

assessment was the router configuration. There were a total of 426 different tests run on both the individual (IOS) routers and (CatOS) switches as well as the total network as a whole (the latter involving simulating traffic on the network to determine the viability of the routing configuration between routers and switches).

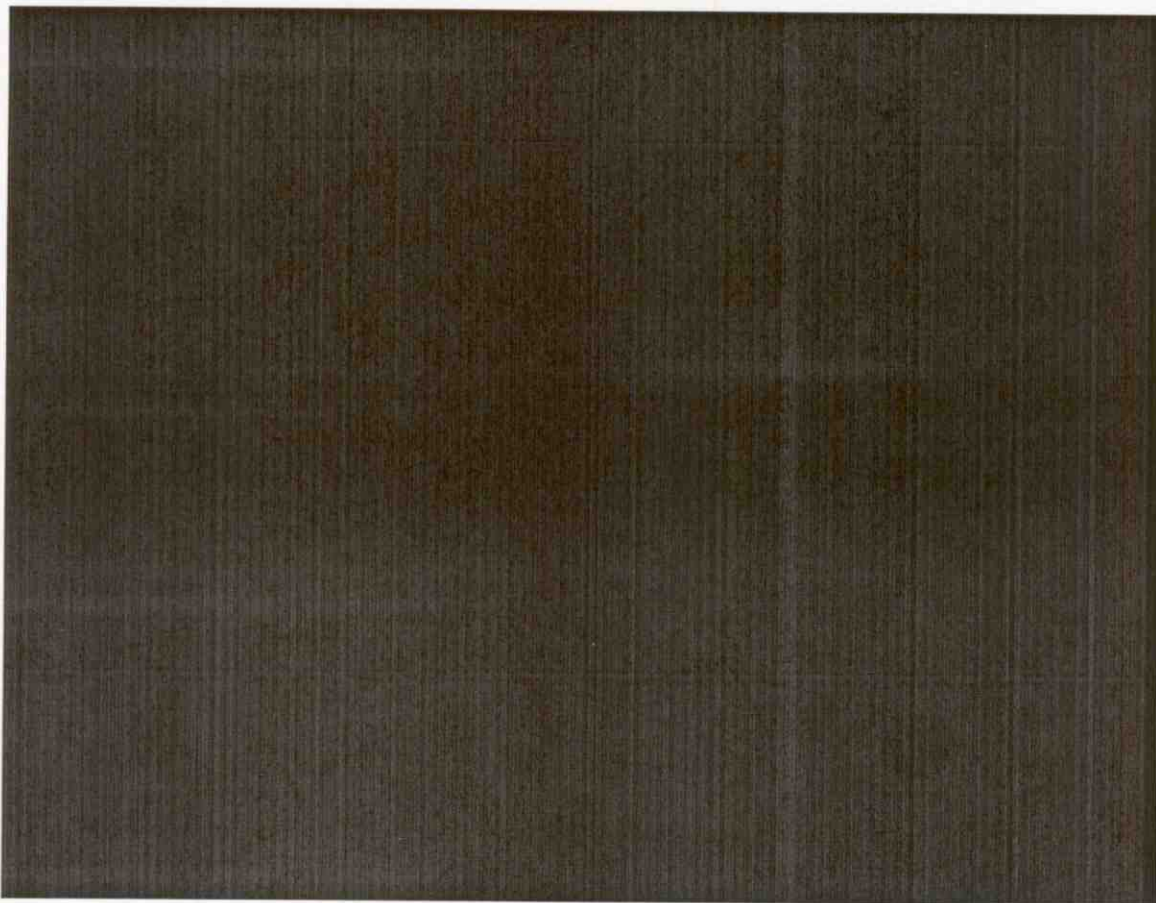


Figure 4-6. [Redacted]

Of the 426 test that were run, no major errors were detected [Redacted]

[REDACTED]

4.6 System Performance Monitoring

The team obtained information from interviewed employees of HEC, ITD, HFD, HPD, Greater Harris County 9-1-1 Emergency Network, and Northrop Grumman to discuss how the performance of the systems were monitored. [REDACTED]

[REDACTED] The team primarily focused on the monitoring capability for the HEC portions of the public safety system and the ITD networks. A similar analysis needs to occur for the HPD and HFD systems.

