

TEX-AN Next Generation

State of Texas Department of Information Resources

Capacity Management Plan

Network Service Monitoring

Network monitoring is the linchpin for all aspects of CenturyLink's network management scheme. We currently monitor more than 15,000 network elements globally to provide statistics and data for accounting, performance and fault management, ensure environmental stability, and monitor remotely the progress of change management activities.

Management Capabilities

At CenturyLink, we proactively optimize our network and fix potential network issues before they become service-impacting events. In order to assist in managing our Network Monitoring capabilities, we constantly analyze results and proactively update our monitoring capabilities with emerging technologies. We have stringent requirements and network report cards to help determine our progress internally. Our self-checking strategies help define future goals and implementation procedures to ensure that we are prepared to exceed the expectations of our customers.

Signaling and voice operations are supported by the Switch Management center. This center is located in Littleton, CO and is fully staffed 24x7x365. In the event of a catastrophic center failure, a back-up center is located in Denver, Colorado. Quarterly failover exercises are performed to ensure proper operations continuity.

Switch Management utilizes various network management systems (NMS) to deliver alert/log status for operator review and action. Agilent's Netexpert alarm system is used to monitor Time Division Multiplexing (TDM) alarms, as well as Signaling System 7 (SS7) alarms. Micromuse's Netcool is used to monitor SNMP alarms for the Advanced Intelligent Networks and the Next Generation Voice over IP (VoIP) softswitch technologies. HPOpenview currently monitors the Calling Card Platform, the CenturyLink Hosted Web Contact Center, and the Operator Services Platform. Work is currently taking place to migrate these platforms into Micromuse's Netcool. Tier II technicians in Switch Management maintain command and control of alarms and outages reported through the NMS. They diagnose and repair troubles, then document actions taken to mitigate the alarm condition. Tier II technicians also coordinate additional resources needed for repair and restoration with Field Operations and Advanced Technical Support.

The Advanced Technical Support/Engineering Technology Management (ATS/ETM) team manages and coordinates Configuration Management. Dedicated lab resources are used within engineering to regression test any change to production. Any problems identified during testing are addressed by the team before implementation into production is allowed. Once an optimal configuration is established, the templates are stored and used as the golden configurations for the network deployment and implementations to the production environment.

ATS/ETM establishes provisioning guidelines that are based on the engineering limits of the product and the results from capacity testing in the lab. These guidelines are turned into procedural documents for workgroup use. This prevents load balance issues from occurring at installation.

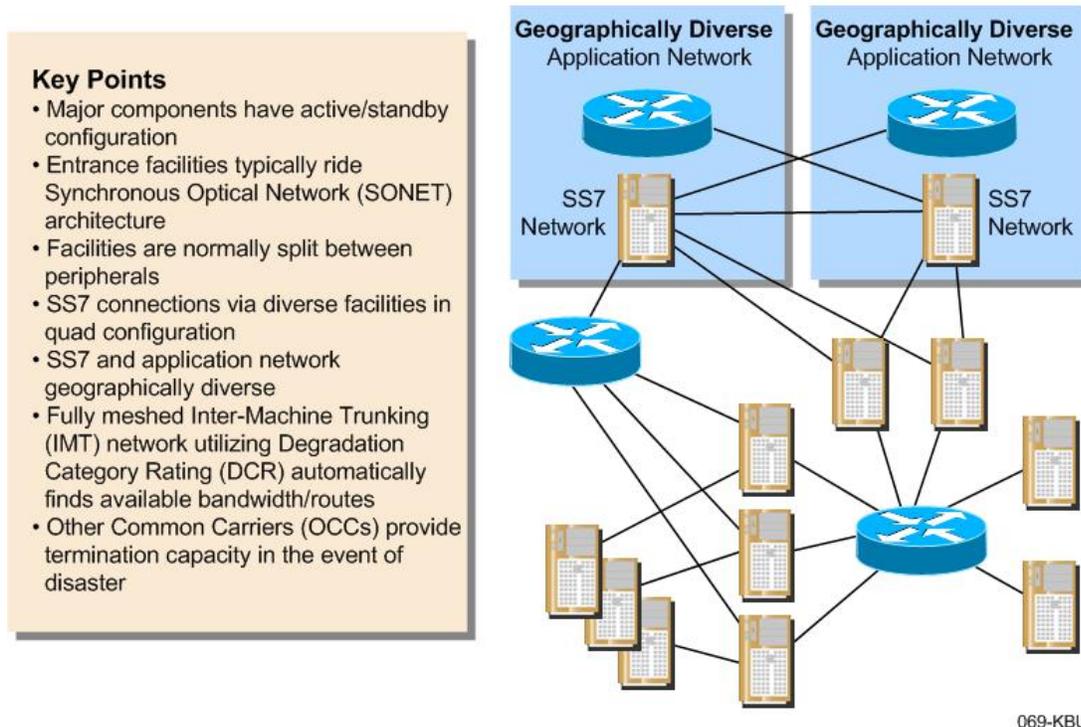
As customer dialing patterns change and exceed the engineered capacity limits, there is an internal process used by Switch Management for engaging the provisioning workgroups to quickly redistribute the circuits across other network elements.

