

SUITABILITY TEST REPORT

for

**Tivoli Systems, Inc.
TME 10™ NetView 5.0a
Windows NT**

Network Manager Component

April 23, 1998

Prepared by



National Product Line Asset Center
1000 Technology Drive, Suite 1000
Fairmont, WV 26554

1.0 SCOPE

1.1 Introduction

This Suitability Test Report (STR) defines and records the test preparation and test results from suitability testing TME 10™ NetView version 5.0a for NT. NetView is one component of an integrated product suite of network management applications developed and marketed by Tivoli Systems, Inc.

TME 10™ NetView 5.0a is a network device management application that focuses on providing configuration, automation, performance and fault management capabilities. It utilizes an open architecture to allow for easy integration with other TME 10 and third party management applications.

1.2 Test Environment

TME 10™ NetView 5.0a was suitability tested against command center product line requirements and architectural constraints, using a test network comprised of: 4 Sun™ SPARC™ Ultra 1 workstations running Solaris™ 2.5.1, 5 Gateway 2000® PC's with Windows 95, 3 Gateway 2000® PC's with Windows NT 4.0, 2 HP printers, 1 Sun™ printer, 1 Sun™ IPC running SunOS™ 4.1.3 and 1 Cisco router.

Part Name	Version	Manufacturer
TME 10™ NetView	5.0a	Tivoli Systems, Inc

2.0 SYSTEM REQUIREMENTS

The vendor recommends the following system requirements:

Processor	Intel PC or Alpha PC. (For Intel PC's Pentium 90 MHz. Minimum.)
Memory (RAM)	48 MB for Intel PCs, 64 MB for Alpha PCs. (Additional memory will improve performance and is necessary for large networks).
Paging Space	128 MB.
Operating System	Windows NT® 4.0 or later.
Protocol	TCP/IP protocol installed and configured.
Other	SNMP Service installed and configured.

3.0 TEST RESULTS

The results obtained during testing of the Tivoli Systems, Inc. product, TME 10™ NetView 5.0a for NT, are shown in the following table. The table contains the *Criteria Number*, *Criteria Description*, *Test Result*, *Explanation*, and *Test Method*. The test methods used to perform the suitability testing included:

Inspection - consists of investigation, without the use of special equipment or procedures, to determine compliance with requirements. Inspection may include comparison of requirements to the vendor supplied product, documentation, and/or information. It may also include the results of technical interface with product vendor representatives.

Test - is the evaluation of functional operation by use of equipment or instrumentation, simulation techniques, and the application of established principles and procedures to determine compliance.

4.0 CRITERIA SOURCE REFERENCES

The criteria used in the suitability testing process were developed from the following source references:

- Generic Command Center Architecture (GCCA) Report for the Portable, Reusable, Integrated Software Modules (PRISM) Program, Revision A, 5 April 1993.
- Qualified Product List (QPL) Capstone Test Plan for the Portable, Reusable, Integrated Software Modules (PRISM) Program, Revision 0.1, 29 June 1995.
- Network Manager Class Requirements for the Portable, Reusable, Integrated Software Modules (PRISM) Program, Revision 1.0, 7 July 1995.

