Results on the Evaluation of NetReality, Inc. WiseWan 202 System for Traffic Shaping Performance

Ferial El-Mokadem

September 2000

MITRE
Washington C3 Center
McLean, Virginia

Abstract

This report presents results on the evaluation of the NetReality, Inc. WiseWan bandwidth management system WiseWan 202, software version 3.2. Test results of the WiseWan 202 System evaluation indicate that the WiseWan can effectively identify and provide favorable transmission performance to traffic marked as mission-critical while adhering to user-specified rules and priorities. WiseWan provides three effective traffic-shaping capabilities that deliver distinctively high throughput for mission-critical traffic in the presence of congestion on the links and with other traffic sharing the link bandwidth. In addition, WiseWan's real-time network monitoring and extensive performance reporting capabilities provide network administrators with a useful insight into network utilization performance.

Table of Content

Section **Page**

Results on the Evaluation of NetReality, Inc. WiseWan 202 System for Traffic Shaping Performance

Ferial El-Mokadem
The MITRE Corporation

This report presents results on the evaluation of the NetReality, Inc. WiseWan bandwidth management product. The WiseWan system is a WiseWan 202, software version 3.2. The evaluation was performed in the summer of 2000 in the PC/LAN laboratory of the MITRE Corporation in Reston, VA. This work was performed under the auspice of the mission-oriented investigation and experimentation (MOIE) "***Operational Dynamics of Quality of Service (QoS)"***; an Army MOIE sponsored by the Defense Information Systems Agency (DISA) for fiscal year 2000.

Test results of the WiseWan 202 System evaluation indicate that the WiseWan can effectively identify and provide favorable transmission performance to traffic marked as mission-critical while adhering to user-specified rules and priorities. WiseWan provides three effective traffic-shaping capabilities that deliver distinctively high throughput for mission-critical traffic in the presence of congestion on the links and with other traffic sharing the link bandwidth. In addition, WiseWan's real-time network monitoring and extensive performance reporting capabilities provide network administrators with a useful insight into network utilization performance.

1. INTRODUCTION

Managing the transmission capacity of DoD networks to provide sufficient bandwidth to fully support the mission-critical traffic applications of deployed forces has become an increasingly complex task. Transmission capacity in the tactical arena provided by a combination of MILSATCOM and/or leased commercial SATCOM is always in short supply and is costly to acquire. Furthermore, the priorities for user access to DoD wide area network (WAN) communications assets and degrees of end-to-end performance vary for different user communities and applications during the phases of a deployed force mission, often changing in a matter of minutes. Quality of Service (QoS) mechanisms and Policy-Based Network Management (PBNM) provides a means to do sophisticated traffic shaping and policing required for allocating available transmission resources to tactical network users according to various criteria. Examples of user connection criteria are 1) the priority of user information at each phase of the mission, 2) the minimum tolerable time needed for delivery of user information, and 3) the statistical nature of the network traffic.

One of the main objectives of this MOIE is to explore the utility of existing and emerging QoS networking and PBNM products that could be implemented into DoD networks to support the communications needs of deployed forces. Using both laboratory testing and simulation efforts, a variety of QoS networking and PBNM products are being evaluated for their specific QoS techniques and capabilities that might deliver improved performance necessary to deployed forces' mission-critical traffic applications. The evaluation is focused on the merits of the various approaches to QoS networking, including traffic shaping, admission control techniques, and queue management algorithms to determine which is the best solution. Some of these techniques are

implemented in network elements such as routers and hosts or in stand-alone devices such as the WiseWan system from NetReality.

This paper presents the results on the WiseWan system evaluation for traffic shaping performance. It is organized as follows: Section 2 provides an overview of the WiseWan Bandwidth Management system and its architecture. Section 3 presents the test configuration and test cases used to evaluate the different types of traffic shaping policies implemented by the WiseWan. Section 4 provides the test results, and Section 5 provides a summary of our findings and concluding remarks. Appendix A contains the technical specifications of the WiseWan equipment.

2. OVERVIEW OF WISEWAN BANDWIDTH MANAGEMENT SYSTEM

The NetReality WiseWan bandwidth management product is a modular hardware/software platform that provides various schemes for managing network bandwidth by providing real-time monitoring of WAN lines and adaptively shaping WAN traffic to guarantee that the performance of mission-critical traffic does not suffer during periods of congestion. WiseWan allocates traffic according to bandwidth available while adhering to predefined traffic shaping policies. There are five traffic classification types:

- Applications and Protocol
- Direction
- Host (subnet, net, and user group)
- Schedule
- Circuit

There are three types of traffic shaping actions implemented by WiseWan:

- Prioritization
- Bandwidth Guarantees
- Bandwidth limiting

Prioritization traffic shaping scheme prioritizes traffic according to user specified policies to offer effective bandwidth utilization on heavily congested WAN lines, but does not guarantee any amount of bandwidth to priority traffic. There are five traffic priorities: low, medium, medium-high, high, and passthrough.

Bandwidth Guarantees traffic shaping scheme sets the amount of bandwidth to be received by mission-critical traffic on heavily congested lines without granting priority to any other type of traffic.

Bandwidth Limiting traffic shaping scheme configures a limit on the peak allowable bandwidth available to non-critical traffic across network links, whether or not any other traffic is offered on the link.

WiseWan can also provide traffic blocking per traffic classifications or conversation.

WiseWan combines the traffic shaping schemes with full-featured, real-time network monitoring, traffic statistics gathering, and extensive performance reporting capabilities. Network monitoring includes real-time line statistics presented in kilobits per second

(kbps), % utilization reports, and host conversations on the line, for both inbound and outbound directions. The reports help pinpoint networks bottlenecks and isolates busiest talkers, and identifies which data transfer jobs have been slowing the network.

2.1 WISEWAN SYSTEM ARCHITECTURE

The WiseWan system consists of the following three main components (see figure 1).

WiseWan Acclerator – is a hardware-based device physically connected on the wide area network (WAN) access link. It provides real-time monitoring, traffic shaping, and decoding of all frames that pass through and sends all analyzed information to the centralized WanXplorer Server.

WanXplorer Server – stores all analyzed information from the WiseWan accelerator via consistent polling.

WanXplorer Console – provides two applications: WanXplorer and WanShaper Console. WanXplorer monitors and reports network activity. WanShaper Console enables users to define traffic shaping policies and configurations, as described above. The WanXplorer applications can run on Windows 95 and higher, Sun Solaris, Windows NT Server, and Windows NT Workstation.

A WiseCable physically connects the WiseWan accelerator to the WAN link. WiseCable is an intelligent cable that can bypass any power failure or hardware breakdown of the WiseWan accelerator.

A WanTel component supports the WiseWan recognition of VoIP traffic. This component was not used in our system configuration because no voice traffic was used.

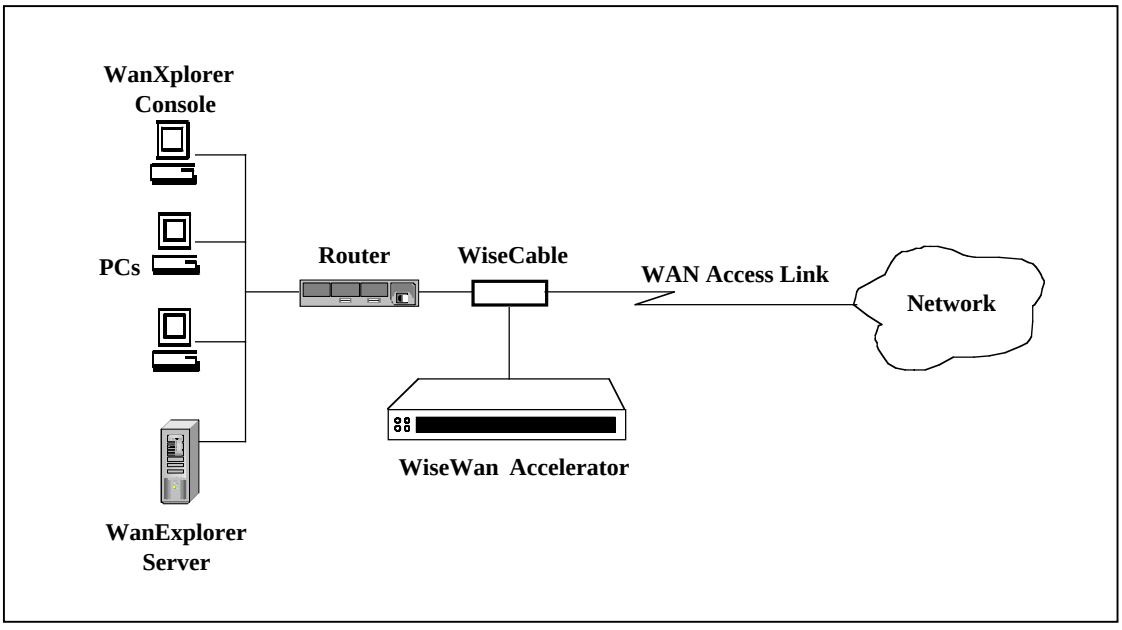

Figure 1. WiseWan System Layout

3. WISEWAN TESTING

3.1 GOALS

We proceeded with the WiseWan 202 evaluation testing in a controllable laboratory environment with the following goals:

1. Evaluating WiseWan ability to classify traffic on the basis of various criteria, including source/destination address, port, protocol, application, etc.
2. Testing WiseWan ability to dynamically allocate available capacity on WAN lines to selected network users according to user specified policies.
3. Testing WiseWan ability to limit access of lower-priority bandwidth-intensive traffic on fixed-capacity WAN lines in order to enhance throughput for mission-critical traffic.
4. Validating the accuracy and repeatability of WiseWan measurements of line utilization and conversations bandwidth.
5. Assessing how easily users can define and deploy WiseWan traffic shaping policies.

