

# NETKIT WORKS®

..... An Operations Support System Solution

NetKitWorks® benefits organizations that exploit disparate and distributed Control Systems in critical infrastructures. NetKitWorks® value proposition is to enable network operations centers to secure their equipment, to lower their operating costs, to automate management tasks, to improve the quality of service and to better leverage assets and human resources that oversee their communication and data acquisition systems.

NetKitWorks owners can secure the management access to a wide range of Network Elements found in financial and medical POS (Point-of-Service) networks, SCADA (Supervisory Control/Data Acquisition), Telephony, Transmission and Distribution, etc. NetKitWorks allows overseers of such infrastructures to considerably minimize the time consuming tasks of accessing heterogeneous equipment and of problem isolation, discovery and analysis. Meantime-to-restore failed equipment is significantly reduced, helping maximize equipment uptime and allowing organizations to exceed their QoS commitments.

## What is NetKitWorks?

An innovative and scalable Security and Service Management tool that extends the intelligence and connectivity of the OSS activation layer. NetKitWorks leverages the serial or Ethernet console port built into most Network Elements to provide Field Service and Engineering personnel with a non-blocking, secure, workgroup environment for managing, activating and troubleshooting multi-vendor equipment.

## Key Innovations

NetKitWorks® boasts several technical and process innovations. It blends role-location based *access control* with the ability of users to *simultaneously access* the administrative console of any Network Element. Authorized users see what their peers see, and subject to access privileges can exchange write access to effect changes to managed equipment. Process improvements stem from its inherent design that relieves users and administrators from the burden of tracking *network addresses* and *prerequisite protocol & sign-on* information for each piece of equipment, while providing an easy to administer *multi-layered* security mechanism. An integrated *wiki* complements the collaborative aspects of NetKitWorks® by allowing users to organize, publish and share operational information.

NetKitWorks® complements in-band SNMP management systems, by enabling a new out-of-band connectivity paradigm and an operational environment conducive to collaboration and cross-training. The benefits are unhindered accessibility and radically improved monitoring, troubleshooting and resolution of problems.

# NetKitWorks® System Architecture

**NetKitWorks®** architecture is based on the interworking of the following systems that may be deployed as a management overlay to any existing equipment infrastructure.

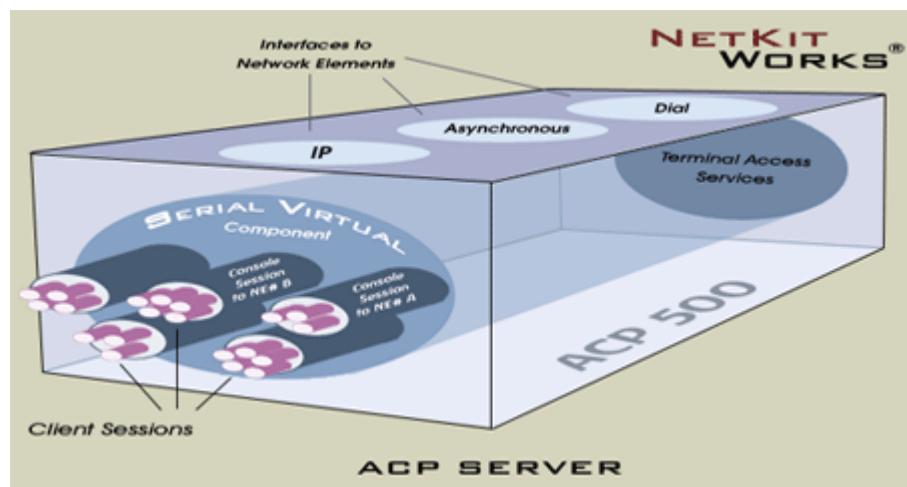
## The Portal

**The Portal** is a suite of Windows 2000/XP Server based applications that provide configuration services, authentication, authorization, routing, access and provisioning services for all the elements of a NetKitWorks® system. The Portal features two-tiered Web system for universal access and ease-of-use by administrators and users alike.

- The **Manager Portal** for supervisory & security personnel.
- The **Client Portal** for users to register and access managed **Network Elements**.

