Errigal Telecommunications Solutions
155 MONTGOMERY ST.
SUITE 700
SAN FRANCISCO, CA 94104

White Paper – Monitoring DAS Networks

Carriers Cannot Afford Downtime

By
Padraig Tobin, Errigal CEO

February, 8, 2010

During the past few years Errigal has seen first-hand how unmonitored or under-monitored DAS networks adversely affect the provider. This paper provides the reader with fact-based arguments, based on Errigal's direct contact with wireless IT officials, as to why monitoring a wireless network saves money resulting from downtime, and reduces subscriber churn.

Contents

Introduction

Over the past 20 years, the cellular industry has grown exponentially. What used to essentially be a captive market for the subscriber has now become fiercely competitive. Indeed, customers currently show almost no loyalty to any particular carrier. Instead, they demand reliable coverage. If their current provider has downtime, subscribers simply take their telephone number and leave for another provider. As Distributed Antenna Networks (DAS) technology has grown, so has the need to keep wireless networks up and running – all the time. This can only be accomplished by utilizing sophisticated monitoring tools. There is a high probability of at least one outage or impairment for each node every year. As a result, a carrier with 5,000 nodes could lose about $58,000 a day if its' wireless network failed.

The Emergence of DAS Networks

In the 1990s wireless carriers experienced astonishing subscriber growth as mobile penetration grew annually across the United States and around the world. This almost-out-of-control escalation led to quickly designed wireless networks. Subscribers saw little difference between carriers, and were excited just to have a cell phone. They tolerated patchy networks with huge and ubiquitous coverage holes. Having mobile coverage indoors, especially in large office buildings, was considered a lucky bonus just 15 years ago. But, still, subscribers managed this inconvenience by falling back on their landline telephones for indoor communications.

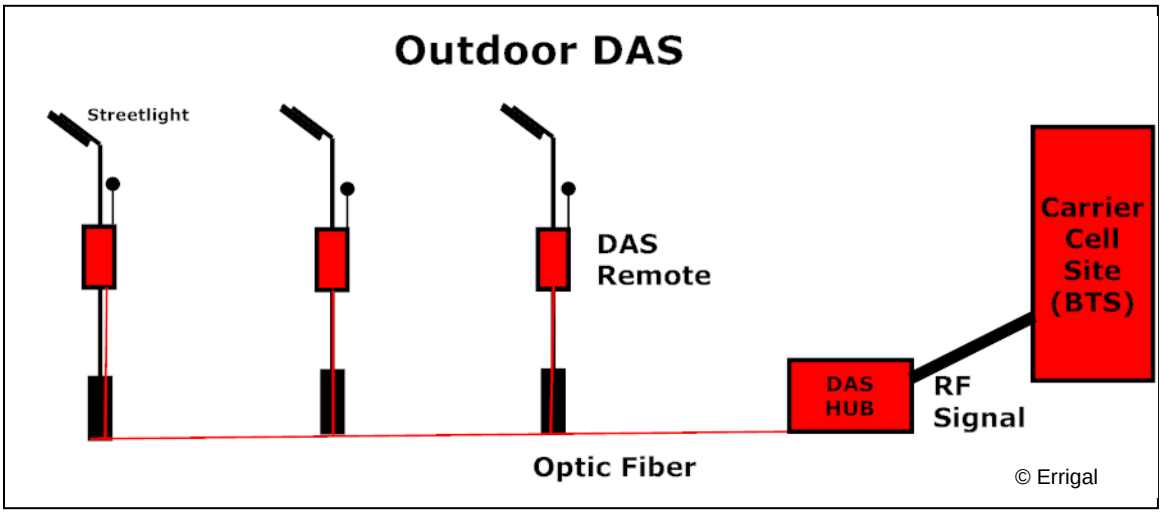
However, the new millennium has seen subscriber levels in most of the developed world reach saturation levels. Any significant subscriber growth today is typically at the expense of other carriers (one loses and another gains). Driving this nomadic and disloyal subscriber base is the advent of local number portability (the ability to move your phone number to any carrier). Subscribers now differentiate carriers according to real or perceived network quality.

And where a wireless network could occasionally be tolerated when voice was the principle form of data being transferred, subscribers, glued to their Blackberry or iPhone browser, are adamant about high-data coverage (especially in-building coverage). The stakes are high: smartphones carry, by far, the highest profit per subscriber.

Using macro cell sites to cover deep inside a building with many walls and perhaps even with reflective windows is not practical. The power required to do so would interfere with the delicate frequency planning of a dense urban area. Additionally, to have a dedicated cell site for every small coverage hole in a city would be cost prohibitive.

Instead, the most common wireless network solution today is DAS. The DAS system is attached to a cell site and relays the same signal to multiple antennas throughout a building or region. There are two main types of DAS solutions: passive and active.