3.2 TEST CONFIGURATION

The network configuration for the WiseWan lab evaluation testing is set to represent a subset of a hypothetical scenario with joint force commanders responding to a notional crisis. In this scenario, the commands are grouped in four nodes; three of which are situated in one LAN separated from the fourth node by a single bottleneck WAN link. Three nodes on one LAN emulate entities supporting a component commander (e.g., Army, Maritime, or Air component commander) and the node on the other side of the WAN link emulates the Command Joint Task Force (CJTF).

Figure 2 shows the lab's test setup for the four-node network configuration scenario. It consists of two LANs interconnected by a single 1 Mbps link. The WiseWan 202 system is placed between two routers, a Cisco 4000 and a Cisco 3600 router pair.

Traffic data for the lab testing is selected to emulate some of the diverse types of mission-related, information exchanges (IEs) that might take place among the user entities in the four nodes, such as:

- Mission-critical, data intensive exchanges that may include graphic-intensive maps
- Mission-critical, small sized exchanges, of high priority requiring timely delivery; e.g., data for situational awareness
- Video conference traffic at fixed bit rate (384 kbps or higher)
- Routine-priority, data intensive exchanges
- Low-priority, data intensive traffic, such as weather forecasts

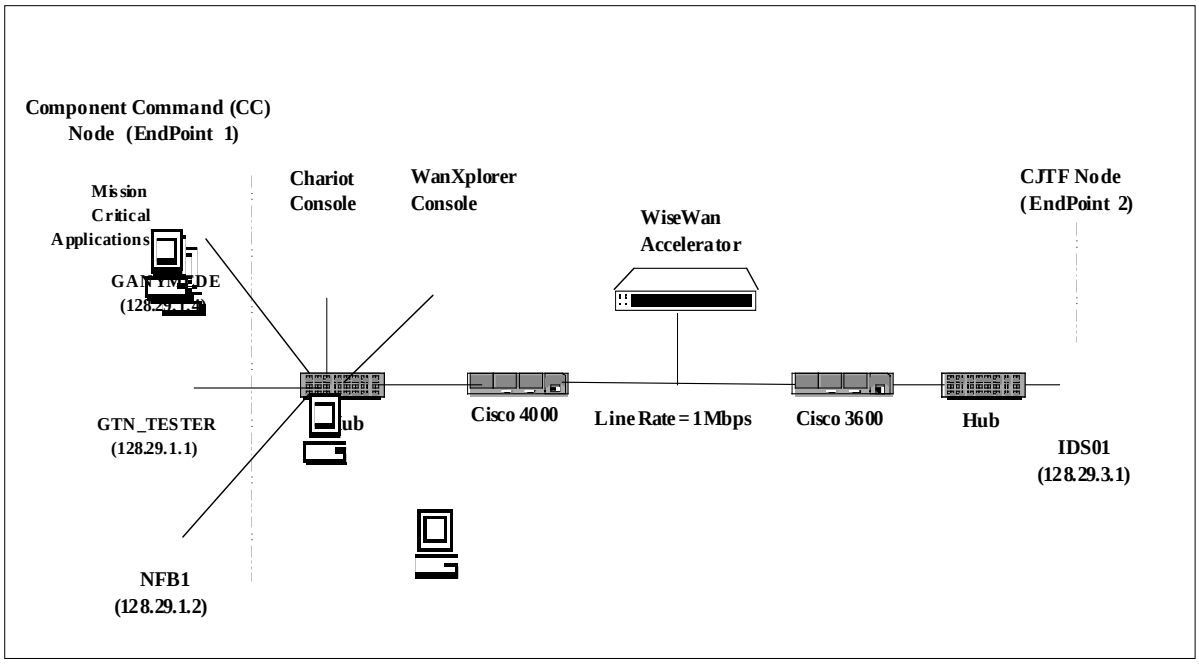

Figure 2. Lab's Test Configuration

3.3 TRAFFIC CONFIGURATION

The Chariot Console and Endpoints software from netiQ (previously Ganymede) were used to generate the traffic loads for the lab testing. The Chariot console resided on a PC running Microsoft Windows NT Server operating system version 4 Service Pack 4. Chariot endpoints resided on four PCs running Microsoft Windows NT Server operating system version 4 Service Pack 4. They provided the mean to make logical connections between Endpoints to reflect flow of traffic in the network configuration and to measure the performance of traffic throughput. The following identifies the applications selected for each EndPoint.

Host Address	Host Name	
128.29.3.1	IDS01 (CJTF)	Emulates the CJTF node with an FTP server, SAP/R3 server, HTTP server, and a video teleconferencing facility.
128.29.1.1	GTN_TESTER	Emulates an entity at the component command (CC) node uploading low-priority FTP files to a remote FTP server at the CJTF node.
128.29.1.2	NFB1	Emulates an entity at the CC node involved in a video teleconference (VTC) with the CJTF node (IDS01) at 384 kbps.
128.29.1.4	GANYMEDE	Emulates an entity at the CC node exchanging mission-critical, high-priority applications consisting of a mixture of large-sized exchanges (HTTP) and small-sized exchanges (SAP/R3) with a remote server at the CJTF node (DS01).

Table 1 provides a description of the Chariot applications selected to emulate the flow of network traffic during the tests, a mix of messages of various length, large files, and streaming traffic.

Table 1. Chariot Application Scripts

Traffic Application	Chariot Script File Name	Description
Pair 1: Web Graphics (Mission-critical)	HTTPGIF.SCR	This script emulates the traffic of an HTTP GIF (graphical image file) transfer. Endpoint 1, as the client, requests a GIF file from Endpoint 2, as the Web server. The default file size is 10,000 bytes.
Pairs 2 - 5: SAP/R3 (Mission-critical)	SAPAUTHP.SCR SAPINV.SCR SAPLOGIN.SCR SAPPUROR.SCR	The four scripts, each with its own connection, emulate a set of small-sized exchanges between EndPoint 1 and EndPoint 2. They represent a series of symmetric and asymmetric request/responses related to a business transaction.
Pair 6: Video Streaming (Low-Priority)	IPTVV Script	This streaming script emulates a Cisco IP/TV Media Server, streaming a video file. link. The file is encoded as MPEG, and contains both audio and video elements. The send_data_rate is set at 384 kbps.
Pairs 7 and 8: File Transfer (Send) (Low-Priority)	FILESNDL.SCR	These scripts emulate sending a file from Endpoint 1 to Endpoint 2, and getting a confirmation back. The default file size is 100,000 bytes.

3.3 TEST CASES

We first conducted baseline tests to establish metrics for the throughput of the mission-critical data traffic applications from the Chariot when no congestion was present on the 1 Mbps link and under congested link conditions, without using WiseWan traffic shaping capabilities. Congestion was created by adding high-volume, low-priority data traffic and a VTC representing low-priority streaming traffic that contend for the link bandwidth with the mission-critical traffic.

We then tested the effectiveness of WiseWan in providing better bandwidth management and allocation of traffic on the congested 1 Mbps link based on predefined policies. We compared the resultant throughput of mission-critical traffic applications under the WiseWan three traffic shaping schemes: Prioritization, Bandwidth Guarantees, and Bandwidth Limiting, and observed their impacts on low-priority traffic.

We conducted the following five test cases.

Test 1 – Baseline test, no congestion, without WiseWan traffic shaping capability

Test 2 – Baseline test , congested link, without WiseWan traffic shaping capability

Test 3 – Congested link, with WiseWan "Prioritization" traffic shaping

Test 4 – Congested link, with WiseWan "Bandwidth Guarantee" traffic shaping

Test 5 – Congested link, with WiseWan "Bandwidth Guarantee" traffic shaping

Test 1 – Baseline Test, No Congestion

Test 1 consisted of creating a flow of mission-critical application traffic between Hosts 128.29.1.4 (GANYMEDE) and 128.29.3.1 (IDS01), using the Chariot Endpoints software residing on both hosts. One Web HTTP application and four SAP/R3 applications, all TCP-based, were used to emulate a mixture of large and small-sized mission-critical exchanges.

