



*Multiple connectivity options catered to your needs*

### Benefits

- World-class network security
- Reliability and resilience
- Seamless integration
- Managed network service
- Flexibility

## The secure IP network

### *Connecting to SWIFTNet's IP-based network layer*

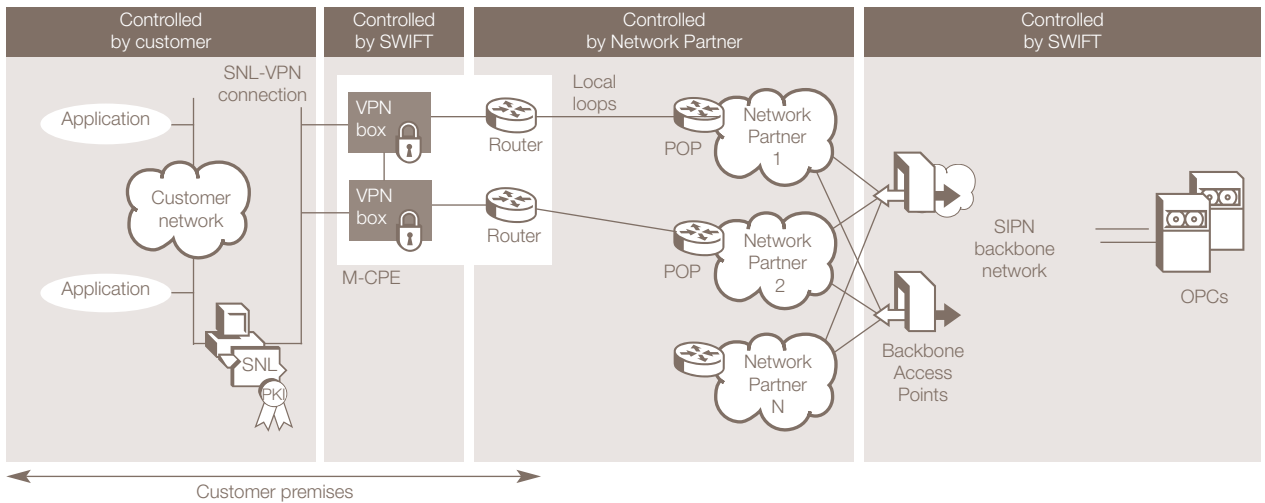
The secure Internet protocol network (SIPN) is SWIFT's secure, resilient and global private network, providing the robust transport services over SWIFTNet that are required by our users.

All of SWIFT's customers, from large global banks to a small, specialist financial institutions, look to SWIFT for global and seamless network connectivity. SIPN caters to you all by supporting a broad array of access options, from dedicated high-speed access by Managed Customer Premises Equipment (M-CPE) to dialup access for low-volume users.

### Benefits

- World-class network security  
We are committed to maintaining our clear leadership in providing you with the most secure financial communication services in the world. SIPN harnesses state-of-the-art security mechanisms and algorithms, including IPSec and VPN technology, to guarantee exactly that.
- Reliability and resilience  
Our customers rely on the SWIFT network for mission-critical processes. As a result, SIPN has been designed from the ground up to offer the very highest levels of reliability and resilience available. This includes automatic and transparent fallback to a backup connection when required, without affecting your business applications.

- Seamless integration with your network infrastructure  
SIPN provides for seamless integration into your existing network environment. It implements Network Address Translation and offers the possibility of installing security features such as firewalls and Demilitarised Zones (DMZs).
- Managed network service  
SWIFT offers the option of a fully-managed connection service. By managing and monitoring the network end points as well as SIPN itself, SWIFT guarantees full end-to-end security and resilience.
- Flexibility: partnership with well-established network providers  
In an effort to offer our customers maximum choice and flexibility, we have carefully selected a number of Network Partners for you to use to connect to SWIFT. This choice also gives you the opportunity to avoid dependency on a single supplier for your network connectivity.



Multi-vendor secure IP network

**Multi-vendor secure IP network**

SWIFT has adopted a multi-vendor model for SIPN. This model uses state-of-the-art security and offers high resilience and capacity while avoiding dependency on a single supplier. In addition, a multi-vendor environment allows customers to leverage existing relationships by creating competition among Network Partners. You will be able to connect using one or more Network Partners, who will provide and install one or more M-CPEs and local loops at your premises. These connections are routed by the Network Partners over their IP networks to the Backbone Access Points, which are under full control and ownership of SWIFT.

These Backbone Access Points are interconnected through the fully-resilient SIPN backbone network owned by SWIFT. The Backbone Access Points also serve as secure tunnel aggregators for customer connections.

