whose IT staff prefers to outsource this service.

> **IP Quality of Service (QoS)**—By differentiating between types of IP traffic and giving priority to the most urgent or time-sensitive, the service provider can offer differentiated classes of service—not possible until now with DSL services.

> **High availability**—SpeedStream 5930/ 5935 ADSL Business Gateways support high availability with a redundant configuration option and dial backup functionality. The gateway instantly detects if the DSL line is unavailable and, if so, automatically establishes a backup connection with the service provider.

Rapid service deployment to a large area
Based on the ITU G.922.1 Annex A/B and ETSI ITS101388 ADSL standards, the SpeedStream 5930/5935 ADSL Business Gateways can be deployed rapidly, enabling service providers to quickly begin earning service revenues. Integration costs and resource requirements are reduced because the gateway combines the functions of a DSL modem, switch, router, VPN security appliance, and firewall in a single chassis. Provisioning is faster and requires fewer resources because 5930/5935 ADSL Business Gateways can be installed by the business customer via a browser-based interface.

With extended reach, simplified provisioning and management, and support for value-added services, SpeedStream 5930/5935 ADSL Business Gateways enable service providers to leverage their existing DSL infrastructures for more customers, more revenues, and better service.

SIEMENS

Global network of innovation

Value-Added Services

Managed firewalls

SMBs and teleworkers increasingly recognize the urgency of protecting sensitive business information transferred over the Internet. Often lacking the IT resources to address their security vulnerabilities, these customers are a receptive audience for outsourced security services. With 5930/5935 ADSL Business Gateways, service providers can offer either a basic business firewall or an ICSA-compliant stateful inspection firewall for enterprise-grade security (figure 1). Service providers can quickly provision highly secure VPNs using the configuration and management protocols that best fit their environment: HTTP, SNMP, SSH, or Telnet. VPNs can be configured to support Internet Protocol Security (IPSec) with Internet Key Exchange (IKE), Triple Data Encryption Standard (3DES), Layer 2 Tunneling Protocol (L2TP), and L2TP inside of IPSec. A VPN accelerator increases IPSec 3DES VPN throughput to up to 8 Mbps. By offering security services, the service provider delivers additional value over its existing infrastructure.

Quality of Service (QoS) for enterprise teleworkers

SMBs employ growing numbers of teleworkers who need reliable, secure high-speed Internet access. This creates an opportunity for service providers to manage swelling traffic volume, thus adding value to their broadband services. SpeedStream 5930/5935 Business Gateways enable the service provider to assign priority to specified types of traffic using IP Quality of Service (QoS) features, such as DiffServ and Weighted Fair Queuing (WFQ). Thus, the service provider or its SMB customer can offer the teleworker a separate service for personal use, without affecting network performance for business-critical tasks (figure 2).

Flexible, secure management

Ease of management directly affects service profitability. SpeedStream 5930/5935 Business Gateways speed provisioning because business customers can install them without assistance, using an intuitive, browser-based interface. Role-based management gives the service provider the flexibility to decide which functions the customer can access and which remain under the service provider's exclusive control (figure 3). And the ability to maintain users and roles centrally, in a RADIUS database, reduces the management burden as the service grows. With simple, secure management, the service provider can introduce its ADSL service for SMBs and teleworkers more quickly, begin earning revenues sooner, and scale rapidly.
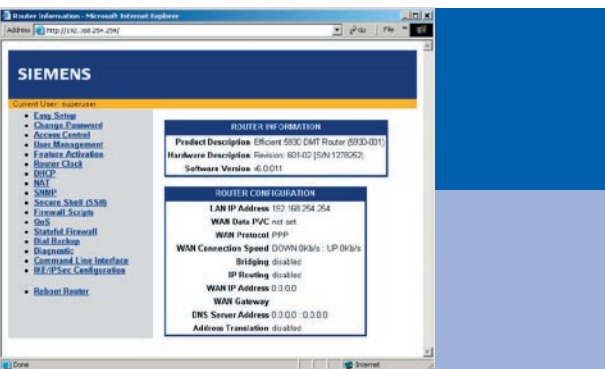
SpeedStream 5930/5935 ADSL Business Routers

