



## NNI Plan

1. CenturyLink agrees to implement network to network interface connections as required at both the Network and Security Operations Centre (NSOC) and the Sam Houston Building (SHB) at a minimum. Qwest's design will encompass building dedicated fibers into the operations centers. With this fiber build, the capacity of the circuits can vary depending on the type of transport desired. During the initial build CenturyLink will turn up 1 Gig Ethernet circuits that will be homed to the CenturyLink POP. These connections will give the State access to the CenturyLink backbone for all services that traverse the CenturyLink network. Other transport handoffs will be available with this NNI connection for services to be turned up.
2. During deployment of network services CenturyLink can install many types of equipment for service delivery. As other services from CenturyLink will be delivered equipment types may vary. For the install NNI deployment the equipment that will be installed is Fujitsu 7120.

The Operating Environment of the 7120 is:

- Temperature –20 to +65 °C (–4 to +149 °F)
- Humidity 5 to 90% (non-condensing)
- Maximum power consumption 275 W per shelf
- Maximum heat dissipation 938 BTU/hr
- Power Input –48 VDC, redundant feeds
- UPS/Batteries

CenturyLink will work with DIR on specs for rectifier.

### *Physical Characteristics*

- FLASHWAVE 7120 shelf (2RU)
    - Weight (fully loaded) 16.5 lbs (7.5 kg)
    - Dimensions (H x W x D) 3.5 x 17.3 x 11.0" (90 x 440 x 279 mm)
  - FLASHWAVE 7120 passive shelf (1RU)
    - Weight (fully loaded) 9.1 lbs (4.1 kg)
    - Dimensions (H x W x D) 1.73 x 17.3 x 11.0" (44 x 440 x 279 mm)
3. Capacity management is handled by our Network Operations Group with the CenturyLink network. Circuits are examined to assure they can carry the correct traffic and stay within the SLA measurements. Capacity is also determined by the product that is transported across the NNI and its bandwidth profile.

In general, CenturyLink's traffic management philosophy relies on "right-sizing" the network to handle the traffic offered to it by planning and making available capacity before it is actually needed. Every CenturyLink TeraPOP is connected via multiple backbone circuits to a minimum of two (in most cases three) other TeraPOPs over diverse physical facilities. Usage reports are gathered for all such backbone circuits (defined as those circuits that interconnect core backbone devices) and reviewed weekly. Any individual backbone circuit with a 95 percentile utilization greater than 40% or peak utilization greater 60% (over a given sampling period) is flagged for upgrade. In addition to simply monitoring circuit utilization



under normal operating conditions, traffic flows on the backbone are regularly modeled for potential failures due to fiber cuts/hardware failures, etc. This modeling helps predict traffic utilization patterns due to abnormal network conditions. Using such modeling data we are able to identify those backbone circuits that must be upgraded to conform to the planning threshold of 40% utilization even under failure conditions. Although CenturyLink's primary approach is to make adequate capacity available for normal as well as abnormal network conditions, CenturyLink is also evaluating the use of Bandwidth-reserved LSPs across the core network for certain traffic types — the current network architecture with physical separation between those network elements at the edge of the network serving different services (VPN, Internet, VoIP) lends itself naturally to such an architecture.

CenturyLink's design goal for the backbone is 100% packet delivery. The network uses MPLS Fast Re-Route for redundancy and trunk fail-over in the network. CenturyLink's network boasts sub-100 ms routing recovery time in the event of a network outage, as opposed to the 15 to 30 seconds on traditional SONET healed networks that rely on standard Interior Gateway Protocols (IGPs) for failure recovery. This ensures that network availability for sensitive applications such as VoIP and Video does not suffer if there is a link/node failure in the network. CenturyLink provides tools for customers to view the performance of the CenturyLink IP/MPLS network. Performance statistics for the core IP/MPLS backbone are publicly posted, and may be viewed at <http://stat.CenturyLink.net>. The Agilent Firehunter tool is used to gather and report these statistics; it is not based on a proprietary CenturyLink tool.

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.

CenturyLink maintains a proactive monitoring and notification objective of ten minutes of receipt of a customer circuit physical outage event for data services. CenturyLink employs platform-specific alarm thresholds to identify service impairments. CenturyLink's internal systems correlate network alarms to customers; generating a trouble ticket for automatic customer notification. Automatic notification is limited to customers who subscribe to ATM, Frame or IP-based services and comes in the form of e-mail or text page.

Physical circuit outage events are generated as follows:

- SNMP traps are generated from CenturyLink edge routers and directed to CenturyLink's NerveCenter management servers
- The NerveCenter management server uses behavior models to filter out actual physical outage (includes bouncing circuits) events
- Outage events are generated into the NetCool application



- The Alarm Rule Service and Ticket Rule Service then correlate the event to active events and routes valid events for notification to the Proactive Notification tool for automatic dispatch of notification.

