HIGH AVAILABILITY CONSIDERATIONS FOR AN END-END CABLE IP NETWORK

Navin R. Thadani
Cisco Systems, Inc.

Abstract

As Cable MSOs start deploying PSTN replacement voice services (over IP), availability and reliability become important considerations. However, there is a lot more to high availability than the number of nines on a certain network device.

In addition to looking at device level availability, it is also important to understand the availability of the end-end network taking into consideration the various system level inter-dependencies. Further, it is even more important to understand, evaluate and design a network keeping in mind "service availability". In the case of a voice service, two popular service availability metrics are the number of calls dropped and the number of ineffective attempts.

This paper reviews the availability requirements of a "primary line" (PSTN replacement) voice service, dispels some of the popular five 9s myths about the PSTN; and then establishes a framework by which to analyze and design a network to achieve the required level of service availability.

The paper also outlines some of the modifications in terms of redundancy as well as routing optimization that may be required on the edge, in the regional networks as well as the backbone networks in order to support PSTN equivalent voice over IP networks. In other words, it reviews some of the changes that need to be made for transport at the edges and between distribution networks in order to support highly available and reliable services such as voice over IP and digital broadcast video. It outlines the evolutionary path of the current High Speed Data IP networks to highly available service delivery platforms in the future.

PSTN AVAILABILITY MYTHS

The issue of availability is surrounded by several myths and misconceptions. Three of the popular myths are mentioned below …

1. The PSTN provides 99.999% (five 9s) of availability and reliability end-end.
2. One needs fives 9s level availability on every platform in order to achieve PSTN equivalence.
3. Every failure in the network is recovered in less than 50 milliseconds.

THE FIVE NINES MYTH.

PacketCable (VoIP Availability and Reliability Model for the PacketCable™ Architecture - PKT-TR-VoIPAR-V01-001128) does an excellent job in dispelling some of these myths. It notes that the idea of PSTN reliability being FIVE 9s is incorrect. It clearly breaks down the different subsections of the PSTN network and draws a direct analogy to an equivalent IP network. As per these requirements, the end-end availability of a VoIP network should be greater than 99.94% to achieve equivalence with the PSTN.

In addition, PacketCable also specifies some "service availability" metrics. These include the number of calls dropped and the number of ineffective attempts.

As per the report, there should not be more than 1 in 8000 calls dropped (or cutoff calls), and no more than 5 in 10,000 ineffective attempts. These are exactly the same as the PSTN requirements on availability and service availability as set forth in Bellcore GR series specifications.

Cutoff calls arise due to failures in the bearer path of the voice call. At the two end points of the bearer path (that is the CMTS facing the customer and the PSTN gateway facing the PSTN in the case of an on-net to off-net call) a cutoff call may occur due to a failure on a line card and a failure to copy call state information to the standby line card (in the event that there is redundancy). However, in the rest of the network, there is no concept of call state (being IP). Let's say there is a failure, in a core router in the network, and it takes 40 seconds to reroute traffic to the alternate path. One has to imagine that an end-user would get frustrated and hang up the phone after a certain period of time. This should also be considered to be a cutoff call.

Hence in the realm of IP, a cutoff call could occur due to two reasons. Inability to maintain call state at the end-points in the event of a failure, and/or, inability to recover traffic within a certain cutoff call threshold in the event of a failure at the end-points or in the core of the network.

In reality, the cutoff call threshold is user dependent, but most IP telephony providers are settling on 3 seconds as that threshold. That is, if there is a failure in the network, and the user experiences "dead air" for more than 3 seconds, they would hang up and it would be counted as a cutoff call. Cutoff calls are sometimes referred to as "Calls Dropped" and can also be measured as defects per million. For example, 1 in 8000 cutoff calls could also be referred to as 125 Defects Per Million DPM(Calls Dropped) or DPM(CD).

Ineffective attempts arise due to failures in the signaling path of a voice call. As per the PacketCable definition, "an ineffective attempt occurs when any valid bid for service does not complete because of a fault condition (e.g., hardware or software failure)". That means, if a user is trying to make a call but cannot due to a signaling path failure, it is counted as an ineffective attempt. However, here again we have to define a threshold. The popular ineffective attempts threshold that exists in the industry today is 30 seconds. Hence if a user is trying to make a call, it doesn't get through, he/she tries again and the call is completed the second time, as long as the whole process completes in less than 30 seconds, it is not counted as an ineffective attempt. Ineffective Attempts could also be expressed as Defects Per Million or DPM (Ineffective Attempts) or DPM(IA). So 5 in 10,000 ineffective attempts could be stated as 500 DPM(IA).

THE 50 MSEC MYTH

Originally the 50 msec threshold was established in the 1980s because the voice channel banks that were used in carrier networks could not tolerate failures that lasted more than 200 msec. When failures exceeded that threshold, a Carrier Group Alarm (CGA) would be activated causing the channel bank to perform a "trunking condition" procedure that would terminate all connections on that particular T3 line. Since the outage budget had to be less than 200-300 msec, 50 msec emerged as the de facto standard. This decision was ironic because by the time the de facto standard was actually adopted, newer technology allowed a CGA timer of 2 secs. We must bear in mind that this is for circuit switched

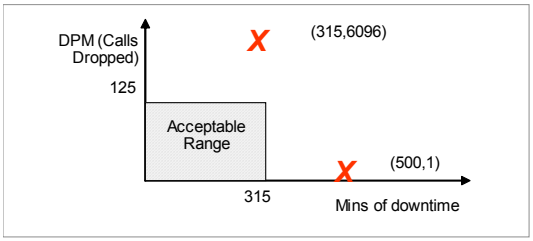
technology. In the case of IP, all signaling is message based. Hence there is no hard and fast requirement for 50 mesc recovery. Rather, a more practical "user perceived threshold" of 3 secs can be adopted for a "dropped call".