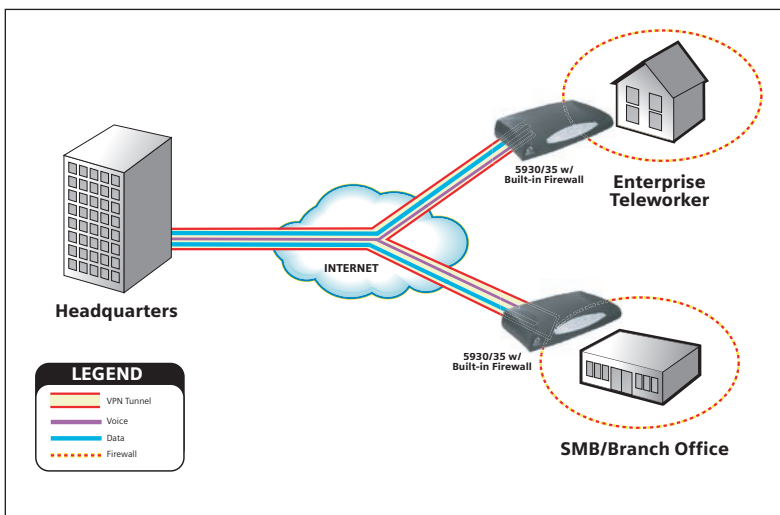**Figure 3:** SpeedStream 5930/5935 ADSL Business Gateway user interface.

LEGEND
- VPN Tunnel
- Voice
- Data
- Firewall

Figure 1: SMBs and teleworkers use SpeedStream 5930/5935 for ADSL access, firewall, and secure VPN.

LEGEND
- VPN Tunnel
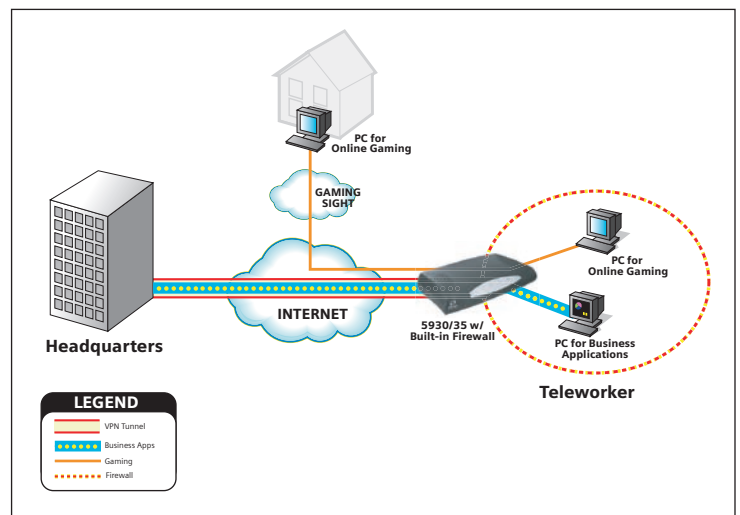- Business Apps
- Gaming
- Firewall

Figure 2: Using IP QoS features the service provider can assign higher priority to business applications than to personal applications, such as online gaming, for example.

