THE TOLLY GROUP

The authoritative, unbiased source for IT certification, research and testing

February 2006

A white paper commissioned by Avaya, Inc.

Document #206107

Building Survivable VoIP for the Enterprise

Leveraging Avaya MultiVantage® Solutions to Deliver Business Continuity

TOLLY Up to Spec CERTIFIED

Terms of Usage

USE THIS DOCUMENT ONLY IF YOU AGREE TO THE TERMS LISTED HEREIN.

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase must be based on your own assessment of suitability. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions and certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks. Commercially reasonable efforts were made to ensure the accuracy of the data contained herein but errors can occur.

The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. The Tolly Group provides a fee-based service to assist users in understanding the applicability of a given test scenario to their specific needs. Contact us for information. When foreign translations exist, the English document is considered authoritative. To assure accuracy, use documents downloaded from The Tolly Group's Web site.

Tolly Group Vendor Service

With more than seventeen years experience validating leading-edge Information Technology products and services; The Tolly Group has built a global reputation for producing accurate and unbiased evaluations and analysis. We employ time-proven test methodologies and fair testing principles to benchmark products and services with the highest degree of accuracy.

Our "Up-to-Spec" service provides the custom testing complement to the "standard", granular tests offered in "Tolly Verified". See our Tolly Group Home Page.

Plus, unlike narrowly focused testing labs, The Tolly Group combines its vast technology knowledge with focused marketing services to help clients better position product benchmarks for maximum exposure.

This document was authored by:

- Charles Bruno,
  Executive Editor
  The Tolly Group

Table of Contents

Building Survivable VoIP for the Enterprise

Introduction

For every Enterprise, telephony is an essential business tool. Loss of telephony almost universally translates into lost corporate productivity. While a construction company, say, can keep building in the field when corporate has an outage, the impact is soon felt when the field can no longer reach corporate.

Furthermore, where businesses are built on telephony-oriented applications like contact centers or interactive voice response services, every minute of downtime means more than just lost productivity, it means lost revenue that might never be recovered.

And, while IP-based telephony has introduced previously unimaginable flexibility, telephony and related applications, conversely, can now be adversely affected if IP data network outages occur to which the telephony system cannot properly respond.

With this in mind, Avaya has architected its MultiVantage® telephony solution to go beyond the mere elimination of outages caused by any "single point of failure" in its systems or the network across which it runs.

Its distributed architecture and effective implementation allow virtually uninterrupted business continuity even in the face of disastrous outages – like the complete loss of a main data center. Additionally, Avaya offers sophisticated "preventative" measures that can dramatically improve both conversation quality and connectivity when the IP WAN is performing marginally or experiences a connectivity failure not quickly recognized by the network routers.

To illustrate these capabilities, Avaya built a comprehensive, multi-location Enterprise "microcosm" in the company's Doral, FL, Customer Solutions Lab facility. The company commissioned The Tolly Group to conduct a detailed examination of these capabilities "in action" and provide an analysis of the results and their implications for Enterprise customers.

Executive Summary - Survival of the Fittest

Overview

Backup data centers, distributed systems and emergency planning are all essential parts of a business continuity strategy. You've got your data centers mirrored on opposite sides of the continent, your regions and branches are equipped with servers and telephony gear and you've invested in building a multi-path wide-area network among all these disparate locations. But unless the computing and telephony gear is architected to "survive" by automatically reconfiguring to mitigate failure conditions, your investment might not deliver the return you expected.

Understanding exactly how your critical systems – and our focus here is telephony – will respond in both "worst" case and lesser outages is essential to assuring that your business continuity plan will deliver as expected.

VoIP You Can't Kill

Imagine, for a moment, the "worst case" – that your main data center goes down – completely and totally all at once. An earthquake has cut all its connections with the outside world and delivered sufficient damage that even your diesel-powered generators provide little benefit. All your centrally-controlled systems - including your telephone systems - have been affected.

How long will it take before the users located outside of the disaster zone will have access to their data applications running at your alternate site? Will they be down for hours as the backup systems are brought online and checked out? Might it turn into a day or more if complex systems need to be brought "in sync" with the state of the failed data center or offline or offsite backups need to be brought in and loaded?

In less than the time it takes personnel to make even initial assessments of the situation, your Avaya-based telephony system components – leveraging distributed intelligence – have detected the outages (within as little as three seconds) and have begun the process of automatically reconfiguring themselves to reconstitute the remaining elements into a "best available" network.