Given the findings in PacketCable, it is clear that …

1. The PSTN does not offer 99.999% end-end. Although certain components in the PSTN network may be five 9s (as is also the case with IP equipment) the end-end network meets a specification of > 99.94%.
2. It follows that all devices in the network do not have to be five 9s, rather, the end-end network should be > 99.94%.
3. All failures do not have to be recovered in less than 50 milliseconds. Failures should be recovered within the calls cutoff and ineffective attempts threshold and the end-end network should cause no more than 1 in 8000 calls cutoff and no more than 5 in 10,000 ineffective attempts. The industry accepted practical thresholds for calls cutoff is 3 seconds and that of ineffective attempts is 30 seconds.

These three metrics together (availability/downtime, cutoff calls and ineffective attempts) are required to define an operating range. We can't use only availability to understand end-user service experience. The end-end availability budget as specified by PacketCable is 99.94% and this translates to 315 minutes of downtime per year.

Now, consider for example, a network that has one major failure and a user sees an outage for 500 mins. That means he/she cannot make a call for more than 8 hours. Is this acceptable? If they were on the phone at the time of failure, it would constitute only 1 dropped call, but exceed the downtime budget. At the same time, there could be repeated failures in the network, each of 3.1 seconds in duration. This would allow us to have 6096 Dropped Calls but still be within our 315 minute downtime budget.



Similar logic can be used to see why we need the third metric – Ineffective Attempts. Let's say for example, that the call control server is down, but the data path is up. This would mean 100% availability as per our downtime definition but the user will still not be able to make any calls.

CALCULATING AVAILABILITY AND SERVICE AVAILABILITY METRICS

In this section, we will cover some basic theory around calculation of these metrics, but will not get into too many details around the math. The main focus of this paper as mentioned earlier is to establish a framework by which to analyze and design networks for High Availability.

Availability:

Availability is commonly defined as MTBF/(MTBF+MTTR). Such a definition for availability is good for a simplex system (a system comprising one box). However, in a network that consists of a number of trunks and routers, most failures are partial failures. As a result of a partial failure some customers will not receive service, while others have un-interrupted service. Also, even within a router or a switch only one line card may go down, and users connected

to other line cards may not see any disruption in service. Hence availability is defined with respect to a customer of the network. To compute availability, we only need to consider the components along the path needed to provide service to a single customer and then average this over all customers.

In addition to partial failures described above, we also have to take into consideration redundancy. For example, certain components such as line cards may be configured in terms of 1:N Active standby or 1:N Load sharing.

In order correctly calculate the availability of a single part such as a line card or route processor; one has to take into account several factors such as …

a. Switchover time – the amount of time taken to switchover from the active component to the standby component.
b. Active Coverage Factor – the probability that a failure is successfully detected and switched over
c. Standby Coverage Factor – the probability that the standby is in working condition and can successfully take over.

We can use a Markov State definition for each component like a route processor, line card etc within a router or a switch. This is illustrated in Figure 1 for 1:N redundancy.

Given the value of the parameters in the legend, the above Markov chains can be solved giving the probabilities in all the different states in the chain.

For a given type of redundant part, the combined part availability, combined part MTBF and combined part MTTR are calculated as shown in the equations in Figure 2.

Based on the above equations, once we calculate the availability of each and every component along the path of a voice call we take a product of these individual availability numbers to get the availability of the overall system or network.

It is important to note that this gives us just the availability and downtime of the system or network and does not provide us any insight in terms of whether the service (in this case voice) is available or not. For that we need to examine two other "service availability" metrics; calls dropped and ineffective attempts.

CUTOFF CALLS/ CALLS DROPPED / DPM(CD)

From a high level, based on the definition of dropped calls, it is easy to see that this metric is a function of the MTBF.

The Calls Dropped contribution by each component (line cards, route processor, chassis, power supplies etc) along the path of a single user needs to be calculated.

For each component, we calculate the DPM(CD) as shown in Figure 3 (all parameters are assumed to be in hours) …

For an average 3 minute call. This can also be expressed more generically as shown in equation A in figure 3…

Where for each failure, the switchover time (in case of a redundant part) or the repair time (for a non redundant part) is greater than the calls dropped threshold of 3 seconds.

INEFFECTIVE ATTEMPTS / DPM(IA)

We follow a similar process to calculate the Ineffective Attempts contribution per component along the path of a single user.

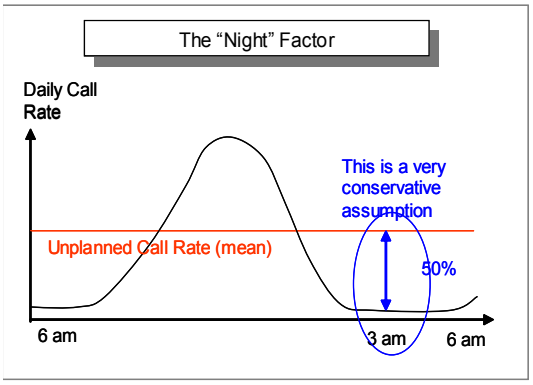
Again, we only count each failure where the switchover time or repair time is greater than the ineffective attempts threshold of 30 seconds.