Passive, as the name suggests, uses components which feed off the original RF signal, usually piped around a small region or building to passive antennas via co-axial cable. Active DAS represents a step forward where a large area can be covered by a single site (BTS). The signal is piped to active (powered) components which rebroadcast the signal. The signals are piped from the cell site after first being modulated onto fiber (although sometimes CAT-6 or co-axial). The main advantage of using fiber is that the signal can be rebroadcast many miles away to what is called a “remote” or “node” which will convert it back to the original signal. A remote costs only a fraction of the price of a cell site and, as long as the original cell site has the capacity, coverage holes can be strategically filled in with low-power signals that won’t upset the RF planning the way ramping up BTS power often does.



DAS deployments were initially popular because they could accurately apply coverage the hard to reach places (large arenas, tunnels, skyscrapers) but they have gained more popularity as a deployment with less visual impact than a macro site. Many townships push for DAS as a solution in place of a large macro tower inside the borders of the town. DAS nodes have been growing at a much faster rate than regular cell sites. In fact, the growth of DAS networks is expected to expand annually at about 25% over the next 5 years, as the world market for active DAS goes from $2.5 billion in 2009 to more than $9 billion in 2014, according to ABI Research.

The Importance of a Neutral Host DAS

Initially, to prevent the disruption of multiple carriers installing DAS equipment, network administrators at public buildings and campuses insisted there should only be one DAS network deployment on their property. The idea was that major carriers should share the responsibility for the equipment. This led to each carrier sharing the cost of deployment and getting the benefit of full service in the building. There are compelling financial reasons to share DAS equipment between carriers so “neutral host” DAS providers began to install equipment to be shared. This required that DAS vendors provide equipment that

can handle multiple RF technologies and frequencies (e.g. GSM and CDMA on different frequency bands). The Neutral Host model has been successful in aiding carriers provide coverage in the hard to reach places. It also levels the playing field since all carriers benefit equally, and is not a mechanism for them to differentiate themselves from their competitors.

Why Monitor a DAS Network?

With such growth occurring in the industry it is to be expected, much like the early days of mobile phones, that there will be growing pains and quality assurance issues. Today the modern carrier does not question whether their cell sites (BTS) should be monitored. The capital cost of a cell site can be from $100K to $400K and monthly lease and other maintenance costs can add enormously to the outlay. It is nowadays inconceivable to not monitor cell sites and specialized network operations centers have been set up nationwide. The cost of not monitoring this investment would be considered foolhardy, but it is not lost revenue that is the main concern of a cell site outage. It is the customer migration to competitors due to poor quality coverage. Subscribers seldom call their carrier to tell them they don't have coverage. More likely they will abruptly move to another carrier that they believe has better coverage or less outages.

The case for monitoring DAS networks, however, may not be as immediately obvious. Carriers may be used to seeing DAS networks as a much lower investment than their cell sites, and not deserving of monitoring. Just the contrary is true because of the increasing amount of network traffic going through DAS systems. For example, the traffic generated by a new in-building a system is 80% new traffic. The trend toward DAS systems usage is expected to grow annually.

Anecdotally, our experience is that some carriers have chosen not to monitor all their DAS equipment and have experienced outages that lasted weeks. Without software monitoring system in place, only targeted traffic analysis some period afterward the outage may flag that there was a hardware fault on the DAS equipment, although they still may not know which DAS node. Subscribers that had coverage from that DAS node had no coverage while that node was down, and may have already left the carrier.

Consider these statistics related to active DAS outages:

In this table, resolution tickets for approximately 3,000 nodes were analyzed over a calendar year. Following is the breakdown of over 2,348 incident tickets that led to service loss or impairment:

Resolution to Outage	% Of Occurances
Power Cycle Required on Remote Hardware	23.9%
Local Electrical Power Outage	19.8%
Commication Router Required Reset	9.8%
Fiber Optics Damaged Or Broken	9.5%
Remote Hardware required replacing	6.9%
Reset Circuit Breaker	4.8%
Replaced Node Component	4.7%
RF Powerlevels adjustements	4.4%
Replaced or Repaired Electrical Components	4.3%
Fiber Option Connections Required Cleaning	3.7%
Replaced Hardware on HUB	3.4%
Remote Reset	2.4%
hub power cycled	2.4%

It is interesting to note that not all outages require site visits. The most-common problem was a hung remote that required a power cycle; a fix that is often performed remotely. Some of the outages were minor; requiring a change in power levels is essentially a quality-of-service adjustment. But the vast majority of issues listed above did cause actual outages, at either the remote (which took out one node) or at the hub which may have taken out up to a dozen nodes. A local electrical power outage essentially corrects itself when the local utility restored power, but what is not captured in the ticket is the amount of maintenance required to regain network stability.

Perhaps the most surprising aspect of the data is the large number of incidents. Over 2,000 service-affecting incidents among 3,000 sites means there is a high probability of at least one outage or impairment for each node every year. One of the carrier's operations managers that had several unmonitored DAS nodes was asked how long a typical node remained down when there was an outage. His response was essentially that he had no way of knowing. In fact, unless a customer complained or there was a discrepancy in BTS traffic stats, he would not be aware if a DAS went down.

