# SpeedStream®

# SpeedStream® 5950 SDSL/SHDSL Business Gateway

## Choose between SDSL or SHDSL

### Built for Business

For cost-conscious business customers who need high performance, the new Symmetric High-Density Digital Subscriber Line (SHDSL) standard[1] is fast becoming the access method of choice. Compared to SDSL, SHDSL offers increased reach and bandwidth plus a big bonus: standardization. For these reasons the SHDSL market is projected to grow substantially in the small and medium business (SMB) market.

Now, service providers can quickly and cost-effectively provision SHDSL services for their business customers, with the SpeedStream® 5950 SDSL/SHDSL Business Gateway. What's more, service providers can add value by offering managed services such as firewalls, Virtual Private Networks (VPNs), and differentiated classes of service.

#### Easy Migration from SDSL to SHDSL

The SpeedStream 5950 SDSL/SHDSL Business Gateway can be configured for either SDSL or SHDSL via a simple command. The ability to offer either access method through a single device facilitates the transition from SDSL to SHDSL.

The reasons for migrating to SHDSL are compelling. Compared to SDSL, SHDSL has 30% more reach, with translates to at least a 60% larger coverage area. With up to 2.3Mbps symmetric bandwidth on a single copper pair, SHDSL supports higher bandwidth services, such as Voice over IP. And its standardization eliminates traditional interoperability problems between Digital Subscriber Line Access Multiplexers (DSLAMs) and customer premises equipment.

#### Enterprise-grade features for small and medium businesses

Incorporating the latest technological advances, the SpeedStream 5950 SDSL/SHDSL Business Gateway combines the functions of a DSL modem, managed 8-port 10/100Base-T Ethernet switch, ICSA-compliant firewall, VPN security appliance, and full-featured router—all in a single chassis.

Service providers can offer multiple managed services at the time of service introduction, or start with one or two and add others, gradually increasing service revenue. 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 premium services such as managed VoIP and managed videoconferencing.

> **High availability**—The SpeedStream 5950 Business Gateway supports high availability with a redundant router configuration or dial backup functionality. The gateway automatically establishes a backup connection if it detects a DSL link failure.

The feature-rich operating system enables service providers to provision and manage all value-added services remotely, from a single interface, speeding service activation and eliminating the expense of on-site installation. An intuitive, browser-based interface allows business customers to install the gateway without assistance, reducing service provider operational expenditures.

With extended reach, simplified provisioning and management, and support for value-added services, the SpeedStream 5950 SDSL/SHDSL Business Gateway enables service providers to leverage their existing DSL infrastructures for more customers, more revenues, and better service—with an assurance of interoperability with other standards-compliant equipment.

1 International Telecommunications Union (ITU) standard G.shdsl, also known as ITU G.991.2

# SIEMENS

### Global network of innovation

# Value-Added Services

## SpeedStream 5950 SDSL/ SHDSL Business Gateway

### Managed Data Networking Services

The IP Quality of Service (QoS) and security features in the SpeedStream 5950 SDSL/SHDSL Business Gateway enable service providers to offer managed data networking services that meet the business requirements of SMBs and enterprise branch offices.

For example, consider a prospective customer with three offices across the state that needs an inexpensive solution for data backup, videoconferencing, and application hosting. By deploying the SpeedStream 5950 SDSL/SHDSL Business Gateway at the customer premises and managing it from the Network Operations Center (NOC), the service provider could offer (figure 1):

> SDSL access, SHDSL access, or even a mix

> Firewall management—either a basic business firewall or ICSA-compliant stateful inspection firewall for enterprise-grade security

> VPNs with support for Internet Protocol Security (IPSec) with Internet Key Exchange (IKE), Triple Data Encryption Standard (3DES), Layer 2 Tunneling Protocol (L2TP), and L2TP inside of IPSec

> Internet videoconferencing

> Application hosting

By delivering managed services, the service provider gains new customers, reduces churn, and delivers valuable services for which customers are willing to pay a premium.

### Backup for T1/E1 services

When a T1/E1 subscriber needs a high availability contingency plan, the traditional offer has been a back-up T1/E1 line—effective, but expensive. Now, with the SpeedStream 5950 Business Gateway, the service provider can use SDSL or SHDSL as the backup circuit for customers within the service area, dramatically reducing costs for both the service provider and customer. Both the T1/E1 and DSL paths can be used simultaneously; if one fails, the other automatically picks up the load. It's a particularly cost-effective approach because both circuits are active all the time (figure 2).

To configure DSL as the contingency for a T1/E1 primary line, service providers use the gateway's Virtual Router Redundancy Protocol (VRRP) feature. For Internet access, the secondary path is ATM over DSL. For dedicated point-to-point contingency, the service provider can configure the gateway for dedicated ATM or IP-VPN. With the latter option, an IPSec tunnel is mapped across the Internet to a corporate site.
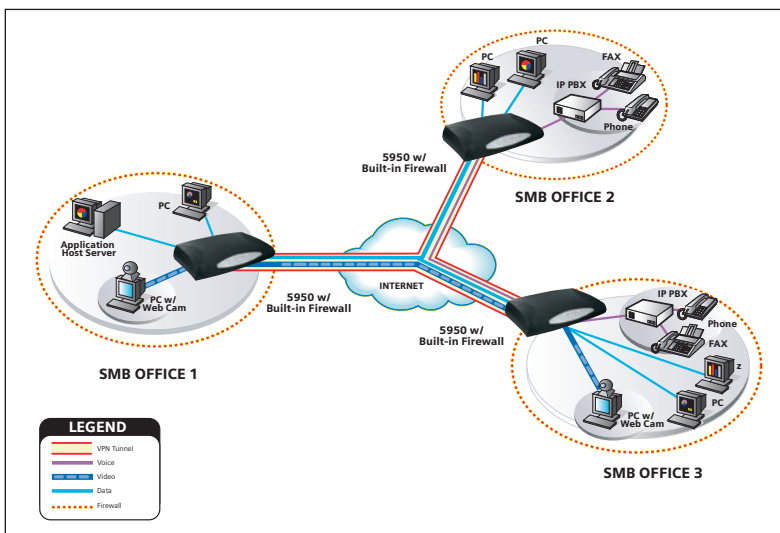


**Figure 1:** Multi-location SMB using the SpeedStream 5950 SDSL/SHDSL Business Gateway for SHDSL access, firewall, VPN, and advanced applications.
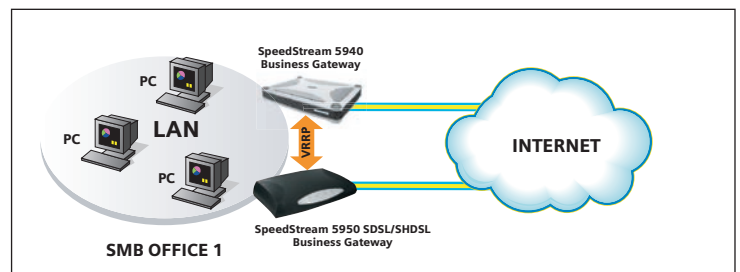


**Figure 2:** SMB office with T1 primary access and SHDSL/SDSL backup.

| 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 |
| **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 |

# technical

## *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
- SHDSL: Compliant with SHDSL ITU G.991.2 Annex A or B; G.hs ITU G.994.1
- SDSL interoperable with many DSLAM implementations
- Supports symmetric line rates 192Kbps to 2,312Kbps downstream and upstream
- Embedded Operations Channel (EOC) support

### LAN Interface
- Built-in 8-port 10/100 Base-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 5950 back panel view

# SIEMENS

Global network of innovation