## The Server

**The Server** is based on NetKit Solutions' 500 series **Access Communication Platform**. Hundreds of Servers may be supported by the Portal, each equipped with Asynchronous and Ethernet secure ports to attach co-located managed Network Elements. High speed WAN ports, integrated dial-up modems and Ethernet Interfaces extend the reach of a Server to remote **Network Elements** via WAN or VPN infrastructures and via existing third party terminal servers. When enabled for NetKitWorks, the ACP provides routing, protocol-device mediation, serial virtual tunnels for users collaboration and a soft switchboard allowing 1-to-1 or n-to-1 secure connections between NetKitWorks® Clients and the **Network Elements**.



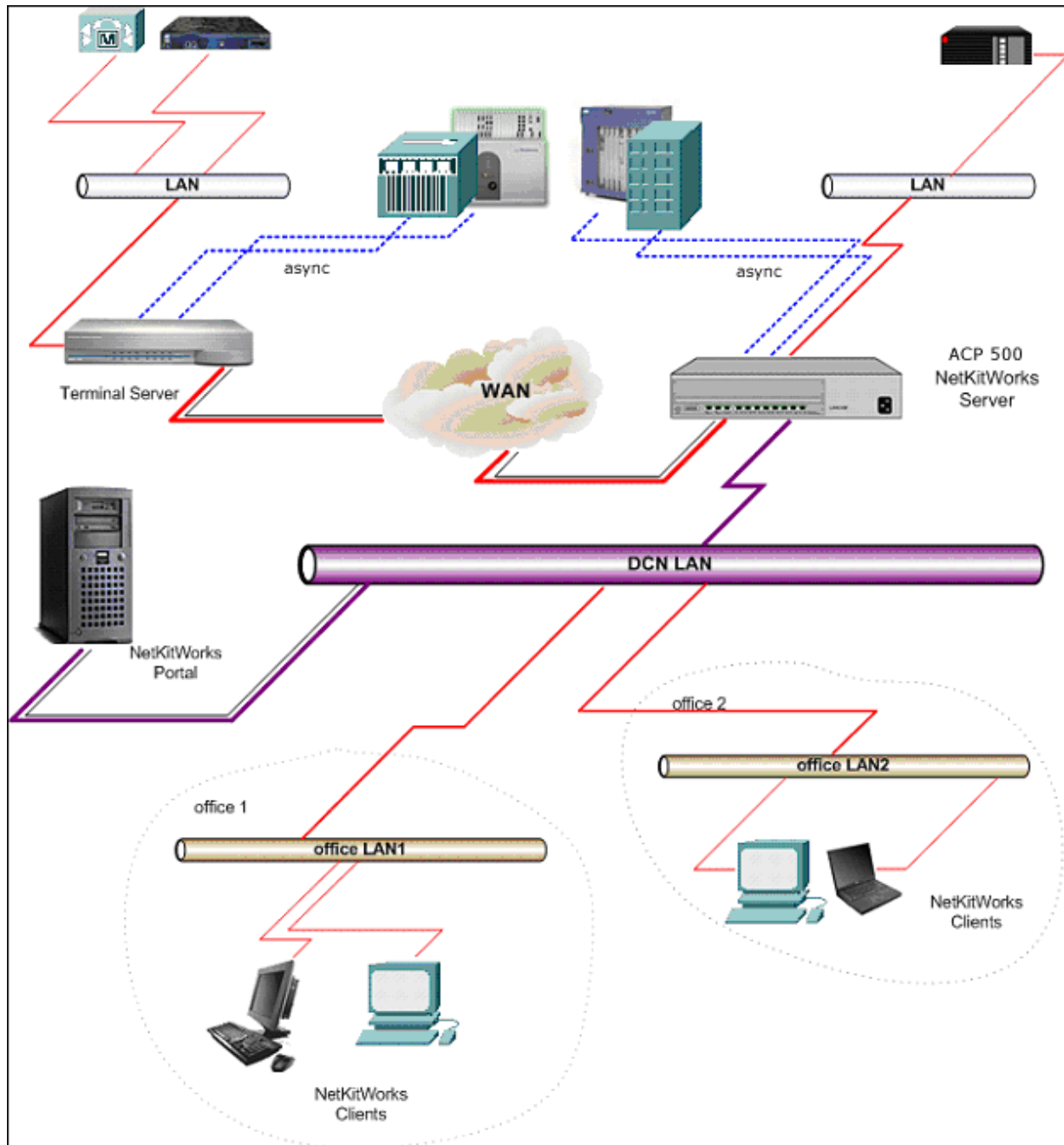
## The Client

**The Client** integrates a TTY/VT100/Telnet terminal emulator, a data recorder, a messenger module and a Tcl/Tk scripting engine into a PC application that is downloaded and kept synchronized from the Portal. Users launch the Client application whenever they need to carry out a management session with a **Network Element**.