TREATMENT OF PLANNED DOWNTIME

From the derivation of the equation of Calls Dropped, we see that the term "in-coming call rate" appears, but is cancelled from the numerator and denominator. This means that the DPM(CD) (and DPM(IA) for that matter) is for a uniform call rate. Since in the previous section we were calculating unplanned DPM(CD) and DPM(IA) the implicit assumption is that it was for the mean call rate over a 24 hour period.

However, when equipment is upgraded or we have to perform any kind of scheduled or planned maintenance, there is also a certain amount of downtime and associated loss of service in terms of calls dropped and ineffective attempts. To calculate the effect of scheduled outages on service availability, we can use a similar method as above with the exception that instead of a summation across a number of random failures (as is the case with unplanned outages), we look at only calls dropped or ineffective attempts that are caused due to the outage time during the upgrade (say twice a year).

Most often, scheduled maintenance is done late at night (say 3am) to minimize the impact of downtime on service availability. Now, the incoming call rate at 3 am is significantly lower than the mean call rate. Hence we would have to factor down the DPM(CD) and DPM(IA) by the ratio of the call rate at 3am to the mean call rate, to arrive at terms that are comparable and additive.



In fact an analysis of the average call volume to the call volume at 3 am (maintenance window) shows a 10-15% night factor. Please see figure 4.

EXAMPLE OF USING THE OUTLINED FRAMEWORK TO ESTIMATE THE AVAILABILITY AND SERVICE AVAILABILITY OF A CERTAIN NETWORK DESIGN

We will now use the theory outlined above and work through an example of how to estimate the availability and service availability of a certain network design. In working through this example we also highlight the importance of a systems view, and the system level interdependencies that come into play. Further, we also stress the role that the layer 3 routing architecture plays in high availability in a network.

Consider the network shown in Figure 5. It consists of a non redundant CMTS connected to a non redundant aggregation router. This then connect to a pair of redundant core routers which then connect to a pair of redundant switches in the data center behind which are the voice components like the Softswitch, PSTN gateway, provisioning servers etc.

Step 1: Reliability Block Diagram

The first step in understanding the availability and service availability characteristics of a network is to lay out a detailed reliability block diagram of all the components involved in the path of the voice call. Please refer to figure 6 for more details.

In our basic example, the CMTS consists of 3 components; the RF line card, the route processor and the FE uplink card. This is a simplistic scenario because in reality there are a lot more components including power supplies, timing cards, software (on the route processor and line cards) etc. So our 3 components are shown in series in the reliability block diagram below, because they are single points of failure.

The aggregation router is also assumed to have 3 components; the FE line card, the route processor and the GE line card. The FE line card is shown in series because it is a single point of failure, but the route processor and the GE line card are shown in parallel because they are assumed to be intra-chassis redundant in our hypothetical configuration.

Similarly, one has to define the detailed RBD for the rest of the network as well. This includes the core router (in which all components will be in parallel), the Data Center switch, the PSTN gateway and the IP Softswitch.

Figure 6 represents the hardware components. However, we also need to model software as series or parallel components. We assume the CMTS has software on the route processor and line card. In this case since they are non redundant, they are modeled as serial components. Similarly software on the aggregation switch and core router route processors have to be modeled in parallel as they are set up in a redundant fashion.

Step 2: Failure scenarios – Estimating MTTR and switchover time.

The second step in this process is to evaluate in detail the potential outage for a voice call in the event of failures for each component along the path of the voice call. In order to do that, we have to evaluate the upstream and downstream outage for each failure. Further, we need to take into account system level dependencies such as routing. For example if a line card fails, the outage time may be dependent on how fast layer 3 can detect the failure and route around it, both in the upstream and downstream directions.

In addition to the unplanned failures described above, we also need to estimate the outage caused due to planned upgrades.

The table shown in Figure 7 outlines the possible outage times due to various possible failures in the network. As mentioned above, this takes into consideration (where applicable) the routing system interdependencies. Further, at this stage, we also need to estimate the outage time due to software upgrades. For example, in the case of the CMTS it may take from 5-11 minutes (including reboot time and routing table set up time) for a CM/MTA to register with the provisioning system and then start passing traffic. In the case of the aggregation router, this time will also be dependent on the route table establishment time. This can be anywhere from a few seconds to a few minutes depending on the complexity of the routing setup.

Step 3: Estimating MTBF and failure rates

Having laid out the reliability block diagram and the failure scenarios, we need to estimate the MTBF of each component (hardware and software). Hardware MTBF is usually obtained from manufacturers databases. Software MTBF typically is collected from network operations be measuring the unplanned software reboots or other failures over a period of time for a sample set of devices.

With each of these assumptions in place we now use the theory described in the previous section to calculate the availability, calls dropped and ineffective attempts contribution per element (such as CMTS RF line card, route processor etc).

The idea is to reduce the above diagram to its serial equivalent components by calculating the combined MTBF and combined MTTR of each of the components involved. This is done using the Markov States described in the previous section.

The overall availability, DPM(CD) and DPM(IA) for the entire network are calculated using the formulas shown in figure 8.

The availability/downtime results for Case 1 are represented by the first bar in figure 10. The DPM(CD) and DPM(IA) results are shown in figure 11.

