



Communications Devices, Inc

[Products](#) | [Support](#) | [Site Map](#) | [Contact Us](#) | [CDI UK](#)

## Products

Search:



[Download PDF version](#)

### Port Authority 88

8 host ports 8 power reset ports

Secure console port access regardless of the status of the network



[Available in 4 port version!](#)

#### Features:

- Internal V.90 modem
- Optional IP network interface for telnet access
- Access from 1 to 8 Data Ports @115.2KB plus 8 Power Reset Ports
- RSA SecurID ready
- Power boot remote equipment from your desktop securely!
- Self-contained database (unlike RADIUS & TACACS)
- Two (2) Factor Authentication with DES Encryption
- Five (5) types of DES Tokens
- TDES full encryption with UniGuard Client
- Fully managed by the [DDM](#), NT based Manager
- Compatible with CDI [UniGuard](#) and [UniGuard Client](#),
- [Cabling Options](#) for ease of bulk installs

#### The problem with RADIUS and TACACS

Routers installed in the field are all connected to a network. When this network goes “down”, the only way to reach the router is to dial into the console port for remote maintenance. This opens up a “back door” to the network which many network managers lock with RADIUS or TACACS. The problem with these protocols is that they require the network to be functioning in order to contact the security server. This is in direct conflict with the purpose of the console port which is only used when the network is “down”. Therefore RADIUS and TACACS provide inadequate security for router console port protection.

#### The Solution

The Port Authority connects directly to up to eight console ports and provides the highest level of protection regardless of the state of the network. This is done by maintaining an internal security database that is updated by a central database on an “as needed” basis. This internal database provides fast, reliable, two factor authentication every time a technician accesses the router. By using switching to connect one modem to eight routers, The Port Authority saves line and equipment cost continually.

#### User Profiles, Control Access to Specific Firewalls or Routers

Each user profile contains a permission list that limits port access to only those devices associated with that user ID. Some Users can have access to all devices while others may have access to only one or more devices.

**Central Manager Software NT**

[DDM, Distributed Database Manager](#), can maintain an unlimited number of UniGuards and or Port Authority devices remotely from a single workstation. This eliminates the need to update each unit individually when there is a database change. This software program automatically maintains the database of each remote device and is capable of down-loading the entire database of units manually or automatically at preset times. Reports can also be extracted automatically.

