

SIEMENS



Remote networks

Easy remote access to machines and plants

Industrial Remote Communication

Brochure

Edition
05/2015

siemens.com/remote-networks

Many ways of connecting to remote networks

Increasing bandwidths, higher speeds and performance levels, as well as falling communication costs are all opening up new possibilities in both public and industrial environments.

It's now easier than ever to connect your widely distributed plants, remote machines or mobile applications via remote networks. Siemens offers a wide range of modems and routers for establishing the ideal connection to remote networks over dedicated lines, public switched or cellular telephone networks, or Internet – regardless of whether wired or wireless, IP-based or analog.

The IP-based network components of SCALANCE M and SCALANCE S can be used widely in the fields of telecontrol, teleservice and any other application for industrial remote communication. These devices protect remote networks and the communication between them against unauthorized access and data espionage by means of integrated security functions like Firewall and VPN encryption.

In addition, SINEMA Remote Connect, a management platform, facilitates secure and straightforward administration of communication connections.

The remote networks portfolio for IP-based networks is suitable for use in many different industries, such as:

- Water/wastewater treatment plants
- Oil and gas supply
- District heating networks
- Power distribution
- Pumping stations
- Transportation systems
- Plant and machine building

In the field of wind energy and photovoltaic plants, this portfolio also enables a global network to be set up for condition monitoring.

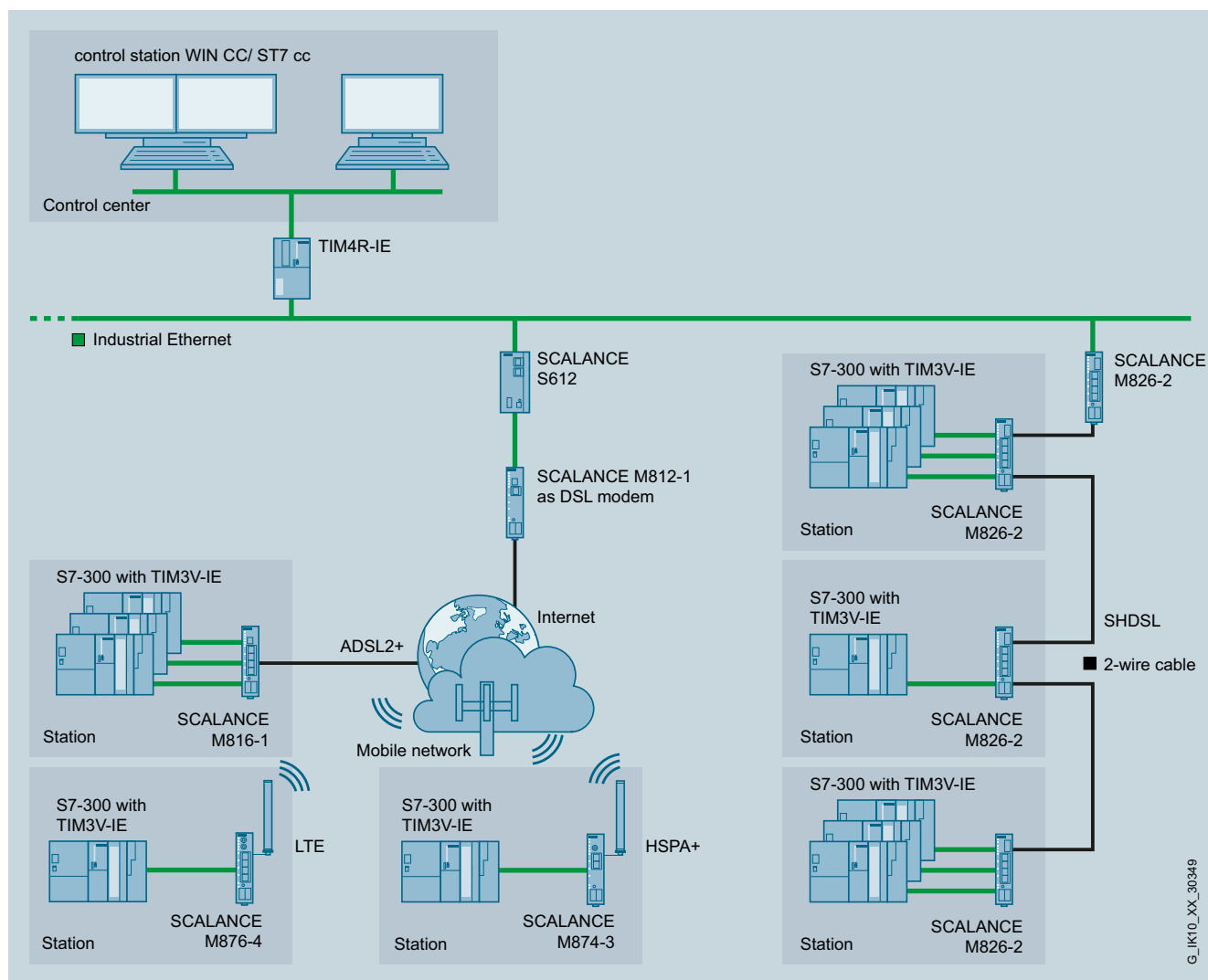
Siemens also offers modems for dedicated line and dialup networks, for the connection of analog remote networks. For more information, visit:

siemens.com/remote-networks



Your benefits with the Siemens remote networks portfolio:

- Low investment and operating costs for operator control and monitoring of remotely connected substations
- Reduction in travel and personnel costs thanks to remote programming and diagnostics
- IP-based and analog routers for any application
- Higher standard of data communication security thanks to integrated encryption and access protection mechanisms
- Commissioning and diagnostics via user-friendly web interface
- Easy and secure administration of virtual private network (VPN) connections
- Greater clarity in the control cabinet thanks to space-saving SIMATIC module design
- Integrated into TIA (Totally Integrated Automation)
- 5 years warranty for all SCALANCE products*



Application example - telecontrol: Various options for connecting substations

*) applies to all SCALANCE products with delivery date since January 1st, 2015

SCALANCE M



The SCALANCE M portfolio consists of industrial modems and routers for wireless or wired access, depending on the application requirements. The products facilitate efficient connection of stationary and mobile stations to a control center. Extensive security functions, such as firewalls and VPN encryption, offer protection during transmission of data.

Wired routers

Wired SCALANCE M routers support the cost-effective and secure connection of Ethernet-based subnets and automation devices via existing cable infrastructures. This portfolio includes devices for connection to two-wire cables or wired telephone and DSL networks.

Your benefits:

- Simple connection of local networks using IP communication via WAN
- Low transmission costs, thanks to economical high-volume tariffs
- High process availability due to redundant transmission paths






			
	SCALANCE M812-1	SCALANCE M816-1	SCALANCE M826-2
Article No.	6GK5 812-1AA00-2AA2	6GK5 816-1AA00-2AA2	6GK5 826-2AB00-2AB2
Standard	ADSL2+	ADSL2+	SHDSL
Frequency bands	Public networks	Public networks	Private (existing infrastructure)
Bandwidth	Downlink: 25 Mbit/s; Uplink: 1.4 Mbit/s	Downlink: 25 Mbit/s; Uplink: 1.4 Mbit/s	Up to 15.3 Mbit/s
DI/DO	1/1	1/1	1/1
DSL connection system	1 x ADSL2+ (RJ45)	1 x ADSL2+ (RJ45)	2 x SHDSL (terminal block)
LAN interfaces	1 x RJ45	4 x RJ45	4 x RJ45
Temperature range	0°C ... +60°C	0°C ... +60°C	-40°C ... +70°C
Safety class	IP20	IP20	IP20
Security	VPN (IPsec)/ NAT/ Firewall	VPN (IPsec)/ NAT/ Firewall	VPN (IPsec)/ NAT/ Firewall
Special characteristics	Redundant power supply; Network management via SNMP	Redundant power supply; Network management via SNMP	Redundant power supply; Network management via SNMP
Advantages			
	<ul style="list-style-type: none"> ■ Cost-effective connection to DSL provider networks thanks to ADSL2+ support ■ Flexible use as router or modem without need for configuration 	<ul style="list-style-type: none"> ■ Cost-effective connection to DSL provider networks thanks to ADSL2+ support ■ Secure direct connection of multiple stations via integrated 4-port switch 	<ul style="list-style-type: none"> ■ Connection to existing two-wire infrastructure thanks to SHDSL support ■ Wide range of possible network topologies – e.g. point-to-point, line, link aggregation (4-wire) ■ Low investment and operating costs for operator control and monitoring of remotely connected substations

Wireless routers

The wireless SCALANCE M routers use the globally available, public cellular telephone networks (2G, 3G, 4G) for data transmission. This makes them a cost-effective alternative to the set-up of corporate wireless networks. The wireless routers are used whenever there are no other transmission mediums, such as dedicated line or public telephone network, available.