It is also important to note that closing tickets is advantageous for proactive notification. Not only does it ensure chronic circuits will be appropriately tagged for each occurrence in our ticketing system, but it also ensures that you will be contacted if an outage event occurs, as you will not have a ticket open for a current issue.

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.

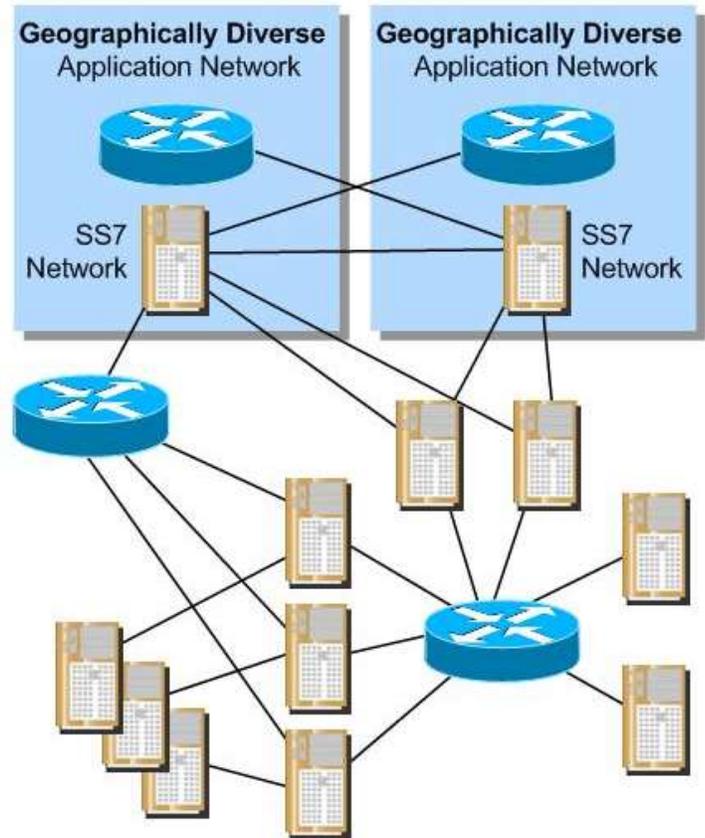
Performance Management includes automated switch notifications that deliver measurement reports to various database systems. This allows individual workgroups to monitor the resource limits that are the threshold for each configuration. Thresholds are intentionally established at low values to provide 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

#### Key Points

- Major components have active/standby configuration
- Entrance facilities typically ride Synchronous Optical Network (SONET) architecture
- Facilities are normally split between peripherals
- SS7 connections via diverse facilities in quad configuration
- SS7 and application network geographically diverse
- Fully meshed Inter-Machine Trunking (IMT) network utilizing Degradation Category Rating (DCR) automatically finds available bandwidth/routes
- Other Common Carriers (OCCs) provide termination capacity in the event of disaster



069-KBU

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

4. 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.

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.

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 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 24 x 7 x 365 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 24 x 7 x 365 escalation support for network technicians and leverage Technical Support and vendor resources as required to quickly mitigate issues.

CenturyLink network operation centers (NOCs) have full visibility and control of the platform with 24-hour management and proactive notification when problems occur. Issues that occur at the CenturyLink Transport level are handled in like manner as those for individual circuits. Should an issue arise at the transport level that may be customer affecting, CenturyLink will determine the affected customers and generate a Remedy child ticket from the Master ticket and send out proactive notifications to affected customers that are set up for Proactive notification through text messaging to cell phone or text pagers and can be sent as an email notifications also.

Within the CenturyLink network infrastructure, we provide filtering for Telnet and SNMP access to the Backbone routers, BGP access-lists to permit or deny the incurrence or propagation out of network advertisements, per-customer prefix filters to only accept their network advertisements, Blocking of Private AS and bogon advertisements, ACL's denying private IP address ranges both in and out. In the



event of a DoS attack, we will implement temporary filters to stop the attack on the edge routers. Additionally, new tools are deployed within the CenturyLink network to detect, prevent and minimize the effects of attacks on the CenturyLink network or its customers (Arbor, UnicastRPF), in addition to allowing customer control of DoS mitigation by the use of Black Hole Filtering via BGP.

CenturyLink secures and scales the network by the use of security domains. CenturyLink has a single private core network to converge all IP traffic while keeping traffic types separated into what we call Security Domains. Specifically, CenturyLink uses a single core to carry all IP traffic by segregating traffic at the edge based on type; each type of traffic is a Security Domain. We have edge routers that are physically dedicated to a single Security Domain -- Private VPN, Public Internet, and VoIP. Each Security Domain uses its own dedicated LSP mesh across the shared core for transport of its traffic.

CenturyLink has a single MPLS core and overlaid on that are three different full meshes of LSPs – one for each Security Domain. LSPs for a single Security Domain originate and terminate on edge devices within that Security Domain. Interconnection between Security Domains is and will only be done via application layer firewalls. See illustration below:

