Pipeline
Knowledge Is Power

www.pipelinepub.com Volume 3, Issue 11

Not for distribution or reproduction.

Carrier-Grade: Five Nines, the Myth and the Reality

by Wedge Greene & Barbara Lancaster

Carrier-grade power

What is the hard fast requirement for Carrier-Grade? Is "five-nines" or *99.999% up* or *0.99999 available* a hard, fast requirement of telecommunications or is it the telecommunications equivalent of an Urban Myth? From a common sense perspective, the meaning of *availability* is clear, and given the essential nature of telecommunications, the necessity of five-nines is easily understood. But when you want to measure it, and hold someone accountable for delivering that availability, you must establish an *operational definition* for it. We asked a cross section of telecom and OSS experts if they knew the origin of five-nines and surprisingly some answered that in reality there was 'no such thing.' (We suspect that these folks skipped their Statistical Analysis classes, or perhaps meant to say that measuring five-nines is not sufficient to achieve Carrier Grade performance…) Wikipedia has a useful entry for "The myth of the nines" which supports the latter:

> "In information technology, the **myth of the nines** is the idea that standard measurements of availability can be misleading." [Wikipedia, http://en.wikipedia.org/wiki/Myth_of_the_nines]

So we set out to track down just what *carrier-grade* is and where it comes from.

For the thirty years we have been in this industry, **five-nines** was the number one rule-of-thumb: the most basic underlying tenant of hardware construction, network design, and the expressed goal of every network system. It is the very heart of the operational war stories on which we were raised. For example, there is the case of telecom power requirements – the very foundation of the 'set apart' and 'we are different' basis of Point of Presence (POP – the local building where telecom switching equipment was placed) construction. Power loss was once identified as the single greatest threat to telecom network reliability as alternating circuit equipment was prone to costly service variations (telecom could not rely on cycle timing from a power utility) and unacceptable equipment failure rates. So DC rail-based power was mandated for telecom POP construction and every carrier-grade network element had to run off that DC power. For certain, it made power failovers remarkably straightforward with all those batteries. Even computing servers (where they were lightly scattered across voice POPs) had to have DC powered versions. Never mind that high voltage DC rail power can fry your personnel six ways from Sunday, once all POPs were powered by DC, the domestic network

© 2006, All information contained herein is the sole property of Pipeline Publishing, LLC. Pipeline Publishing LLC reserves all rights and privileges regarding the use of this information. Any unauthorized use, such as distributing, copying, modifying, or reprinting, is not permitted. This document is not intended for reproduction or distribution outside of www.pipelinepub.com. To obtain permission to reproduce or distribute this document contact sales@pipelinepub.com for information about Reprint Services.

"failures attributable to power outages over the last n years (*N being variable in the stories*) could be counted on one hand." And this is true, DC power in POPs is remarkably reliable, probably six-nines reliable considered, in full, as a redundant system. But the story of DC power and five-nines availability is an oral tradition handed down from those who taught us and to those we taught.

NOC Targets

Also it is very real that the yardstick standard for availability of networks to be delivered by the Network Operations Center was 99.999%. This was not a soft target. Performance reviews of NOC management were frequently based on hitting that target. Availability was the number one KPI for networks and NOCs were tasked with restoring any outages so that network availability would be maintained. But early on in the then-named Network Management Forum (now the TeleManagement Forum), participants of the newly formed SLA group (though it was not called SLA back in 1994) realized that each of them had different ways of computing that figure for availability. It took years to hammer this out to an agreement on what to count and how to calculate it. (For more details, see the current SLA Handbook Solution Suite Version 2.0) But in reality, every standards group, and even every industry, seems to have a different way of defining availability. What-to-count as an outage becomes "key".

Wedge Greene has a personal experience with the traps lying in wait for those trying to measure and report on availability. Back in the early nineties when he was a signaling and routing specialist, but because he had software and systems experience, he was yanked out of his comfortable theoretical work and tasked with developing a system to report on the quality of the early frame relay network. A big requirement was to measure the availability of the network and produce one monthly number for availability. He was a data guy and trained as a scientist and engineer. So he set out to "measure" availability – directly measure availability. His team developed automated methods of pinging every network port and of correlating down and up link alarms; by merging these two methods (direct measured ping non-responses and interpolated differences in time between down link alert and uplink alert), an automated measure of network up time was generated. This was sent up the management chain every month. After a few months, down from the management chain came the request to generate this KPI weekly, next month it became a demand for daily data. Finally the newly appointed General Manager of the division paid a personal visit to Wedge. The GM needed to find out why the network was "so bad". The automated network availability figures were much lower than five-nines. Five-nines availability was the corporate standard and the accounting people were "going to shut down the network if the quality did not immediately improve." In the face of this terrible report card, the VP of Engineering was blaming the VP of Operations ("You cannot run a network or fix anything on time") who was tossing the responsibility right back ("You provided us inferior equipment"). Furthermore the Voice Network division, using a different set of calculations, said their network met five-nines and this is what all the customers expect. "Your inferior data network is dragging us down."