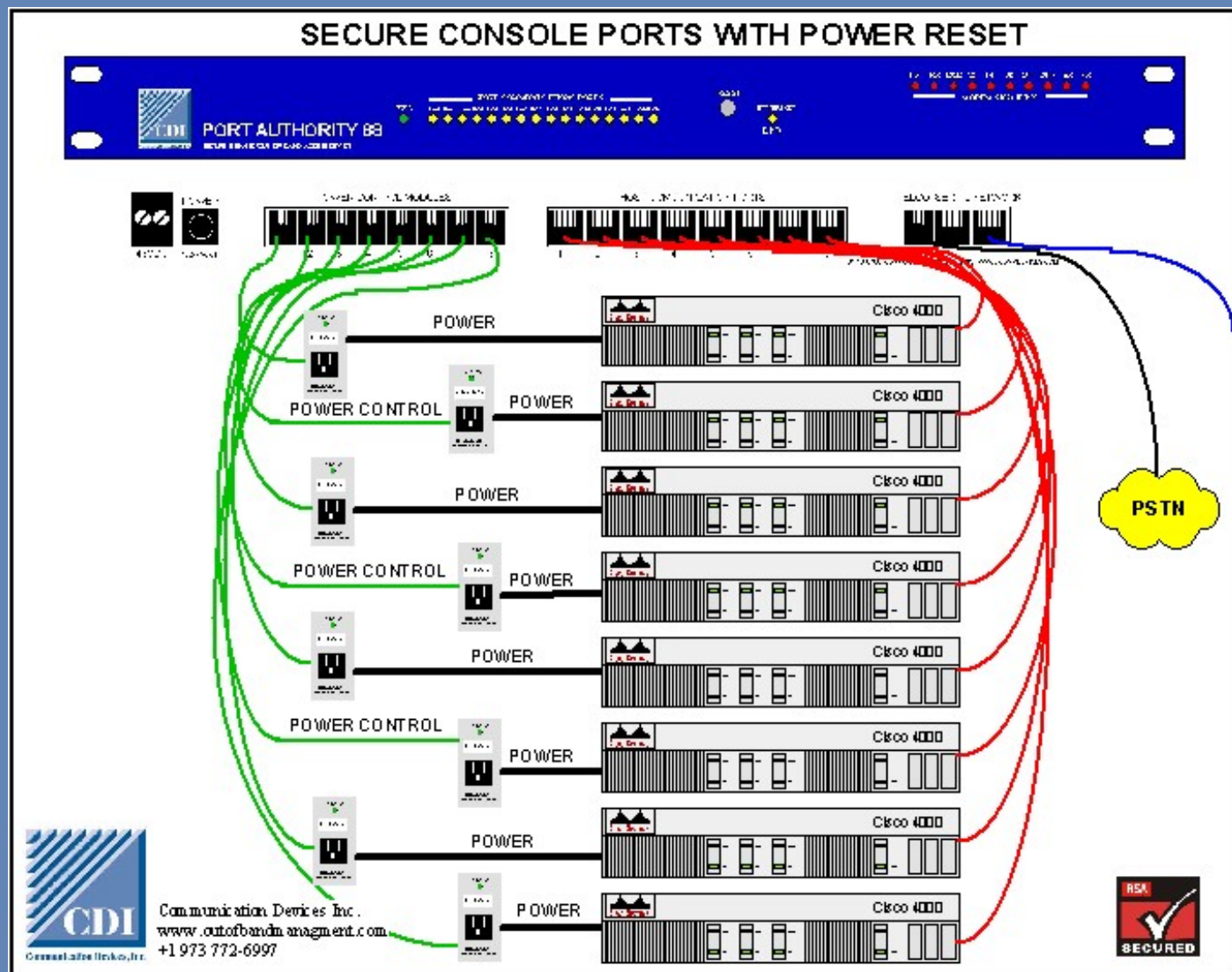
**Port Connections**

The device can be ordered for DTE or DCE [port connections](#) and contains Eight (8) Power Reset Ports.

**Power Reset Ports (8)**

The Power Reset Ports connect to Power Modules and can be used to power cycle a locked up device. Computer equipment that locks up can often only be cleared by disconnecting and reconnecting the power. Power Modules are ordered separately.

[Download this diagram](#)



**The Application**

The above diagram shows a typical sight installation of a Port Authority 88. The sight is accessed by a number of technicians accessing the maintenance port of remote Routers, Servers and other equipment. This is a cluster of 8 devices plus 8 Power Reset Ports, all protected by a single Port Authority. Smaller sights can be protected by Port Authority 44's or UniGuard-V34s. The Security Manager is operating CDI's DDM Distributed Database

Manager software.

### **The Field Technicians**

Access can be via dial-up or direct telnet. The field technicians will be authenticated using the an RSA SecurID card or other token. Full Triple DES encryption can be enabled. They will then gain access to the appropriate Maintenance Port. The Port Authority can selectively allow technicians access to some or all of the connected devices.

### **The Database Administrator**

With a single keystroke, the Administrator can change a database of users for a group of devices and download the new database of users to all devices in that group. All devices or selected groups can be downloaded automatically at preset times. Reports such as an Audit Trail, Status report, Equipment groups with the Users assigned to the various groups and other reports can be extracted manually or automatically using the Distributed Database Manager.

### **Ordering Information**

**PA-88** Port Authority 8-8. Secure remote access switch with built in modem, 8 Host ports plus 8 Power Reset ports. Optional network interface for telnet, Optional power control modules.

**PA-44** Port Authority 4-4. Secure remote access switch with built in modem, 4 Host ports plus 4 Power Reset ports. Optional network interface for telnet, Optional 4 power control modules.

**PCM-US-1** Power control module allows one device to be power reset by a Port Authority, Power Reset Port.

### **[International Approval List](#)**

**Port Authority 84 | [IP Option](#) | [48VDC Option](#) | [Power Control Module Option](#)**

©Copyright 2001, Communications Devices, Inc.

