



Communication Devices Inc.

<http://www.commddevices.com>

Port Authority *AES*

Secure In/Out of Band Management Terminal Server
with the Advanced Encryption Standard

- ✓ NIST certified AES & 3DES
- ✓ RSA SecurID Ready
- ✓ FIPS 140-2 level-2 compliant
- ✓ 4 and 8 ports versions available
- ✓ Network interface optional
- ✓ Self-contained Database
- ✓ Centrally Managed
- ✓ Power control up to 8 devices



Port Authority 88 or Port Authority 44

The Problem

Access to console ports on Routers, Firewalls, Network Appliances, etc., cannot be protected by network security when out of band access is required. Secure Out of Band Management and Network security are mutually exclusive events.

The Solution

The Port Authority connects directly to multiple console ports and provides the highest level of protection regardless of the status of the network. This is done by maintaining an internal security database that is updated by a "patented" central database manager on an "as needed" basis. This internal database provides fast, reliable, AES, two factor authentication. Full **NIST certified AES** or 3DES encryption can be enabled by using a UniGuard Client(s) at the NOC center.

RSA Secured

The Port Authority has the ability to authenticate RSA tokens "on board" without needing access to the network. If the network option is installed the device can check for access to the RSA Server prior to authenticating on board.

Network Capability

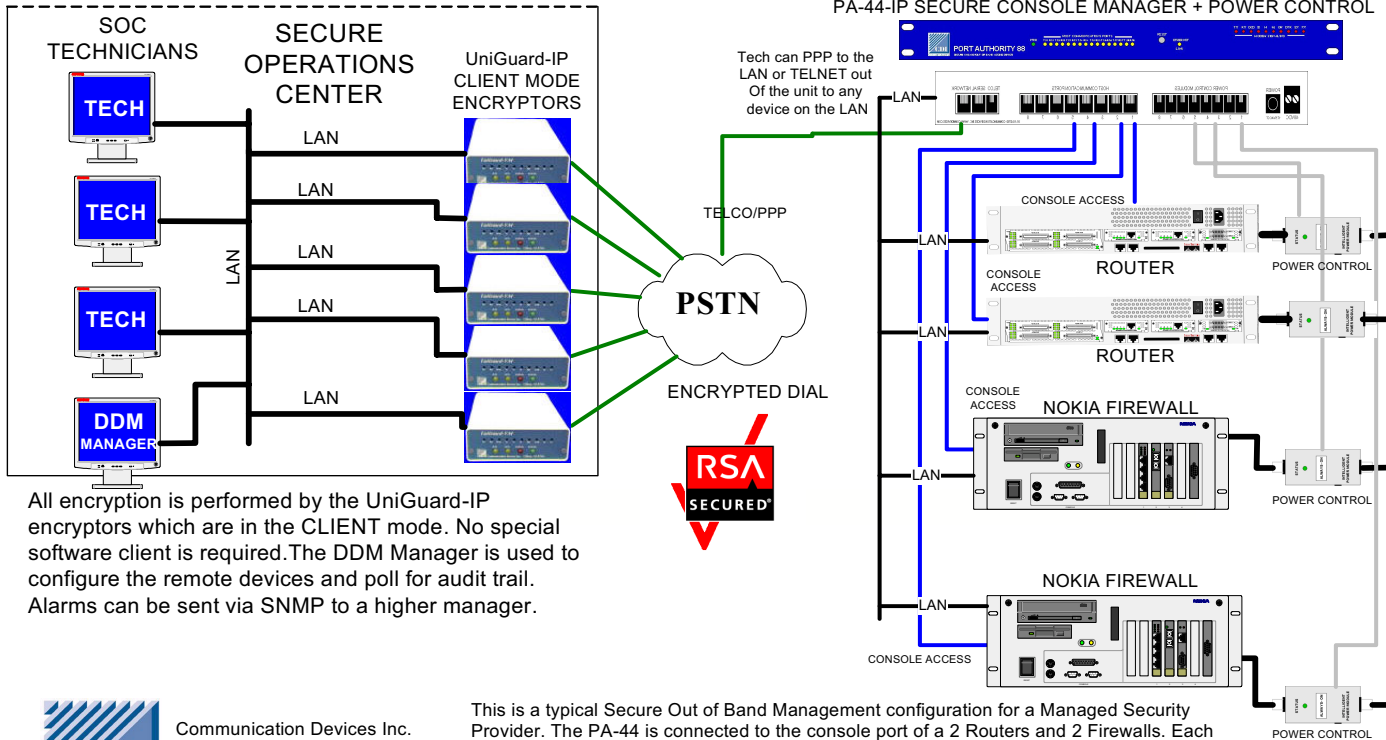
An optional network interface provides in band access to the device supporting **hardware** encrypted network access along with real time monitoring, reporting, etc.. The device will also check the telco line status periodically and report back to the manager.

Security Management

DDM, Distributed Database Manager, can manage an unlimited number of CDI devices remotely from a single(ODBC) or multiple(SQL) workstations. This eliminates the need to update each unit individually when there is a database change. Audit trail reports are extracted automatically.

<http://www.outofbandmanagement.com>

SECURE OUT OF BAND MANAGEMENT WITH POWER CONTROL OVER DIAL-UP WITH REMOTE PPP & TELNET



All encryption is performed by the UniGuard-IP encryptors which are in the CLIENT mode. No special software client is required. The DDM Manager is used to configure the remote devices and poll for audit trail. Alarms can be sent via SNMP to a higher manager.



Communication Devices Inc.
1 Forstmann Court
Clifton, NJ 07011
1.973.772.6997

This is a typical Secure Out of Band Management configuration for a Managed Security Provider. The PA-44 is connected to the console port of a 2 Routers and 2 Firewalls. Each product is also being power controlled by the PA-44 via a power control module on each power cable. In the event of a problem, the SOC technician can 3DES dial-up to the PA-44. This will then allow console access and power control of each device. The tech can also PPP connect to the remote LAN or TELNET out of the unit to a remote device. At no time is the PA-44 relying on network security to operate as the network is in question when the device is used.

Optional Network Capabilities

The Port Authority can have an optional network interface. This will allow in band access for technicians as well as real time reporting and access to the DDM manager. The following protocols are supported.

- Encrypted Telnet
- Remote PPP Access
- SNMP
- Radius, Syslog, Real Time Events
- Real Time Telco Status

Part Numbers

Specifications

PA88-AES	Standard 8 port unit 8 power control	Length	8 inches (20 cm)
PA44-AES	Standard 4 port unit 4 power control		Width
PA88-AES-IP	Standard 88 with network interface	Height	
PA44-AES-IP	Standard 44 with network interface		Weight
PA88-AES-48	Standard 88 with 48VDC interface	Power	
PA44-AES-48	Standard 44 with 48VDC interface		Misc.
PA88-AES-IP-48	PA88 with network and 48VDC	Global	
PA44-AES-IP-48	PA44 with network and 48VDC		Global
PCM-US	Power control module 110VAC	Add -US, -UK, -EU, for international power supplies	
PCM-EU	Power control module 220VAC		