The Client runs on NT/W2000/XP & W7 workstations and uses a secure communication protocol with both the **Portal** and the **Servers**.

## NetKitWorks® Topology

The diagram below depicts a setup where the **Server** is used by **Clients** to access remote and local **Network Elements**. To extend the reach of the ACP, a traditional terminal server, wired to the remote NEs, is networked with the ACP via a Wide Area Network, while local NEs are simply wired to the asynchronous and Ethernet interfaces of the ACP.



# NetKitWorks® Portal

The Portal features a two-tiered Web system. The **Client Portal** allows users to self-register, to download the Client application and to conduct management sessions with authorized **Network Elements**. It also allows users to communicate electronically and collaborate when managing NEs. The **Manager Portal** enables administrators and security personnel to provision network addresses, access tokens and access rights that regulate the operation and the connectivity of Clients, Servers and **Network Elements**.

## Features

- **Self Registration**

Users may use their Internet Explorer to self-register anytime and anywhere. The Portal may be set up to grant immediate access rights to newly registered users or may require them to be activated and pre-vetted prior to using the network.

- **Centralized Provisioning**

Users' access privileges and security tokens for accessing Network Elements are provisioned at the Portal. The Portal maintains and automatically synchronizes the information across Servers and Clients.

- **Authentication & Authorization**

Users and their workstations may be vetted by the Portal to control who and from where they may access selected **Network Elements**. Following authentication, the Portal displays the name of NEs that the user may access along with the pertinent access privileges.

- **Access Privileges**

The Portal supports different access privileges for each **Network Element**, which may be tailored to reflect the user's level of expertise or role within the organization. In addition to read-write and read-only privileges, access may be further tailored by restricting the user to a predefined set of function keys pre-configured to issue commands or to perform elaborate control functions by launching scripts.

- **Gatekeeper**

To secure **Network Elements**, to optimize network usage and expedite connection setup, users are not cognizant of the network topology, network addresses, logon tokens and procedures required to access a Network Element. Upon selecting a target NE from the authorized list computed by the Portal, users are automatically routed to the Server that regulates the path to the target NE. Once connected, the Client transactions are governed by the credentials provisioned at the Portal.

- **Chat**

Users may exchange non-intrusive messages while collaborating. For each Network Element, the Portal maintains a log of all messages exchanged by current and previous users allowing users to leave notes to each other and to review notes exchanged by their peers.

- **Wiki Bulletin Board**

The Portal features a 'Wiki' type Web site subsystem where users can post, revise, update and append information. No elaborate programming skills are needed. Users can simply click an 'edit' button to add comments or make changes to what may be likened to a giant bulletin board.

# NetKitWorks® Server

The NetKitWorks® **Server** leverages the ACP protocols, terminal adaptation and mediation services and the array of WAN & LAN physical interfaces. Every Server is typically wired via its serial and Ethernet interfaces to the management port of co-located **Network Elements** or may utilize a Telnet connection to establish a shared 'Console Session' to a remote **Network Element**. The **Server** may establish up to **128** console sessions with remote and local NEs.

## Features

- **Auto-Logon**

The **Servers** automatically establish management sessions with target Network Elements using logon scripts and security access tokens downloaded by the Portal. This relieves the administrator from manually configuring each Server while safeguarding sensitive information at a central site. Auto-logon alleviates the need for users to be cognizant about logon procedures and access details that vary by type of Network Element.

- **Permanent Standby Sessions**

The **Servers** automatically establish and maintain permanent console sessions with their assigned Network Elements. This allows users to gain instant access and to collaborate from anywhere and at any time, and allows the Server to continuously monitor and log equipment events.

- **Time stamping**

The **Server** time-stamps all ingress & egress traffic from NEs prior to forwarding it to the **Clients** and or to the **Portal** for archival. This allows one or more users to analyze current and past management events using a common timeline that is not affected by the location, speed and throughput of a user connection.

- **Workgroup Management**

The **Servers** regulate the number of concurrent users per Network Element and reconcile their read and write access privileges to ensure non-blocking and orderly management sessions. The Server also allows participants to view the identity of their peers, displaying their access control status and time of connection.

- **Secure Interfaces**

The **Server** monitors and reports all physical and logical disconnections of managed equipment. It may also be provisioned to block further use of its interfaces following such interruptions to safeguard against external taps.