The link utilization and the throughput of the single conversation running over the link were measured in both directions, inbound and outbound, using the WanXplorer Console real-time reports. The throughputs of individual traffic applications were also measured on the Chariot Console and compared with the WanXplorer Console report[1]

This test was conducted without any benefits from the WiseWan traffic management capabilities to establish a baseline for the throughput of mission-critical traffic under ideal condition (i.e., when no other traffic shares the link).

Test 2 – Baseline Test, With Link Congestion

Test 2 consisted of adding more traffic to run over the 1 Mbps link and create congestion. A video streaming application using the Real Time Protocol (RTP) was introduced between Hosts GTN_TESTER and IDS01. The application, IPTVV, emulated a video teleconference running at 384 kbps. FTP applications were also introduced between Hosts 128.1.2 (NFB1) and IDS01, emulating low-priority, data intensive exchanges.

Test 2 provided traffic setting in which three conversations with different requirements for bandwidth and latency were contending for the 1 Mbps link capacity. The test was conducted without any benefits from the WiseWan traffic management capabilities (i.e., all traffic was treated equally) to establish a baseline throughput for mission-critical traffic applications under congested link condition.

The link utilization and the throughput of the three conversations running over the link were measured in both directions, inbound and outbound, using the WanXplorer Console real-time reports. Throughput of individual applications were also measured on the Chariot Console and compared with the WanXplorer Console report. The impact of link congestion on the throughput of mission-critical traffic was observed.

Test 3 – WiseWan "Prioritization" Shaping

Test 3 consisted of the same logical connections and traffic flows used in Test 2. It was first conducted, Test 3a, by setting the WiseWan traffic shaping policy to provide a "Passthrough" priority to the conversation between Hosts GANYMEDE and IDS01

[1] The Chariot Console provides throughput measurements for each individual application script while the WanXplorer measure the total throughput of conversation between two hosts. One should add the measured throughputs on the Chariot and compare it with the WanXplorer measurement.

carrying mission-critical applications. All other traffic was identified as default priority "Medium" traffic.

The link utilization and the throughput of the three conversations running over the link were measured in both directions, inbound and outbound, using the WanXplorer Console real-time reports. Throughput of individual applications were also measured on the Chariot Console and compared with the WanXplorer Console report.

Observations were made of performance enhancements to the throughput of mission-critical applications that resulted from activating the WiseWan "Passthrough" capability as well as the impact on other traffic throughput.

Test 3 was then repeated, Test 3b, with the WiseWan traffic shaping policy set to provide a "High" priority to the conversation between Hosts GANYMEDE and IDS01 carrying mission-critical applications, while all other traffic remained at the default priority.

Test 4 - WiseWan "Bandwidth Guarantee" Shaping

Test 4 consisted of the same logical connections and traffic flows used in Test 2. It was first conducted, Test 4a, by setting the WiseWan to guarantee a minimum bandwidth of 400 kbps in both directions to the conversation between Hosts GANYMEDE and IDS01 carrying mission-critical applications. All other traffic was identified as default "Medium" priority traffic.

The link utilization and the throughput of the three conversations running over the link were measured in both directions, inbound and outbound, using the WanXplorer Console real-time reports. Throughput of individual applications were also measured on the Chariot Console and compared with the WanXplorer Console report.

Observations were made of performance enhancements to the throughput of mission-critical applications that resulted from activating the WiseWan "Bandwidth Guarantee" capability as well as the impact on other traffic throughput.

Test 4 was repeated, Test 4b, with the guaranteed bandwidth for the conversation between Hosts GANYMEDE and IDS01 carrying mission-critical traffic was 300 kbps.

Test 5 - WiseWan "Bandwidth Limiting" Shaping

Test 5 consisted of the same logical connections and traffic flows used in Test 2 and was set to examine the WiseWan "Bandwidth Limiting" scheme for traffic shaping. It was conducted by setting the WiseWan to limit the bandwidth consumed by conversation between Hosts GTN_TESTER and IDS01 (carrying low-priority FTP traffic) to 100 kbps.

The link utilization and the throughput of the three conversations running over the link were measured in both directions, inbound and outbound, using the WanXplorer Console real-time reports. Throughput of individual applications were also measured on the Chariot Console and compared with the WanXplorer Console report.

Observations were made of performance enhancements to the throughput of mission-critical applications that resulted from activating the WiseWan "Bandwidth Limiting" capability as well as the impact on other traffic throughput.

4.0 TEST RESULTS

Baseline Tests: Test 1 results provided a baseline throughput of 799 kbps (inbound) for mission-critical traffic between Hosts 128.29.1.4 and 128.29.3.1, in an ideal condition (i.e., with no congestion and no other traffic sharing the link). When high-volume, low-priority FTP traffic and video streaming traffic were injected on the link emulating two new conversations between host pairs 128.29.1.1 and 128.29.3.1, and 128.29.1.2 and 128.29.3.1 in Test 2, the throughput of the mission-critical traffic plunged to 187 kbps (a 77% reduction) due to the link congestion.

WiseWan Traffic Shaping Tests: The results of the WiseWan traffic shaping testing (Tests 3, 4, and 5) indicated all three traffic shaping capabilities worked well to provide effective performance advantage to the mission-critical traffic applications on the congested link in accordance with specified policies. The three traffic shaping schemes delivered various distinctive results to the throughput of mission-critical traffic. The low-priority video streaming traffic was still allowed to flow. However, the impacts of these schemes on the lower-priority traffic were different.

Table 2 provides a comparison of the traffic shaping results on throughput of mission-critical and low-priority traffic.

Table 2: Comparison of WiseWan Traffic Shaping Test Results

Test	Mission-Critical Data Traffic Throughput (kbps)	Low-Priority Data Traffic Throughput (kbps)	VTC Traffic Throughput (kbps)
Test 1 - No low-priority traffic, no link congestion (No Traffic Shaping)	799	0	0
Test 2 - Congested link (No Traffic Shaping)	187	380	384
Test 3a - "Passthrough" Priority	521.8	50	384
Test 3b - "High" Priority	334	240	384
Test 4a - 400 kbps "Bandwidth Guarantee"	549	30	384
Test 4b - 300 kbps Bandwidth Guarantee	529	50	384
Test 5 - 100 kbps "Bandwidth Limiting"	469	100	384

(Note that the effective link bandwidth available for sharing between the mission-critical and low-priority data traffic types is about 600 kbps, since the video streaming traffic occupied a fixed 384 kbps portion)

The WiseWan "Prioritization" traffic shaping capability increased the throughput of the mission-critical traffic on the congested link when marked "Passthrough" priority, but on the expense of reducing throughput of the low-priority FTP traffic to almost nil. A "High" priority setting provided balanced allocation of link bandwidth between the mission-critical and low-priority conversations while giving some advantage to mission-critical throughput.

The WiseWan "Guaranteed Bandwidth" traffic shaping capability provided distinctive advantage to mission-critical traffic but also on the expense of the low-priority FTP traffic throughput.

The WiseWan "Bandwidth Limiting" traffic shaping capability, a proactive approach to link congestion problem, delivered its expected result of limiting the link bandwidth consumption by the low-priority FTP traffic to the specified value (100 kbps) thereby freeing more link bandwidth to be consumed by the mission-critical traffic.

Figure 3 through 9 provide the graphs obtained from the WiseExplorer and Chariot consoles indicating real-time line utilization, throughput of host conversations, and throughput of individual applications for all tests, with some observations following each figure.

A Discussion

In the early stage of the WiseWan testing, both the "Prioritization" and "Bandwidth Guarantees" capabilities of the WiseWan did not work properly; that is; WiseWan did not deliver the specified prioritization advantage to the throughput of mission-critical traffic. A discussion with NetReality engineers revealed the following information about the WiseWan Shaper operation.

The "Prioritization" and "Bandwidth Guarantees", both adaptive shaping schemes, become effective only when congestion on the line exceeds a specific congestion threshold. The congestion threshold is set at a fixed value of 96% by the WiseWan developers.

In the earlier tests, the traffic injected on the line from the Chariot produced congestion on the line that was measured between 93 and 95 percent, apparently not congested enough for the adaptive shaping to take place. Once the traffic on the line was increased and utilization reached 96% and above, the WiseWan "Prioritization" and "Bandwidth Guarantees" capabilities were successfully realized. We have the following reservations regarding this occurrence:

1. WiseWan publications failed to provide an indication of the specific value of congestion threshold for adaptive shaping operation.
2. The congestion threshold for the WiseWan adaptive shaping is considered very high. In some cases, network users would like to have WiseWan prioritize traffic at a lesser value of line congestion.

