T-Synergy Corporation

Managing Video Networks

Abstract

The videoconferencing industry is slowly moving from ISDN circuit switched networks to IP packet switched networks because of easy integration with desktop computers and significantly lower cost for equipment, data transport, and contractor support.

The major problems inherent in carrier grade and enterprise grade network management are a result of a vendor-centric testing viewpoint that concentrates on reported problems (reactive troulbleshooting) with the individual pieces of equipment rather than on the proactive functioning of the network. The equipment and systems available are usually intended for one vendor's equipment and one data transport and protocol. They are poorly suited to migration from legacy systems to new standards. They are poorly suited to large networks with multiple vendors.

Carrier-grade and enterprise-grade videoconferencing systems require user interfaces that are independent of data transport and protocol technology and independent of vendor's proprietary interfaces. They need the simplicity of functional test selection and knowledge-base assisted test result interpretation. By designing from the carrier/enterprise point of view, such systems can be provided.

Contents

Managing Video Networks

Introduction

The videoconferencing industry is slowly moving from ISDN circuit switched networks (H.320 protocols) to IP packet switched networks (H.323 protocols). H.323 is the standard for new videoconferencing equipment because of easy integration with desktop computers and significantly lower cost for equipment, data transport, and contractor support. Most of the existing end-user (codec) and infrastructure (gateways, MCUs, etc.) equipment is still H.320. Managing a video network has been notoriously difficult with ISDN networks, because of factors such as bonding and inverse multiplexing. It is far more difficult and expensive to manage hybrid networks that include both ISDN and IP.

The major problems inherent in the current network management approach are a result of a vendor-centric viewpoint that concentrates on reported problems (reactive troulbleshooting) with the individual pieces of equipment rather than on the proactive testing of the network. Test equipment and systems exist to diagnose individual pieces of endpoint or infrastructure equipment, and to monitor networks for protocol violations and circuit failures. Most test equipment and systems are not capable of migrating from legacy equipment to newer data transport and protocols. Current test equipment and systems are not designed for easy endpoint selection, automated testing, or proactive network management. Current test equipment and systems only operate with a single data transport network and protocol. Mixed networks require separate equipment and knowledge for each segment. Current test equipment and software is difficult to use and returns complex test results that require expert knowledge to interpret. Because of the steep learning curve and low productivity of users, current test equipment and software is most suitable for tiny, homogenous networks with a small number of endpoints. In today's environment, carrier-grade and enterprise-grade videoconferencing networks may have thousands of endpoints of mixed types (ISDN and IP). A video network management system must be able to handle the demands and complexity of a combined system.

The primary requirements for today's videoconferencing network management are:

- Complexity must be hidden from the usersTechnology independent user interface
  - Integration of multiple data transport and protocol standards (ISDN and IP).
  - Encapsulation of migration details to minimize learning curve.
  - Vendor independent user interface
    - Hide variations between codec vendor's user interfaces.
    - Hide variations between test equipment vendor's user interfaces.
    - Hide variations between data transport and protocols.
    - Administrator can install competitive vendors equipment using a function-oriented interface.
    - Network managers can perform function tests on any vendor's codecs or network elements with automatic selection of appropriate test equipment.
  - Functional user interface
    - Enable users/administrators to directly monitor and control "transactions," not components.
    - Fast and easy administrative definition of endpoints.
    - Fast and easy administrative definition of network elements.
    - Fast and easy administrative definition of test equipment.
    - Fast and easy selection of endpoints for testing.
    - Automatic selection of appropriate test equipment and test sequences based on endpoint(s) selected.
- Reactive troubleshooting
  - Selection of endpoint(s) automatically determines appropriate test equipment and test sequences.
  - Selection of endpoint(s) automatically includes other participating endpoints and network elements in the same conference.
  - Fast and easy test result interpretation with "expert" knowledge base assistance.
- Proactive network management
  - Scheduling and automation
    - Pre-conference endpoint and network element testing.
    - Automatic interval testing of endpoints and network elements.
  - General network fault and alarm monitoring.
    - Communications failures.
    - Device alarms.
    - Test and protocol alarms.
    - Export alarms to other fault monitoring systems.

- Scalability
  - Network size for carrier and enterprise systems.
    - Thousands of endpoints.
    - Multiple subnetworks.
  - Multi-user environment
    - Scalable number of client workstations.
    - Centralized, remote, and localized network testing.
    - Automatic resource allocation.
  - Multiple simultaneous tests.
    - Automatic resource contention resolution and optimization.

By considering all of these requirements together, a single integrated system can be created that fulfills the network management needs of carrier and enterprise videoconferencing systems.

Functional User Interface

For carrier and enterprise grade systems, the user interface must be functional rather than endpoint device or test equipment oriented. The basic functions are administration, network status and alarm monitoring, and testing.

Administration

Administration consists of defining users, endpoint devices, network elements, and test equipment. In addition, the application itself may require support functions such as backups and report offloading.

User Administration

User administration has two requirements:

- Overall access to the system must be restricted for security.
- Individual users must be restricted to specific priviledges and functions for security.

Device Administration

- Devices are located in rooms.
- Rooms are located in locations (buildings).
  - Locations have country, state/province, and city address information.
- A company may have multiple locations.

For devices that already exist, the user should be able to select the device, administer its parameter settings, and modify administrative data such as the company, location, and room.

For new devices, if the company, location, and room already exist, the user should be able to start with the existing information. Otherwise, the company, location, and room must be created first.

Standard editing functions such as additions, modifications, and deletions apply to both administrative information and technical parameters.

Network Status and Alarm Monitoring

The alarm monitoring function collects data for the network status display. Together the alarm and status displays present information about network and device health.