Your benefits:

- High data rates allow the transmission of mass data or images in real time
- Provider independent
- Connection of extremely remote substations is possible

					
	M876-4 for LTE	M876-3 for UMTS (EV-DO & CDMA2000)	M875 for UMTS	M874-3 for UMTS	M874-2 for GSM
Article No.	6GK5876-4AA00-2BA2	6GK5876-3AA02-2BA2	6GK5875-0AA10-1AA2	6GK5874-3AA00-2AA2	6GK5874-2AA00-2AA2
Standard	4G	3G	3G	3G	2 – 2.5G
Frequency bands	GSM 900/1800 MHz UMTS 900/1800/ 2100 MHz LTE 800/900/1800/ 2100/2600 MHz	GSM 850/900/1800/ 1900 MHz; UMTS 800/850/900/ 1900/ 2100 MHz; EV-DO: 800/1900 MHz	GSM 850/900/1800/1900 MHz UMTS 800/850/1700/1900/2100 MHz		GSM 850/900/1800/ 1900 MHz
Bandwidth	Downlink: up to 100 Mbit/s (LTE) Uplink: up to 50 Mbit/s (LTE)	Downlink: 14.4 Mbit/s (HSDPA); Uplink: 5.76 Mbit/s (HSUPA); Forward Link: 3.1 Mbit/s; Reverse Link: 1.8 Mbit/s	Downlink: 14.4 Mbit/s (HSDPA); Uplink: 5.76 Mbit/s (HSUPA)		Downlink: 237 kbit/s; Uplink: 118 kbit/s
DI/DO	1/1	1/1	0/0	1/1	1/1
Antenna connectors	2x SMA	2x SMA	2x SMA (Rx Diversity)	1x SMA	1x SMA
LAN interfaces	4x RJ45	4x RJ45	2x RJ45	2x RJ45	2x RJ45
Temperature range	-20 °C ... +60 °C	-20 °C ... +60 °C	-40 °C ... +75 °C	-20 °C ... +60 °C	-20 °C ... +60 °C
Safety class	IP20	IP20	IP20	IP20	IP20
Security	VPN (IPsec/OpenVPN)/ NAT/ Firewall	VPN (IPsec)/ NAT/ Firewall	VPN (IPsec)/ NAT/ Firewall	VPN (IPsec)/ NAT/ Firewall	VPN (IPsec)/ NAT/ Firewall
Special characteristics	Redundant power supply; network management via SNMP; text message alerts; managed 4-port switch		KBA/ EN50155 With railway approval	Redundant power supply; Network management via SNMP	
Advantages					
	High security standards by means of a firewalls (stateful packet inspection) and VPN connections (IPsec) as an integral component of the Industrial Security concept				

SCALANCE S

SCALANCE S components ensure secure access to globally distributed systems, machines and applications. They protect automation cells, and any devices that do not have their own protective functions, from unauthorized access such as espionage and manipulation. Data transmission is encrypted by means of VPN, and the communicating parties are authenticated.

Firewall rules permit not only device-specific, but also user-specific access control. The user only has to log in to the SCALANCE S device which activates a user-specific ruleset.