During interviews with ITD, MITRE was informed that the ITD may set up a Network Operations Center (NOC) to provide centralized network management functions for several organizations including HEC. The idea is still at early inception stage and the scope focuses only on detecting network outage alarms and providing centralized problem resolution in a timely manner. The NOC will also report uptime and downtime statistics. In other words, the function of the planned NOC is mainly to react to incidents when they occur. [REDACTED]

[REDACTED]

The Scope of Service identifies requirements for system performance monitoring. During interviews with HEC IT staff and Northrop Grumman, MITRE attempted to gain an understanding of what tools were in place and how they were used for monitoring and reporting system performance.

The interviews showed that the system is not being adequately monitored and reported. Basically, the HEC IT staff and Northrop Grumman have a process for system monitoring and reporting on an as needed basis. This process is put in place whenever an outage or significant lack of performance occurs. The process that is in place during normal operations is not clear.

The following paragraphs provide a brief description of possible network monitoring tools that could be used. Some of these capabilities exist in Northrop Grumman's existing configuration but are proprietary. The City of Houston should determine if these proprietary tools could provide the monitoring capabilities needed or if commercial tools are needed.

Performance monitoring and reporting tools fall into three broad categories that are applicable to the system:

- Client monitoring
- Network and server monitoring
- Application-level monitoring

The client monitoring tools gathers metrics about the end-user experience, such as response time for specific interactions in the application. It may be useful for measuring CAD Transaction Response, as defined in Section 15.10.3 of the Scope of Services. [REDACTED]

[REDACTED] However, these applications are data-intensive and should only be used as a tool to occasionally gauge the system load to aid in the decision on allocating resources.

Network and server monitoring tools monitor the performance of system infrastructure, connection status, and assist in error detection. They usually use SNMP and RMON agents with real-time event filtering for fault alerting and problem resolution. For non-SNMP equipment, a protocol mediation solution or a proxy agent can mediate standard alarm outputs from various types of equipment to SNMP. They can collect statistics and report throughput, uptime, data link utilization, CPU usage, packet loss, packet latency, etc. Some platforms may also be able to check on connections involved with any given application and provide information about the host server as well. Basic SNMP statistics collection, storage, exception reporting ("Top-N" lists, etc.) and historical trend graphing are built in to most of the major network monitoring platforms, and there are a number of commercial products focused specifically on performance. Concord Communications is one of those with the broadest coverage and largest customer base. HP OpenView series of solutions also provide comprehensive monitoring capabilities. There are also open source tools (MRTG is widely used). HEC is currently considering adopting a network performance monitoring tool.

It must be noted that generic tools used for monitoring network performance usually are not capable of detecting application-level problems. A better approach for application-level monitoring is application instrumentation, which involves writing specific code within an application to check key transaction performance indicators, such as message queue length, waiting time, and completeness of transaction. It may also report other measurements; e.g., response time, database connectivity, system load, etc. An application-monitoring tool may help avoid some of the incidents; e.g., B4, B5, B6, B9, B10, and A2 from happening again.

A caveat application instrumentation is an invasive method that requires modifying the original application and may be too resource-intensive. The Application Response Measurement (ARM) and Application Instrumentation and Control (AIC) technical standards and APIs have been published by an industry consortium for some years and adopted by a number of leading providers of performance monitoring tools. The system managers can monitor transactions by using simple function calls embedded in the application code. An agent captures these calls and sends them to an ARM or AIC reporting application, such as the IBM Tivoli Management Environment platform. This popular platform is by far one of the best solutions in the industry to enable end-to-end management of all elements in a multi-vendor environment, from the network, to computers, to applications and databases, and to business management of IT services. Northrop Grumman has stated that the ARM tech suite is installed by default. The tool can monitor CPU performance by user and additional functions are available through all-on licenses.