Now, in Case 2, we make some modifications to the network design and add some High Availability features to the network devices.

Some of these are listed below.

- Redundancy at the edge of the network (on the CMTS). Line card, route processor and WAN card redundancy.
- Inter-chassis redundancy on the aggregation routers. The CMTS is then dual homed to the redundant pair of aggregation routers.

Please refer to figure 9 for more details on the network topology for case 2.

In addition to the topology modifications from Case 1, in Case 2 we are also assuming some form of routing optimization for High Availability. Since this is a simple directly connected Ethernet network, we would need to reduce the SPF computation hold timer to about 1 second (default value being 5 seconds) so as to reduce some of the failures in case 1 (which were about 6 seconds) to <3 seconds so as to avoid any dropped calls.

In cases where the network is more complex, with say Layer 2 SONET (or any multi-access) connectivity between the aggregation routers and a distribution layer, the routing optimization can get significantly more complex. In this case we may need to reduce the OSPF hello and dead timers in addition to the SPF computation timer. The default values of hello and dead timers in OSPF are 10 seconds and 40 seconds respectively; and were set more than 10 years ago keeping in mind data applications that did not need fast convergence. As a result, without optimization it is possible to see some failures causing outages in the region of 40-45 seconds. However, reducing the dead timer to say about 1.5 seconds and setting the hello timer to 0.5 seconds with three hellos per dead timer will get the detection time down to about 1.5 seconds. Hence it would be possible to see total outages in the region of less than 3 seconds. In certain cases depending on the complexity of routing in the network, static routing in

certain parts of the network and reduced timers in others can lead to even sub second convergence.

There is however a tradeoff in this case where if the timers are set too low, it may cause instability in the network. This can cause serious problems as a failure on one line card which would have otherwise affected service only to a set of customers, has now propagated to the rest of the network taking down service for a far grater number of subscribers.

In addition to the routing architecture modifications, we also assume certain basic HA features on the network elements. For example in the CMTS, if the route processor fails, the cable line cards are not reset and the CMs are not dropped. We also assume that call state in maintained during switchover to the standby route processor (whether it is within the same chassis or implemented in an inter-chassis fashion).

Given the discussed enhancements from case 1 to case 2, we have to re-define the Reliability Block Diagrams and the failure scenarios and redo the mathematical analysis.

The results for Case 2 are shown in figures 10 and 11.

In case 3, we assume no additional network topology changes. However, we implement advanced HA features which enable us to upgrade software or hardware with interruption to service. For example, we can switch off one route processor, have all CMs/MTAs be serviced by the standby route processor (without dropping calls or losing call state), upgrade software on the primary RP, and then switch back over again.

In addition, implementation of advanced monitoring and early warning (especially on the RF side) HA software on devices will help further reduce downtime and improve service availability.

The results for case 3 of the network are also shown in figures 10 and 11.

COMPARISON OF RESULTS

As can be seen from figures 10 and 11, the base case network can be expected to be down for about 102 minutes per year for the average customer. This consists of about 56 minutes of unplanned failures (that can happen at any time of the day) and about 46 minutes of planned downtime (that occurs at 3 am in the morning, when the likely-hood of a call in progress is extremely low).

The PacketCable availability budget for this portion of the network is 71 mins of downtime per year. Hence the base case network is about 71% over the PacketCable budget.

By introducing redundancy on the CMTS and the aggregation routers, optimizing the routing architecture and implementing HA features that maintain calls sate even in the event of RP failure, enabling the line cards to continue forwarding traffic we can reduce these numbers by 60%. This brings us to a total of about 41 minutes of downtime per year, which is significantly better than the PacketCable guidelines.

By further adding more advanced HA features like the ability to upgrade software without service interruption and advanced HA monitoring features, this number can be driven down to 15.5 minutes of downtime per year.

In the case of Calls Dropped, we see that the base case network will have about 26 calls dropped per million and by making the recommended enhancements, this can be reduced to about 9 DPM(CD). Similarly DPM(IA) can be reduced to about 20 from a current 128.

It is important to note that PacketCable does not break down the DPM(CD) or DPM(IA) budget by network component, so it is difficult to derive a 'budget' for this portion of the network. However, it is important to note, that this portion of the network (the CMTS, Local IP network and voice components) can contribute only about 5-7% of the end-end DPM(CD) budget. This means that even if the CM, the HFC plant, and the IP backbone (or PSTN network depending on the mode of transport) contribute about 90% of the 125 DPM(CD) budget, the network will still meet the guidelines.

Cable MSOs must conduct a similar analysis for the CM and the HFC network to determine whether the end-end network meets the PacketCable guidelines for PSTN equivalent voice service.

CONCLUSION

There is much more to availability than the number of nines on a box. In order to design a highly available network, one has to keep in mind end-end network availability and more importantly the *service availability*. In the case of voice, these are calls dropped and ineffective attempts.

When analyzing and designing a network for availability, there are complex system level dependencies and interaction between devices that need to be considered. Routing plays a critical role in highly available networks.

In addition, for an IP network to be equivalent to a PSTN in terms of availability, it does not have to be five 9s end-end; rather, it needs to be greater than 99.94%. It should also meet the
end-end service availability metrics of < 125 DPM(CD) and <500 DPM(IA).

