

EnterpriseAM
Network
Probe



Building a clear Picture of the Network

An enterprise's IT infrastructure constitutes a significant capital investment and is a strategic resource. To effectively manage both the network and scarce IT resources, IT managers and CIOs need to have a clear understanding of the network's architecture and the assets accessing the network. Despite the prioritization given to the security infrastructure, the network remains a challenging mix of the known and unknown. Eracent's technology provides the tools to maintain a complete inventory of new, legacy and proprietary networked devices in an easy to use, easy to implement and cost effective solution.

The Network Probe Option™ of EnterpriseAM™ analyzes any network regardless of size and complexity, utilizing a variety of strategies to uncover the multi-layered and sophisticated architecture. The demands for this information include solving the following issues:

- >> Insure IPv6 compliance
- >> Eliminate rogue devices and access such as unauthorized wireless access points
- >> Uncover networked equipment to phase out, or that was scheduled to be phased out but is still reporting
- >> Identify incorrectly configured or no longer used equipment that serves the network such as data transport equipment



TRANSPARENCY WITH NETWORK PROBE

By coupling standard identifiers with a wide array of unique device attributes, Eracent's solution places no constraints on what devices can be discovered or how they are identified. The solution gives IT managers and CIO's all the information they need to manage critical networks and sets a new standard for device inventory accuracy. The Network Probe Option is uniquely capable of collecting the level of detail necessary to go beyond simple device identification, including probing how devices are interconnected. Devices are identified and tracked regardless of their physical location or configuration.

Network Probe collects two types of data elements; identifying elements and informational elements. Identifying elements are the only ones used to distinctly identify the device on the network. Informational elements are used to describe characteristics about the device. New elements of either type can easily be added without architectural changes to the database schema, or the reporting engine.

Network Probe identifies network devices by principally collecting any combination of the IP address, and/or NIC address of the device, LAN Manager and/or NetBios name or domain of the device, the serial number and/or asset tag number, any unique identifier assigned to the device and/or the type of device and/or the make, model and manufacturer. Network Probe can also be configured to recognize other specific device identifiers as required.

Organizational Requirement

Probes the network to build a comprehensive picture of the network architecture

Identifies devices by rigorously pursuing all avenues for device identification in order to gain the most complete information

Collects all potentially valuable data elements with a rules engine that carefully identifies unique assets

Represents the network so that assessment of integrity, lack of single points of failure, and relationships between items are clear

Provides easy access to reports of the data elements of the network

Network Probe Functionality

Discovers:

- >> Across platforms (Windows/UNIX/MAC, more)
- >> All types of networked devices (routers, printers, switches, VoIP telephony devices, more)
- >> Whether networked at the time or at any time
- >> With out-of-box integration to popular third-party applications such as HP OpenView™ or Microsoft SMS™ picture of the network architecture

Uses a series of methodologies such as:

- >> IP address
- >> NIC address of the device
- >> LAN Manager and/or NetBios name or domain of the device
- >> DNS name
- >> SNMP OIDs
- >> Slot Switch information
- >> WMI service
- >> Windows network management API
- >> Serial number and/or asset tag number
- >> Any unique identifier assigned to the device
- >> Type of device
- >> Make, model and manufacturer
- >> Configurable to recognize other specific device identifiers as required

Collects data elements such as:

- >> A numeric value which indicates the discovery source
- >> The device description as reported by SNMP
- >> The host name of the device
- >> The domain name of the device
- >> The name and version of the operating system the device is running
- >> The amount of physical RAM on the devices
- >> The ID currently logged onto the device's console
- >> The version of the firmware the device is running
- >> The network operating system the device uses
- >> The numeric value representing the device manufacturer.
- >> The version of the device itself
- >> Based on external, customizable commands

Graphically represents the collected information:

- >> At a top level to summarize the architecture
- >> To give a visual representation of status
- >> With drill down capabilities to document fail-over paths

Reporting features include:

- >> Web-based
- >> Easy user access
- >> Standard reports
- >> Management level reports
- >> VDetail reports
- >> Exception reports
- >> Ad hoc reporting

THE NETWORK PROBE ADVANTAGE

The Network Probe Option provides a foundation of information for all of the projects that require an extensive knowledge of the network. Whether identifying and removing single points of failure, finding lost devices, or working on the more classic goals of high availability and maintainability, the data collected offers a level of accuracy for those projects that has not been possible. The discovery must be broad, reliable and easily fed into other tools. IT professionals should evaluate the completeness of the information and supplement or replace existing tools as necessary to build confidence in the information about their network.

The diverse demands on this data require highly flexible analysis and reporting tools. EnterpriseAM with Network Probe provides end users with a central command station for viewing their network at any level and from any angle graphically. They can also design reports to match their specific interests. Through the analysis of the data collected by the Eracent Network Probe, IT professionals now have the ability to detect, locate, and prevent any single point of failure before a problem can occur.

DISCOVER NEW DEPTHS

Eracent provides this functionality in the Network Probe option for the EnterpriseAM product. Organizations that use Eracent's Network Probe to perform the critical tasks that are part of network discovery have a total awareness of the IT infrastructure. Combining the ability to not only discover assets and their configuration, but adding in the ability to perform a "deep probe" on any type of reportable device gives the Eracent user the ability to solve issues that plague both the operational and business aspects of IT.

Contact Us At:

Phone: +1.908.537.6520

Email: sales@eracent.com

EMEA Sales & Product Information:

Bristol, UK

+44 (0) 1454-203615

Email: Info@eracentemea.com

Corporate Headquarters:

Eracent, Inc.

8133 Easton Road

Ottsville, PA 18942

Email: info@eracent.com

www.eracent.com