

# Guardian®

..... A suite of OAM&P Applications

---

## Introduction

Guardian® portfolio of applications is aimed at furthering the roles of both the Nevada and the ACP platforms as Point-of-Sale Network Access Servers by providing extensive back office support systems for Call Detail Records collection, Transaction Monitoring and Reporting and Caller authentication. Guardian® allows Service Providers to provision the Nevada and ACP platforms as a shared point-of-sale access infrastructure.

Administrators of the ACP platform may also leverage Guardian® to effectively exploit the ACP as a protocol mediation and adaptation gateway for transporting legacy protocols and for mapping legacy devices to IP equipment infrastructure.

Guardian® applications may be used to provide one or more of the network services described below for the Nevada Platform.

- **Authentication & Authorization**
- **CDR Collection**
- **CLID Validation**
- **Mnemonics Resolution**
- **Node Status Viewer**
- **POS Transaction Monitor**

Guardian® applications may be used to provide one or more of the network services described below for the ACP Platform.

- **Authentication & Authorization**
- **CDR Collection**
- **Mnemonics Resolution**
- **Node Status Viewer**
- **POS Transaction Monitor**
- **Call Routing Services**

Guardian® is implemented as a suite of Erlang Applications featuring a Web interface for universal access and ease of use. The Erlang/ OTP middleware provides a real time integrated database and allows the deployment of mirrored Guardian® systems for 24x7 mission critical networks. The current GUARDIAN environment is Windows 2000/XP compatible.

## AUTHENTICATION & AUTHORIZATION

This application allows network administrators to centralize the authentication, validation and authorization process for asynchronous devices, telnet Clients, and PPP users to:

- Access network resources via the ACP and Nevada nodes, and
- Access ACP and Nevada management resources.

The application enables the nodes to:

- Authenticate Asynchronous, Telnet, SSH & PPP connections by verifying that the user ID & password provided is valid
- Validate that the user is allowed to access the target network resource through that node
- Authorize access to the nodes' administrative components
- Grant users different levels of access privileges (Read only, Read-Write) when accessing the administrative components.
- Use predefined user's network access attributes to govern the user's session

## CDR COLLECTION

The CDR COLLECTION application collects and stores Call Detail Records generated by both the ACP and Nevada nodes. ACP and Nevada components may be selectively provisioned to generate CDRs that capture both statistical and accounting type information such as duration, destination address and volume of data transacted via the affected node component. The ACP and Nevada management utilities may also be provisioned to generate CDRs that may be used as audit trail records.

Call Details Records are automatically transmitted by the ACP and the Nevada components when enabled. The CDR COLLECTION application may filter the CDRs for the desired information. CDRs may be stored locally in Guardian® or in customer provided MS SQL or Oracle database servers.

## MNEMONIC RESOLUTION

The MNEMONIC RESOLUTION application allows network administrators to centralize the provisioning and the resolution of user's mnemonics used at ACP and Nevada nodes

The ACP & Nevada nodes may use the Guardian® application to parse mnemonics entered by asynchronous and Telnet users. A mnemonic is a character string used in lieu of a standard command string. Mnemonics can be restricted to selected nodes or may be valid on any node.

## CLID VALIDATION

The CLID VALIDATION application allows network administrators to centralize Caller ID screening for ingress ISDN calls terminated by Nevada Dial Access Servers

Nevada may use the Guardian® application to screen incoming ISDN calls for preauthorized E.164 Calling Numbers. If the number provided by the ISDN network is not authorized, Nevada is instructed by Guardian® to reject the call request from the ISDN network ensuring that errant or rogue calls are not consuming valuable Nevada resources and eliminating unwarranted telephone charges. Network administrators can authorize network wide (accepted by all the Nevada nodes) E.164 numbers or restrict E.164 numbers to selected nodes.

## NODE STATUS VIEWER

The NODE STATUS VIEWER application captures the operational status and critical performance attributes of the ACP and Nevada nodes under management.

The application provides performance snapshots of a node's interfaces and internal resources along with daily, weekly, monthly and yearly graphs to assist in performance trend analysis.

## POS TRANSACTION MONITOR

The POINT-OF-SALE TRANSACTION MONITOR application mines the CDRs generated by Nevada nodes, and collected by the CDR COLLECTION application, to compute and display, in near real time, operational performance information about point-of-sale transactions.

The application also enables Service Operators who exploit Nevada systems as a shared infrastructure to provide a secure web access for their customers to monitor the operational performance of their "virtual POS network".

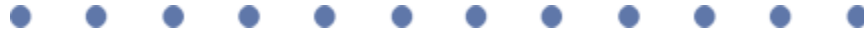
The application also provides a **WIKI** subsystem that may be exploited by Service providers and their customers to share operational information and a **PDF Report Generator**.

## CALL ROUTING SERVICES

The SERVICE ROUTER application may be exploited by ACP nodes to optimize the provisioning and the management of routing and access tables throughout the network.

The SERVICE ROUTER provides the ACP nodes with several types of Call Control Services:

- A central point for network routes selection
- Address translation and address mapping for routing X.25 traffic over IP networks using XOT, NSOCK or LOUDP encapsulation
- Address translation and address mapping for routing IP traffic over X.25 networks using RFC 1356
- Address translation and address mapping to allow interoperability of Telnet clients, IP Hosts, X.25 Hosts, Asynchronous hosts and Telnet Hosts over both X.25 and IP network infrastructure
- Provides Closed User Group (CUG) validation and remapping over both X.25 and IP network infrastructures.



NetKit Solutions is a provider of network products for applications spanning the Transaction and Operations Support System markets. Over 70,000 ACP nodes have been deployed worldwide by telecommunication Service Providers and Enterprises to interconnect remote locations and Central Offices, to improve resiliency and to resolve challenging protocol mediation problems.

NetKit Solutions, LLC  
1125-A Business Center Circle  
Thousand Oaks, CA 91320  
USA  
Tel: +1 805.214.0980  
Fax: +1 805.214.0970

NetKit Solutions UK Ltd  
8 Basepoint Enterprise Centre  
Stroudley Road, Basingstoke  
HANTS, RG24 8UP  
United Kingdom  
Tel: +44 (0) 1256 300080  
Fax: +44 (0) 1256 300087

[www.netkitsolutions.com](http://www.netkitsolutions.com)



Form Number PB GUA-01D, 04/2007