In under five minutes all of your remaining locations have rebuilt themselves as a single, unified "5-digit dial" telephony system. It makes one wonder whether most users will even notice that the telephone system was down at all?

Yes, our tests proved that even in the most massive failure imaginable, the Avaya MultiVantage telephony anchored by Communications

Manager 3.0 automatically and without any human intervention re-established a unified (i.e. 5-digit dial) corporate telephony system utilizing all of the resources in the locations that remained online.

Follow-on Outages Handled

What are the chances of a second outage following close on the heels of the first? Several years ago when a massive power failure hit the Northeast United States, many companies took multiple hits.

In some locations without generators, battery backup may have kept them online for some time. Then, as batteries drained, those sites went offline as well.

After our initial test, we deliberately introduced another serious failure into our telephony network already dynamically "rebuilt" by the Avaya components – we completely severed the IP network connectivity of one of the regional offices from the rest of the corporation.

As before, this office recovered its full functionality in just a few minutes. In fact, Avaya's system automatically re-routed their 5-digit corporate dialing across the PSTN so users could continue to dial other corporate locations as they could before the network failure.

IVR in an Instant:

While not a formal part of this test, Avaya engineers demonstrated how systems like Interactive Voice Response can be remapped to backup systems within minutes and needing only a single command from the telephony system administrator.

Controlled Recovery – Your Business Drives the Recovery Process

When disaster strikes, the toll on your business can be enormous. The last thing you want is for the recovery process of your telephony system to trigger additional uncontrolled downtime.

Some telephony vendors tout automatic recovery as a beneficial "feature." As soon as the network is up, the system attempts automatically to reconfigure to its previous state. In fact, when you realize that "automatic" in this case is a synonym for "uncontrolled," it is something to be avoided as an "automatic" reconfiguration could be triggered in the middle of the work day and cause outages itself.

Avaya believes that your business requirements should drive when the "recovery" to original configurations should take place. Thus, this process is placed under the complete control of the system administrator who can "rebuild" the system to its original configuration either a component at a time if need be or all components at the same time to ensure a smooth transition back to the original state. Such a reconfiguration can even be scheduled to take place during off hours, unattended, to minimize any potential disruption to business.

Never a Single Point of Failure

Knowing that you've got superior protection in the event of catastrophe, let's turn to the more mundane situation – dealing with a single point of failure within a telephony infrastructure.

No matter how well a vendor builds a box, human nature remains out of their control. An incorrect cable disconnected in a data center can trigger an "outage" even if the supposedly failed gear is working perfectly – but just can't be "seen" by the rest of the network.

Anticipating this and other situations, Avaya has delivered a system that dynamically deals with and "heals" outages often without any interruption at all to the system users.

The brains of the system runs on a mirrored pair of dedicated Avaya servers. The two are in constant contact with each other via a dedicated fiber-channel link (which allows them to be situated up to 10km apart - for "safety" sake). "Health Check" communications between them via the IP network allow for them to determine which should control the system at any given time.

When we "downed" one of the servers in mid-conversation with other calls "ringing," there was an instantaneous, non-disruptive failover to the alternate server. No user would even notice that the primary server had failed.

As we moved to studying the chassis that housed the interface boards that supported traditional analog/digital phones, VoIP phones and WAN interfaces, we illustrated that there, too, a single failure could rapidly and automatically be overcome.

When the chassis power supply was removed, the switchover to the optional second power supply was imperceptible from a service perspective. When the card that handles communications between the interface chassis and the main server was pulled, calls were uninterrupted while the backup board took over that function.

Similarly, when the cards that handled the VoIP phones were pulled, conversations remained up (as that card isn't needed after the conversation is established) and the backup card rapidly took over.

As traffic passes between the VoIP network and a traditional phone network, a media processor card makes that transformation. This card, too, can have a backup. In the event of a failure, all active calls stay up.

Importantly both the media processor and the control LAN (CLAN) processor cards are considered "system-level" resources. That is, they are available to any VoIP phone in the system and not just the VoIP phones "connected" to the chassis in which these cards reside.

Rebounding from Outages:

Depending on the nature of the outage, many users will not notice that the telephone has gone down because, for them, it hasn't.

- In a WAN outage, only users tied to an affected media gateway experience a three- to five-minute outage as the network reconfigures to an alternative media server. For users not on the affected gateway, network services remain uninterrupted.
- In the event of an interruption between the phone and the control LAN card, existing phone calls remain unaffected while only feature operations, such as conferencing, are temporarily suspended until the phone registers with another gatekeeper or control LAN card.

Thus, even in the cases of multiple failures where the main and the backup cards go "down," VoIP phones automatically will seek out other available telephony resources – even those physically located in other sites if need be.

Ironically, this translates to an even better likelihood of survival for VoIP phones than traditional phones since, unlike traditional phones, the VoIP phones are not physically "tethered" to any one chassis. Thus, they have even more options for recovery in any number of possible failure situations.

Robustness at the Branch

At the branch office, where connectivity options are typically more limited and network bandwidth may be limited as well, Avaya offers a number of intelligent features that not only provide robustness in the face of failure but can optimize the user experience in situations where network resources are limited.

From Marginal to Magnificent – Converged Network Analyzer

So far, we've looked at "black or white" situations – where a component is either down or up. Your redundant network "kicks in" when a primary link fails but what happens when the primary path is not down but severely degraded or when a link failure remains invisible to your network routing protocols because of the VPN technology you are using. Without the Avaya Converged Network Analyzer (CNA) 3.0, both scenarios spell trouble. With it, your users will likely never notice either problem.

Once calls are in progress, VoIP telephony end-points have no control over the path that their call takes – and thus a degrading link will degrade calls with no mitigating action taken until and unless the link drops completely.

With CNA implemented on the network, link quality is actively monitored and routes can be changed in real time to optimize voice and other critical traffic as well as to detect and route around outages not immediately detectable by routers.

In our test, we degraded an existing conversation by impairing – but not breaking – the link it was traversing. Without CNA, the sound became choppy and of marginally low quality for business use. When CNA was enabled, it immediately instructed routers to use an alternative path between the end points. Without a break in the conversation and with no actions required by other party to the call, voice quality immediately returned to normal.

In another scenario, we modeled a common scenario – the use of a VPN tunnel as part of the wide-area network. In such cases, routers lose visibility to the part of the connection within such "tunnels" and cannot immediately respond to an outage within the VPN.

When we deliberately triggered such an outage, it produced over 20 seconds of "dead air" before the router (without CNA) recognized the outage and routed around it. Unfortunately, such a length of time would likely cause users to consider the call "disconnected" and respond by hanging up.

When repeated after CNA was enabled, a barely audible "tick" of less than a second in duration was detected as CNA immediately detected the outage and instructed routers to route around it. Conversation participants would have been completely unaware that an outage even occurred.

Avaya's intelligent, distributed implementation of IP-based telephony in Communication Manager 3.0 combined with its impressive Converged Network Analzyer 3.0 capability can deliver superior performance and availability sure to satisfy even the most demanding Enterprises.

Essential Elements of IP Telephony

System Control

Figure 1: Avaya S8710 Media Servers

Every telephony system requires a component that controls all the activities for the unified, corporate wide system. In Avaya's implementation, that control element is found in the S8710 Media Server. (This is implemented in a rackmountable enclosure using standard server hardware that Avaya has certified and is delivered as a turnkey system.) That system is deployed in a fault-tolerant paired configuration at the HQ/data center location. Fully functional media servers, either single-server (e.g. S8500) or dual-servers (e.g. S8710), that mirror the main system, are typically deployed at regional data centers. Avaya calls these "Enterprise Survivable Servers" – or ESS – and any one of these on the IP network can take over the entire network should the redundant system at the main location go offline for any reason.

For branch offices, customers can choose to implement an ESS as well. Alternatively, they can implement just "local" survivability. This feature allows a branch to be functional if it is cut off from the the main Media Server as well as all of the ESS systems.

Connectivity

Figure 2: Avaya G650

Now, to the hardware. Years ago the "control" software, telephone connections and trunk lines would all physically be housed in the same box. With today's modular approach to telephony that is no longer true. Functions are implemented in modules – cards that can be slotted into a modular chassis that allows a customer to "build to order" the features and functions for a given location.

Avaya offers two different housings – its G650 which has 14 slots. This is the chassis of choice to deploy in larger locations. Up to five G650 chassis units can be "stacked" and interconnected to provide additional capacity. Such stacks behave as a single integrated unit. For smaller locations, the more compact H.248 gateway provides the housing for the various connectivity modules.