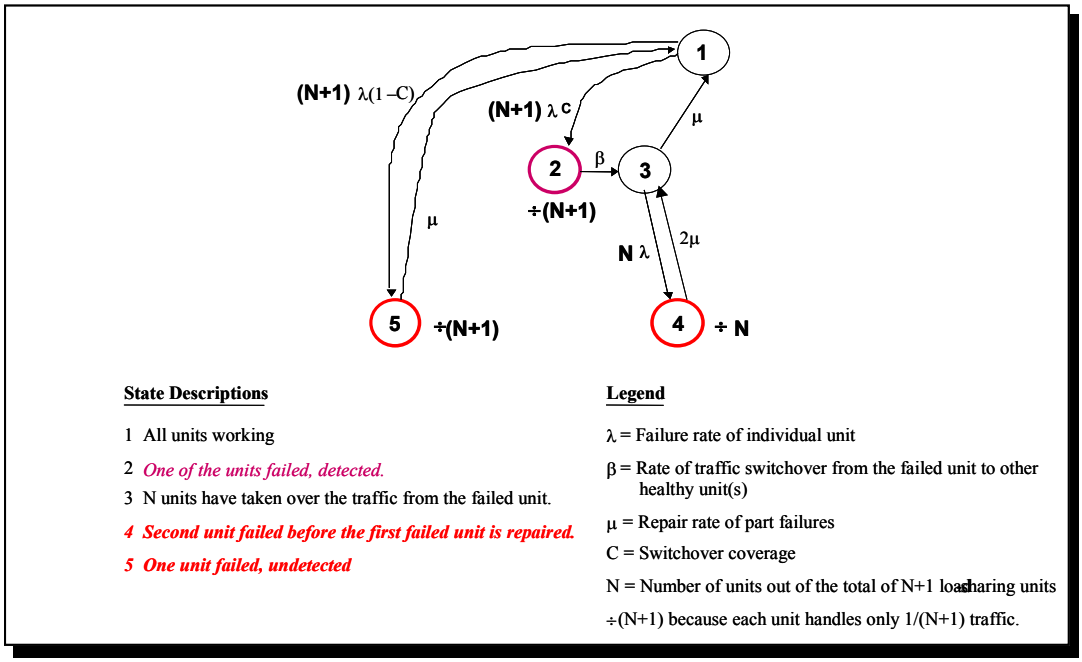
It follows that all failures do not need to be recovered in less than 50 msec as long as the number of dropped calls and ineffective attempts do not exceed the above requirements.

The framework established in this paper can be used to evaluate the availability and service availability of an IP network, study the effect of redundancy at different points in the network, and make an economic based decision in terms of the increase in availability for a certain amount of capex.

Lastly, it is possible for a well designed IP network to meet and in certain cases exceed the availability of the PSTN.

ACKNOWLEDGEMENTS

The author would like to thank the following people from Cisco Systems for their invaluable guidance and contribution to this paper – John Chapman, Jim Forster, Madhav Marathe, Henry Zhu, Alvaro Retana, Paul Donner, and Latha Vishnubhotla.



State Descriptions

1 All units working

2 *One of the units failed, detected.*

3 N units have taken over the traffic from the failed unit.

4 Second unit failed before the first failed unit is repaired.

5 One unit failed, undetected

Legend

λ = Failure rate of individual unit

β = Rate of traffic switchover from the failed unit to other healthy unit(s)

μ = Repair rate of part failures

C = Switchover coverage

N = Number of units out of the total of N+1 load sharing units

÷(N+1) because each unit handles only 1/(N+1) traffic.

Figure 1 (1:N Active Standby – Markov State Diagram)

$$Availability_{combined} = sum\ of\ \ probabilities\ that\ the\ redundant\ \ parts\ \ are\ in\ non\ \ failure\ markov\ states$$

$$MTBF_{combined} = \frac{1}{sum\ of\ \ transition\ rates\ \ from\ non\ \ failure\ states\ to\ \ failure\ states}$$

$$MTTR_{combined} = \frac{1 - Availability_{combined}}{Availability_{combined}} \times MTBF_{combined}$$

Figure 2: Availability Equations

$$\frac{\sum_{all-incidents>3\sec} Existing\_calls\_dropped \times 10^6}{Total\_Calls\_Attempted}$$

$$\frac{\sum_{all-failurescenarios>3\sec} (Existing\_calls\_at\_time\_of\_failure) \times (number\ of\ \ failures\ of\ that\ scenario) \times 10^6}{Total\_calls\_in\_one\_year}$$

$$\frac{\sum_{all\ failurescenarios>3\sec} (Incomin\ g\_Call\_rate \times length\_of\_call) \times (\frac{1}{MTBF} \times 365 \times 24) \times 10^6}{(Incomin\ g\_call\_rate) \times 365 \times 24}$$

$$\sum_{all-failurescenarios>3\sec} \frac{3}{60} \times \frac{1}{MTBF} \times 10^6$$