In response to our inquiry, NetReality informed MITRE that later this year it would be releasing a shaping-per-PVC agent. This new feature will provide for priorities and guarantees in effect at all time, regardless of congestion. When implemented, this feature will remove our concern about the 96% congestion threshold for adaptive shaping.

Test 1 Results: Mission-Critical Traffic in the Absence of Line Congestion

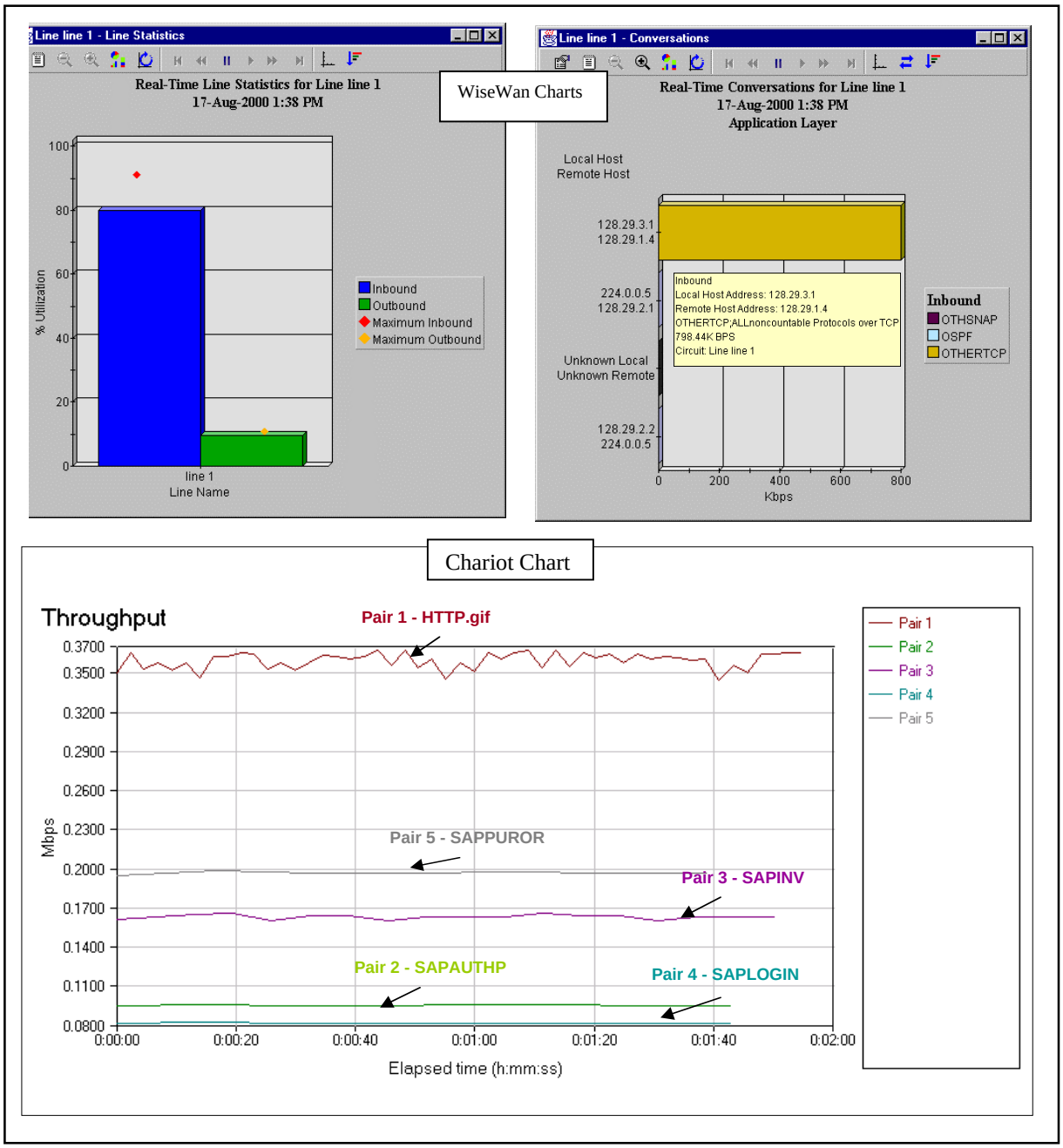

Figure 3. Real-time Line Statistics and Throughput Measurements for Test 1

Observations:

- Baseline throughput for mission-critical conversation between Hosts 128.29.1.4 and 128.29.3.1 is 799 kbps (inbound), when the 1 Mbps link is not congested.
- Bottom chart provides throughput of individual application components of mission-critical traffic generated by Chariot.

Test 2 Results: Mission-Critical Traffic in the Presence of Line Congestion

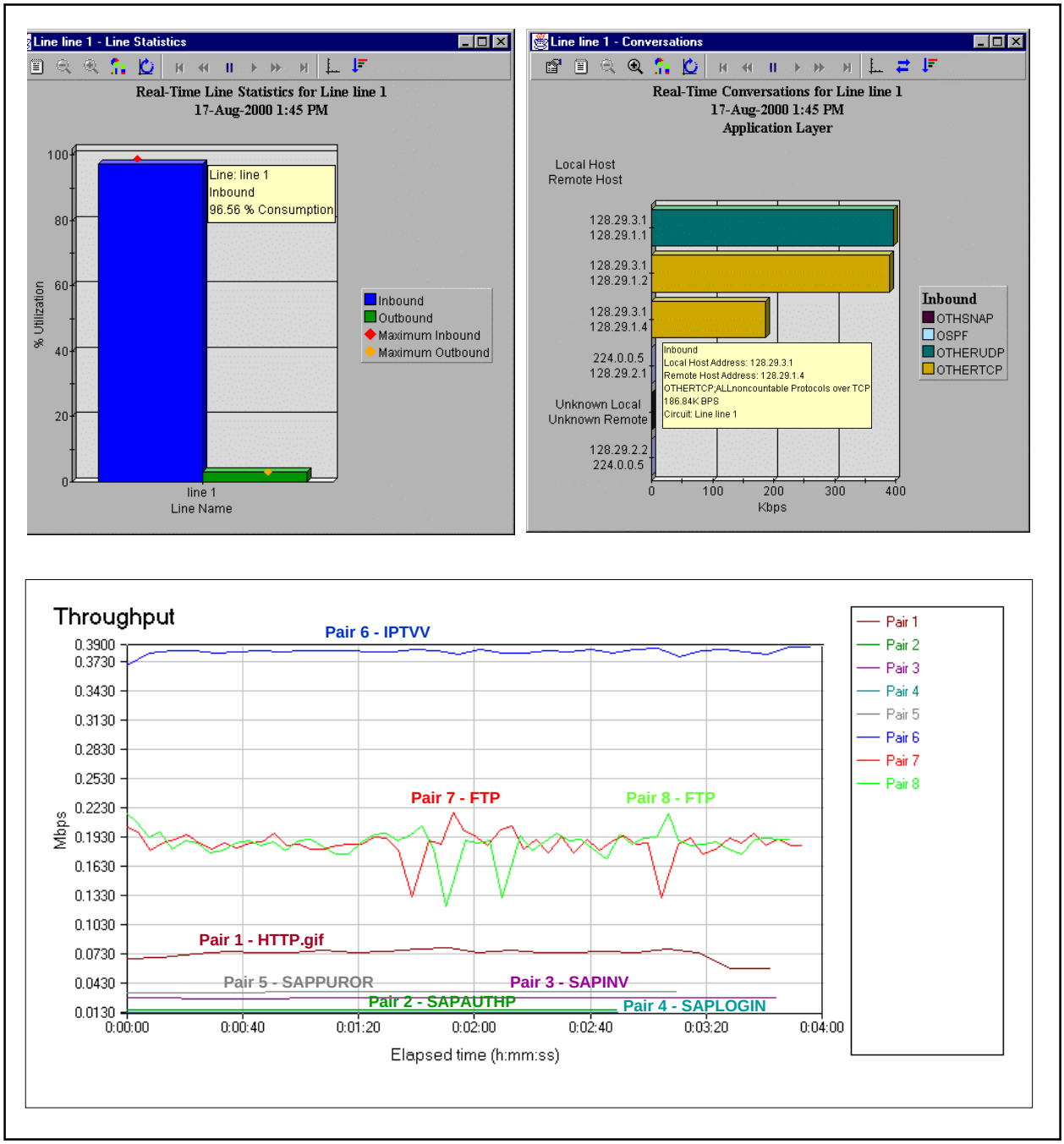

Figure 4. Real-time Line Statistics and Throughput Measurements for Test 2

Observations:

- Throughput of mission-critical conversation is significantly reduced to 187 kbps (77% reduction) because of high-volume, low-priority traffic sharing the 1 Mbps link.
- Video streaming application flows at 384 kbps and the average throughput of the combined FTP data traffic is 380 kbps.