IPSI

Figure 3: Sample H.248 system with installed modules

This mandatory module – the IP Server Interface – is responsible for all the communications between the G650 chassis and the Media Server – all of which takes place across an IP network. Without this module none of the other resource cards can be part of the system. Fortunately, multiple IPSI cards can be provisioned – one primary, one for backup – in a G650 stack.

DCP

The Digital Communications Protocol module is used to provide the physical connectivity for traditional Avaya digital phones. While usually present, it is not a mandatory component of today's VoIP systems.

CLAN

The Control LAN module is responsible for controlling VoIP phones and linking them "logically" to the intelligence of the Media Server. While typically a CLAN module will be configured to control co-located VoIP phones, it is perfectly capable of providing this service to any VoIP phone on the IP network. Thus, the flexible nature of the CLAN adds dramatically to the overall robustness of Avaya's VoIP solution.

MedPro

The Media Processor card is responsible for converting voice from IP to TDM and vice versa at the point where calls travel between the VoIP and traditional telephony domains.

Trunk Cards

DS1 Interface

The DS1 Interface module is responsible for digital connectivity to the Public Switch Telephone Networks (PSTN) to enable long distance and local telephone service. It supports ISDN Primary Rate Interface (PRI), Central Office trunks, Direct Inward Dial (DID) trunks, and TIE trunks.

Central Office Trunk

The Central Office Trunk module is responsible for analog connectivity to the PSTN to support central office trunking.

Survivable Scenarios – Across the Campus and Across the Country

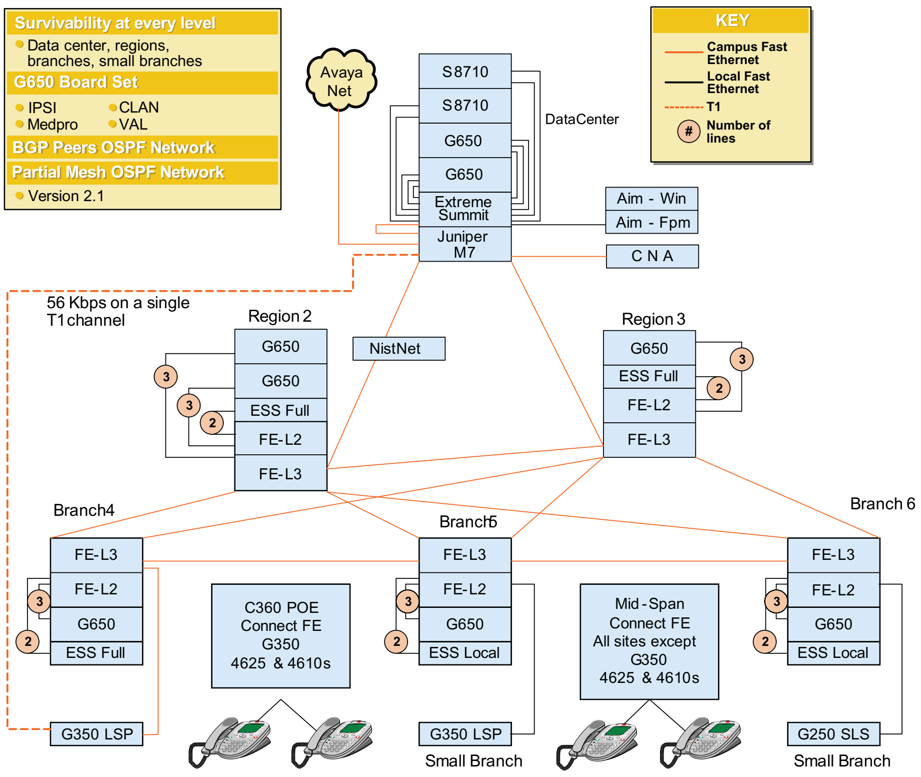
Setting the Stage – A Corporate Telephony Microcosm

Overview

To prove Enterprise-class survivability, typical enterprise equipment was brought to bear in a dedicated lab. The test environment included telephony gear as well as all supporting IP LAN and WAN infrastructure for a headquarters location, two large regional offices, three large branch offices as well three smaller branch offices – nine locations in all. All locations were linked via a partial mesh network that provided at least two communications paths among the HQ site, regions and large branch offices (each small branch office had an IP connection to its nearest large branch office). (See Figure 1, next page.)

Furthermore, each location was outfitted with an appropriate level of survivability option. As noted earlier, Avaya telephony users are not limited to leveraging "backup" gear physically co-located with them. In many cases, users can "fallback" and "failover" to network resources located anywhere on their company's internal IP network.