Figure 3: Calls Dropped Equations

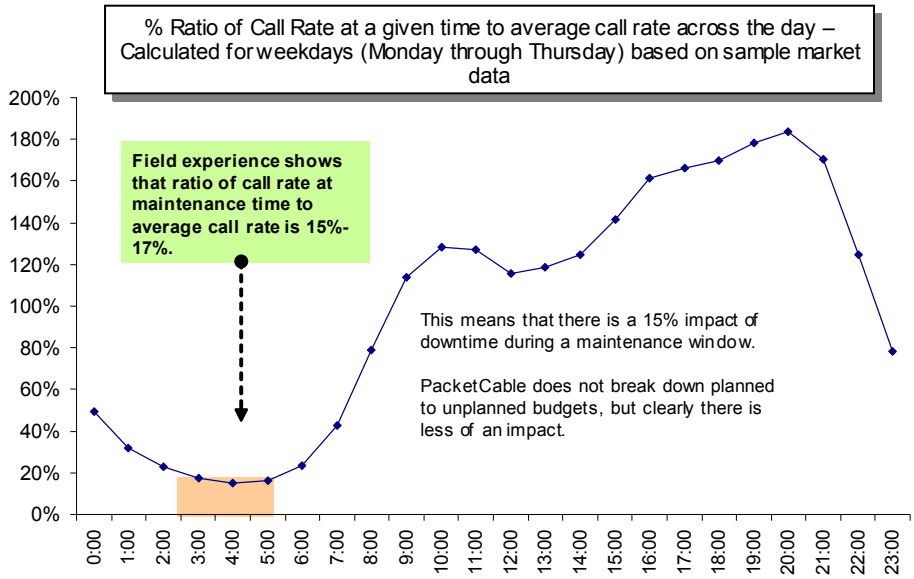


Figure 4: Example "Night Factor" – average call rate across a 24 hr period

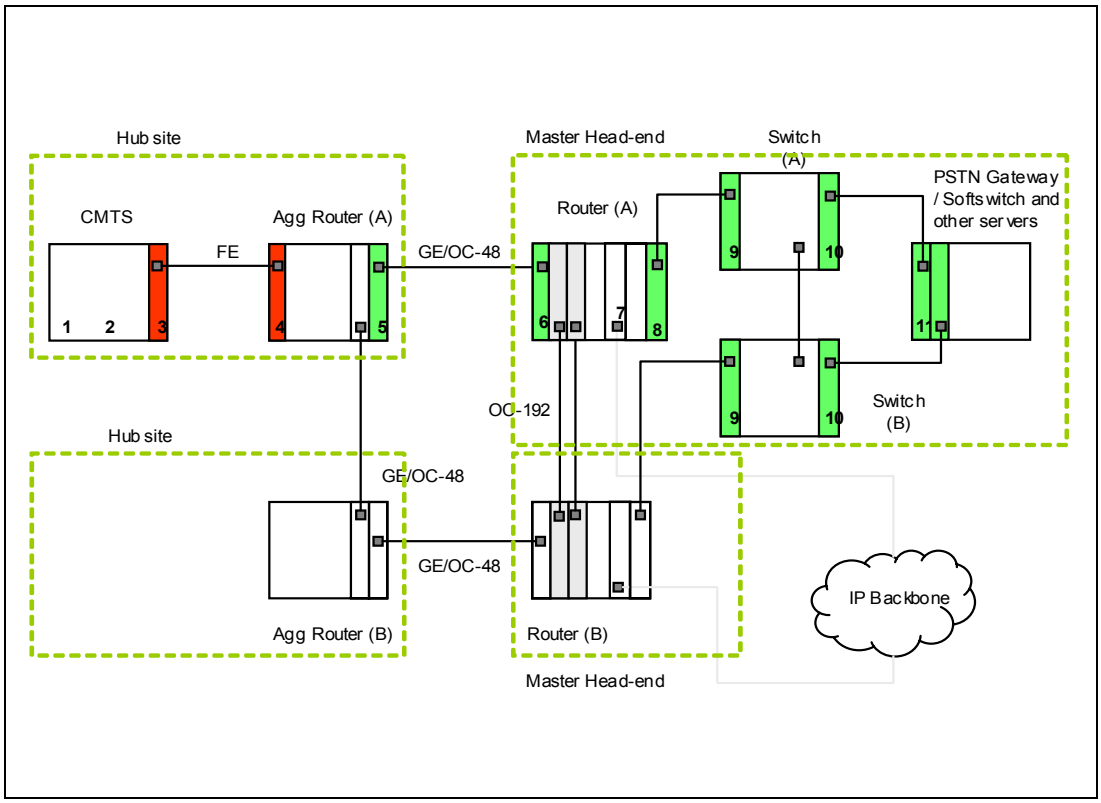
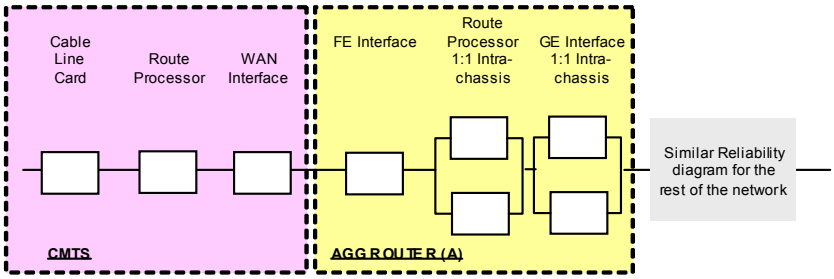


Figure 5 : Case 1: Network diagram

RELIABILITY BLOCK DIAGRAM (RBD)



MTBF, MTTR, Switchover time and coverage assumptions for every component in RBD

MTBF (hrs)	120,000	150,000	250,000	250,000	400,000	250,000
MTTR	3 hrs	3 hrs	3 hrs	3 hrs	3 hrs	3 hrs
Switchover Time	NA	NA	NA	6 secs	6 secs	6 secs
Active Coverage Factor	NA	NA	NA	98%	98%	98%

Similar Assumptions for the rest of the network.