Criteria Number	Criteria Description	Test Result	Explanation	Test Method
1.0	Architectural Characteristics			
1.1	The Network Manager should be capable of working in small (0-50 nodes), medium (50-150 nodes), and large (over 150 nodes) networks.	Y		Testing
1.1.1	The NM should be capable of handling the magnitude of management information that could be generated in a large (i.e., over 150 nodes) network.	Y		Inspection
1.2	The NM should be able to provide a hierarchical view of all devices managed by the NM. This view should be represented as a hierarchical map that incorporates explodable icons, which can spawn a sub-map that represents another level of detail. At the lowest level, icons should represent specific devices from which status information can be accessed.	Y		Testing
1.3	The NM should allow grouping of devices based on functionality, location, security, or any other user-defined category, and perform management on those groups.	Y		Testing
1.4	The NM should support manager-to-manager transmissions of: Access control information. Device status change information. Network configuration changes. (Others?).	Y		Inspection
1.5	The NM should provide for functionality which is contained in separate modules which allows the user to choose those functions required and avoid inclusion of non-required functions.	Y		Testing
1.5.1	The user of the NM software should be able to make software configuration changes (based on changes in the environment) without vendor technical support.	Y		Testing
1.6	The NM should be capable of distributing its manager/agent processes among multiple network devices.	Y		Testing
1.7	The NM should be capable of running on multiple platforms.	Y	The version tested was for NT. However, a Solaris version is also available.	Inspection
2.0	System Interface Criteria			
2.1	The NM should support a graphical representation of the network. Comment: This requirement deals with the topology (e.g., token ring, star, bus, node, etc.) of any given level of geography.	Y		Testing
2.1.1	The NM should support the ability to provide a hierarchical map.	Y		Testing
2.1.2	The NM should support the ability to represent unmanageable devices in the map.	Y		Testing
2.1.3	The NM should support the ability to show both physical and logical maps.	Y		Testing
2.1.4	The NM should support the ability to tailor the icons that represent the network and network interfaces.	Y	Icons can be selected from the supplied list to represent an object. However, there is no capability to create a new icon.	Testing
2.2	The NM should provide an interface to access the information off of the Directory Server when one exists.	Y		Testing

Criteria Number	Criteria Description	Test Result	Explanation	Test Method
3.0	Security Features			
3.1	The NM should provide a means to identify and authenticate users via user identification and passwords.	N	This is performed by the operating system's User Manager's Administration tools.	Testing
3.2	The NM should provide user access controls.	Y		Inspection
3.2.1	The NM should provide the capability to restrict access to applications.	Y	This can be achieved utilizing the TME 10 Security Management Module (Tivoli Systems, Inc.) residing on top of the TME 10 Framework.	Inspection
3.2.2	The NM should provide the capability to restrict access to files.	Y	This can be achieved utilizing the TME 10 Security Management Module (Tivoli Systems, Inc.) residing on top of the TME 10 Framework.	Inspection
3.2.3	The NM should provide the capability to restrict access to queues and other resources.	Y	This can be achieved utilizing the TME 10 Security Management Module (Tivoli Systems, Inc.) residing on top of the TME 10 Framework.	Inspection
4.0	Implmentation Constraints			
4.1	If Unix-based, the NM should support current POSIX requirements (FIPS Pub 151).	N	Platform tested was Windows NT.	Inspection
4.2	If Unix-based, the NM product should use the X-windows standard.	N	Platform tested was Windows NT.	Inspection
4.3	If Unix-based, the NM should support the Open Software Foundation (OSF)/MOTIF graphical user style guide.	N	Platform tested was Windows NT.	Inspection
5.0	Configuration Management			
5.1	The NM should provide the capability to define new managed object types. The definition should include attributes, including the range and types of values to which the attributes can be set.	N	The user is allowed to select from several types of objects and define parameters/change attributes for the device.	Testing
5.2	The NM should provide the capability to set SNMP parameters and process allocation.	Y		Testing
5.3	The NM should provide the capability to modify the relationships (i.e. roles) of network resources.	Y		Testing
5.4	The NM should provide the capability to remotely examine device statistics, threshold values, and Local Area Network (LAN) connections.	Y		Inspection
5.5	The NM should provide the capability to specify initialization and shutdown procedures for network devices.	Y	This is accomplished using the Management Information Base (MIB) applications if the network devices include initialization/shutdown MIB support via SNMP.	Inspection
5.6	The NM should provide for graceful degradation and restoration of the network.	Y	This is accomplished via MIB applications if the devices support that via SNMP.	Inspection
5.7	The NM should provide the capability to verify each user's authorization for performing either specific or categories of	Y		Inspection

