HAGELIN-CRYPTOS
CRYPTO AG

Ethernet Encryption HC-8552 1G Multipoint

Ethernet has emerged as a universal protocol for use in the LAN/MAN/WAN range by governmental agencies and military organisations as well as by service providers and civilian organisations. This end-to-end network technology provides an open platform for application-independent transport of all information between multiple locations. The network can be local, national or international in dimension. To benefit from these advantages despite global network risks, you should install Ethernet Encryption HC-8552 1G Multipoint, a highly secure system from Crypto AG designed to protect your sensitive information.

If you use fast Ethernet connections, they are typically routed in today's network configurations to run over publicly accessible ground where they are not protected against attacks by electronic means. You can resolve this problem with an efficient, easy-to-handle and highly secure unit from Crypto AG called Ethernet Encryption HC-8552 1G Multipoint. This completely transparent high-performance system provides unrestricted encryption without loss of performance (no additional overhead) in full wire speed operation and is a reliable security platform for all your applications featuring Ethernet LAN/MAN/WAN backbones. Used in carrier and service provider networks, it supports multiple scenarios like point-to-point, point-to-multipoint and multipoint-to-multipoint.
The system also enables the use of unicast, multicast and broadcast applications as well as redundancy and load-balancing scenarios for overlying applications. Voice, video and real-time applications are ensured, too, because the system supports class of service (CoS). You are not required to make any network adjustments or do any reconfiguring to install this system in the network. Encryption takes place in a separate tamper-proof security module with symmetric, customer-specific algorithms profiled by your security manager. This prevents attacks, both by cryptographic and mechanical means. The periodic change of the communication keys takes place automatically without interrupting operations. The centralised offline and online security management makes it easy for you to set up and update cryptographic parameters.
Ethernet Encryption HC-8552 1G Multipoint is compatible with the other Ethernet Encryption Multipoint systems from Crypto AG.

Key features

- Powerful 1Gbps Ethernet Encryption
- Wire speed performance at layer 2 for Ethernet Networks, no encryption overhead
- Bump-in-the-wire design for plug-and-play installation
- Protection for point-to-point, point-to-multipoint and multipoint-to-multipoint networks
- Protection for unicast, multicast and broadcast traffic
- Sophisticated Security Architecture
- Highly secure, hardware-based encryption with secret, customer-specific algorithm
- Comprehensive algorithm profiling by customer
- Powerful Security Management Centre

Cryptography & Security

Algorithm

- Customer-specific cipher algorithm HCA-820
- Customer managed profiling of algorithm with variety > 10^{506}
- Mutual key agreement scheme for generation of short-term communication keys
- Each encrypted channel uses independent communication keys
- Built-in high quality true random generator
- Self synchronising cipher mode

Keys

- Customer-defined master communication keys stored in tamper-proof security module
- Master communication keys and communication keys with variety > 10^{38} (128 bit, optionally 256 bit)

Key management

- Manual key input via user interface
- Copy/backup of keys and installation data with Security Data Carriers (SDC)
- Offline with SMC-1100 Broadband and SDC
- Online with SMC-1100 Broadband
- Online inter-unit management

Tamper-proof design

- Identity based access control
- Block function
- Emergency clear
- Tamper evidence
- Tamper detection & response (reset to ex-factory state)
- Metal housing with mechanical lock
- Built-in security module

Services

Services supported

- Ethernet Private Line (EPL)
- Ethernet Virtual Private Line (EVPL)
- Ethernet Private LAN (EPLAN)
- Ethernet Virtual Private LAN (EVPLAN)

Networks supported

- Ethernet over MPLS (EoMPLS)
- Ethernet over SDH/SONET (EoSDH)
- Provider Backbone Transport (PBT)
- Metro Ethernet

Network topologies

- Point-to-point (P2P)
- Point-to-multipoint (P2MP)
- Multipoint-to-multipoint (MP2MP)

Traffic types

- Unicast/multicast/broadcast
- Voice/video/data

Features

User interfaces

- Keypad
- LCD display
- Status LEDs

Payload (home/world) interfaces

- IEEE 802.3z 1Gbps Ethernet
- Optical transceivers SFP, MSA (Multi Source Agreement)
- Optical LC / 1000Base-SX, -LX, -ZX

Management interfaces

- Local management 100Base-T/RJ45
- Remote management 100Base-TX/RJ45
- Alarm relay RJ45
- Diagnostics interface RS-232/RJ45
- Built-in smart card reader

Management

- Security Management Centre (SMC-1100)
- Inband and out-of-band management via IP
- Local management via keypad and display
- Local management via browser based user interface
- Remote management via ciphered browser connection (RAD-1100)
- Remote software update
- Time Server Support (SNTP)
- Network management system (NMS) integration support (SNMPv1/Standard MIB II)

VLAN / Class of Service

- Supports 802.1q VLAN (1 or 2 tags)
- Supports 802.1p CoS (1 or 4 classes)

Bandwidth

- 200Mbps or 1Gbps

Peer units

- 2 or 99

Performance

- Throughput 100% wire speed
- Latency @ 64 Byte Frames ≤ 3µs
- Latency @ 1'518 Byte Frames ≤ 30µs

Maintenance

- Built-in test equipment (BITE)
- Transparent mode

Power supply units & cooling

- Redundant hot pluggable PSU
- AC input, 100…240VAC/50…60Hz
- DC input, 48VDC, ± 25 %
- Power consumption < 100W
- Redundant cooling with 6 fans

Mechanical

- 19" rack mounting/2 units high
- 444 mm × 350 mm × 88 mm W/D/H
- 8.6 kg

Reliability

- MTBF: 100'000 hrs

Environmental data

- Operating temperature: 0 °C…+50 °C
- Storage temperature: -25 °C…+70 °C
- Humidity: 5 %...95 %, non-condensing

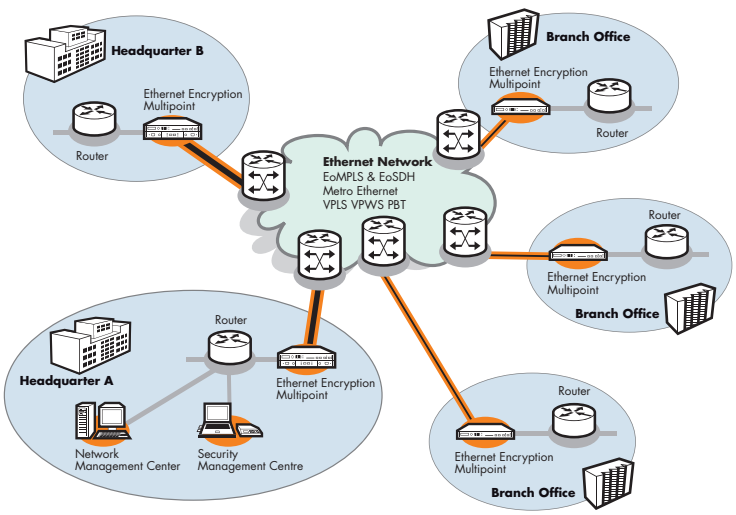
EMC / Safety

- EN 55022 class B/EN 55024
- EN 60950-1/EN 60825-1

Quality system / Conformity

- ISO 9001:2000
- CE (European conformity)

Ethernet Encryption Multipoint



Accessories

- Security Management Centre SMC-1100 Broadband
- Remote Access Device RAD-1100
- Security Data Carriers SDCs
- Optical transceivers SFP for various distances and wavelengths

Crypto AG, P.O. Box 460, CH-6301 Zug, Switzerland, www.crypto.ch