Status Display

The network status display shows the received device alarms, test failures, and protocol errors or warnings for a selected subset of endpoints and network elements. Each device may be in an unknown, normal, or alarm state. Different subsets and sort orders are based on filter and sort selection controls. Filter controls formats

include device selection trees, option groups or drop-down lists. Sort controls are usually option groups or drop-down lists.

Alarm Display

The alarm display shows a list of alarms received from devices, test failures, and protocol errors or warnings. It does not include devices with normal or unknown status unless an attempt has failed to determine device status.

Alarm filtering allows alarms processing in order of priority from critical alarms (communication failure) to device major, to device minor (port). Alarm filtering also allows processing of specific types of alarms (communication, transport, device). The alarm filters also allow distribution of workload to different users based on severity or type of alarm.

Alarm History

A database of alarm history allows searches to find the history of specific devices, during a particular interval, and other criteria. This may assist network managers in determining trends or repetitive failures.

Testing

A carrier or enterprise grade network requires both reactive troubleshooting and proactive testing. In both cases, device selection depends on device identification or location rather than data transport or protocols. Automated test equipment selection depends on data transport or protocol information that is available after device selection.

Test History

A database of test history allows searches to find the history of specific devices, during a particular interval, and other criteria. This may assist network managers in determining trends or repetitive failures.

Reactive Testing (Troubleshooting)

Troubleshooting tests are usually in response to reported problems. The problem report may originate from a videoconference user, or display on the network status or alarm consoles. Troubleshooting tests usually run interactively so that the network manager can observe the results as the test progresses.

Test Selection

Reactive tests have the following general requirements for test selection:

- Tests may require operator interaction. This includes tests such as error injection tests, tests that require manual loopback, and tests that require synchronization for separate send and receive paths. Other standard tests that do not require operator interaction are also useful.
- Automatic selection of test equipment based on the endpoint(s) selected for testing minimizes operator error.
- Test equipment and resources must be dynamically allocated at the time the test is run.
- Test suite is determined by the network manager's knowledge and experience in troubleshooting problems, and/or by specific customer-defined methods and procedures.

Test Result Interpretation

To the extent possible, the results of signaling and data transport analyses display in simple form for easy problem determination. Automatic analysis based on a "knowledge base" determines the output.

Test Scheduling

Most troubleshooting tests run interactively so that the network manager can observe the results as the test progresses. The notable exception is a "soak" test that repeats at short intervals to detect intermittent problems, or to allow "healing" of network or device defects.

Proactive Testing

Proactive tests are used to verify equipment and network operation before regularly scheduled conferences, or on a regular basis to detect problems before they become service affecting. Proactive tests are generally scheduled.

Interactive troubleshooting to sectionalize and correct the problem usually follows when problems appear during scheduled proactive testing.

Test Selection

Proactive tests have the following general requirements for test selection:

- Tests should not require operator interaction.
- Test equipment must be automatically selected based on the endpoint(s) selected for testing.
- Test equipment and resources must be dynamically assigned at the time the test is run.
- Test suite must be automatically selected to stress the tested equipment or network elements enough to detect most existing or incipient problems.

Test Result Interpretation

While complete information on test results may be available, it is more important to identify devices or network elements that have problems so follow-up troubleshooting ensues. Test failure should raise device, test, or protocol alarms than can be immediately seen on the system status and/or alarm display. The general reason for test failure is usually more useful than specific test details.

Test Scheduling

Proactive test scheduling includes the following:

- Once, at a specific time, on a specific date
- Hourly, at a specific number of minutes after each hour from a starting time and date until an ending time and date
- Daily, at a specific time, on one or more specific days of the week
- Weekly, at a specific time, on a specific day of the week
- Monthly, at a specific time, on a specific day of the month

Scalability

Usually, scalability implies making a system bigger. However, the same ease-of-use features that make a system desirable on a large scale are also desirable for small systems. Ease-of-use features reduce the costs of training and reduce the time and cost for sectionalization. Less time spent determining problems means less time out of service and better customer acceptance.

Network Size

Network size should be linearly scalable with required equipment. The ability to accommodate multiple units of each type of test equipment is only part of the solution. Test equipment distributed throughout the network eliminates network loading. Only the equipment control information and test results need cross the network so that server capacity rather than data rate limitation controls scalability. Server capacity is easy and inexpensive to incremented as the network grows.

Distribution of protocol analysis equipment allows monitoring of subnetworks to determine subnet loading and QoS as well as routing or interworking between subnets.

Multiple Users

A client-server architecture provides networked workstations. There are several ways of distributing networked workstations:

- Keeping workstations on a single LAN allows load distribution among several users and solves jurisdictional problems. Load distribution can be based on alarm severity, alarm type, or geographic area responsibility.
- Portable (laptop) remote workstations on wide area networks allow more flexible distribution of end users and simplify some types of maintenance.

Simultaneous Tests

Most test equipment has the capacity to run more than one test at a time. Assigning specific capacities to individual users or workstations limits resource utilization when the individual users or workstations do not need the assigned capacity. Dynamic resource allocation allows both interactive and scheduled tests to be run with maximum resource optimization.

Conclusion

Carrier and enterprise grade video network management systems require independence of data transport and protocol technology. They need the simplicity of location-based device selection, automatic test equipment selection, functional test suite selection, and knowledge-based test result interpretation. The use of client-server networked workstations and distributed test equipment allow linear scalability. By designing from the carrier/enterprise point of view rather than the vendor point of view, such systems can result in lower costs for training, faster response times, less system outage, and superior adaptivity to meet users' demands.