Feature	Benefit
Enterprise-Grade Security	
Basic Business Firewall	Secures users' networks from suspicious packets and denial of service attacks with four preset, easy-to-implement configurations, customization capabilities, and detailed event logs
ICSA-COMPLIANT Stateful Inspection Firewall	Provides enterprise-grade security to users who need further assurance for business sensitive data and applications
Secure Virtual Private Network (VPN) with IPSec, IKE, DES, and 3DES encryption	Secures the datapath from interception, examination, alteration or corruption by authenticating and encrypting data for all authorized network clients
VPN Accelerator	Maximizes IPSec 3DES VPN performance
Powerful, Secure Management	
Remote and local management	Maximizes opportunities for managed services by providing tools to allow management over SNMP, Telnet, HTTP, or the console port. On-board scripting engine simplifies development of standard configuration scripts for mass-deployment
Secure management	Protects administrative access and communications with IPSec and SSH for authentication and encryption
Role-based management	Enables multi-level managed services by restricting the ability to view or change the configuration with up to 4 different predefined roles (up to 15 users names in the local database)
RADIUS management authentication	Reduces the cost of management by authenticating administrators in a single database
IP Quality of Service	
Weighted Fair Queuing (WFQ)	Enables value-added services by optimizing router throughput based on real-time or other latency sensitive traffic types
DiffServ	Enables differentiated services and SLAs by optimizing end-to-end throughput based on traffic types
High Availability	
External dial backup	Maximizes uptime by automatically using an external modem to connect to the Internet if the WAN link or IP datapath fails
Integrated dial backup modem (5930 only)	Simplifies contingency management and maximizes uptime by allowing users to automatically connect to the Internet if the WAN link or IP datapath connection fails
Virtual Router Redundancy Protocol (VRRP)	Maximizes uptime by automatically rerouting traffic to an alternate router if the WAN link or IP datapath fails
Simplified Deployment	
Self-installation	Enables users to self-install services with no additional software and minimal knowledge of service and networking settings through any Web browser
Easy diagnostics	Simplifies self-installation by allowing users to access critical information to troubleshoot and correct issues without on-site technical help
Network address translation (NAT/NAPT)	Simplifies IP address assignment by hiding the address information of the end-user's local network
8-port 10/100Base-T Ethernet switch	Provides optimal LAN connectivity and performance
Reliable Investment	
Single, integrated solution	Provides a single point of management which minimizes deployment, support costs, and space required
Platform and operating system independent	Reduces the cost of operations, due to interoperability with the IEEE 802.3 standards

Software Features

Security

Secure Management
- User authentication (PAP/CHAP) with PPP (RFC 1334, RFC 1994)
- Password control for configuration manager
- SNMP community name reassignment
- Telnet/SNMP port reassignment/Access Control List
- Role-based management
  - Four pre-configured templates
  - Up to 15 user names stored in the local database
- RADIUS management authentication support
- SSH and IPSec secure management channels

Basic Business Firewall
- Filter on source and/or destination IP address/port value
- Filter on SYN, ACK flags and ICMP
- Apply input, output, transmit, and receive filters on each interface
- Stateful inspection when NAT is enabled
- Logging and scripting

ICSA-Compliant Stateful Inspection Firewall
- Provides enterprise-grade firewall protection from
  - Common Denial of Service (DoS) attacks and exploits including Killwin, Land, Ping of Death, Smurf, Teardrop, Tiny Fragments, and WinNuke
  - Distributed Denial of Service (DDoS) attacks including ICMP, SYN and UDP floods
  - Other hacking attacks including IP address sweeping, IP spoofing, port scanning
- Opens ports to serve legitimate requests and automatically closes them when the request or session ends
- Full-time Stateful Packet Inspection with built-in support for most popular applications
- No pre-defined limit on the number of rules that can be created and applied
- All firewall messages can be logged to the router console and to syslog servers
- Maintains a log of the most recently dropped packets in the browser-based user interface

Secure Virtual Private Networking
- L2TP, IPSec, and L2TP inside of IPSec
- No pre-defined limit on VPN tunnels
- IPSec Tunnel and Transport modes with AH and ESP
- Internet Key Exchange (IKE) including Aggressive Mode
- DES (56-bit) and 3DES (168-bit) encryption
- Supports Perfect Forward Secrecy (DH Groups 1 and 2)
- Provides protection from replay attacks
- Implements RFCs 1321, 1828, 1829, 2085, 2104, 2401-2410, 2412, 2420, 2437, 2451, and 2631 (Groups 1 and 2)

Configuration, Management and Monitoring
- Easy setup through a browser-based user interface
- Configuration and management using HTTP, serial console, SNMP, SSH, or Telnet
- Out-of-band configuration and management using serial console port
- Supports dedicated routed management PVC in bridged and routed mode
- TFTP download/upload of new software, configuration files, and scripts
- Stores backup copy of firmware on dual bank flash memory for system recovery
- Performance monitoring data available using SNMP
- Dynamic event and history logging
- Network boot using a BootP server (RFC 2131, RFC 2132)
- Syslog server support