Figure 4: ESS Lab Test Bed



Avaya's Communication Manager 3.0 drove the telephony part of the test. Avaya's Converged Network Analyzer was used for the network quality and rapid recovery tests.

Corporate HQ

At the main "corporate" site, the system is anchored via an S8710 Media Server pair. VoIP and digital phone connectivity is provided via a "stack" of G650 media gateways – presenting a single system image. The media gateway is outfitted with a variety of redundant components explained in detail in the testing section later in this document.

Regional Sites

Under normal circumstances, the telephony hardware located at the regions communicates with and is controlled by the S8710 Media Server with which it communicates across the IP network. In our test, an Enterprise Survivable Server (ESS) was also deployed at each region. The ESS, as noted, is capable of taking over control of not only its own region but any other sites on the internal IP network should the main S8710 Media Server pair become unavailable or unreachable for any reason.

As in the headquarters configuration, the G650 media gateway was deployed as the base unit to contain all of the various connectivity modules. Because the hypothetical user base at the region was deemed smaller than at HQ, single, stand-alone G650 media gateway (rather than "stacks") was deployed.

Branch Sites

Branch and region size, naturally, will vary depending on customer. For our test, we configured a "larger" branch office that used a G650 media gateway and "smaller" branch offices outfitted with either G350 or G250 "H.248" media gateways. These smaller branches were on the IP equivalent of "tail circuits” having Layer 2 connectivity with a single larger branch and being part of that larger branch's IP subnet.

Each "large" branch was also outfitted with an ESS system but those systems were configured as "local" servers. That meant that they would only advertise their availability to local resources – called "community" by Avaya – and not the corporate network at large.

The small branches had "local survivable processor" modules in their G350 units so that they could still function as standalone phone systems should their Ethernet/IP connectivity to the larger branch be cut off.

Network Details

The Headquarters and all regional/branch locations were connected to an internal IP network. This network implemented a partial mesh and provided at least two paths between any two locations. (The only exception to this statement was with the "small" branch offices which had just a single Ethernet path to a single "large" branch.)

Since only a single test set was related to the effects of restricted bandwidth and network impairments, the basic connectivity across "locations" was via Fast Ethernet connections provided by Layer 3 Extreme Summit switches. Additional Layer 2 connectivity was provided by switching modules integrated into several of the Avaya platforms.

The network implemented OSPF to control path selection with a Juniper M7 router implemented at the HQ site. Avaya's Converged Network Analyzer system was used for the tests involving optimizing call quality and rapid detection of outages.

The CNA system involved deployment of the CNA server – which was implemented as a BGP peer to the Juniper router – as well as deployment of a number of CNA "agents" around the internal network to provide real-time monitoring of path quality on the IP network.

To create the error conditions that would challenge CNA, testers relied upon two general network connectivity scenarios. The first scenario allowed the NIST net to impair the data network. The second scenario involved a Layer 2 tunnel set up through the network. This is used to show how CNA responds to network conditions that only impacted the VPN.

First, a network simulation and impairment tool was implemented between the HQ and a branch location. It appeared to the users of the network as a two-port IP router. The public domain NistNet (*http://snad.ncsl.nist.gov/itg/nistnet/*) provided this function.

Another test involved simulation of a Layer 2 "tunnel" that blocked the Juniper router's ability to make an immediate detection of a downed link (something that CNA can detect). To implement this, the OSPF link was directed through a Layer 2 VPN built on an Extreme switch.

Test 1: Single-Server Failure Background

Avaya implements its "brains" for Communications Manager 3.0 as a pair of coupled "media servers" – in our test, the 8710s. These systems are built on a base of Linux which has been "hardened" by disabling unused components of the OS.

The systems not only communicate via an IP/Ethernet connection but also through a dedicated fibre-channel link. According to Avaya, this link is used to provide a high-speed path for the memory shadowing that helps provide for "hitless failover" should a server go offline. To aid in detecting the need to trigger that failover, Avaya notes that a constant series of health checks flow between the systems across Ethernet connections.

Proof Points

Various methods were used to verify which of the media servers was active. One call was set up across it and a "conversation" started. Another was attempted and the target station allowed to ring.

At this point, power was removed from the active server simulating an instant and complete failure of that device. The backup server was observed to take over instantly without the active or ringing calls being affected.

Scenarios Supported

Proves resistance to "single point-of-failure" with respect to the main media server.