Not for distribution or reproduction.

© 2006, All information contained herein is the sole property of Pipeline Publishing, LLC. Pipeline Publishing LLC reserves all rights and privileges regarding the use of this information. Any unauthorized use, such as distributing, copying, modifying, or reprinting, is not permitted. This document is not intended for reproduction or distribution outside of www.pipelinepub.com. To obtain permission to reproduce or distribute this document contact sales@pipelinepub.com for information about Reprint Services.

Business Operations Architects

Not for distribution or reproduction.

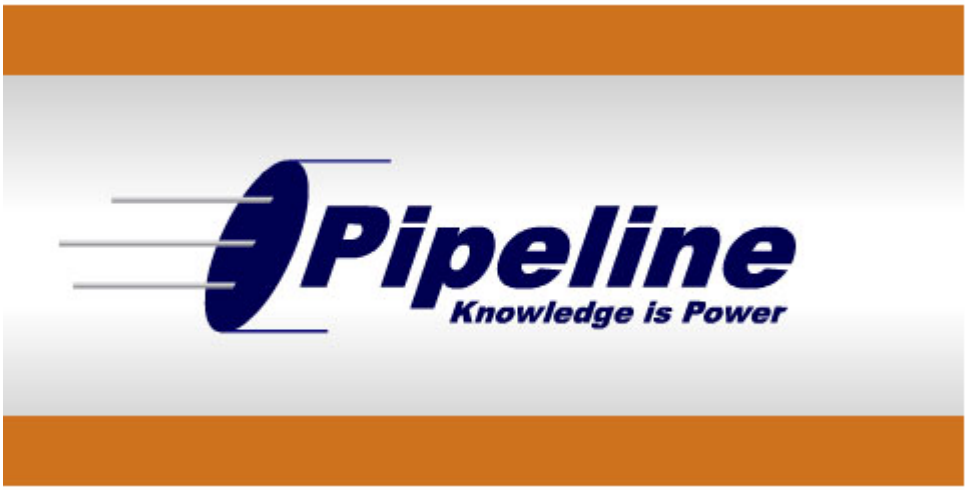
Wedge spent a day presenting the methodology for measuring and computing availability. He stood firm that the measure was absolutely precise, but not necessarily *accurate* since they could not control the removal from service of terminating CPE routers at the customer presence. He then explained the difference between precise and accurate. He tried to explain that normalization (or adjustments) was not empirically possible and the measure should be just one of many indications of customer usage after uptake. Further, he showed that the number was steadily getting better as more units were deployed and more customers placed commercial applications on their VPNs (and so kept their routers running). It was here that Wedge learned that this approach to calculating availability, that the data guys had developed from ground zero (read through IETF group brainstorming sessions), was not the normal telecom approach.

It seems that in order to meet the GOAL of five-nines, which had somehow become transferred from an individual network element requirement to an overall network requirement, the voice telecom NOC had successively kept ruling outages out of the computation of "availability." Voice people reported availability out of their trouble ticket system. There was no direct measurement of the network. Availability was computed from the time a ticket was opened until it was closed. Than came the exclusions: only customer opened tickets counted – proactive restorations did not count (if the tree fell and no one noticed before it was propped up, it did not fall), then the beginning of the outage start time was from the time the ticket was opened (a somewhat long time from when the problem physically occurred), and lastly, any time the ticket was transferred to the customer ("on the customer's clock") did not count. And even above this, scheduled maintenance down time did not count toward availability. The Voice NOC had seemingly *qualified away* rigor in order to meet the mandated goal of five-nines. (Once again proving the rule that you get what you measure.)

Essentially the Voice NOC was not wrong, nor the Data division right. What the NOC was measuring was compliance with a customer-oriented SLA, a Service Level Agreement, and not really an availability measure. The Data division was measuring availability as "measured uptime," or the probability the network could be used at any specific time the customer wished to use it. Today we clearly understand the difference between SLAs and Availability, and define them in

© 2006, All information contained herein is the sole property of Pipeline Publishing, LLC. Pipeline Publishing LLC reserves all rights and privileges regarding the use of this information. Any unauthorized use, such as distributing, copying, modifying, or reprinting, is not permitted. This document is not intended for reproduction or distribution outside of www.pipelinepub.com. To obtain permission to reproduce or distribute this document contact sales@pipelinepub.com for information about Reprint Services.

separate and individually appropriate ways. So the justification session worked, and Wedge Greene henceforth started attending standards meetings as an Operations guy.