TEX-AN Next Generation

State of Texas Department of Information Resources

Performance Management includes automated switch notifications that deliver measurement reports to various database systems. This allows individual workgroups to monitor the resource limits that are the threshold for each configuration. Thresholds are intentionally established at low values to provide early alerts to capacity issues. Examples would include SS7 capacity alarms generating at 35% capacity. Capacity is closely monitored and maintained at less than the 50% load factor so either path of the redundant system could carry the entire load if needed. See the figure below for a related drawing on this application.

CenturyLink's Network Diversity



If thresholds are exceeded and alerts identify the offending component, ATS/ETM are engaged to load balance the network to fail safe configuration levels.

Security Management maintains control and access to switching elements. Switch level commands are established based on user responsibilities; access is limited to those with a specific business need. Each user in a workgroup is assigned an individual user identification or access mechanism to allow access to the level required to perform their functions. Activity logs are recorded and maintained for all switch access and command level entry. These logs are viewed daily by the security group for invalid access attempts. Access Control Lists (ACLs) are created on router elements limiting communication to only network elements. This minimizes the opportunity for any denial of service attack from entering the production network.

The Transport/Switch Network Management center, which includes expertise in the areas of fiber protection, transport network management, and switch network management, monitors CenturyLink's backbone network to ensure the highest levels of network reliability. Each functional area of expertise provides coverage over

TEX-AN Next Generation

State of Texas Department of Information Resources

three shifts, with supervisory oversight and leadership by a manager. These functional areas combine to form a full service Network Operations Center that ensures network quality and reliability.

Network technicians provide 24x7x365 customer and network support. These technicians are the first line of customer contact, providing immediate customer ticket awareness/status and issue escalation (within the first hour) to network engineers or the exchange carrier as warranted by each specific issue condition.

Network engineers provide 24x7x365 escalation support for network technicians and leverage Technical Support and vendor resources as required to quickly mitigate issues.

Technical Capabilities

The first step in updating our systems for new products and systems is to survey leading-edge industry tools. If these do not satisfy our requirements, we use our extensive Information Technology (IT) resources to develop or further customize tools that meet our needs. Prior to rolling out new services, we test these new tools to ensure that all aspects of Proactive Network Monitoring capabilities are addressed. Specifically, we develop and test the rules that we employ to ensure that we capture what is most important to our customers and that new services are integrated seamlessly into our existing suite of product offerings.

In order to round out the suite of systems and tools that CenturyLink uses for Network Management, we employ industry leading commercial products to ensure effective monitoring of our network. The tools that we use for network monitoring have the capability to interface with our fault, accounting, and configuration management systems and tools. The table below lists our current major network monitoring systems.

Current Major Network Monitoring Systems.

CenturyLink network monitoring systems and tools allow us to monitor the overall performance, health, and reliability of our global network.

| System/Tool | Function | Features | Benefit |
|----------------------------|--|---|--|
| Telenium/NMA | Environmental and Layer 1 Network Monitoring | Supports multiple vendors' fiber and copper equipment. Supports multiple management protocols for data gathering. Prioritizes alarms. | Enhances efficiency by centralizing alarms. Adapts to new products and services. Enhances productivity of operation staff. |
| HP Openview/ CiscoWorks | Layer 2 Network Monitoring and Configuration | Views Network topology and status. Interfaces into network elements. Supports multiple vendor products. | Isolates Geographical network problems. Provides remote access to resolve network events. Adapts to new products and services. |

TEX-AN Next Generation

State of Texas Department of Information Resources

| System/Tool | Function | Features | Benefit |
|--------------|--|--|---|
| NerveCenter | Layer 2 Network polling and rules-based logic for alarming | Provides alarm modeling logic. Configurable SNMP polling. | Customizes rules-based alarming. Monitors key Layer 2 network parameters. |
| Concord/BRIX | Layer 3 Network Performance and Service Level Assurance (SLA) Monitoring | Configures polling using multiple protocols. Generates reports. | Monitors key Layer 3 network parameters. Enables adherence to Key Performance Indicators (KPI) and SLAs. |

These Network Monitoring systems afford us the capability to identify and resolve network events proactively before they become faults.

Operational Capabilities

Network Monitoring and Fault Management go hand-in-hand. The geographically diverse 24 x 7 Network Operations Centers (NOCs) referenced under Fault Management are the same centers that monitor our network. CenturyLink has implemented an electronic automated Line Management System (LMS) throughout the nationwide backbone infrastructure to monitor the physical protection of the fiber and assist in locating any disturbances. Furthermore, it is CenturyLink policy that all field operations personnel are assigned a segment of fiber that they must visually inspect daily for any activity that may endanger the fiber.

Configuration Management

CenturyLink understands that our execution of the Spirit of Service™ requires a state-of-the-art Configuration Management process and dedicated configuration management group. To this end, CenturyLink has a rigorous and standardized Configuration Management process across all of our network services support functions. The process includes notification to the impacted customers. Within CenturyLink, the Configuration Management process includes a requirement to notify and/or obtain approval from impacted areas of CenturyLink and key customer accounts. Because we focus on the customers' needs before, during, and after the change event, CenturyLink minimizes risk of service impact throughout the change event.

CenturyLink schedules activities with a minimum lead time of 10 days and understands the Customer's right to reschedule within a 5-day window. CenturyLink works with customers when rare emergency situations arise and a 10-day notice is not feasible. CenturyLink also works with and notifies the Customer of any large scale changes in the Network that may have an impact on the network. Those changes might include major upgrades, software releases, or replacement of equipment. CenturyLink identifies and schedules maintenance windows during pre-determined times and windows to minimize any impacts to the Customers. CenturyLink submits any planned changes to the customer by required means of notification. CenturyLink also provides

TEX-AN Next Generation

State of Texas Department of Information Resources

affected Customers access to a network configuration database (to include CenturyLink's facility maps and node geographical information applicable to their voice and data network access) through the Portal, giving the Customer an opportunity to perform impact analyses. This database enables the Customer to assess how network changes may impact services to the customer by giving them the ability to directly correlate the infrastructure involved with the network change with the services that ride that infrastructure. The data is presented in the form of a topographical map that allows the user to click on a facility to drill down to specific services provided over that path or via that node.

CenturyLink's maintenance windows are scheduled based on local time at the location where the work is performed. CenturyLink works with the Customer in coordinating and scheduling maintenance activity. For example, our experience in working with customers located in Asian/South Pacific countries has shown that we can minimize customer impact by scheduling maintenance activities on Friday nights. The CenturyLink Configuration Management process is flexible enough to handle international services that span multiple time zones:

- Planned maintenance is typically scheduled between 10 PM and 6 AM in the time zone in which the work is to occur
- CenturyLink takes proactive steps to work with customers to find an appropriate time to work on international circuits when there are known scheduling issues. As an example, on 10/17/06 CenturyLink experienced an emergency maintenance requirement on a transport system in Japan. CenturyLink proactively negotiated with customers for the best time to schedule a card swap that resulted in 2 minutes of downtime in a 1-hour maintenance window.

Management Capabilities

CenturyLink has a dedicated Configuration Management group that manages all network change activities within CenturyLink. This group is responsible for the following:

- Acts as the control point to ensure that required internal organizations are involved and change tickets contain the most updated information and documentation
- Serves as the interface between CenturyLink and our customers. The Configuration Management group notifies customers of network events that are potentially service impacting
- Evaluates all planned maintenance activities
- Incorporates all customer contacts into the process
- Designates appropriate approval levels
- Governs process for all levels, to ensure that the process for each change is followed
- Ensures that fundamental technical and safety requirements are met

CenturyLink performs all of our network changes and configuration management activities during a designated maintenance window to minimize the impact to the customer. Maintenance activities are pre-planned and tracked via CenturyLink's Work Delivery System (WDS), which has an approval process to ensure that proper resources are available, tools and equipment are available, an approved Method of Procedure (MOP) has been developed, a back out plan has been prepared, and the technician has the required

TEX-AN Next Generation

State of Texas Department of Information Resources

training to complete the work. Network operations and field technicians also are engaged in the change management process so both are aware of and have resources available during the maintenance window.

Technical Capabilities

Underlying the standard process for controlling configuration change at CenturyLink is the technology strength we bring to the table. Whether it is the discipline we bring to the deployment of assets into our network or the system we use to manage and monitor the actual configuration change event, we use technology to ensure CenturyLink continually performs at or above the expectations of our customers.

CenturyLink manages configuration change requests in our proprietary configuration management system, WDS, which is specifically designed for effective change management. CenturyLink already has this system in place and uses it successfully and effectively in our commercial and Customer market units. By standardizing the change management process and using the WDS system, CenturyLink has been able to manage changes to our network in a manner that minimizes risk to our customers.

CenturyLink has network laboratories that are used to test new technology, including new hardware, new software, and new versions of existing software. In addition to the manufacturer’s testing and certification, each new addition to our network goes through a rigorous in-house certification process. The resources within the lab emulate the CenturyLink network, so the impact of changes can be tested in the lab environment prior to being implemented in the production network. This ensures that new hardware and software does not negatively impact the CenturyLink network and our customers when it is deployed.