It is interesting to examine why active DAS nodes are often left unmonitored. Wrongly, DAS has a stigma attached to it that is left over from the days when DAS usually referred to passive components that were un-monitorable or carried small amounts of traffic. When nodes were monitored, the NMS (Network Management System) was typically not set up notify wireless network managers when a fault occurred. The end result is that service impairments or outages may go unnoticed. According to a number of operations managers interviewed at both system integrators and carriers, a DAS system is still considered a small part of their network traffic – even though they are growing annually. Additionally, one of the biggest reasons DAS nodes remain unmonitored appears to be the cost and perceived bother of connectivity to the NMS. This could mean installing a phone line, DSL or in some cases a wireless card at the hub, or dedicating a channel on the site T1 for network monitoring. This is often seen as an unnecessary dedication of an expensive resource often with monthly bills.

The truth is that monitoring a DAS is seldom expensive or complicated. For example, the cost of leasing an outdoor neutral host DAS node varies between $5,000 and $12,000 a year. Usually only a hub will require connectivity back to the NMS. If there is an average of 10 nodes per hub, one DSL line at $50 a month can be used to monitor equipment that carries an annual investment of between $50,000 (10 x $5,000) and $120,000 (10 x $12,000). The cost of the connectivity is not significant in the overall annual investment. The cost of an outage on this equipment is also quantifiable. There are three components affecting the cost of an outage:

(1) Quality impact causing customer churn (customers leaving carrier)
(2) Lost Revenue from the coverage hole
(3) Wasted costs associated with the non-functioning DAS

By far the greatest cost will be the lost subscribers (churn). Subscribers, who depend on the daily coverage of a DAS node, tend to leave a carrier if the service area they require is covered by a competitor. If the carrier believes that coverage is in place where it isn't customers can be expected to leave. Customer churn typically represents approximately $4,000 in present value lifetime revenue per subscriber. This figure, although almost certainly the highest impact will be ignored from the analysis since the number or customers abandoning a network because of DAS quality of service is not easily calculated.

More easily quantified is the complete waste of the costs associated with the remote node. To get a rough idea, leasing a neutral host node would cost approximately $500 to $1,000 a month. Assuming that this is better than a "value neutral" investment (i.e. the strategic and monetary value to the carrier is at approximately $750 a month), we can consider this to be the minimum cost to a carrier if the node is not functioning but they are paying for it anyway.

Looking at the table below, we can conservatively say that there is approximately a 50% probability that there will be an outage or significant service impairment to a node in any given year, based on historical data.

It is impossible to determine how long it will take to detect a problem once it has occurred - if a system is unmonitored. But the following chart quantifies the additional cost per week if an outage goes undetected or unrepaired. In a 5,000 node system we can put forward the following estimates:

Assumptions	
Probability of an outage in a given year requiring intervention	0.5
Nodes	5000
Incidents	2500
Cost Per Month for Node	700

Avg Days Before Repair	Wasted Investment
1	$ 58,333
7	$ 408,333
14	$ 816,667
21	$ 1,225,000
28	$ 1,633,333

The minimum cost to the company having an average repair time of a week instead of a day is approximately $350,000 ($408,333 - $58,333) in a 5,000 node network. If the average repair time goes to a month, the wasted investment will be well over a million. In reality, this cost is probably insignificant compared to the cost of lost subscribers, and the strategic issues with having a multitude of remote nodes not functioning with the carrier remains unaware.

Extrapolation to In-Building DAS Nodes

The data above primarily relates to outdoor das systems which may have higher failure rates due to fiber cuts, exposure to the elements and power cuts. One can assume that the quality of DAS equipment is similar and has similar failure rates. The following repairs should be comparable whether the DAS nodes are indoor or outdoor:

- Power cycle required on remote hardware
- Fiber optics damaged or broken
- Remote hardware required replacing
- Fiber optics required cleaning
- Replaced hub hardware

These repairs make up over 50% of all service-effecting impacts. If the probability of a service-effecting outage requiring intervention is 25% instead of 50% in a given year per node, it is still a huge risk to have your remotes go down with no knowledge of it.

Conclusion

Now that active DAS nodes make up a larger and larger percentage of traffic in urban areas, they should require the same attention to network monitoring that is given to regular cell sites (BTS). To be sure, there are direct costs associated with DAS outages but the most compelling reason is customer churn. Carriers now compete primarily on network quality; not having coverage where you think you do causes customers to find another carrier. When urban areas have the majority of traffic covered by DAS nodes, the

response to the question “How many DAS nodes are down at the moment?” should never be “I don’t know.”

About Padraig Tobin, Errigal CEO

Padraig Tobin started with Motorola over 20 years ago and witnessed the explosive growth to wireless telecommunications from the inside. He has become a recognized industry expert in wireless telecommunications on both the technology and business side and has worked with Verizon, Sprint, Telus and many others in order to develop their networks. Padraig has a BSEE from University College Dublin, Ireland and an MBA from Columbia Business School, New York.

About Errigal Inc

Errigal is one of the leaders in Operations Support Software (OSS) in the Wireless Telecommunications space since 1996. Errigal now runs the largest DAS Network Operations Center in the United States (by node count) and has broken significant new ground with bringing best practices and process automation to a completely new area of telecommunications.