Not for distribution or reproduction.

Hardware Origins

Let us backtrack a bit. It is likely that the origin of five-nines availability comes from design specifications for network elements. It also seems likely that the percent measure came before the current MTBF (Mean Time Between Failures) and MTTF (Mean Time To Fix) measurement, since it is a simply expressed figure and the MTTF requirements often match the % calculation while being expressed as an odd-ish number. However, 99.999% is not so accurate, fundamentally when you examine it closely, because of the fuzziness of the definition of availability. So in MIL-HDBK-217 and Bellcore/Telecordia TR332 they standardized these measures. The basic hardware design measures became:

MTBF - the average time between failures in hardware modules

MTTR - is the time taken to repair a failed hardware module.

In practice, these numbers are mostly estimates that the manufacturer makes about the reliability of their equipment. Because telecom equipment frequently is expensive, not deployed in statistically significant sample set sizes, and rushed into service as soon as it passes laboratory tests, the manufacturer estimates its reliability.

It is not clear when the measure of reliability of an individual network element became the measure of overall network availability – but it did: customers don't care if one element fails, or dozens fail. Customers only care that the service they are paying for and rely on works as offered. It is also interesting to note that this five-nines either transferred from network elements to computing systems. Today computer server reliability is critical to the network availability, so it is actually convenient that both seek the same standard for describing quality.

Defining Availability

© 2006, All information contained herein is the sole property of Pipeline Publishing, LLC. Pipeline Publishing LLC reserves all rights and privileges regarding the use of this information. Any unauthorized use, such as distributing, copying, modifying, or reprinting, is not permitted. This document is not intended for reproduction or distribution outside of www.pipelinepub.com. To obtain permission to reproduce or distribute this document contact sales@pipelinepub.com for information about Reprint Services.

IEEE Reliability Society - Reliability Engineering subgroup defines "Reliability [as] a design engineering discipline which applies scientific knowledge to assure a product will perform its intended function for the required duration within a given environment." Reliability is the flip side of the availability coin.

From a common sense perspective, the meaning of availability is clear. But when you want to measure it, and then hold someone to task for delivering that availability, you must define an *operational definition* for it. Federal Standard 1037C and MIL-ST-188 define telecommunications availability as a *ratio* of the time a module can be used (if a use request existed) over a period of time. It is a ratio of uptime to total time. Expressed otherwise, it is the proportion of time a system is functioning. But what is overlooked, and actually somewhat funny, is that five-nines is actually referring to a *logarithmic unit* derived from the number of nines following the decimal point.

Further, is availability an average or a probability? Generally, if you are building a network element, you would define availability as a "probability of failure". But if you are an engineer in a NOC running a report, you would define availability as an average. Whereas, according to Cisco, the number of defects in a million is used to calculate software availability and time does not enter directly into the calculation.

While NEBS is mostly concerned with safety, the NEBS standards - Telcordia (GR-63 CORE and GR-1089 CORE NEBS Level 3) also provide goals for central office reliability of network hardware.

Setting Availability Requirements

Cisco says: "Increased availability translates into higher productivity, and perhaps higher revenues and cost savings. Reliability implies that the system performs its specified task correctly; availability, on the other hand, means that the system is ready for immediate use. Today's networks need to be available 24 hours a day, 365 days a year. To meet that objective, 99.999 or 99.9999 percent availability is expected."

You see this figure everywhere. "Carrier grade means extremely high availability.

Not for distribution or reproduction.

© 2006, All information contained herein is the sole property of Pipeline Publishing, LLC. Pipeline Publishing LLC reserves all rights and privileges regarding the use of this information. Any unauthorized use, such as distributing, copying, modifying, or reprinting, is not permitted. This document is not intended for reproduction or distribution outside of www.pipelinepub.com. To obtain permission to reproduce or distribute this document contact sales@pipelinepub.com for information about Reprint Services.

In fact, the requirement for availability in commercial telecom networks is 99.999%... and is known as fine nines reliability." [*Carrier Grade Voice Over IP*, a book by Daniel Collins]

However you define it, five-nines of availability is a pretty tough target to hit. This corresponds to 5.26 minutes of *unplanned* downtime in a year. It is rather unlikely that if the NOC engineers must be involved in a restoration it will take less than 6 minutes to get notification of the outage, auto process the alarm, display the alert information, look up and display any related information, have a NOC engineer acknowledge the alert, open a trouble ticket, diagnose the root cause, determine the likely fix, launch the device interaction tools, change the necessary items on the device, and restart the service. Hence the overwhelming need to automate the entire process, relying heavily on redundancy to provide seamless transfer from the failing element to a healthy element. But of course, one expects that any specific element module will actually go more than a year without fault, so the availability target can be averaged out to meet the NOC goal of five-nines.