Test 3a Results - Mission-Critical Traffic Placed at "Passthrough" Priority

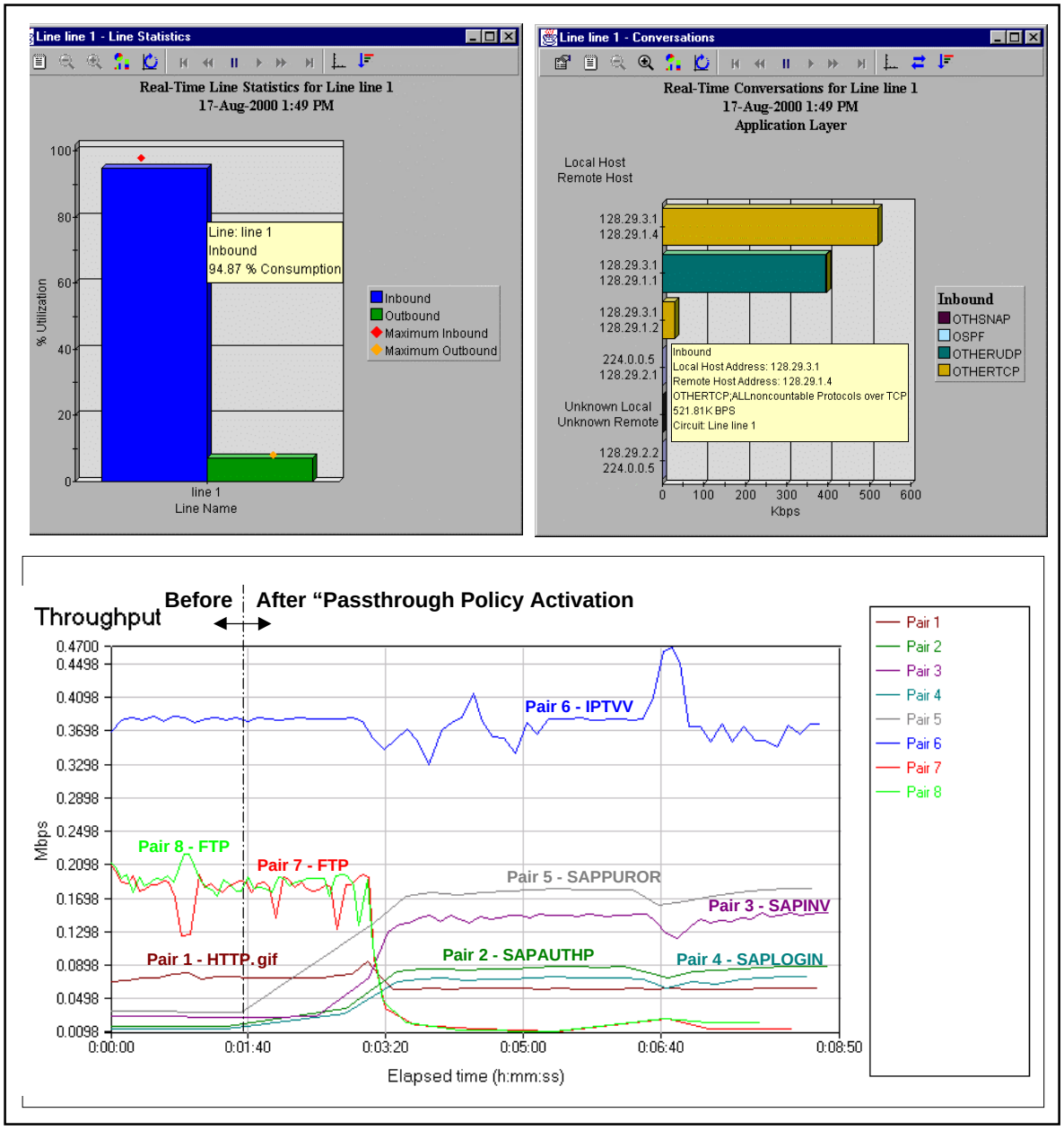

Figure 5. Real-time Line Statistics and Throughput Measurements for Test 3

Observations:

- The WiseWan delivered the mission-critical data traffic at 521.8 kbps rate when its priority was set to "Passthrough". Throughput of the low-priority FTP data traffic dropped to about 50 kbps.
- Bottom chart provides the before and after effects on throughput of all traffic applications. Observe the enhancements to mission-critical HTTP and SAP applications and degradation to FTP throughput after activation of WiseWan "Passthrough" policy.

Test 3b Repeat Results - Mission-Critical Traffic Placed at "High" Priority

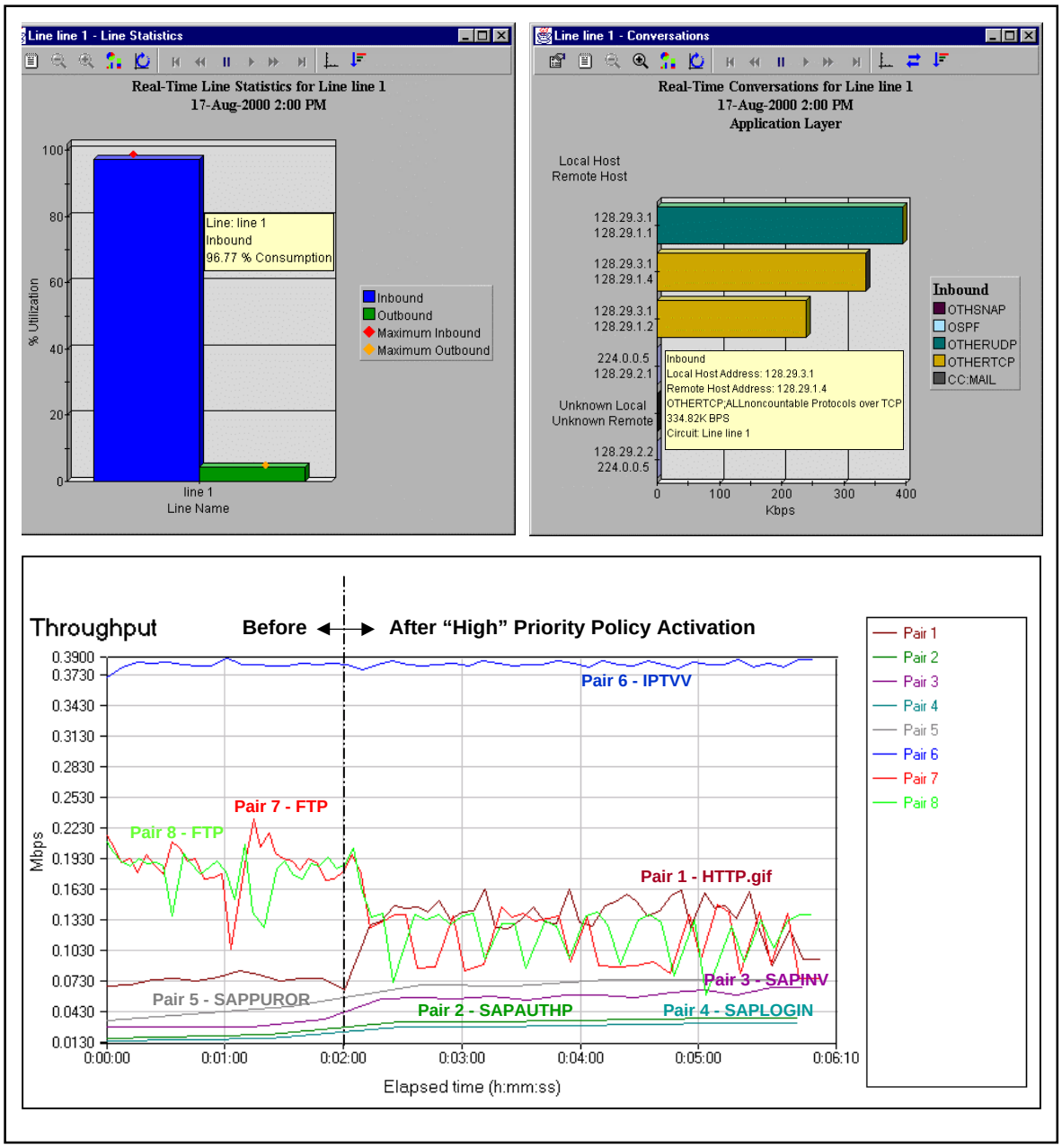

Figure 6. Real-time Line Statistics and Throughput Measurements for Test 3

Observations:

- The WiseWan delivered the mission-critical traffic at 334.8 kbps when its priority was set to "High". Throughput of low-priority FTP traffic dropped to about 240 kbps.
- Bottom chart provides the before and after effect on throughput of all traffic applications. Observe the enhancements to mission-critical HTTP and SAP applications and degradation to low-priority FTP throughput after activation of "WiseWan "High" priority policy.