Deployment Notes

The use of fibre channel between the two servers allows for systems that are "tightly coupled" from a failover perspective but that can easily be deployed in locations up to 10 kilometers (6.2 statute miles) apart in order to avoid any outage should environmental conditions cause difficulties at one of the locations.

Test 2: Single IP Server Interface Module Failure

Background

The IP Server Interface – IPSI – module in the G650 provides the communications path for all chassis modules to communicate with the Media Server or its backup ESS systems. The Avaya architecture allows for another IPSI module to be inserted in another G650 of a stack. One module will always be active and the other will function as a hot standby ready to come online automatically and immediately should the active IPSI fail or otherwise go offline.

Proof Points

Testers verified that both IPSI modules were connected and which one was actively handling communications. A call was initiated between a phone on the local G350 and another station in the network and the connection was left open. Another similar call was placed but allowed to ring unanswered. At this moment, the IPSI card was pulled. Testers verified that the call "in progress" did not drop. The "ringing" call continued to ring and was answered without problem.

Scenarios Supported

Proves resistance to "single point of failure" with respect to communications between the G650 chassis and the main Media Server or any ESS system.

Deployment Notes

While there is no reason to believe that the IPSI modules would fail, the fact that the module serves as the path through which all other modules must communicate with the server, it is a good idea to spec a backup IPSI configuration for critical locations.

Test 3: Single Control LAN (CLAN) Module Failure

Background

The CLAN module in the G650 provides the control function for a group of VoIP phones and H.248 Media Gateways. Without the CLAN, a VoIP phone would lose features like speed dial and conferencing. Furthermore, while an in-progress conversation would not be interrupted, no new conversations would be able to be set up.

Proof Points

Testers verified that the VoIP phone being used was registered to and controlled by the CLAN module which was to be "failed." A call was placed and connected from that phone to another phone on the system. The CLAN module was failed by removing it from the G650 chassis.

While the conversation was unaffected, the VoIP phone functions – speed dial, conference and other "soft buttons" – did not work. This was anticipated as the CLAN module providing those services was no longer available.

Within 30 seconds, testers observed that the VoIP phone screen resets (without breaking the call in progress) as the VoIP phone locates and registered with another CLAN module and became, again, fully operational.

In fact, while not part of our original test plan, our testers were interested in knowing what would happen if the second (and only other) CLAN module on the G650 was also failed. When that failure was introduced the phone sought out another available CLAN resource elsewhere on the IP network and, once again, was fully operational in only 30 seconds.

Scenarios Supported

Proves resistance of VoIP phone users to "single point-of-failure" of the CLAN module to which their VoIP soft or hardphones are currently registered.

Deployment Notes

It is important to understand the scope and flexibility of CLAN robustness. Unlike, for example, the IPSI where only a single IPSI module is ever active in a chassis, all CLAN modules are active and handling VoIP phones.

Furthermore a VoIP phone is not limited to registering with a CLAN module at its own physical location. Depending on system configuration choices, a VoIP phone in, say, Chicago, can register with CLAN module located in, say, St. Louis if no CLAN is online in Chicago.

Test 4: Single Media Processor (MedPro) Module Failure

Background

The Media Processor module in the G650 provides conversion of voice from IP to TDM and vice versa. Any traffic moving between the VoIP and traditional telephony segments of the network requires the services of a media processor. A given G650 chassis can be outfitted with more than one media processor module to provide extra capacity as well as backup.

Proof Points

Testers set up a call between digital phones connected to separate IP-connected G650 units in different "locations." These phones would need to pass through the media processors in their respective G650 units to communicate.

The media processor in one of the units is taken offline. As expected the call drops. The call is redialed and is immediately handled by a second media processor in the same chassis or stack.

Scenarios Supported

Proves resistance of VoIP phone and digital phone users to "single point of failure" of the Media Processor module that is required to traverse the IP-TDM boundary.

Deployment Notes

It is important to understand that a media processor is always involved when a VoIP phone attempts to communicate with a non-VoIP phone. It is also used between digital phones when those phones need to use the IP backbone to communicate. It is not used for calls between two IP phones.

Test 5: Power Supply Module Failure

Background

The importance of the power supply requires no explanation. The G650 can support a second power supply even though the entire chassis can be run with just one power supply.

Proof Points

The test scenario, as in most previous cases, involved a call in progress and a call ringing. In this state, the power supply was pulled. Neither call was interrupted and users were unable to detect any changes as the failover was instantaneous.