This averaging and predicting of element reliability becomes very clear with another precisely defined measure from MIL-HDBK-217 and Bellcore/Telecordia TR332:

> FITS - the total number of failures of the module in a billion hours (i.e. 1000,000,000 hours).

Our civilization likely will not last a billion hours which is 117,041 years, so of course this measure must be estimated, computed from component parts, or derived from very large sample sets (like number of chips produced in a year). **Bellcore** (Telcordia) standards TR-332 Issue 6 and SR-332 Issue 1 provide guideline models for predicting failure.

But consider the "bad apple" example - i.e. if one system crashes for 24 hours, and all others work without interruption for the month, the 24 hour outage might be averaged across a large base of installed units. When the number of installed units is large enough, this yields a number that would remain within the required 5 nines of up time. More specifically, if a service provider installs a product described as "carrier grade" or providing five-nines availability, should the service provider expect that this is the product reliability standard expected of every single network element, or should the service provider expect that some of the elements may perform at a much degraded level, and that it is only the world wide "law of large numbers" that is used to measure carrier-grade? You see, it isn't just that one bad apple in a group of network elements can skew the overall numbers – there are actual customers and real traffic affected by that "bad apple" element. Way beyond some theoretical measure, the effect on customers might be quite severe – certainly outside the guarantees of any customer SLA, and almost certainly extracting a penalty payment from the carrier, and likely attracting a fine from the regulator as well. As we shall see later, the problem of "one versus many" is being addressed by several groups.

The bottom line is that units will fail, so five-nines hardware availability is actually a design game of building systems which are always covered, i.e. they are redundant. This is the next telecom rule-of-thumb: no "single point of failure" (SPOF) shall exist.

Supplying Redundancy

Not for distribution or reproduction.

© 2006, All information contained herein is the sole property of Pipeline Publishing, LLC. Pipeline Publishing LLC reserves all rights and privileges regarding the use of this information. Any unauthorized use, such as distributing, copying, modifying, or reprinting, is not permitted. This document is not intended for reproduction or distribution outside of www.pipelinepub.com. To obtain permission to reproduce or distribute this document contact sales@pipelinepub.com for information about Reprint Services.

Redundancy is the addition of information, resources, or time beyond what is needed for normal system operation. Both hardware and software can be made redundant. Hardware redundancy is the addition of extra hardware, usually as backups or failovers or for tolerating faults. Software redundancy is the addition of extra software, beyond the baseline of feature implementation that is used to detect and react to faults. Information redundancy is the addition of extra information beyond that required to implement a given function and includes configuration and data duplication, replication, and backup databases. Hardware and software work together using information to provide redundancy, usually by having software monitor for abnormalities and initiate the configuration changes necessary to switch service to backup hardware, servers, and standby software programs.

Not for distribution or reproduction.

IBM says of SPOF – "A single point of failure exists when a critical function is provided by a single component. If that component fails, the system has no other way to provide that function and essential services become unavailable. The key facet of a highly available system is its ability to detect and respond to changes that could impair essential services."

SPOF is defined against an interacting system. One establishes the level and layer of redundancy in the system design. But systems can be decomposed into smaller sub-groups and eventually into units. How far down does the SPOF rule apply? Is this like a fractal which always holds its pattern no matter what smaller piece you choose to examine? Well practically, a base level for redundancy is reached beyond which failures are not automatically compensated for. This last level is called the "high-availability" unit. Both hardware and software can be built and marketed as "high availability". High availability is consistently used by telecommunications vendors to describe their products, perhaps even more often than the umbrella term "carrier grade".

But building a system entirely of high-availability units will not itself guarantee the system dynamics will remain carrier-grade. This is because systems can shift performance even as each of the individual units remain within their tolerance. Also, during the time a high-availability unit performs a switchover, the larger system could react to the out of expected performance. So the corollary rule to SPOF is "install multi-layered redundancy" in the network system as a whole. This does not excuse bad design of a failure prone network or software element; but it does shield the product and the customer from that "bad apple".

Networks and Systems Dynamics

© 2006, All information contained herein is the sole property of Pipeline Publishing, LLC. Pipeline Publishing LLC reserves all rights and privileges regarding the use of this information. Any unauthorized use, such as distributing, copying, modifying, or reprinting, is not permitted. This document is not intended for reproduction or distribution outside of www.pipelinepub.com. To obtain permission to reproduce or distribute this document contact sales@pipelinepub.com for information about Reprint Services.