- **Tcl/Tk Scripts & SNMP alarms**

Recovery from network isolation, commonly experienced by faulty Network Elements is greatly enhanced by the Server ability to monitor and process the console events of Network Elements. **Server**-based scripts look for predefined data patterns and are able to trigger local actions or SNMP TRAPS helping identify looming problems and expedite problem resolution.

- **Archival**

The **Server** can capture console traffic of selected **Network Elements** for archival at the Portal.

# NetKitWorks® Client

A Windows application, the Client provides full TTY/VT100/Telnet terminal emulation for communicating with a wide range of Network Elements via the Servers' Serial, Ethernet or WAN interfaces. The Client may also be directed by the Portal to establish direct a management connection with selected Network Elements, bypassing the ACP Server when and where it is not possible or practical to deploy a Server.

## Features

- **Classic Windows GUI**

For ease of use, the **Client** features the traditional appearance of Windows applications; a Title bar, Menu bar, Function Keys bar and a Status bar. The application working area has Windows bars, a text window and a timestamp window for data displayed in the text window.

- **Terminal Emulation**

Once the **Client** is connected to the Network Element, it senses the traffic format and automatically adopts the required terminal emulation mode. The user need not be cognizant of the terminal type or the protocol that are required to interoperate with the **Network Element**.

- **Function Keys**

The **Client** features customizable buttons which are defined by the administrator to send commands or to perform certain actions by executing local scripts downloaded by the Portal. Buttons are uniquely tailored for each **Network Element** and may be used to restrict certain users to a set of actions, to standardize the user interface across a range of equipment or to simplify management tasks.

- **Concurrent Sessions**

A user may launch multiple instances of the **Client** to control and monitor multiple Network Elements from a single workstation. Each **Client** session has its own Chat room, application Working Area, Access Control Rights and Scripts allowing a user to conduct several independent management sessions with different types of **Network Elements**.

- **Telnet Secure Connections**

The **Client-to-Server** communication uses secure connections to safeguard sensitive information. The **Client-to-Portal** communication also uses secure connections to exchange control information.

- **Archival**

While NetKitWorks® Servers may be setup to archive the traffic of all or selected **Network Elements** at the Portal, each **Client** can also be used to record a session traffic and to archive it on the user's workstation.

# NetKitWorks® Highlights

## Compatibility

NetKitWorks® is compatible with both serial and IP based console ports. As an out-of-band management system, NetKitWorks® interconnects to **Network Elements** via their asynchronous, synchronous or Ethernet console ports. The ACP Server provides a broad set of protocol, terminal emulation and hardware options to accommodate the wide range of physical and logical administrative interfaces encountered on Network Elements.

## Monitoring

The **Portal** dashboard provides the administrator with a real time capture of current and past console management sessions. The information captured the user ID and time of connection and is a useful tool for monitoring trends, user activity and unauthorized access attempts.

## Network Migration

NetKitWorks® may be deployed as an overlay management system over different types of network transport infrastructures as it supports connection and connectionless types of Data Communication Networks. The integration of NetKitWorks® in current network architectures is further simplified by its ability to leverage customer owned terminal servers.

## Redundancy

Network administrators may deploy redundant Portals to ensure a 24x7 operation. The Portal Erlang software environment provides the replicating database mechanisms to maintain synchronization between redundant Portal systems ensuring that NetKitWorks® Clients and Servers can interoperate with the secondary Portal should the primary one fail or become inaccessible.

## Security

Users are allowed to connect to a **Network Element** only if they have the appropriate credentials and only via selected workstations if so provisioned by the network administrator. As network addresses and logon details for the **Network Elements** are not made public, NetKitWorks® provides an effective method to secure managed equipment from rogue users. The **Server** 'secure physical connections' provide an added layer of security by shielding the **Network Elements** from unauthorized wiretapping.



NetKit Solutions is a provider of network products for applications spanning the Transaction and Operations Support System markets. Over 75,000 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  
U.S.A.  
Tel: +1 805 214 0980  
Fax: +1 805 214 0970

NetKit Solutions UK Ltd  
9B Basepoint Enterprise  
Centre  
Stroudley Road, Basingstoke  
HANTS, RG24 8UP, UK  
Tel: +44 (0) 1256 300080  
Fax: +44 (0) 1256 300087

**<http://www.netkitsolutions.com>**

Form Number PB NKW-01M