Test 4a Results - Mission-Critical Traffic "Bandwidth Guarantee" Set at 400 kbps

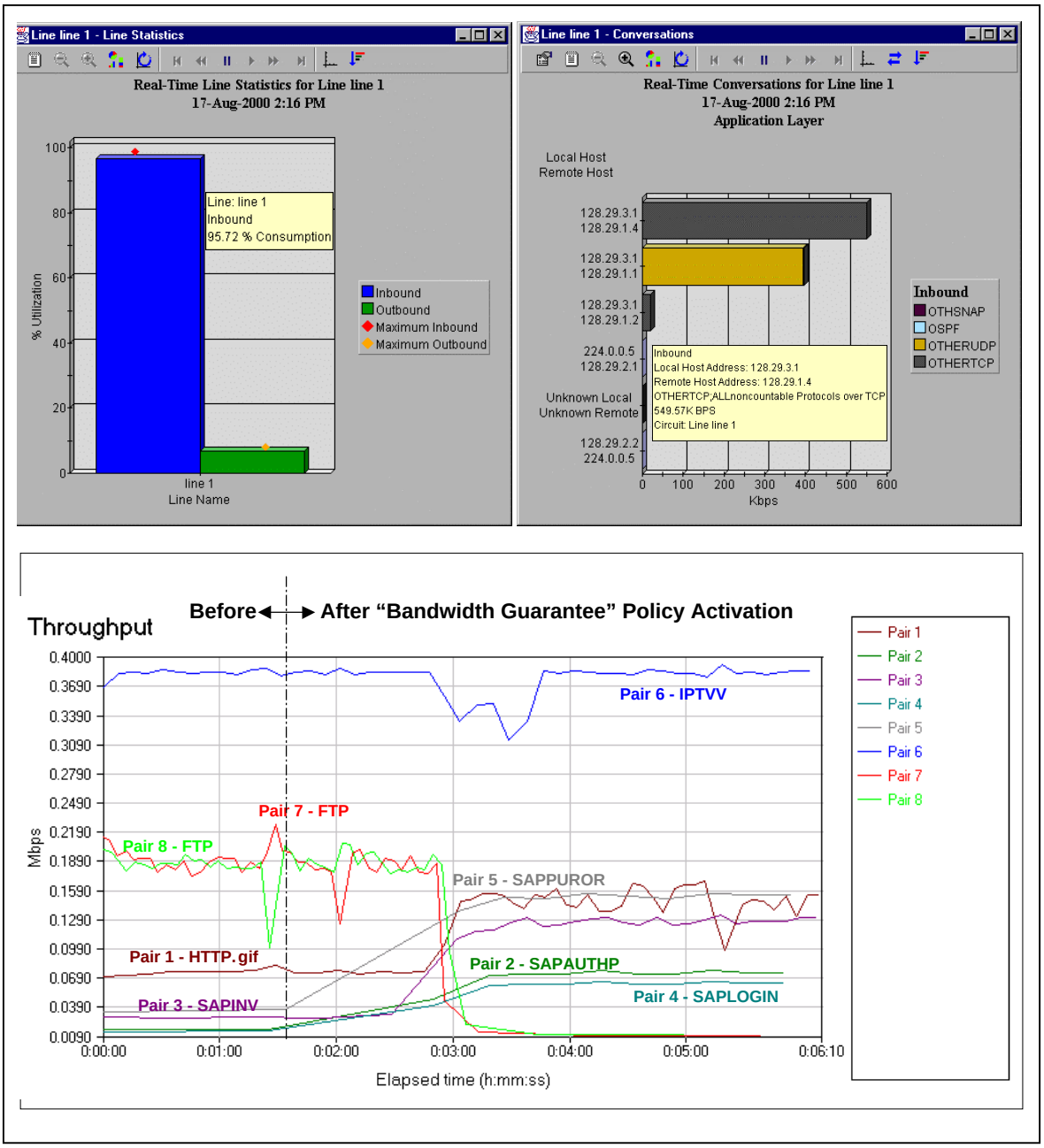

Figure 7. Real-time Line Statistics and Throughput Measurements for Test 4

Observations:

- The WiseWan delivered the mission-critical traffic at 549.5 kbps when "Bandwidth Guarantee" shaping set to 400 khz. Throughput of FTP traffic plunged to about 30 kbps.
- Bottom chart provides the before and after effect on throughput of all traffic applications. Observe the enhancements to mission-critical HTTP and SAP applications and degradation to low-priority FTP throughput after activation of policy.

Test 4b Results - Mission-Critical Traffic "Bandwidth Guarantee" Set at 300 kbps

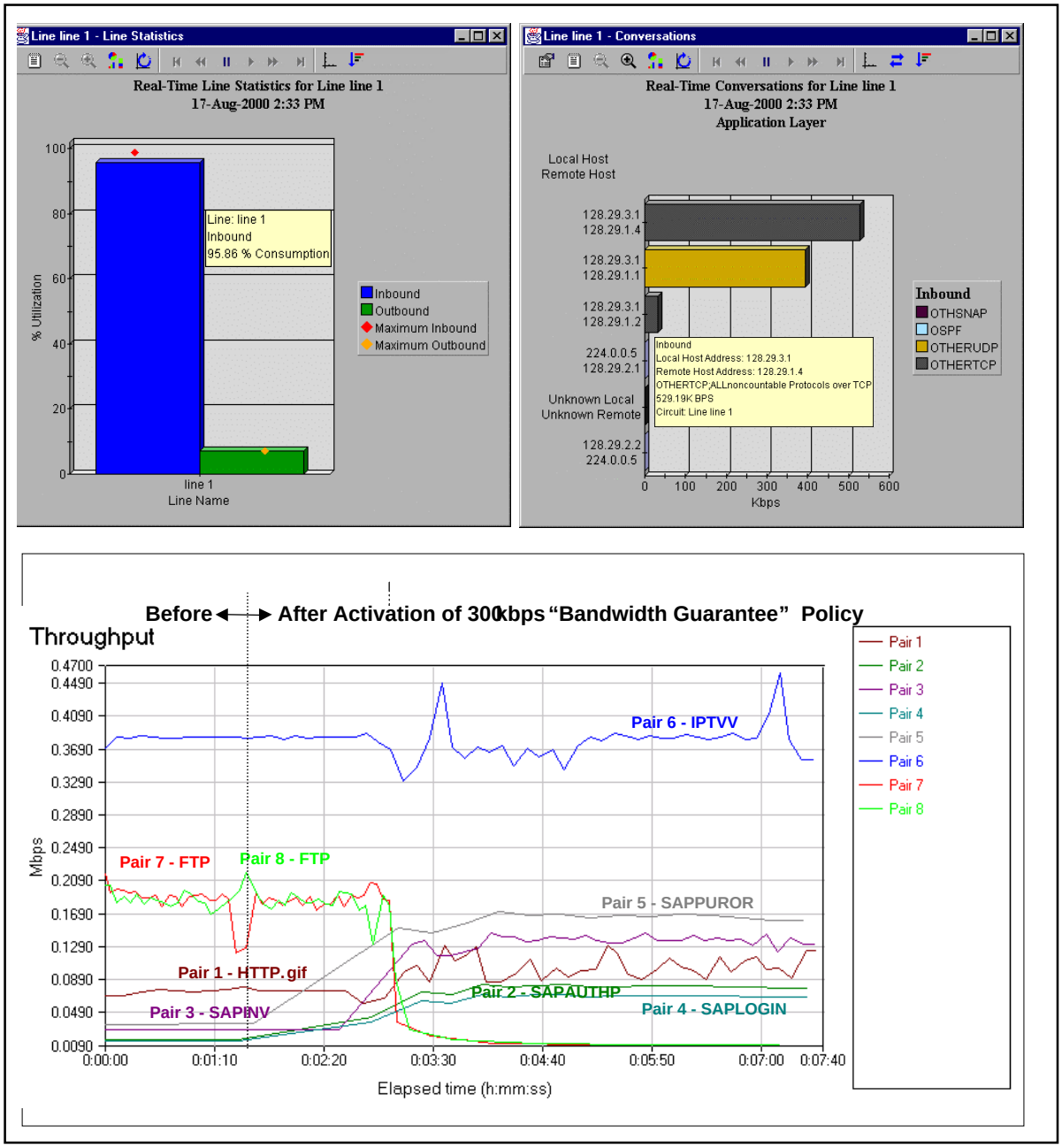

Figure 8. Real-Time Line Statistics and Throughput Measurements for Test 4

Observations:

- The WiseWan delivered the mission-critical traffic at 529.2 kbps when "Bandwidth Guarantee" shaping is set to 300 khz. Throughput of FTP traffic plunged to 50 kbps.
- Bottom chart provides the before and after effect on throughput of all traffic applications. Observe the enhancements to mission-critical HTTP and SAP applications and degradation to low-priority FTP throughput after activation of policy.