Figure 6: (Reliability Block Diagram and Markov Parameter Assumptions)

Example Network - BASE CASE
Unplanned Failures

	Upstream	Down-stream	Upstream Notes	Downstream notes	Total Outage	Calls Dropped ?
CMTS						
1 Route Processor	3 hrs	3 hrs	This is a Single point of failure. Once this component fails, there is no path upstream and the outage time depends on someone physically going to change the card. According to PacketCable this time will be in the region of 4hrs	Same as upstream	3 hrs	YES
2 Cable Line Card	3 hrs	3 hrs	Same as above	Same as above	3 hrs	YES
3 WAN Card	3 hrs	3 hrs	Same as above	Same as above	3 hrs	YES
Aggregation Switch						
4 Route Processor	2 secs	2 secs	Lets say the switch has dual route processors, but is not running any specific HA software. The route processor failure resets the line cards. The directly connected core router detects the failure within 1 sec and takes 1 sec to recompute its routes via the second aggregation switch. The outage in this direction would be 2 sec.	Once the FE line card is reset, the CMTS detects it within 1 sec and takes 1 sec to recompute its routes via the second aggregation switch	2 secs	NO
5 FE Line Card	3 hrs	3 hrs	This is a single point of failure	This is a single point of failure	3 hrs	YES
6 GE Line Card	0 secs	2	The CMTS continues forwarding traffic to Agg router 1 because its is the only path available	The core router detects the failure of the GE card on Agg Router (A) almost immediately, and then delets that route from its table. It then starts forwarding traffic intended for the CMTS through Agg Router (B) via the OC192 interface. Agg Router (B) still has a valid path for the CMTS because it is connected to a different line card on Agg Router (A)	2 secs	NO

Similar FAILURE SCENARIOS for the rest of the network

Figure 7: (Failure Scenario Examples for Base Case 1 Network)

$$Availability_{network} = \prod_{all\ series\ equivalent\ components} Availability_{component}$$

$$DPM(CD) = \sum_{all\ series\ equivalent\ components\ in\ bearer\ path} DPM(CD)_{component}$$

$$DPM(IA) = \sum_{all\ series\ equivalent\ components\ in\ signaling\ path} DPM(IA)_{component}$$

Figure 8: Formulas to calculate end-end network and service availability

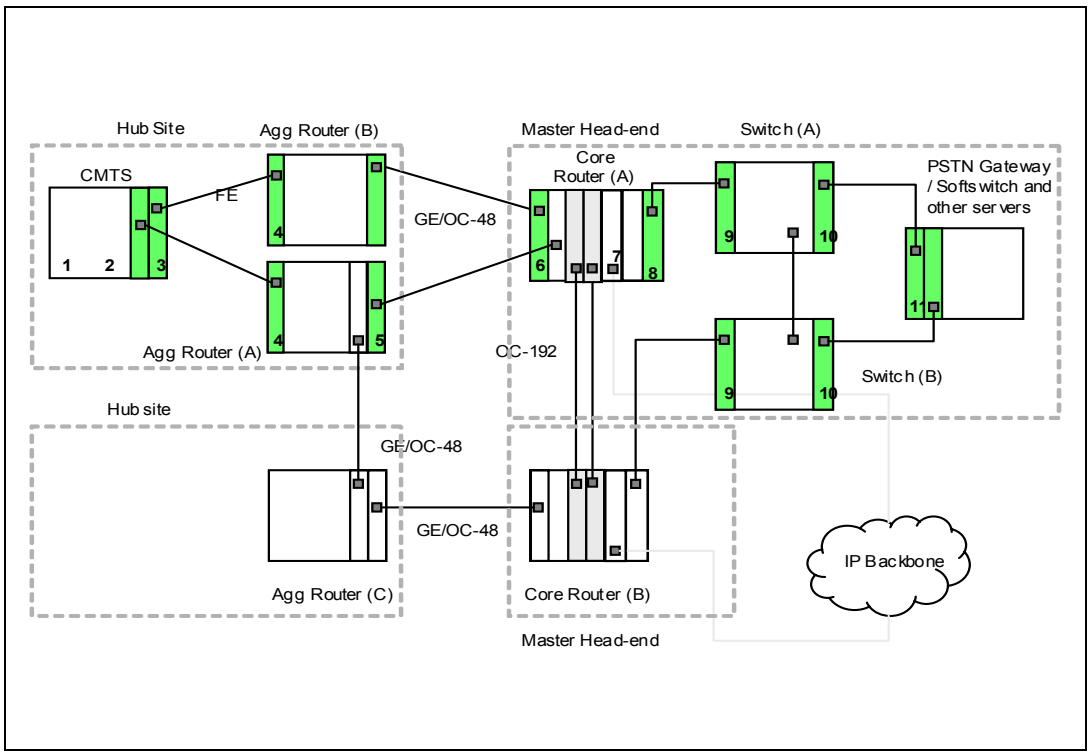


Figure 9: (Case 2 – Network enhanced for HA)