In terms of software version consistency, CenturyLink has a policy of deploying a common software version across the network. This reduces unintended risk due to inconsistent versions of software in a production environment.

Operational Capabilities

Within CenturyLink, the Configuration Management process is rigorous and is designed to minimize risk to the CenturyLink network and our customer base. This includes a policy that is known internally to CenturyLink as Question Your Work. This policy has resulted in a significant reduction in human error and has driven a culture of successful change management at CenturyLink. Prior to beginning any work activity, technicians are required to ask themselves the questions on the list below. The work will proceed only if the answer to all of the questions is YES. See CenturyLink’s Question It chart in the table below.

Question It.

The CenturyLink Question Your Work policy has been successful in minimizing human error.

| | |
|---|--|
| Q | Qualifications and training. Do you know what is required to do the job? |
| U | Understanding. Do you know what constitutes a successful completion? |
| E | Exposure. Have you minimized our risk? |
| S | Supporting documents. Are they complete and error free and logical? |
| T | Time. Is it the right time? |
| I | Instructions for the job. Are they clear and complete? |

TEX-AN Next Generation

State of Texas Department of Information Resources

| | |
|---|---|
| O | Oops! Do you have a back-out or restoral plan? |
| N | Notification. Have you notified everyone that needs to know? |
| I | Integrity. Has the appropriate paperwork been submitted to ensure database integrity? |
| T | Testing. Have you ensured the customer's circuits are active and working correctly? |

If the answer to any of the questions is NO, or the technician performing the work is uncertain, work activities will not begin until a resolution is found.

A MOP document is required for all significant change activities. The MOP is a multi-page document which details step-by-step instructions that specify how the change activity is performed. The MOP is developed, reviewed, and approved weeks in advance of the scheduled change activity. If the MOP is lacking a back-out plan or is missing relevant steps, the Change Activity is not approved and changes are made to the MOP.

Significant change activities routinely include an audio conference bridge that is maintained throughout the duration of the change activity. The purpose of the audio bridge is to facilitate communication with all participants that need to be part of the change activity. This includes CenturyLink Field Operations, Center Technicians, Center Management, and Tier 3 Technical Engineering support as appropriate. If, during the change, additional resources are required, the Operations Center pages the required staff who are summoned to the audio conference bridge.

Our operational experience dealing with the required changes in the CenturyLink network to accommodate the growth and customer requirements is an integral part of how we deliver the Spirit of Service™ to our customers. This process provides customers with new levels of insight and confidence in the reliability and scalability of CenturyLink's networks.

In order to meet the specific requirements set forth by the customer with respect to optional Network Monitoring and Management Services, CenturyLink provides the additional hardware and software to access said services. CenturyLink has demonstrated experience in developing Network Monitoring and Management solutions using our Portal capabilities; we can deploy additional functionality, on an individual case basis, any additional hardware or software.

Fault Management

CenturyLink's Network Management organization is focused on network reliability and performance to reduce the frequency, severity, and duration of fault events. CenturyLink proactively manages our network, using state-of-the-art tools and operational processes that make us a leading provider of telecommunications and data services. Customers have real-time access through the Portal to obtain the latest information regarding network faults. CenturyLink manages the reliability of our network and other carriers used to provide end-to-end service in real-time, with customer controlled access to fault management data through the Portal.

In addition, CenturyLink uses state-of-the-art communication tracking and development tools for proactive monitoring of events, traps, and alarms to ensure network integrity. CenturyLink's goal is to minimize any downtime, service dispatches, or repair issues. Through our inherent systems and team members,

TEX-AN Next Generation

State of Texas Department of Information Resources

CenturyLink isolates and resolves issues before they impact service. Our goal is simple; CenturyLink continues to work toward ensuring our network is always at optimal operating levels.

CenturyLink's state-of-the-art network is monitored continually to track, analyze, report, and record faults to meet specifications for our Customer customers. CenturyLink has both a Customer and internal escalation policy for Customer business activities, including pertinent contact information that is available through the Portal. CenturyLink notifies affected Customers of faults, restoration updates, and impact level, and includes in our report outages of the CenturyLink network switches or facilities, or isolations impacting full service. CenturyLink includes in this report any issues and concerns about catastrophic events (i.e., fires in a transport site) and any service affecting concerns that may be from a CenturyLink team member or vendor.

CenturyLink provides a tracking number, fault description report, date and detected time, Customers that are affected along with locations, and any peripheral information regarding faults and/or locations. CenturyLink provides an estimated time to repair when possible and the circuit Telecommunication Service Priority (TSP) status. Circuit malfunction is reported to affected Customers within 10 minutes. Updates and status are posted on the Portal Web site, with viewing capability to affected Customers for their services.