Test 5 Results - Low-Priority FTP Traffic "Bandwidth Limit" Set at 100 kbps

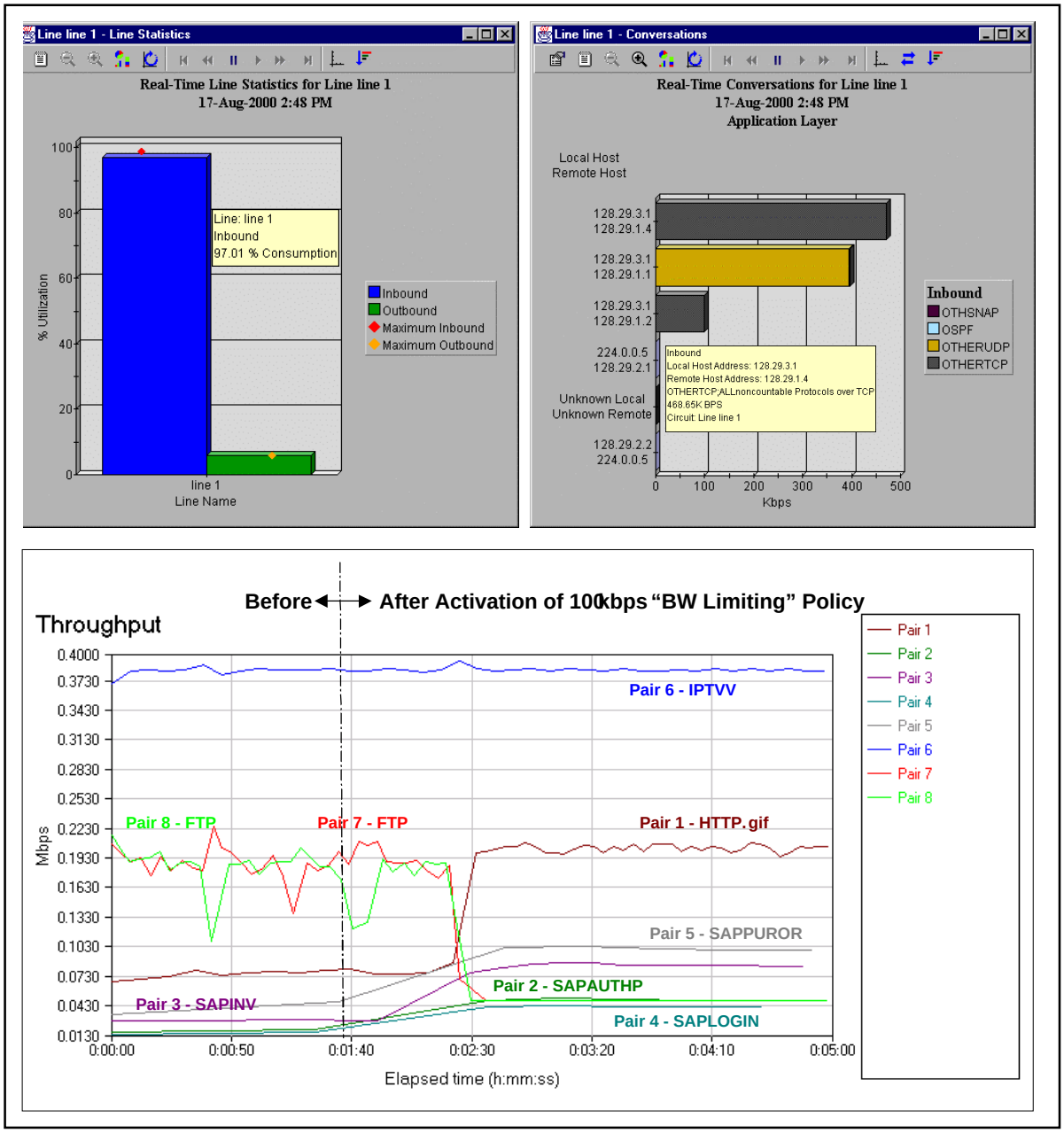

Figure 9. Real-time Line Statistics and Throughput Measurements for Test 5

Observations:

- The WiseWan delivered the mission-critical traffic at 469 kbps when "Bandwidth Limiting" shaping is set to cap throughput of FTP traffic to 100 kbps.
- Bottom chart provides the before and after effect on throughput of all traffic applications. Observe the enhancements to mission-critical HTTP and SAP applications and the limiting of each FTP application throughput to 50 kbps after activation of traffic shaping policy.

5. SUMMARY OF FINDINGS AND CONCLUDING REMARKS

We have tested the WiseWan traffic shaping performance at the MITRE's PC/LAN Laboratory and demonstrated that the WiseWan effectively identified and provided preferential treatment to traffic marked as mission-critical while adhering to user-specified rules and priorities. We have also demonstrated that the WiseWan traffic-shaping capabilities delivered distinctively high throughput for the mission-critical traffic in the presence of link congestion and with other traffic sharing the network links. We conclude that the WiseWan traffic shaping and monitoring capabilities have some merit that warrant considering it for use in DoD operational deployed networks for managing bandwidth usage. However, more extensive evaluation in a more realistic network environment is recommended.

By its nature, the testing in a laboratory's controlled environment is limited to the network configuration at hand as well as the types of traffic applications utilized in the tests. We note here that we have not tested some of WiseWan traffic classification capabilities because of testing environment and time limitations. This includes, for example, testing of the traffic classification by port because the Chariot's traffic applications utilize non-standard TCP ports. We therefore recommend that the laboratory testing be followed by conducting further testing and evaluation of the WiseWan traffic shaping and monitoring capabilities in an operational network environment that include both frame relay and leased line services for a few months.

Before WiseWan can be considered for implementation in DOD operational deployed networks, there are several non-trivial implementation issues that require special consideration. First, the guidelines for typical implementations of QoS networking in deployed networks are to be developed. Second, the traffic shaping mechanisms that would best be implemented to provide performance advantages to mission-critical traffic while balancing traffic loads on network links should be carefully selected to make as many users as happy satisfied, in a balanced result which meets threshold for entire traffic. (As noted in the test results in Section 4, some algorithms worked to increase the throughput of traffic marked for preferential treatment while crushing other traffic throughput.) Third, it is important to investigate the QoS capabilities and queue management mechanisms that would be implemented in network routers in combination with WiseWan traffic shaping and monitoring capabilities to provide increased preferential advantage to mission-critical traffic.

It is hoped that the evaluation of the WiseWan in an operational network environment for few months would help provide guidelines to some of these considerations.

APPENDIX A

TECHNICAL SPECIFICATIONS OF NETREALITY WISEWAN

A.1 WISEWAN ARCHITECTURE

A.1.1. WiseWan™ Three Tier Data Flow Management System

A.1.1.1 Accelerator

- High powered hardware platform, enabling wire speed packet processing.
- Multi-module embedded agent software, using a standard based operating system.
- Topology-neutral CPE that can be deployed anywhere between the router and the switch.
- Standard based SNMP management that can be managed by any SNMP manager.

A.1.1.2 WanXplorer Server

- Central management software running on Sun/Solaris or MS/ Windows NT, using an industry standard SQL database. Enables easy integration with third party applications.
- Management of multiple accelerators from one central location.
- Standard based integration with leading management platforms, such as HPOV and CiscoWorks.

A.1.1.3 WanXplorer and WanShaper GUI

- Management Console GUI JAVA application that can be executed as an application, or through a Web browser.
- Configure Shaper policies.

A.2 WISEWAN ACCELERATOR MODULES

A.2.1 WanShaper™ Bandwidth Management and Traffic Shaping

- Queuing and priority based traffic shaping.
- Adaptive shaping based on real-time circuit based traffic monitoring.
- Policy based bandwidth management of integrated voice and data traffic.
- Rule based priority scheme classified by users, caller/destination, servers, applications and time of day.
- Optimization of Frame Relay congestion control.
- Monitoring of actual shaping performance for policy optimization.
- Embedded Web support for standalone operation.

A.2.2 WanTel™ On-the-WAN Voice & Data Traffic Management

- Enhanced management and control facilities for voice-over-WAN traffic.
- Monitoring and analyzing integrated voice sessions.
- Prioritizing voice and data transmissions for best bandwidth utilization.
- Accounting of voice and data by conversation parties, VoIP session type, time-of-day, conversation length and data used.
- Voice Service Level reports.
- Standard Voice over Frame Relay (VoFR) traffic monitoring.

A.2.3 WanSentry™ Real-time Monitoring and Analysis

- Full featured RMON2 WAN monitoring capabilities up to Layer 7.
- Physical Line monitoring, Layers 1 and 2.
- Minimization of bandwidth consumption for monitoring functions using efficient SNMP based get bulk mechanism.

- Storage of history information for short and long intervals spanning several hours.