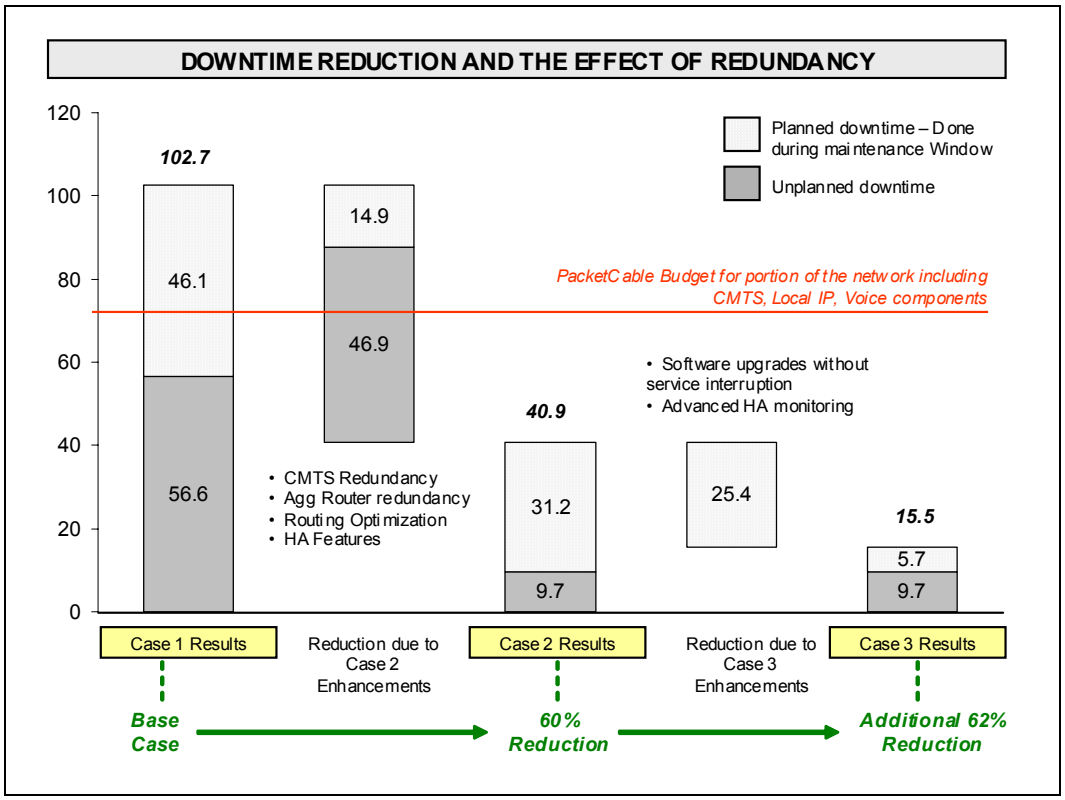


Figure: 10 (Downtime results for the end-end network – Case 1, 2 and 3)

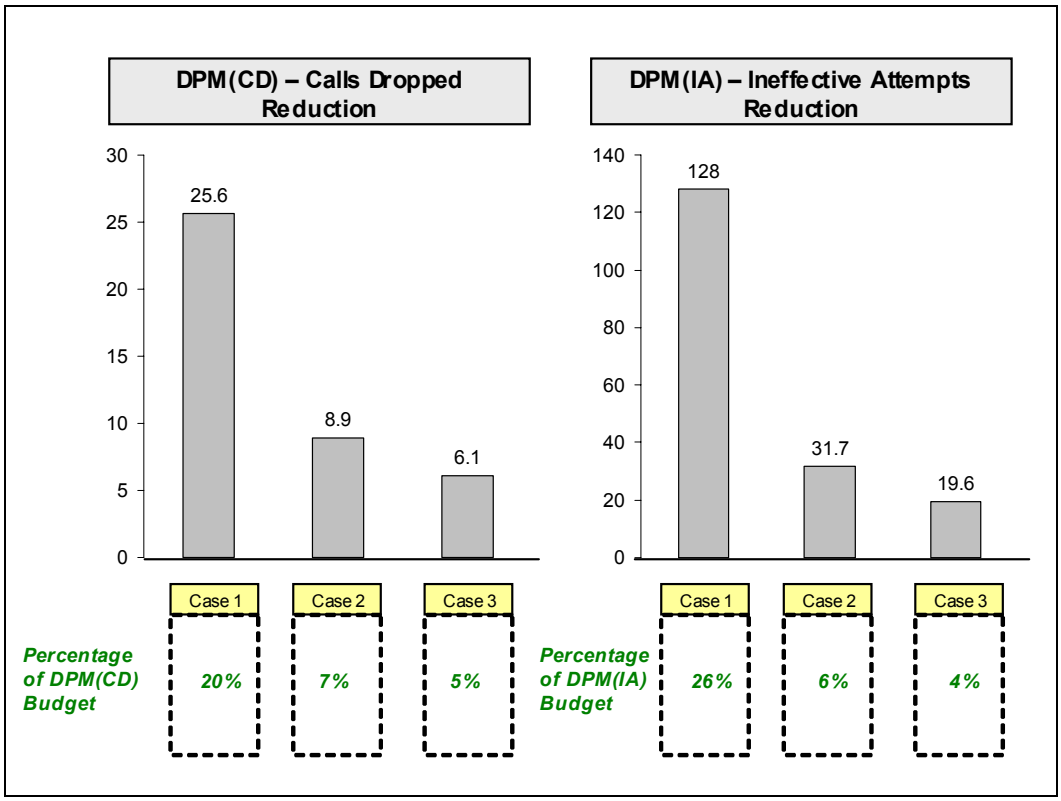


Figure: 11 (Service Availability results for Case 1, 2 and 3)