We maintain that layering redundancy must involve considerable design scope. In fact, network design in service providers is frequently compartmentalized with one technology group not knowing what the other does. This is especially true for vendors specializing in just one technology or compartmentalizing their product teams. The classic example is ATM and SONET. Many networks were built with ATM ridding over SONET. SONET rings have very fast failover restoration. But ATM was also designed with restoration implemented through signaling and routing adjustments. When a transport layer error was detected, the SONET switched fast; meanwhile the ATM network layer began reacting to the notification of the outage to adjust itself. It might also switch unnecessarily. Or it may have to react to a routing link-weight model which is no longer appropriate given the change in SONET path.

So competing redundancy requires a carrier and vendors to have strong architectural oversight groups which look at both the big and the small picture to catch these redundant efforts and unexpected system interactions of multi-layered redundancy. Such a group is economically justifiable because redundancy costs a lot. It is certainly responsible for most of the difference in costs of carrier-grade verses consumer grade equipment. Optimizing multi-layer and intersystem redundancy will pay for itself via streamlining these otherwise competing or redundant redundancies.

Measuring System Level Availability & reliability

Measuring system availability is actually different from individual element availability. If a string of network elements are directly dependent on each other, say a common circuit which passed though each one, than the availability of the system follows the law of multiplying probabilities. In a 4 node system each of which is five-nines reliable, than the availability would be .99999 * .99999 * .99999 * .99999 = .99996. This partially explains why five-nines was chosen – because it is so close to unity/one that the degradation of availability due to directly dependent probabilities still is very reliable. So the network effect is reduced. (Choosing 0.95 reliability as a standard, for example, would mean that with a string of 12 dependent nodes, one would be in failure mode about half of the time). But with everything built to five-nines, if just one bad apple exists (say with even a stated four-nines reliability), than the string of four nodes as a group becomes .99987 - very close to the reliability of the lowest performing element. In fact, in this case the close-to-unity of the other devices nearly removes them from the equation; the dependent string will always be very near the value of the bad apple, which can be very bad if the apple is actually rotten. In this situation all of the careful design and investment in carrier-grade devices of five-nine reliability becomes economically worthless.

But actual networks are not simply directly dependent one on another. We have seen that redundancy is used to shield the service running in a network from the effects of a single failure in the components of the network. In reality, forms of Markov computations are the best tool for computing availability/reliability in multi-path redundant systems. "Markov Analysis (MA) is a powerful modeling and analysis technique with strong applications in the time-based reliability and availability analysis. The reliability behavior of a system is represented using a state-transition diagram, which consists of a set of discrete states that the system can be in, and defines the speed at which transitions between those states take

Not for distribution or reproduction.

© 2006, All information contained herein is the sole property of Pipeline Publishing, LLC. Pipeline Publishing LLC reserves all rights and privileges regarding the use of this information. Any unauthorized use, such as distributing, copying, modifying, or reprinting, is not permitted. This document is not intended for reproduction or distribution outside of www.pipelinepub.com. To obtain permission to reproduce or distribute this document contact sales@pipelinepub.com for information about Reprint Services.

place. As such, Markov models consist of comprehensive representations of possible chains of events, i.e., transitions, within systems, which in the case of reliability and availability analysis correspond to sequences of failures and repair…. The Markov model is analyzed in order to determine such measures as the probability of being in a given state at a given point in time, the amount of time a system is expected to spend in a given state, as well as the expected number of transitions between states, for instance representing the number of failures and repairs."

But the true value of Markov computations comes in applying it at the design stage. Markov mixing process in complex systems reveals little depressions of stability - think of marbles on a rubber sheet; stable depressions in the sheet form dry lake beds where the marbles will collect. Even if the sheet is slightly shaken, the marbles will bounce and role around, but most will stay inside their depressions – local zones of stability. This can allow richly interacting networks of only moderately high component reliability to be of higher reliability working together than each component devices achieves alone. In fact this is the real world of good network design. While few network designers actually use Markov mathematics explicitly, their decisions taken from a perspective of the complex network as a whole, with all of its interacting and redundant systems, frequently create Markov spaces.

Other approaches should be in the designer's tool-kit. Decision Analysis is can help determine the consequences of any specific design choice on the system and ability to meet utilitarian goals. But there are graphical ways of representing this and simplifying design. Perhaps more frequently used would be Reliability Block Diagram (RBD), Event Tree Analysis, or a Fault Tree diagram.