Scenarios Supported

Proves resistance of all G650-contained resources to "single point-of-failure" of the main power supply.

Deployment Notes

It is important to note that a single power supply can run the entire chassis.

Test 6: Main Server or WAN Failure

Background

The Media Server provides the "brains" of the corporate telephony system. Avaya provides the option of provisioning a "simplex" or "duplex" configuration of those servers – our test used a "duplex" configuration. The failover between machines in a duplex configuration was the focus of Test 1.

In a disaster-scale failure where all connectivity to the central HQ site ceases, the telephony architecture must offer a distributed, "full strength" failover solution that will allow the rest of the Enterprise to regain full functionality (as much as is possible without access to any non-redundant, HQ-based telephony applications) automatically and rapidly.

Avaya delivers this through deployment of its Enterprise Survivable Servers (in essence "clones" of the S8710 Media Server). Multiple ESS machines can be deployed across the Enterprise. The various distributed hardware chassis around the Enterprise are configured to establish connections to a priority ordered list of ESS systems should contact with the Media Server cease for three minutes. (*Note: The time is set to three minutes in order to avoid "flapping" into a complete network re-configuration should a transient connection failure occur. This time can be customer configured to be greater.*)

Proof Points

The test scenario, as in most previous cases, involved a call in progress and a call ringing. In this state, both the active and stand-by Media Servers at the HQ location were taken offline by disconnecting them completely from the IP network. PINGs to these devices were, as expected, unanswered.

The various IPSI modules in the network have a "heartbeat" communication with the controlling Media Server every three seconds. Should that go unanswered, the three-minute timer starts. If the heartbeat communication is not re-established before that timer expires, the IPSIs will "register" with the highest priority ESS server in an attempt to re-establish a functioning telephony environment.

Testers observed that, without any intervention, the G650 and other telephony system components initiated a reset after the three-minute timer expired and within one or two minutes the remaining sites were back online using all available resources.

Additionally, after the systems were successfully online, testers introduced an additional failure scenario – designed to "fracture" the remaining network and isolate a single regional office. All connectivity between this region and the core of the network was removed. As in the previous failure, within three minutes it initiated a recovery, established a connection to a local ESS and brought all local resources online.

This scenario was repeated failing the WAN rather than the Media Servers. This produces the same results – no access to the Media Server from remote locations. Results were the same.

Scenarios Supported

Proves resistance of all G650-contained resources to "single point-of-failure" of the S8710 Media Server and/or the failure of one or more WAN links. Furthermore it illustrates the rapid and automatic "re-build" of the telephony environment even in the face of multiple major failures.

Deployment Notes

It is important that the system recovery process be under the control of the customer and synchronized with the business recovery plan. This is especially important as there is some unavoidable down time associated with "switching back" to the pre-disaster configuration. Some competing solutions simply attempt to reconfigure automatically as soon as resources are on line again. That is a bad idea as such an "automatic" function can "automatically" crash critical functions like call centers at an inopportune moment.

Avaya allows the "migration" back to pre-disaster configurations to be controlled in a modular fashion and either initiated "on command" from the system administrator or scheduled to occur automatically at a time that is beneficial for the corporation – at 2 a.m., for example, rather than at 2 p.m.

Test 7: Branch Resilience and Control

Background

Branches often communicate with the core of the network via WAN links - and sometimes rather low-speed WAN links. It is not unusual for a WAN connection to fail for reasons outside of the customer's control. When a backup WAN connection is available it is important that it can automatically be brought into service. Furthermore, while customers want to utilize the fixed cost IP network link to the core of the network, slow links can only carry a certain number of simultaneous calls before being overloaded and delivering degraded call quality to all users of the link. This multi-faceted test case illustrates how Avaya handles both of these situations.

Avaya's Inter Gateway Alternate Routing – IGAR – provides a sophisticated set of functions to optimize use of system LAN/WAN resources when bandwidth is constrained and does this "behind the scenes" so that end users need not be aware of network infrastructure issues or change their dialing habits.

Proof Points

Testers disconnected the primary LAN connection. The G350 (H.248) media gateway at the branch location automatically re-routed call control (to the Media Server) across the backup WAN connection. Because that WAN was only 56 Kbps, the system used the constrained WAN for call control only while it routed the voice call (bearer) through the PSTN.

In the follow-on scenario, the IP network link into the core was configured to allow only two simultaneous calls (as more would degrade quality). Testers initiated a third call and verified that it automatically was routed over the PSTN.