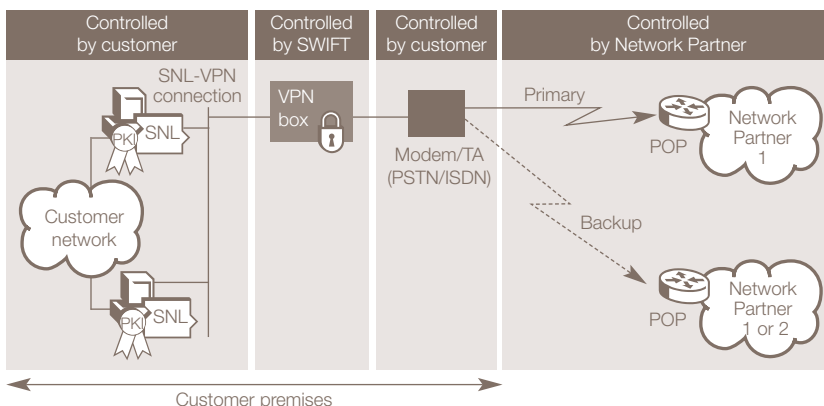
These tunnels guarantee a fully transparent and secure SWIFT-controlled data path through the IP-VPN networks.

To achieve this, a VPN box will be installed at your site to establish a secure end-to-end tunnel between your site and the Backbone Access Point. The customer connection options (connectivity packs) contain sufficient flexibility to address resiliency and capacity requirements. AT&T, Colt, Orange Business Services and BT Infonet are our Network Partners. More information can be found in the Partners section of [www.swift.com](http://www.swift.com).

**Connectivity options**

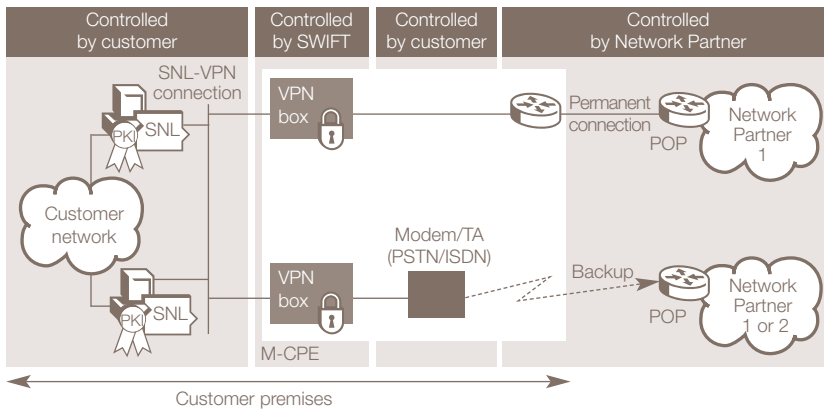
SWIFTNet connectivity options fall into two main groups:

- Dialup connections  
The connection is established via a VPN box and a dial modem or terminal adapter. Spare equipment and dialup to an alternative SIPN POP can provide backup when required.
- Permanent connections  
You can choose to have dialup as your backup connection (Dual-I or Dual-I ISP local loop), or you can have backup via a leased line (Dual-P M-CPE). Another possibility is to opt for a multiline configuration, which consists of two (or more) independent leased lines and uses mechanisms at the level of SWIFTNet Link and/or Alliance Gateway to handle all resilience aspects.



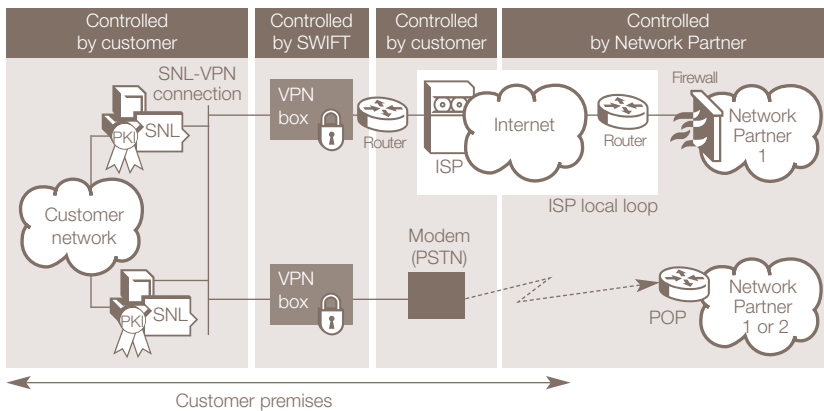
**Dialup**

For low-volume users, SWIFT provides a simple dialup option. Access to SIPN is provided through a PSTN or ISDN line. The dialup equipment, including the VPN box, is ordered and purchased directly by the customer. The VPN box (connected to an external dial modem or terminal adapter) will be configured by SWIFT with the required prime and backup telephone numbers.