It all works together

"Downtime usually translates into significant productivity and revenue losses for many enterprises. Maximizing network uptime requires the use of operational best practices and redundant network designs in conjunction with high-availability technologies within network elements." [Cisco]

Availability is of course only one part of the complex concept of Carrier-grade. Several other "ilities": Reliability/Dependability, Maintainability, Manageability, Scalability, Accountability, and Durability are directly contained in the concept – sort of the faces of one six-sided dice. Too these, Securability and Survivability are recent critically expected features. Just because a single KPI, the notorious five-nines, is the flagship indicator, does not exclude the specifications for these other factors. This is very evident in the Bellcore documents which, in addition to all these, link in Safety. With software and servers, Reliability, Availability, Serviceability, Usability, and Install-ability combine in the acronym RASUI.

Getting Realistic: Big Customer Requirements

Not for distribution or reproduction.

© 2006, All information contained herein is the sole property of Pipeline Publishing, LLC. Pipeline Publishing LLC reserves all rights and privileges regarding the use of this information. Any unauthorized use, such as distributing, copying, modifying, or reprinting, is not permitted. This document is not intended for reproduction or distribution outside of www.pipelinepub.com. To obtain permission to reproduce or distribute this document contact sales@pipelinepub.com for information about Reprint Services.

The US Government has issued a comprehensive RFP [Networx Universal RFP; TQC-JTB-05-0001; 05/06/2005] for bidders wishing to supply the next generation network for the US Government. Considerable thought has gone into setting acceptable quality levels for networks – taking into account the differing use needs and technical facilities of each network technology. This is perhaps the most complete, openly viewable and usable description of realistic network service goals. Many dozens of tables describe the acceptable availability and other quality measures for each network technology. Further they go a step further and provide for both normal and mission critical network needs. "For certain services, when required by agency customers, two service levels are specified. Routine service levels apply for most Government applications. Critical service levels are defined for Agency applications requiring higher levels of availability, performance, or restoral <sic>criteria." Voice networks are generally given normal availability goals of 99.5% and critical service goals of 99.95%. Data network technologies are usually about one magnitude more stringent – 99.95% for normal use and 99.995% for critical service uses. Networx provides a modern and realistic reliability guideline for networks. It is the new baseline benchmark, below which a network is unacceptable, and above which is the narrow window of competitive differentiation.

Nevertheless, SLA's are subject to extreme competitive pressures, which have backed their availability promises right up against the wall. "Verizon Business's Network Availability Commitment is to have its IP Network available 100% of the time … Verizon Business will credit Customer's account if Verizon Business fails to meet this Network Availability Commitment during any given calendar month." ['Verizon business SLA for DSl.pdf'] Since 100% availability is very difficult to achieve, SLAs become a kind of amortization game. You give an SLA with the up front knowledge that you will inevitably give back some revenue to your customers. Access links from the customer premise into the network have always been the achilies heal when engineering for redundancy. Even with low failure rate, a MTTR of about 3 hours on access links forces availabilities that are likely far from 100%. Instead, the revenue loss from SLA penalty payments is offset by increased prices or customer satisfaction with the SLA. In the early days SLAs actually made money. One prominent carrier offered the only SLA and charged a premium because their 'network was so good it could support an SLA.' While truthfully, their network was no better than most other carriers, they earned 10x more in extra income from the higher prices charged than they had to payout for SLA violation rebates.

But today is perhaps different: claims of network performance can be validated more easily by customers. "Because of its built-in redundancy, Internap can offer aggressive performance guarantees, including 100% availability, 0.3% packet loss and 45 milliseconds of latency. "We offer 100% availability border to border, from where a customer intersects our network to where the customer's traffic leaves our network," Flynn says." [Case Study submitted by Carolyn Duffy Marsan of Network World to TMF]

Getting better and better

Not for distribution or reproduction.

© 2006, All information contained herein is the sole property of Pipeline Publishing, LLC. Pipeline Publishing LLC reserves all rights and privileges regarding the use of this information. Any unauthorized use, such as distributing, copying, modifying, or reprinting, is not permitted. This document is not intended for reproduction or distribution outside of www.pipelinepub.com. To obtain permission to reproduce or distribute this document contact sales@pipelinepub.com for information about Reprint Services.

Several organizations are devoted to helping make networks and network components better. For example, there is the Technical Committee on Communications Quality & Reliability (CQR). It focuses on and advocates worldwide communications and reliability on behalf of, and within, the Communications Society (formerly known as the Quality Assurance Management Committee (QAMC)). And while the customer driven goals may be less than five-nines, this level of performance is realistic and achievable across complex networks when best design practices are utilized. The fine-nines, never a requirement myth for equipment, is now moving from myth to reality for networks too.