Updates are generated every 30 minutes and CenturyLink keeps the final status update of a service-affecting fault on the Portal for at least 24 hours after the trouble incident was closed. Access to fault management data and reports is available real-time through the Portal on a 24x7x365 basis. CenturyLink is committed to resolve 90 percent of all service affecting faults that do not require dispatch within four hours, as measured at the Customer level. CenturyLink resolves 90 percent of all service affecting faults that requires a dispatch within eight hours, as measured at the Customer level. The total time to restore (TTR) is calculated as the elapsed time between reporting the trouble and the restored time less the time related to conditions such as planned configuration changes, access issues, security clearances, or long distances relating to travel time to arrive at a site.

Management Capabilities

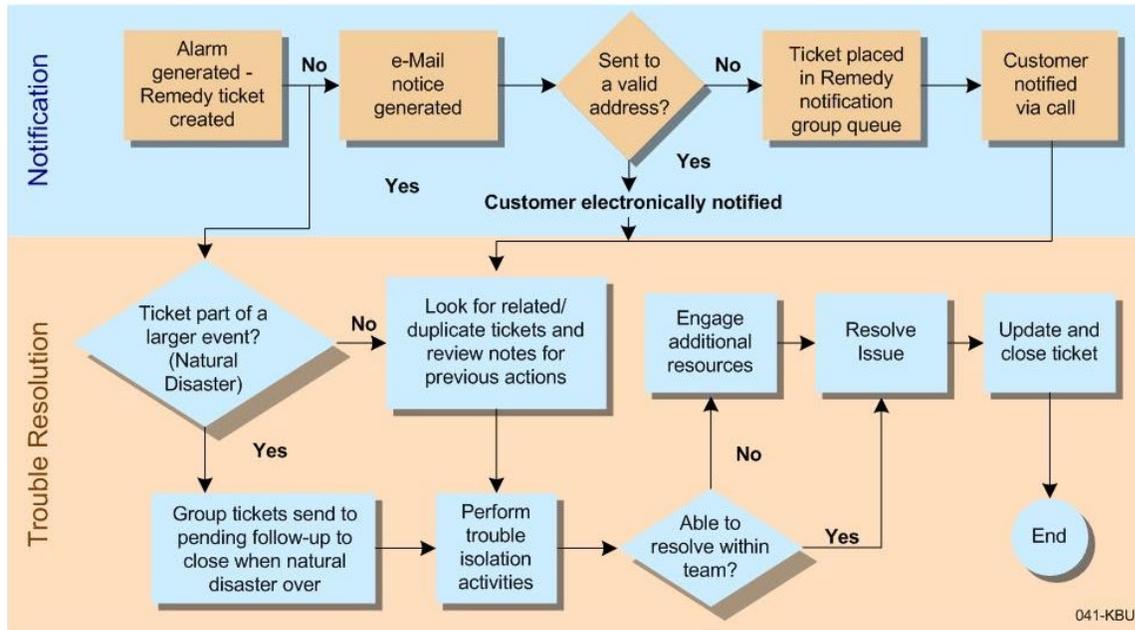
CenturyLink has deployed a robust network management strategy based on proactive monitoring with automatic trouble ticketing for our core services that is designed to minimize risk for our customers. As a result, CenturyLink is able to identify problems and commence restoration activities often before the customer is aware of the problem.

Automatic Ticketing is further augmented by Proactive Customer Notification (PAN), whereby CenturyLink notifies our customers of faults by pager, e-mail, or telephone call. PAN also provides CenturyLink's customers with flexibility to specify certain notification parameters on a service-by-service basis. The figure below illustrates the process flow and active customer notification policies and procedures CenturyLink employs in our proactive network management. CenturyLink takes an active approach in managing our network deliverables to all customers. We understand the importance of fault-free delivery systems and continuous operability relating to voice and data services. CenturyLink takes a hands-on active management approach in promoting and proactively delivering services. Our service delivery and network management sometimes puts CenturyLink into a combined effort with other teammates in delivering those services. CenturyLink drives and manages our team members to the same expectation level and commitment to network management in a manner which is transparent to our customers. CenturyLink provides the same expected level of service on a day-by-day basis, every day of the year.

TEX-AN Next Generation

State of Texas Department of Information Resources

Proactive Notification and Resolution Process



The customer can report performance issues through the Portal or contact the CenturyLink NOC for assistance. This enables the customer to reach the full breadth of CenturyLink’s capabilities by making one call and not needing multiple contact points. This enhances the customer’s repair experience and has led to consistently high customer satisfaction survey results. At CenturyLink, trouble tickets are not closed until the customer agrees that the issue is satisfactorily resolved.