					
	SCALANCE S602	SCALANCE S612	SCALANCE S615	SCALANCE S623	SCALANCE S627-2M
Article No.	6GK5602-0BA10-2AA3	6GK5612-0BA10-2AA3	6GK5615-0AA00-2AA2	6GK5623-0BA10-2AA3	6GK5627-2BA10-2AA3
Bandwidth	10/100/1000 Mbit/s	10/100/1000 Mbit/s	10/100 Mbit/s	10/100/1000 Mbit/s	10/100/1000 Mbit/s
DI/DO	1/1	1/1	0/0	1/1	1/1
LAN interfaces	2x RJ45	2x RJ45	4+1 RJ45	3x RJ45	3x RJ45 + 2x 2 media module ports
Temperature range	-40 °C ... +60 °C	-40 °C ... +60 °C	-40 °C ... +60 °C	-40 °C ... +60 °C	-40 °C ... +60 °C
Safety class	IP20	IP20	IP20	IP20	IP20
Number of VPN tunnels	0	128	20	128	128
Type of VPN tunnel	-	IPsec	IPsec / OpenVPN Client	IPsec	IPsec
Special characteristics			Security zones configurable via VLAN	DMZ port	DMZ port Router+FW redundancy, ring-redundancy: MRP, HRP

SINEMA Remote Connect – the management platform for remote networks

The new management platform for remote networks – SINEMA Remote Connect – is a server application. Using SINEMA Remote Connect, users can easily and securely maintain widely distributed plants or machines by remote access. SINEMA Remote Connect ensures the secure administration of VPN connections between the control centers, the service engineers and the installed plants. Direct access to the corporate network, in which the plant or machine is integrated, is initially avoided. The service engineer and the machine to be maintained each establish an independent connection to SINEMA Remote Connect. The identity of the partners is verified by an exchange of certificates, before any access to the machine is granted. The connection to SINEMA Remote Connect can be set up over diverse media such as cellular phone networks, DSL or existing private network infrastructures.

Your benefits with SINEMA Remote Connect:

- Central administration of all VPN connections
- Simple management of different users
- Telephone book function with SINEMA RC Client for fast and easy connection to SINEMA Remote Connect
- Protocol independent, IP-based communication
- Easy integration of the Siemens routers by auto-configuration
- Special IT knowledge regarding remote access is not necessary
- Easy selection and connection to identical serial machines for original equipment manufacturers (OEM)
- Wide range of remote networks applications, from remote service to remote control

The image displays two overlapping windows from the SINEMA Remote Connect system. The background window is the 'Users and Roles' management interface, and the foreground window is the 'SINEMA RC Client' application.

SINEMA Remote Connect - Users and Roles Interface:

- Header:** SIEMENS SINEMA Remote Connect
- Navigation:** Logged in as 'serviceuser', Log out, System, Remote Connect, User Accounts, Users & Roles, Security, My Account.
- Section:** Users and Roles
- Sub-sections:** Users, Roles
- Search:** Search Filter: All, Exact match, Apply Filter, Show All
- Table:**

Username	First Name	Last Name	Status	Actions
serviceuser	Test	User	Offline	⊞ ⊞ ⊞ ⊞
serviceuser2	Test	Test	Offline	⊞ ⊞ ⊞ ⊞
- Buttons:** Create, Copy, Delete

SINEMA RC Client Interface:

- Header:** SIEMENS SINEMA RC Client
- Navigation:** Settings, English, ?
- Section:** SINEMA Remote Connect Account
- Log off** button
- VPN Status:** CONNECTED
- VPN address:** 10.8.1.4
- Buttons:** Establish VPN tunnel, Terminate VPN tunnel
- Section:** Device list
- Table:**

Name of the device	VPN address	Remote subnet	Virtual local LAN	Status	Location	Actions
S615	10.8.1.2	192.168.1.1	10.10.10.1	online	NbgM	
S615_2	10.8.1.3	192.168.1.1	10.10.10.1	online	NbgM	
- Settings:**
 - ☒ Activate NAT on Client
 - ☒ Using destination NAT settings of the device
 - ☐ Using manual NAT settings
 - NAT configuration** button
 - Showing log files** button
- Exit** button

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit <http://www.siemens.com/industrialsecurity>.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit <http://support.automation.siemens.com>.

Siemens AG
Process Industries and Drives
Process Automation
Postfach 48 48
90026 NÜRNBERG
GERMANY

Subject to change without prior notice
Article No. 6ZB5530-0CB02-0BA0
DR.PN.PA.15.XXBR.95.38 / Dispo 26000
BR 0515 3. GUT 8 En
Printed in Germany
© Siemens AG 2015

The information provided in this brochure contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.
All product designations may be trademarks or product names of Siemens AG or supplier companies whose use by third parties for their own purposes could violate the rights of the owners.