IP Quality of Service (IP QoS)
- DiffServ traffic prioritization through ToS byte marking
- Weighted Fair Queuing traffic prioritization
- Configurable queue weighting
- Configurable traffic prioritization policies by
  - Date, day of week, and time
  - Source and destination addresses
  - Port, protocol, and application

High Availability
- Dial backup support – Integrated v.90 modem
- Virtual Router Redundancy Protocol (VRRP) (RFC 2338) for failover support to other VRRP-capable routers

Protocols

ATM
- Encapsulation (IP, Bridging, and Bridge Encapsulated Routing) (RFC 2684/1483)
- PPP over ATM (LLC and VC multiplexing) (RFC 2364)
- Classical IP over ATM (RFC 2225)
- Classical IP (RFC 1577)
- AAL5
- Virtual Circuit (VC) traffic shaping (CBR, PCR, UBR, VBR)
- No pre-defined limit on VCs
- I.610 OAM F5 end-to-end and segment LoopBack
- Initiates and responds to LoopBack signaling

Frame Relay
- Support of frame relay ANSI T1.618 and CCITT Q.922 formats
- DLCI support
- Inverse ARP support
- LMI support including LMI protocol discovery
- LLCP auto-update
- CIR & EIR rate enforcement
- Network congestion management

PPP (RFC 1661, RFC 2364)
- PPP over Ethernet (RFC 2516)
- PPP over ATM (RFC 2364)
- Bridging (RFC 1638)
- IP Routing (RFC 1331)
- IPX Routing (RFC 1552)
- Multiclass extensions to MLPPP (RFC 2686)
- MLPPP (RFC 1990)
- Data compression of up to 4:1 (STAC™ LZS) (RFC 1974)
- Van Jacobson header compression (RFC 1144)
- Spoofing and filtering (IP-RIP, IPX-RIP, SAP, Watchdog serialization)
- Automatic IP and DNS assignment (RFC 1877)

Routing
- TCP/IP with RIP1 (RFC 1058), RIP1-compatible and RIP2 (RFC 1389), or static routing on the LAN and/or WAN
- Novell® IPX with RIP/SAP (RFC 1552)
- DHCP server (RFC 2131, RFC 2132), relay agent (RFC 1542), and client (RFC 2132)
  - Automatically defers to other DHCP servers on the network
  - Automatically adjusts to changes in LAN IP addressing
  - No pre-defined limit on DHCP clients
- DNS relay
- Multiple subnets on the LAN support NAT, RIP1, RIP2, ARP and IP filters
- Virtual routes can be defined based on user IP addresses or ranges

IP Address Translation
- Network renumbering (RFC 1631)
- Network Address Translation (NAT/PAT/NAPT)
- NAT passthrough support for numerous applications including IPSec, PPTP, H.323, SIP and NetMeeting
- Supports public Web and e-mail servers with NAT

Hardware Features

WAN Interface
- 5930: Compliant with ADSL ITU G.992.1 Annex A and ANSI T1.413 G.DMT, ADSL ITU G.992.2 Annex A G.Lite
- 5935: Compliant with ADSL ITU G.992.1 Annex B G.DMT, ADSL ETSI TS101388, and Deutsche Telekom U-R2
- Supports line rates
  - From 64Kbps to 8,128Kbps downstream
  - From 64Kbps to 1,024Kbps upstream
- Embedded Operations Channel (EOC) support

LAN Interface
- Built-in 8-port 10/100Base-T Ethernet switch with link status LED for each port
- Auto detects full or half duplex operation
- Auto detects regular or crossover cable for easy connection to a switch or hub
- Ports can be configured individually and manually for:
  - Enabling/disabling
  - Speed and duplex
  - Port mirroring

Serial Interface
- One asynchronous serial console port

VPN Accelerator
- Dedicated encryption processor maximizes IPSec 3DES VPN throughput

Product Enclosure
- Front panel LED status for Power, Test, WAN, LAN, and backup
- Rear panel LED status for each Ethernet port link
- Installation options: Desktop or wall mount

SpeedStream 5930 back panel view

SpeedStream 5935 back panel view

SIEMENS

Global network of innovation