Criteria Number	Criteria Description	Test Result	Explanation	Test Method
	configuration management functions.			
5.8	The NM should be capable of reporting on configuration status.	Y		Testing
5.8.1	The NM should provide the capability of agent systems to report configuration changes to their managers as these changes occur.	Y		Testing
5.8.2	The NM should provide the capability to poll their agents in order to determine each agent's (or agent system's) configuration status.	Y		Testing
6.0	Performance Management			
6.1	The NM should provide the capability to monitor performance.	Y		Testing
6.1.1	The NM should provide the capability to monitor the workload of networked devices (e.g., resource utilization).	Y		Testing
6.1.2	The NM should provide the capability to generate event reports as utilization approaches capacity.	Y		Testing
6.1.3	The NM should provide the capability to report on other (i.e. other than utilization capacity) events. The report should specify the event type.	Y		Testing
6.2	The NM should provide the capability to execute performance tests and to collect the results from those tests inputted to the Diagnostic Testing Function provided under Fault Management.	Y		Testing
6.3	The NM should provide the capability of monitoring resource allocations for any resource on the network.	Y		Testing
6.4	The NM should provide the capability to set or modify resource attribute values.	Y		Testing
6.5	The NM should provide the capability to allow NM operators to specify performance tuning methods.	Y		Testing
6.6	The NM should provide the capability to generate performance reports based on user specified criteria.	Y		Testing
6.6.1	The NM should provide the capability to specify the format of all reports.	N		Testing
6.7	The NM should provide the capability to test resource capacity.	Y		Testing
7.0	Fault Management			
7.1	The NM should provide the capability to monitor the events and errors.	Y		Testing
7.2	The NM should provide the capability to log events and errors, to record reports within the managed system that generated the event, (e.g., logging) or error, and then retrieve these reports remotely.	Y		Inspection
7.3	The NM should provide the capability to forecast anticipated faults by allowing the user to set thresholds, which represent performance limits of networked devices.	Y		Testing
7.4	The NM should provide the capability to activate diagnostic and testing procedures.	Y		Testing

Criteria Number	Criteria Description	Test Result	Explanation	Test Method
7.5	The NM should provide the capability to report results from Diagnostic and Testing procedures.	Y	A third party SQL reporting tool may also be utilized.	Testing
7.6	The NM should provide the capability to analyze the results of diagnostic testing.	N	The product provides the results of the diagnostic testing, however, the user has to then analyze the data.	Inspection
7.7	The NM should provide the capability to report failures.	Y		Testing
7.8	The NM should provide the capability to terminate failures.	Y		Testing
7.9	The NM should provide Diagnostic Tests.	Y		Testing
7.9.1	The diagnostic tests should include Connectivity Tests.	Y		Testing
7.9.2	The diagnostic tests should include Data Saturation Tests.	Y	Test can be modeled by manipulating configuration files (text), to modify the behavior of existing tests.	Inspection
7.9.3	The diagnostic tests should include Data Integrity Tests.	Y	Test can be modeled by manipulating configuration files (text), to modify the behavior of existing tests.	Inspection
7.9.4	The diagnostic tests should include Protocol Integrity Tests.	Y		Testing
7.9.5	The diagnostic tests should include Connection Saturation Tests.	Y	Test can be modeled by manipulating configuration files (text), to modify the behavior of existing tests.	Inspection
7.9.6	The diagnostic tests should include Response Time Tests.	Y	Test can be modeled by manipulating configuration files (text), to modify the behavior of existing tests.	Inspection
7.9.7	The diagnostic tests should include Imaging Loopback Tests.	Y	Test can be modeled by manipulating configuration files (text), to modify the behavior of existing tests.	Inspection
7.10	The NM should provide the capability to request dumps.	Y		Inspection
7.10.1	The NM should provide the capability to request statistic blocks.	Y		Testing
7.10.2	The NM should provide the capability to request operational status information of managed network devices.	Y		Testing
7.11	The NM should provide the capability to track corrections to fault conditions.	Y	This can be accomplished via Tivoli Enterprise Console (T/EC) (Tivoli Systems, Inc.).	Inspection
8.0	Security Management			
8.1	The NM should provide the capability to the NM operator (or security officer) to permit or disallow access to security related parts of the network.	Y		Inspection
8.2	The NM should provide the capability to archive and retrieve security related information.	Y	This can be accomplished via the Security Management Module (Tivoli Systems, Inc.) which resides on top of the TME 10 Framework.	Inspection