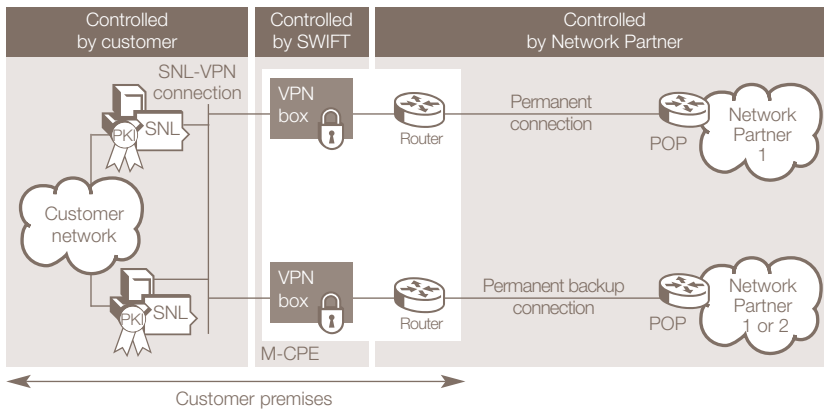
### Dual-I

The SIPN access is implemented through a single router and a pair of VPN boxes in an active/standby configuration. The VPN boxes are colocated and interconnected via a dedicated Ethernet segment. This configuration protects against a failure of the Network Partner's router, leased line and POP, and against a failure of the prime VPN box. Switchover and switchback (after repair) are automatic, and the dial connection will remain up in the meantime. The fallback configuration may, however, be of lower speed than your primary leased line.



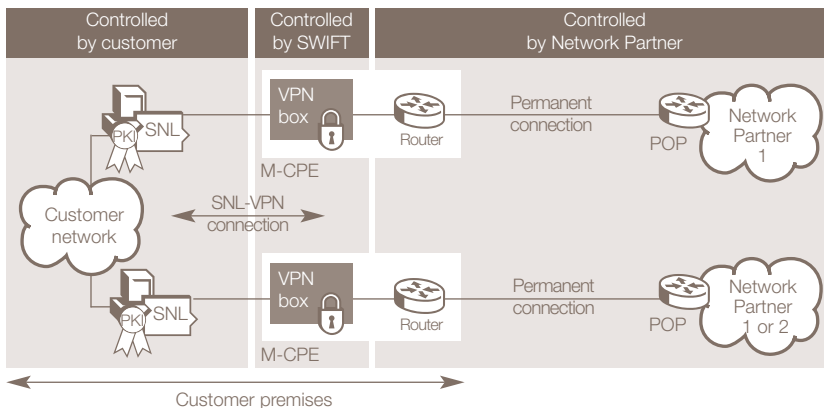
### Dual-IP ISP local loop

This option of the Dual-I configuration has the same functionality as the normal Dual-I. In this access configuration, a SWIFT Network Partner is able to use a local Internet Service Provider (ISP) for connectivity between the nearest access point and the SWIFT customer's site. The Dual-I ISP local loop is not available in all countries. Please contact your SWIFT account manager for more information. A specific ISP local loop factsheet is also available.



### Dual-P

The SIPN access is implemented through a pair of VPN boxes and routers in an active/standby configuration. You have a choice between having both your lines provided by the same Network Partner or spreading them between two Network Partners for increased resilience. In both cases the VPN boxes are colocated and interconnected via a dedicated Ethernet segment. This configuration protects against a failure of the VPN box, the router, the leased line and the POP. Switchover and switchback (after repair) are automatic. The fallback configuration has the same quality as the primary one.



### Multiline

A multiline configuration uses M-CPEs that are not able to recover from network failures. They consist of a unique VPN box connected to SWIFT via a unique leased line. If a connection fails (the VPN box or the line), the SWIFTNet Link using it becomes unable to communicate with SWIFT and another SWIFTNet Link connected to another MCPE must be used. This switchover could be manual or automated, depending on customer configurations.

		Pack 1	Pack 2	Pack 3	Pack 4	Pack 5	
		Dialup interface	Small LAN interface	Medium-size interface	Mission-critical interface	Very large hub, central server	
SNL	Throughput	< 1 TPS		Up to 1 TPS	Up to 5 TPS	Up to 40 TPS	> 40 TPS
	Platform	NT, Win2000		NT, Win2000 AIX, Solaris	NT, Win2000, AIX, Solaris	NT, Win2000, AIX, Solaris	AIX, Solaris
	Backup	Cold backup	Cold backup or Active/standby	Cold backup	Cold backup or Active/standby	Active/standby or Active/active	Active/standby or Active/active
SIPN	SIPN access	Dialup or Dual-I ISP local loop		Dual-I or Dual-I ISP local loop or Dual-P or multiline	Dual-I or Dual-P or multiline	Dual-P or multiline	Dual-P or multiline
	Bandwidth	£ 64 Kbps		64 Kbps	128-256 Kbps	512 Kbps or E1/T1	E1/T1 or above

Overview of connectivity packs

### Connectivity packs

In order to ensure well-balanced systems and to simplify the ordering process, we have defined five connectivity packs that combine the software, throughput and resilience factors into a set of common configurations.

The table above gives a summary of the range of software, platform, backup and line bandwidth options that are required to achieve a configuration capable of supporting a given throughput (expressed in Transactions Per Second or TPS).

### Resilience

For many companies it has become imperative to provide complete redundancy with a requirement for disaster recovery sites, often located in a different building, city or even country.

SWIFT offers you the opportunity to add site resilience by providing additional connectivity pack features and designing switchover procedures to bring the second site online in the event of a failure of the primary site.

*For more information, please contact your SWIFT account manager or visit [www.swift.com](http://www.swift.com)*