# EventWatch

**Product Information**

## Network Fault Management

Network monitoring has traditionally been reactive in nature. In the worst case, the IT department finds out about a network fault after frustrated end-users call into the help desk. While many network faults are preventable, proactive management has historically been a difficult task.

The typical network management system (NMS) is continually flooded with network event messages, which increase exponentially when a device such as a router or switch goes down. The resulting event storm can generate more than a million alert messages. The NMS also generates alarms once certain defined thresholds (for link utilization, CPU utilization, and buffer space) are reached. All these alarms make it exceedingly difficult to troubleshoot problems. Resource-restricted IT managers can only react to the vast number of daily alarms by fighting fires. Consequently, problems are identified and resolved only after they have significant impact on network performance.

## Tavve's EventWatch™

Introducing EventWatch, a self-configuring application for automated network fault and alarm management. EventWatch greatly simplifies network troubleshooting by notifying the appropriate personnel of the root cause of a failure, in less than three minutes, regardless of the size of the network.

EventWatch consolidates events, correlates faults, and eliminates unnecessary alarms. With EventWatch, the root cause of multiple alarms—such as an inoperative router port that causes all downstream devices to send out alarms—can be quickly determined and fixed, before network users are even aware of the problem.

## How It Works

EventWatch automates the network fault management process by using a three-phase approach:

- **Verification**
- **Correlation**
- **Notification**

First, EventWatch verifies that a reported outage is both genuine and critical. Then, EventWatch correlates the event using its own correlation engine and database to determine the root cause of the outage. Finally, EventWatch notifies the appropriate network personnel about the fault via paging, e-mail, pop-up screens, trouble tickets, or log files.

## Key Features

- **Suppression of event storms and transient network failures**
- **Self-configuring and self-maintaining**
- **Layer 2 root cause analysis**
- **Autodiscovery of network topology**
- **Active query of component status**
- **Speed and accuracy**
- **Support of additional protocols**
- **Correlation through frame relay clouds**
- **Notification based on user-defined groups**
- **Quick installation time**

## Verification

EventWatch employs a verification routine that causes transient (false) network errors and noncritical events to be excluded from the correlation process. Transient network errors are a normal part of network operation and occur whenever network latency, congestion, or busy devices cause pings sent out by the NMS to be delayed or lost. Because the NMS interprets transient errors as outages, it reports that a node is down; then, when the transient condition disappears, the NMS sends out messages that the device is up. EventWatch filters out these transient network failures by means of a verification period. If the reported condition goes away during the verification period, EventWatch concludes that it is transient and ignores it.

EventWatch also automatically generates trap filters, based on user-specified criteria, to differentiate between critical and noncritical events. These filters sift through the avalanche of SNMP traps received by the NMS so that only events of concern are processed. Critical events are then processed in one of four ways: (1) the trap is reporting a failure: begin the verification, correlation, and notification phases; (2) the trap is reporting a restored condition: notify the appropriate support personnel that the failure is gone, or cancel the verification in progress; (3) the trap requires immediate notification; or (4) the trap is simply to be logged.

## Correlation

After a network failure has been verified (phase 1), EventWatch begins the event correlation process (phase 2) to determine the root cause of the failure. This process is made possible by the following leading-edge features:

### Independent Correlation Database

EventWatch does not rely on the NMS to provide device or interface information. Instead, it creates its own network topology database containing information on all managed devices, including routers, bridges, and switches. EventWatch often discovers devices, such as routers and switches, that are

# EventWatch

unknown to the NMS. To maintain accuracy, EventWatch refreshes the correlation database after installation, updating any network topology changes.

### Layer 2 Correlation

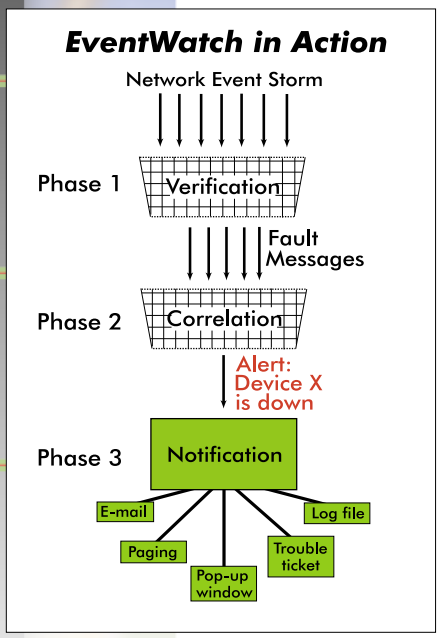
Unlike other fault correlation systems, EventWatch can correlate all the way down to Layer 2 of the OSI model. In the most typical network architecture, devices on local area networks (LANs) and subnets are connected together using hubs and/or switches and bridges. Networks are connected to other networks using routers. These devices correspond to the first three layers of the OSI model, as follows:

| Device | OSI Layer |
|---|---|
| routers | Layer 3 |
| switch ports/bridges | Layer 2 |
| hubs | Layer 1 |

Fault correlation systems typically rely on router paths (Layer 3) to determine the root cause of outages. Thus, when a switch, or a server on a LAN connected to a switch (OSI layer 2), goes down, these systems cannot discover the root cause. EventWatch, however, can correlate all the way down to switch ports and bridges (OSI layer 2). Using MAC information, EventWatch determines the servers, workstations, and network equipment connected to a particular switch.

### Speed and Accuracy

EventWatch employs an active approach to determining root cause, which makes it an extremely fast and accurate fault correlation system. When the correlation engine begins processing, EventWatch needs to know the status of different components in the network. Because NMS systems poll devices in a round-robin manner, waiting for the NMS to poll a particular failure path can take a long time, especially on large networks. Moreover, the reported data may not be current at the moment of the outage for all of the affected devices, which can lead to erroneous root cause analysis.




Instead of passively waiting for the NMS, EventWatch actively verifies component status. This has two advantages. First, it enables EventWatch to correlate the root cause quickly. This phase of the process takes less than two seconds, regardless of the size of the network. Second, it permits EventWatch to accurately determine the status of all key upstream devices. EventWatch checks to see if any device upstream between the NMS and the point of failure is actually the root cause. Fast and accurate correlation leads to fast notification, which in turn leads to quick network repair times.

### Support of Additional Protocols

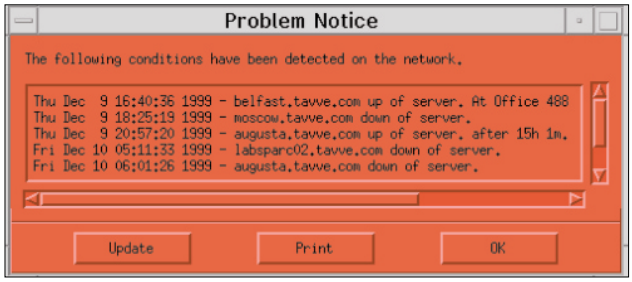
EventWatch's correlation engine is not restricted to TCP/IP networks. It can be configured to process other protocols (including SNA, IPX, and DECNet) as well as device componentry (CPU, file systems, log files, disk drives, and other processes).

### Clouds

EventWatch's correlation engine can also process clouds, which are network elements that cannot be verified. Examples include carrier-provided frame relay clouds, dumb hubs, unmanageable routers, or unverifiable network junctions. EventWatch can even process clouds that are dependent upon other clouds (a highly useful capability for service providers with multiple clients).

## Notification

When a network failure has been verified (phase 1) and its root cause determined (phase 2), EventWatch notifies the network personnel responsible for resolving the problem (phase 3). Five standard notification options come preinstalled: e-mail, alphanumeric page, pop-up alert window, trouble ticket, or log file. Users can mix and match these options. Whatever the ways an organization divides responsibility for the equipment, EventWatch can create notification groups to match equipment with the responsible personnel.




Alert Window

## Easy Installation

Installing EventWatch is easy, and takes less than thirty minutes. Once installed, EventWatch begins monitoring and reporting without any further configuration.

### Platform Requirements

- Tivoli NetView running on IBM AIX or Sun Solaris
- Hewlett-Packard OpenView Network Node Manager running on HP-UX or Sun Solaris

### Hardware Requirements

- 20 MB disk space available

### Memory Requirements

- 32 MB RAM available


**For More Information Contact:**
**Tavve Software Company**
**One Copley Parkway ▪ Morrisville, NC 27560**

**919.460.1789 ▪ fax 919.380.7147 ▪ www.tavve.com**