Criteria Number	Criteria Description	Test Result	Explanation	Test Method
8.2.1	The NM should provide the capability to create and delete security logs or audit trails.	Y	This can be accomplished via the Security Management Module (Tivoli Systems, Inc.) which resides on top of the TME 10 Framework.	Inspection
8.2.2	The NM should provide the capability to read from and write to security logs or audit trails.	Y	The Tivoli Enterprise Console (T/EC) (Tivoli Systems, Inc.) will read and write to/from security and log files via its log file adapter.	Inspection
8.2.3	The NM should provide the capability to start and suspend logging or auditing activities.	Y	This can be accomplished via the Security Management Module (Tivoli Systems, Inc.) which resides on top of the TME 10 Framework.	Inspection
8.2.4	The NM should provide the capability to monitor audit trails or security logs to identify security violation activity.	Y	This can be accomplished via the Security Management Module (Tivoli Systems, Inc.) which resides on top of the TME 10 Framework. Any other security tool that can be plugged into the TME 10 Framework for information sharing and management will also work.	Inspection
8.2.5	The NM should provide reporting and notification of violations or attempted violations.	Y	This can be accomplished via the Security Management Module Desktop Interface (Tivoli Systems, Inc.).	Inspection
9.0	Accounting Management			
9.1	The NM should be capable of recording and generating accounting information.	Y		Testing
9.1.1	The NM should be able to gather information regarding the duration of communications resource usage.	Y		Testing
9.1.2	The NM should be able to gather information regarding the number of service data units used.	Y		Testing
9.1.3	The NM should be able to gather information regarding the quality of service provided.	Y		Testing
9.1.4	The NM should be able to gather information regarding the reason for communications termination.	Y	Communication information can be displayed via the Tivoli Enterprise Console (T/EC) (Tivoli Systems, Inc.).	Inspection
9.2	The NM should provide the capability of specifying accounting information to be collected.	Y		Testing
9.2.1	The NM should provide the capability to specify accounting information based on the definition of a managed object.	Y		Testing
9.2.2	The NM should provide the flexibility for the inclusion of optional attributes for accounting (Accounting Management).	Y		Testing
9.2.3	The NM should provide the flexibility for new attributes to be specified by the NM operator.	Y		Testing
9.3	The NM should allow for standard procedures to retrieve accounting information and to manage the disposition of the accounting information.	Y		Testing

Criteria Number	Criteria Description	Test Result	Explanation	Test Method
9.4	The NM should provide the capability for NM operators to select the format the accounting information is to be presented to users, operators, and administrators.	Y	A third party reporting tool may also be used.	Testing
9.5	The NM should support the ability to read accounting limits for communications resources.	Y		Testing
9.5.1	The NM should support the ability to set accounting limits for communications resources.	Y		Testing
9.5.2	The NM should support the ability to change accounting limits for communications resources.	Y		Testing
9.6	The NM should provide the capability to allow the NM operator to define metrics and accounting information units for accountable resources.	Y		Testing
10.0	General			
10.1	The NM should be a COTS or GOTS product.	Y		Inspection
10.1.1	The NM should have been used to satisfy NM requirements for at least one year in a multiplatform environment.	Y		Inspection
10.2	The NM should have proven performance, reliability, and availability characteristics (e.g., mean time between failure, response time to user inputs) and the vendor should be able to provide data supporting characteristic values claimed.	Y		Inspection
10.3	The NM should have user manuals.	Y		Inspection
10.3.1	The NM should have training support.	Y		Inspection
10.3.2	The NM vendor should provide or make available product upgrades, new versions, updates, patches, bug fixes, and maintenance releases to users, including options for implementing the changes and associated costs for the various kinds of changes.	Y	User must purchase maintenance agreement to access this information.	Inspection
10.4	The NM should have proven conformance to Human Factors Engineering (HFE) requirements applicable to an operational command center. (Ref, USAF Human Factors Engineering Guidelines)	N		Inspection
10.5	The NM should provide programmatic interfaces to support detailed NM requirements.	Y		Testing
10.6	The NM should have a proven and demonstrable installed base, where the network manager products have been installed in DoD or non-DoD applications in which products could be demonstrated.	Y		Inspection
10.7	The NM should be structured into separate functional priced items to allow users to choose the desired capabilities of the product base that satisfy their particular requirements.	Y	NetView is one member of a suite of management tools known as TME 10 (Tivoli Systems, Inc.).	Inspection