And software, once considered hopelessly incapable of quality, now sets itself some of the highest reliability goals. CGL (Linux) OSDL standard allows system registration to 'carrier grade' standards. "Carrier Grade Linux' is a set of specifications which detail standards of availability, scalability, manageability, and service response characteristics which must be met in order for Linux to be considered "carrier-grade" (i.e. ready for use within the telecommunications industry). Improvements are expected. . "Carrier-grade is a term for public network telecommunications products that require up to 5 or 6 nines (or 99.999 to 99.9999 percent) reliability…. The term "5 nines" is usually associated with carrier-class servers, while "6 nines" is usually associated with carrier-class switches." [Wikipedia] As software and servers now press for five-nines, network elements are expected to support six-nines.

QuEST & TL9000

The first step towards quality is agreeing to common standards and uniform ways of measuring something. In a recent interview with Richard Morrow, Director at the QuEST Forum Project at the University of Texas at Dallas, he told us: "When QuEST Forum started there were about 75 different ways of measuring on-time delivery." [Which we note was larger than the number of participating companies.] "Now there is only one way to measure agreed to by all participants."

QuEST Forum [www.questforum.org] is a membership-based trade group which acts as an extension to ISO 9000 for the domain of telecommunications. QuEST is about improving the telecommunications supply chain – specifically about the vendor-service provider relationship. Membership is open to vendors, service providers, and customers. Members of the Forum set the standards and create the TL 9000 specifications. There are two specifications: one covering requirements and another detailing the methods for measuring and reporting quality KPIs. Currently they are at Revision 4. But the main activity of QuEST (much like ISO 9000) is certifying organizations as continuing to meet the TL 9000 standards – about 900 organizations have active certifications. It is not necessary to be a member to apply for certification and being a member does not insure certification. Certification is arduous and involves a multi-day audit. The basic premise is that a service provider can trust that a certified organization will provide a product of known and consistent features because they conform to the TL9000.

ISO 9000 defines strong quality processes and the TL9000 incorporates all of ISO 9000 language, binding these expectations into their certification standard. But Morrow notes that: "Having processes does not mean you will do them, so the Forum is driving a general movement from emphasizing process documentation to emphasizing positive outcomes from processes." The QuEST Forum does this

Not for distribution or reproduction.

© 2006, All information contained herein is the sole property of Pipeline Publishing, LLC. Pipeline Publishing LLC reserves all rights and privileges regarding the use of this information. Any unauthorized use, such as distributing, copying, modifying, or reprinting, is not permitted. This document is not intended for reproduction or distribution outside of www.pipelinepub.com. To obtain permission to reproduce or distribute this document contact sales@pipelinepub.com for information about Reprint Services.

through periodic certification audits and regular collection of data on actual performance to the expected goals.

A certified organization must provide regular measurements, as stated in the measurements handbook, to a central repository which is charted by QuEST, itself certified, and located at the University of Texas at Dallas in Richardson, TX. Feedback of network field experience from service providers is critical to the vendors to improve their products. SOTS – Standard Outage Template System: provides the technology (web portal based) for collecting and reporting on these KPI. This is the quoted 'single agreed standard' and common technology for reporting field performance data from service providers to their vendors. When it started only six manual data submissions were made in a month; now more than 600 data submissions are made each day into the fully automated system. Certified contributors can get reports on this information and how they compare to the rest of the population of certified organizations – but otherwise the data is confidential and proprietary to the QuEST Forum. Even examples of these real-world quality metrics are not available to non-members.

While the telecommunications community builds automatic restoration and redundancy into network designs, in order to improve the service available of every network connection, we have seen that it is still important to have high standards for individual network elements and element modules. Indeed, understanding this, the TL9000 specifically excludes redundant systems restoration used in failover from the computation of an element's down time.

Morrow: "What you do in reaction to the numbers is what counts. It is the impact of the equipment on the customer- essentially this is the customer pain - which is behind the measures. You will work to drive this down if you have industry-wide measurements to compare your performance to."

TeleManagement Forum

Most of the SLA work at the TMF is mature and wrapped up. The SLA Handbook is one of the most widely distributed OSS standards. But the TMF never stops – and it has a current program which aims to do much the same thing as the data collection of the QuEST forum, except for OSS/BSS instead of the supply chain.