For situations that require additional resources or management attention, CenturyLink provides customers with a thorough escalation process that includes access to higher levels of management. This process includes both customer-initiated and internal escalation on network events.

CenturyLink has a proven internal process called the Network Impact Level (NIL) process for quickly assessing outages and communicating the status of outages to senior management. When a network event occurs, the impact is determined and a NIL is assigned to the event that corresponds with the severity of the outage. Each NIL event type has a predetermined response from a technical resource and executive notification perspective.

The benefit that the NIL level process provides the Customer is that the appropriate level of technical and management support personnel are immediately engaged whenever a given NIL level is met or exceeded. The chart below correlates network alarms to the NIL severity levels and includes a short description of their severity levels. CenturyLink monitors network alarm status on a continuous basis 24x7x365 in the Network Operations Centers.

Table 1-4. Network Alarm Definitions and Descriptions.

TEX-AN Next Generation

State of Texas Department of Information Resources

Alarm Severity Warning for all CenturyLink customers, includes planned network events and change management activities

| NIL Designation | Corresponding Definition | Description |
|-----------------|---------------------------------------|---|
| Clear | Non-service Affecting | Non-traffic carrying event on the network, such as failed circuit packs with no traffic provisioned across either working or protect, network visibility issues, and common control cards. This is the default NIL level for opening tickets that do not qualify for the colorized NIL guidelines listed below. |
| Green | Planned Network Event/ Maintenance | Selective network-wide planned event requiring down time that is coordinated with customer notification, such as planned change management activities and emergency preemptive network initiates to avert a greater network outage. |
| Blue | Jeopardy State | Sustained failure of redundant network trunk, link, or element wherein traffic has successfully rerouted with no corresponding customer impact to service. Includes facility environmental components. Jeopardy conditions that clear within 15 minutes do not require paging. If loss of visibility to elements exceeds 15 minutes, send page. |
| Yellow | Minor Service Outage | A service outage network condition causing minor service disruption to the customer base relative to a network segment. For example, 300 blocked calls or two OC12s down. CenturyLink meets all applicable SLAs regardless of alarm status. |
| Orange | Major Service Outage | A service outage network condition causing major service disruption to the customer base relative to a network segment. For example, 5,000 blocked calls or more than two OC12s down. CenturyLink meets all applicable SLAs regardless of alarm status. |

TEX-AN Next Generation

State of Texas Department of Information Resources

| NIL Designation | Corresponding Definition | Description |
|-----------------|--|---|
| Red | Federal Communications Commission/Network Reliability and Interoperability Council (FCC/NIRC) Reportable | FCC and NRIC voluntary trial reportable events. |

If a customer disputes the designation, the customer can escalate the severity designation of a service disruption using the trouble escalation process.

Technical Capabilities

The key to effective fault management is state-of-the-art tools and systems to sectionalize, isolate, and restore services. CenturyLink uses a combination of industry leading off-the-shelf systems and internally-designed tools to deliver our best-in-class network management solution. CenturyLink has deployed redundant, state-of-the-art fault management systems that are geographically diverse. CenturyLink’s toolbox includes the following:

Key Toolsets and Applications Provisioning

CenturyLink uses an engineering order database containing initial and current service configuration information to effectively map critical service delivery points, equipment, and transport mediums.

The CenturyLink Facilities and Equipment database allows a real-time look-up of customer circuits to find related Local Exchange Carrier (LEC) and circuit layout information.

CenturyLink Web-based application interface systems tie directly into the provisioning database to provide additional information, such as customer account representative and customer contact information for proactive notification. CenturyLink provides authorized users with a read-only view to network maps and customer facilities, where icons are used to display network elements. The graphical user interface provides the Customer users with the ability to obtain a quick view of the network health and drill down to obtain detailed status and additional information. The icons are color-coded and depict a status change in real-time. CenturyLink’s network management solution allows the Customer to correlate network alarms with end-user equipment. Additional capabilities of CenturyLink’s network management solution include a customizable report utility for historical reporting, data extraction, and archiving of network alarms and events.

Trouble Ticketing

CenturyLink integrates easy-to-use trouble ticketing systems for creating and maintaining service trouble tickets, and automatically flags chronic circuit issues (three occurrences of an issue on the same circuit within a 30-day rolling period). These systems are populated with data required for the Customers.

TEX-AN Next Generation

State of Texas Department of Information Resources

Troubleshooting

CenturyLink trouble ticketing systems assist in physical layer testing of customer circuits and help to isolate problems as LEC- or customer-related. These systems are critical and integral to performance management. They provide CenturyLink a quick and real-time view into network management.

- *Service Creation System (SCS)*: Primary configuration platform for the Virtual Private Network (VPN) service
- *Element Management System/Network Management System (EMS/NMS) tools*: Bulk statistics and configuration tool to trend performance and isolate chronic issues
- *Firehunter and Brix*: Provide critical performance data to isolate packet loss, latency, jitter, and voice Quality of Service (QoS) conditions on the network
- *SecurID*: Provides two-factor authentication for secure access to CenturyLink equipment

The tools listed enable CenturyLink to manage our network and differentiate faults that are service impacting from those that are non-service impacting. This enables CenturyLink to focus our resources on events that are service impacting. The combination of the tools and systems previously listed and the resiliency of the CenturyLink network results in world-class service for CenturyLink's customers. CenturyLink accomplishes the procedural step of fault management through a commercial application, Telenium, which integrates circuits into a single database for the purposes of real-time telemetry surveillance to the network. The underlying purpose of Telenium is to provide the CenturyLink Network Operations Center (NOC) personnel with a means to view provisioned circuits, as well as detect network alarms and troubles to facilitate fault analysis and problem resolution 24x7x365.

CenturyLink delivers to the Customer a read-only view of the Customer network as used by CenturyLink's NOC. The NOC is staffed 24x7x365 to provide proactive network surveillance and performance management functions. This view provides a real-time status of the network, identify alarms, and isolate service and non-service affecting events. This includes a customizable report utility for historical reporting, data extraction, and archiving of network alarms and events that enables CenturyLink to deliver ad hoc reports.

In a continual effort to ensure that the Customer can be fully engaged in the ongoing management of provisioned telecommunications transport services, CenturyLink provides Web access to the Portal that supports the service assurance and delivery requirements. This Portal includes a trouble management interface that allows the users to electronically input trouble tickets and check their status.

TEX-AN Next Generation

State of Texas Department of Information Resources

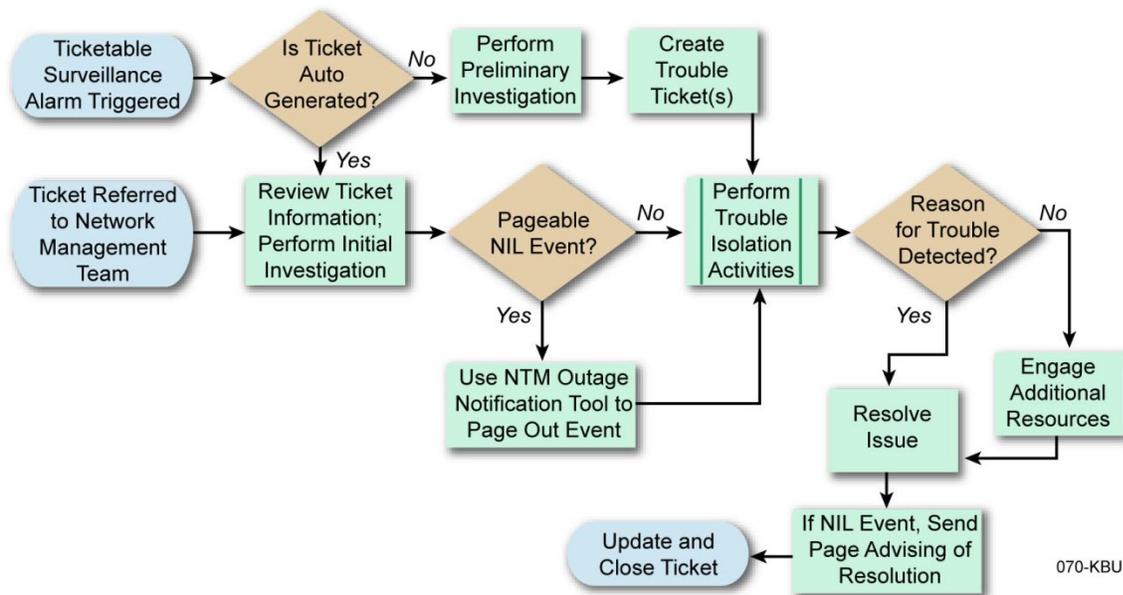
This Portal is part of an ongoing evolution of CenturyLink’s current systems that have been in place for many years, such as our provisioning system, order entry, billing, and trouble ticketing. Network management views give the Customers access to their network alarms and performance statistics. The performance statistics are fed directly from the CenturyLink switches, reflecting real-time views of the network.

Operational Capabilities

By using the network management tools and strategies outlined in this section, CenturyLink personnel are able to manage our network in a way that results in performance that is above industry standards. The NOC personnel are trained in specific areas of expertise to provide handling and resolution of network events. CenturyLink has established NOCs that operate 24x7x365 in geographically dispersed locations. This ensures continuous management across the different platforms that comprise the CenturyLink network.

CenturyLink’s Network Management processes are centered around automatic trouble ticketing on predefined network events and alarm thresholds. This enables CenturyLink to prioritize events and assign work to the events that are service impacting. The figure below depicts CenturyLink’s trouble ticket process.

Trouble Ticket Process

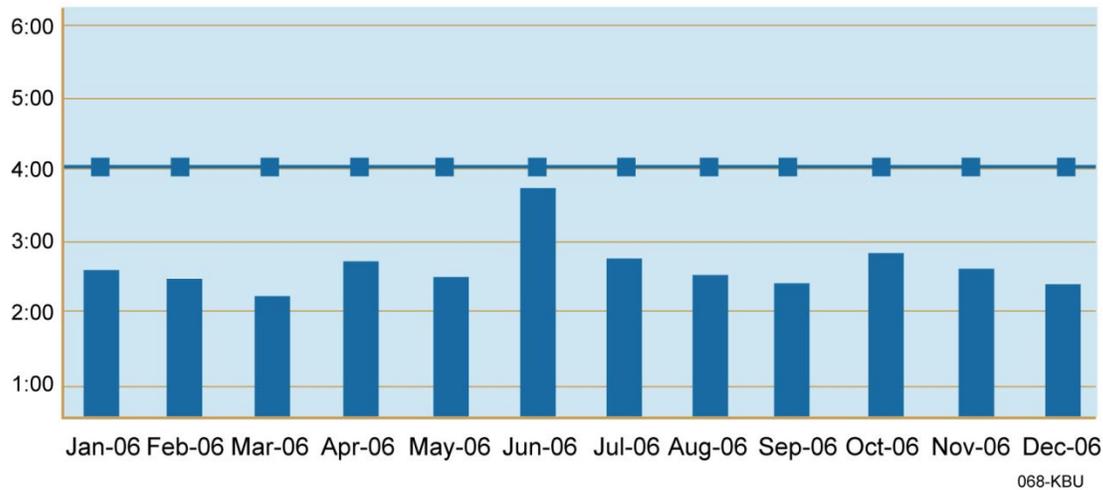


CenturyLink’s Network Management strategy has resulted in consistent performance that is best-in-class. The figure below shows an illustrative example using CenturyLink’s DS-3 and higher service where CenturyLink consistently performs significantly better than our repair objective of four hours, which in turn consistently beats the Customer’s requirement of four hours to repair a non-dispatched fault and eight hours to repair a fault requiring a dispatch. Furthermore, the Mean Time to Repair (MTTR) performance includes situations that require a dispatch out to both a CenturyLink remote location and a potential referral to an LEC.

Monthly MTTR for DS-3 and Above—Includes Dispatched and Non-Dispatched

TEX-AN Next Generation

State of Texas Department of Information Resources



“We were notified about our router when it went down, and even though that office is closed until next week CenturyLink worked with the LEC to get it fixed without any intervention on our part. That's exactly how it's supposed to work and we appreciate it.” (Source: A National Education Organization)

Additionally, when CenturyLink fixes a fault, we fix it right the first time. We verify that the customer is back in service before closing the trouble ticket. CenturyLink’s repeat-repair percentage is in the single digits and is best-in-class.

Security Management

CenturyLink has a longstanding, robust security program with a proven history of providing industry-leading security services to protect CenturyLink’s infrastructure including information assurance processes applicable to databases and OSS and information processing systems. CenturyLink is committed to protecting its customers against threats, attacks or failures of systems, in accordance with best commercial practices. CenturyLink employs a mature, process-based risk assessment approach to ensuring logical and physical security controls are in place and appropriate for our computer centers, network operations centers, secure operations centers, cyber centers and other CenturyLink facilities. CenturyLink’s security-related services are intended to ensure the integrity, confidentiality and availability of information and network assets and to support CenturyLink resources and its wide range of customers and geographical locations.

CenturyLink provides services as an integrated network secure solutions team. The CenturyLink Team assists with the identification of waste, fraud, and abuse. The CenturyLink Network Fraud Operations Center operates as a functional group within CenturyLink Risk Management and owns the responsibility of fraud prevention, detection, and reporting. Using a state-of-the art fraud detection system, the Fraud Operations group analyzes a Customer’s daily calling and usage patterns for variations in the normalized traffic for the Customer. The group also monitors the network 24x7x365 for potential threats related to customer premise equipment. CenturyLink notifies the affected customers within 30 minutes of identifying an unusual or suspicious outage, blockage, or other service-affecting or fraud-related event.

TEX-AN Next Generation

State of Texas Department of Information Resources

The CenturyLink integrated security team's commitment to provide reliable security services to the Customer that meet or exceed their expectations. The CenturyLink integrated security team ensures that all incidents are reported within the required time frame, including: a verbal notification to affected Customers within fifteen minutes for initial discovery; four hours for results of investigations and corrective measures applied; a written Security Breach Notification Report within seven calendar days of said breach; and a monthly report detailing all security breaches for that month.