Scenarios Supported

Proves resistance of branch office deployments both to single WAN failures, as well as the system's innate ability to optimize use of resources when link capacity is limited.

Deployment Notes

It is important to note that using Avaya's Inter Gateway Alternate Routing allows continued use of 5-digit dial – and thus a better user experience – even when outages or usage levels require that those calls traverse the public switched telephone network to reach the target "in house" phone.

Test 8: Dynamic Alternate WAN Routing – Converged Network Analyzer (CNA)

Background

At the moment a conversation initiates across an IP network, network routing protocols should see to it that the best path is selected. And, should a path fail, those same protocols should re-route the conversation on behalf of its participants – and that should happen without causing the call to be interrupted.

While OSPF-based routers can detect a "link down" in around a second, they cannot unfortunately detect links that they cannot "see." Today, with various VPN and tunneling options used to map private IP networks across service provider networks, the OSPF network may well traverse links that are invisible to it. Should such links fail, the recovery time could be 15 to 45 seconds – long enough to cause users to deem their call "interrupted" and hang up.

Perhaps an even worse scenario is when the quality of the path degrades dramatically but does not fail completely. In such case, the OSPF protocol still deems the path valid and does not re-route the call even though quality might be degraded to a point where participants can barely understand each other.

CNA uses both server-based and agent-based measurements to monitor the availability and quality of the IP network in real time. Using industry standard routing protocols – the CNA server uses local BGP peering to direct OSPF routers – CNA reconfigures and optimizes the network in real time – with calls in progress - without even interrupting the call.

Proof Points

Testers placed a call traversing the network link which would be failed or degraded (as appropriate). A constant audio stream ("music on hold") was played across the link so that testers could evaluate the end-user experience.

In the "failure" scenario, VPNs were created to act as tunnels and to hide the presence of several physical network connections from the OSPF network. With CNA disabled, the VPN connection was removed and, as anticipated, traffic for the call ceased – approximately 20 seconds of "dead air" ensued before the OSPF network reconfigured.

The network was reset to its original state, CNA was enabled and a new call established as before. The link was failed. In less than one second, CNA detected the failure on the VPN and instructed the OSPF network to reroute almost instantly. The call remained undisturbed with only a brief "tick" as the outage was being bypassed.

In the "degradation" scenario, CNA again was disabled and a call was initiated as above and traversing the NistNet network emulator. Once in progress, a script was invoked at the emulator to deliberately impair the link by injecting packet loss. Testers could easily hear the result of the impairment as the "music on hold" exhibited both breaks and distortion – ultimately sounding "wobbly" and of insufficient quality for business communication. As the link had not "failed" the OSPF network continued to use it for live traffic.

The network was reset and CNA was enabled. When the impairment was again injected, the "wobbly" sound could be heard for less than 1 second. Within that time, CNA had detected the unacceptably high packet loss and had used its BGP connection to instruct the OSPF network to use a different path. The call remained uninterrupted and it is questionable whether a participant in the call would have even been aware that a problem existed – so rapid was the recovery.

Scenarios Supported

Proves that the Avaya solution set not only protects from failure better than any standalone telephony solution or unaided OSPF routing but that "marginal" conditions can be routed around quickly and dynamically with no disruption even to calls in progress – or any other IP traffic – currently traversing the marginal path.

Deployment Notes

The importance of CNA transcends just the telephony aspects highlighted here. As its domain is the entire IP network, any and all corporate traffic – voice, data and video – can and will benefit from the presence of CNA.

CNA gathers its data from a combination of server-based measurements and agent-based measurements using embedded agents that are placed at key points in the network. Those CNA agents can be implemented as small standalone units or integrated into existing Avaya phones and network infrastructure components – Extreme LAN switches for example – in which case the agent has zero physical footprint.

###

Information technology is an area of rapid growth and constant change. The Tolly Group conducts engineering-caliber testing in an effort to provide the internetworking industry with valuable information on current products and technology. While great care is taken to assure utmost accuracy, mistakes can occur. In no event shall The Tolly Group be liable for damages of any kind including direct, indirect, special, incidental, and consequential damages which may result from the use of information contained in this document. All trademarks are the property of their respective owners.

The Tolly Group, Inc.
3701 FAU Blvd. Suite 100
Boca Raton, FL 33431
Phone: 561.391.5610
Fax: 561.391.5810
http://www.tolly.com
info@tolly.com