Business Transformation Benchmarking Program of the TeleManagement Forum provides a comprehensive and international database of service provider business performance metrics. The first round of metrics associated with service delivery and customer interactions is established and the project is moving forward to gather more results with an expanded base of metrics. Service providers who contribute data on their performance can see how they compare with their competitors and global ecosystem. The whole point is to allow Service Providers to identify internal areas which need improvement along with a comparative realization of what should be the realistic service goal and therefore how much improvement should be possible. Companies contributing their details to the benchmarking study receive free access to the results. Benchmarking results are available for purchase to other subscribers.

Agents

Not for distribution or reproduction.

© 2006, All information contained herein is the sole property of Pipeline Publishing, LLC. Pipeline Publishing LLC reserves all rights and privileges regarding the use of this information. Any unauthorized use, such as distributing, copying, modifying, or reprinting, is not permitted. This document is not intended for reproduction or distribution outside of www.pipelinepub.com. To obtain permission to reproduce or distribute this document contact sales@pipelinepub.com for information about Reprint Services.

But management systems - OSS and BSS - have not yet collectively moved towards concrete measures of five-nines. Current best practices and vendor software solutions just do not cut it; new technology and approaches are needed to reliably manage and report on these vast, complex, next generation networks with their rich multi-service platforms. Perhaps the only technological approaches that will punch OSS performance into five-nines Carrier-grade are true service-oriented architectures and autonomic agents. "The general approaches for dealing with flaws are the same for both hardware and software: (1) prediction and estimation, (2) prevention, (3) discovery, (4) repair, and (5) tolerance or exploitation." [Garland, CMU] Agents offer a convenient level of granularity at which to add redundancy—a key factor in developing robust systems. "Robustness can be achieved through redundancy, and we hypothesize that agents by being naturally smaller and easier to program than conventional systems, are an appropriate unit for adding redundancy." [CAI03 Autonomic Computing Workshop] Agents, when coupled with service-oriented architectures, designed upon web-services, .NET, or RMI, offer a chance to build and deploy applications and management systems that themselves are assembled like networks are assembled from components. Then, the same principles of design which allow for network components to reach six-nines availability and for networks to perform at full carrier-grade five-nines can be used to assemble networks of intercommunicating software agents.

Last Word

It seems likely that the origin of five-nines as a telecom standard came from analyzing "what can we do?" rather than "what must we do." Networks, services and equipment were much simpler back then and five-nines while probably a stretch goal, was achievable in equipment. Today's networks, services, and equipment are much more complicated and contain 1000's of times more physical components and 100's to 1000's of times more software code. Solid state components are individually more reliable and software quality has arguably improved. The expectation for equipment is now six-nines or seven-nines and for software and servers it is five-nines. For many today these remain stretch goals, but there is no question that everyone in the telecom ecosystem expects and demands high availability.

But TL9000 shows us that carrier-grade is more than a measure of availability or any other single quality measure. Carrier-grade is actually an intangible expectation and explicit promise that the equipment vendors will provide the best equipment possible and a clear, immediate communication of issues related to equipment. And that service providers will also provide the best network possible to their customers and keep a clear and immediate communication channel open concerning service impacting situations. And lastly that the supply chain communication is two way, with feedback from the buyer going to the provider so they gauge and support continuous improvement. These behaviors and expectations are captured in the TL9000, particularly its sections on Management Responsibility and Product Realization.

So, it becomes important to measure Carrier-grade quality consistently and accurately using the talked about common standards. It also becomes important to measure and provide "true" values for network availability based on service, i.e. the customer experience. The US government has provided a realistic benchmark with

Not for distribution or reproduction.

© 2006, All information contained herein is the sole property of Pipeline Publishing, LLC. Pipeline Publishing LLC reserves all rights and privileges regarding the use of this information. Any unauthorized use, such as distributing, copying, modifying, or reprinting, is not permitted. This document is not intended for reproduction or distribution outside of www.pipelinepub.com. To obtain permission to reproduce or distribute this document contact sales@pipelinepub.com for information about Reprint Services.

its Networx procurement specifications. We suggest that it is a good starting point of well-defined measures and metrics from which to establish a dialogue with customers, vendors and service providers about the fundamental performance requirements, and then aim for perfection. Maybe we will even get that carrier-grade 100,000 year civilization – if we succeed at establishing redundancy of our civilization too.

If you have news you'd like to share with Pipeline, contact us at editor@pipelinepub.com.

Not for distribution or reproduction.

© 2006, All information contained herein is the sole property of Pipeline Publishing, LLC. Pipeline Publishing LLC reserves all rights and privileges regarding the use of this information. Any unauthorized use, such as distributing, copying, modifying, or reprinting, is not permitted. This document is not intended for reproduction or distribution outside of www.pipelinepub.com. To obtain permission to reproduce or distribute this document contact sales@pipelinepub.com for information about Reprint Services.