A.3 WANXPLORER™ AND WANSHAPER™ MANAGEMENT APPLICATION

A.3.1 Server Module

- Real-time and long term MIB2, Frame Relay, RMON1, RMON2 and proprietary MIB statistics collection.
- Trap based network health monitoring.
- Maintenance-free historical database.

A.3.2 WanShaper Client GUI Module

- Configure WanShaper policies.
- Support configuration of traffic by the following classifications:
  - Applications, including VoIP, Citrix, URL and Mime types.
  - Direction (client and server).
  - Local or remote hosts.
  - Time of day.
  - Line or PVC.
- Support configuration of traffic enforcement actions based on:
  - Five traffic priorities
  - Bandwidth guarantee and limit per traffic classification or conversation.
  - Block traffic.
- Policy classifications that can be used repeatedly including:
  - **Classes:** Defines groups of protocols of the same nature.
  - **Hosts:** Defines IP/IPX networks, IP subnet, or group of IP/IPX hosts.
  - **Schedule:** Defines weekly schedules.
- Supports backup and propagation of policies.
- Enforcement of user authentication.

A.3.3 WanXplorer Client GUI Module

- Supports remote monitoring & analysis.
- Accessible from any web browser, or can run as a standalone JAVA application.
- Hierarchical presentation of the corporate network in a tree format.
- Supports collapsed and expanded hierarchies.
- Automatic detection of line and PVC status.
- Color-coded health indicators for every resource controlled by the system.
- User defined groups of Accelerators, Lines, PVCs, Protocols, Classes and Users.
- Real-time event viewer per System, Line, and PVC, including severity indicators.
- Performance reports for a single Accelerator or a group of Accelerators, Lines, and PVCs.
- Long term historical reports.
- Long term trend reports automatically adjust the report resolution according to report span.
- Intuitive zoom in analysis flow enabled by a drill down option between reports.
- Default drill down from an aggregate instance to a trend report.
- Access control per user views, user authentication.
- Extensive report filters.
- Online Help facility.

A.3.4 Analysis Reports

- Line status and utilization.

- T1: Loss of Signal, BPV, Out of Frame, Red/Yellow/Blue Alarm, Error Seconds, Severely Error Second, Unavailable Seconds, Controlled Sleep Seconds, Path Coding Violations, Line Error Seconds, Bursty Error Seconds, Degraded Minutes, Line Code Violation.
- Top DLCI by voice and data traffic, CIR load, and frames.
- Line consumption by PVC.
- PVC status & performance.
- Network and application layer reports such as, protocol distribution, top conversations, top hosts/callers, conversation trends.
- Shaping performance reports.
- Accounting reports for voice and data.

A.3.5 SLA Reports

- Availability analysis (MTBF, MTTR, line availability).
- Service Level Agreement breaches summary (line availability, response time, congestion).
- Service Level Agreement detailed breaches.
- WAN round trip delay monitoring.

A.3.6 Server Platform

- Sun/Solaris 2.5.1,2.6 and 2.7
- Windows NT server/workstation 4.0

A.3.7 GUI Platform

- MS/Windows 95/98/NT platforms
- Sun/Solaris 2.5.1,2.6,2.7
- MS/IE 4.X, 5.X

A.4 WISEWAN 50™/100™/200™/230™ ACCELERATOR

Part Number	Product name	Form Factor	Line Type	# of Lines	Speed
WW50D-SER	WiseWan 50-SER	Desktop	Serial	1	56/64Kbps
WW50D-CSU	WiseWan 50-CSU	Desktop	CSU/DSU	1	56/64Kbps
WW100R-SER	WiseWan 100-SER	Rack Mount	Serial	1	Up to 384Kbps
WW100D-SER	WiseWan 100-SER	Desktop	Serial	1	Up to 384Kbps
WW100R-CSU	WiseWan 100-CSU	Rack Mount	CSU/DSU	1	Up to 384Kbps
WW100D-CSU	WiseWan 100-CSU	Desktop	CSU/DSU	1	Up to 384Kbps
WW201R-SER	WiseWan 201-SER	Rack Mount	Serial	1	Up to 2Mbps
WW201R-CSU	WiseWan 201-CSU	Rack Mount	CSU/DSU	1	Up to 2Mbps
WW230-CEI	WiseWan 230-CEI	Rack Mount	Serial	1	Up to 2Mbps
WW230-CTI	WiseWan 230-CTI	Rack Mount	Serial	1	Up to 2Mbps

A.5 SUPPORTED INTERFACES

A.5.1 Serial Modules (SER)

Configuration options	Line, Serial
Speed	56K up to 5Mbps (according to model)
Input Interface Type	V.35, X.21, RS232, RS449, EIA530, X.24
Output Interface Type	Same as input
Cable	WiseCable™ fault tolerant serial cable

A.5.2 CSU Modules (CSU)

Configuration options	T1/E1 CSU/ DSU with Drop & Insert Inline T1/E1, Inline channelized E1/T1

A.5.3 WAN (Network)

Speed	(1-24/30) x 56/64Kbps
Interface type	RJ48C or BNC
Frame type	SF, ESF
Line code	B8ZS, AMI, HDB3, B7ZS
Signaling	Robbed bit D4 or ESF, CCS, CAS
Standards	G.703, G.704, G.706, G.823, G.824

A.5.4 Serial

Speed	56K up to 2.048Mbps
Interface type	V.35, X.21, RS232, RS449, EIA530, X.24

A.5.5 T1/E1 (User)

In inline mode	Same as WAN Network
In CSU/DSU mode	Same as WAN Network

A.6 Management Interface

Ethernet	10Base-T
Serial Port	19.2Kbps Asynchronous
WAN	Dedicated or shared PVC

A.6 Hardware Specifications

A.6.1 19” Rack Mount (WiseWan 100/200/230)

Dimensions	17.52 (445mm) Width, 14.57 (370mm) Depth, 1.75" (1U) Height
Power	85 to 265 VAC 47 to 440 Hz, (Internal)
Environmental	0-50°C, 5 to 95% Humidity Non-condensing
Memory	16/32MB DRAM and 4MB flash
Weight	15.4 lb. (7kg)

A.6.2 Desktop (WiseWan 50/100)

Dimensions	11.62 (296mm) Width, 11.65(295mm) Depth, 2.56" (65mm) Height
Power	85 to 265 VAC 47 to 63 Hz (External)
Environmental	0-40°C, 5 to 95% Humidity Non-condensing
Memory	16MB DRAM and 4MB flash
Weight	5.3 lb (2.4kg)
EMC	FCC Part 15, CE

A.7 WISEWAN STANDARDS AND PROTOCOLS SUPPORT

A.7.1 Link Layer Support

Frame Relay, HDLC, PPP, Bay PPP, Timeplex

A.7.2 Frame Relay Standards

- ITU Q.922, Q.933, ANSI T.617 Annex D, Group of four LMI, No LMI
- FRF 3.1, RFC1490 Protocol encapsulation over Frame Relay, Cisco Encapsulation, Cisco TCP Header Compression

A.7.3 Network and Transport Layer Protocols

LLC, SNAP, VSNAP

IP, IPX, SNA, NETBIOS, APPLE TALK, ARP, XEROX

VIP, VECO, DRP, AARP, NCP, SAP, DIAG, TCP, UDP, ICMP, OSPF, RIP,

BRIDGED, BRIDGED ETHERNET, BRIDGED TOKENBUS, BRIDGED FDDI, BRIDGED 802.6, BRIDGED FRAGMENTED, BRIDGED BPDU

A.7.4 Application Layer Protocols

- Over 350 TCP/IP application protocols and additional user defined TCP and UDP ports.
- Supports Citrix MetaFrame Applications, HTTP Mime types and URL.
- Oracle database application or user name
- IPX application protocols.

A.7.5 Voice Over Data Network Standards

VoIP Standards ITU-H.323, H.225, H.245. T.120 RTP, CISCO RTP Header Compression

A.7.6 Network Management Standards

- MIB2 system and interface group.
- RFC1406 T1 MIB.
- RFC1757 RMON1 Alarms, Events.
- RFC2021, RFC2074 RMON2.
- RFC1315 Frame Relay MIB.
- NetReality Application Proprietary MIB, including voice & data monitoring extensions.

A.7.7 Trap Support

Accelerator	Up, Reset, Authentication Failure, Short on Resources, Diagnostic Failure.
Line	Up, Down, Utilization and Error, Rising and Falling alarm, T1 Signal Change.
DLCI	Create, Remove, Utilization out of CIR, FECN and BECN Rising and Falling alarms.

NetReality Proprietary traps

A.8 New Features/Releases

- A WiseWan shaping-per-PVC agent will be released late year 2000. This new feature will provide for priorities and guarantees in effect at all time, regardless of congestion.

- Other new product introductions to be released in the year 2000 include support for HSSI and a T3/E3 WiseWan. This high-speed platform will be used to upgrade to ATM and OC3 in 2001.