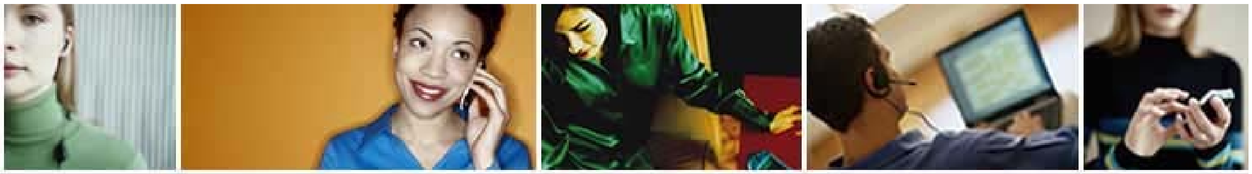


Service Levels of Microwave Systems

Date: February 22, 2006

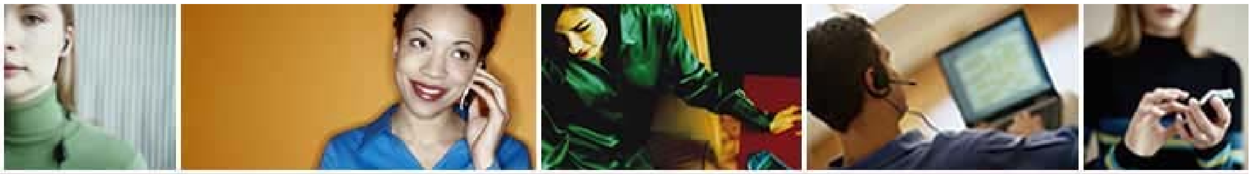


Table of Contents

1 Overview 3

2 Determining Unprotected Wireless availability 3

3 Determining Optical Service Availability 3

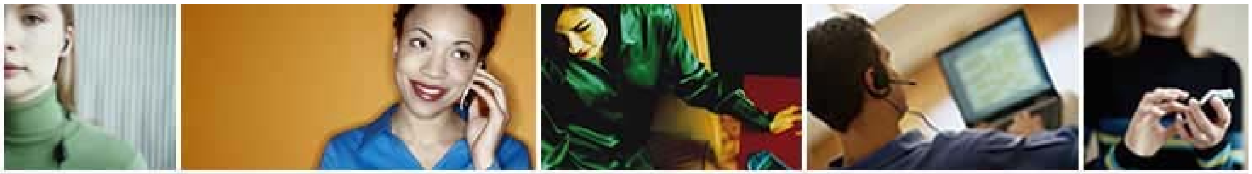
4 Increasing availability through protection 4

5 Other Fault Conditions 5

6 Security and other Wireless Performance Characteristics 6

7 Conclusion 6

8 References 7



1 Overview

This document evaluates the service availability using a DragonWave AirPair wireless system. This is compared to the service availability of a fiber optic link. Additionally, protection options, and other attributes, such as latency and security will be discussed.

To compare reliability, we will use availability, which is the statistical % of time that a service is available per year. The availability of a service is 1 – unavailability. To determine availability, we will use the "Mean Time Between Failures" (MTBF), which is the statistical average number of years between failures. We will also use "Mean Time to Repair" (MTTR), which is the average time to restore service from a failure.

2 Determining Unprotected Wireless availability

The process of estimating radio link ranges is a well understood process and is internationally recognized. Standard, accepted methods for this process are well documented in the form of ITU-530, and analyzed in a separate paper [1]. Using these models DragonWave can accurately predict the path availability of a wireless link. A link can be engineered to a desired availability. For this analysis we will look at links engineered to 99.99% availability. By increasing antenna size, inserting high-power radios, or for shorter links, this availability can be increased 99.995% if required, so we will also look at the service availability of these links.

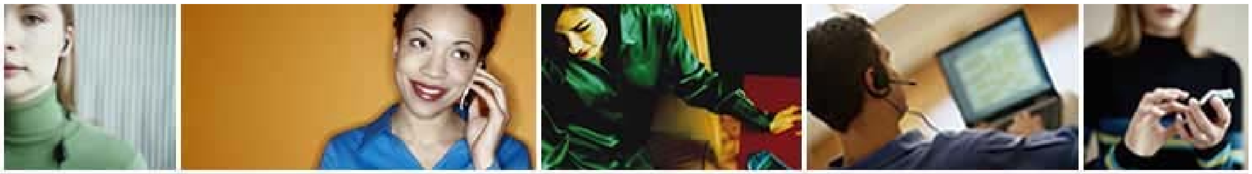
The two contributors to service availability are the link availability and equipment availability. The AirPair Radio and Modem has a combined MTBF of 15 years.[2] We will assume that the AirPair product has an average MTTR of 8 hours. We can calculate the service unavailability using the following equation.

$$U_{service} = U_{path} + 2XU_{equip}$$

Using this equation, the service availability can be calculated as 99.978%. If the path availability was increased to 99.995, the service availability would be 99.983%, as the limiting factor becomes the equipment unavailability.

3 Determining Optical Service Availability

To determine the availability of an optical service, we need to assume a service distance. For this calculation, we will assume 10 Km. For a metro network, the 3 dominant failure modes are maintenance errors, fiber cuts, and equipment failures. Maintenance errors are not well documented, and we will therefore not include them in this calculation. We will assume 10 fiber cuts/1000 Km/year within the metro network, with a fiber MTTR of 12 hours. This time to repair is longer than other failures, as a



fiber cut requires determining exact location of the cut, and then repair each strand within the fiber bundle. Common transponder failure rates have an MTBF of 15 years, with an 8 hour MTTR. For an optical service, the unavailability equation is very similar to a wireless service, as shown below.

$$U_{service} = U_{fiber} + 2XU_{equip}$$

Using this equation, the optical service availability can be calculated as 99.974%. This availability would decrease as the path length increases, or if maintenance failures are included, as shown and compared against the wireless offering in the figure below.

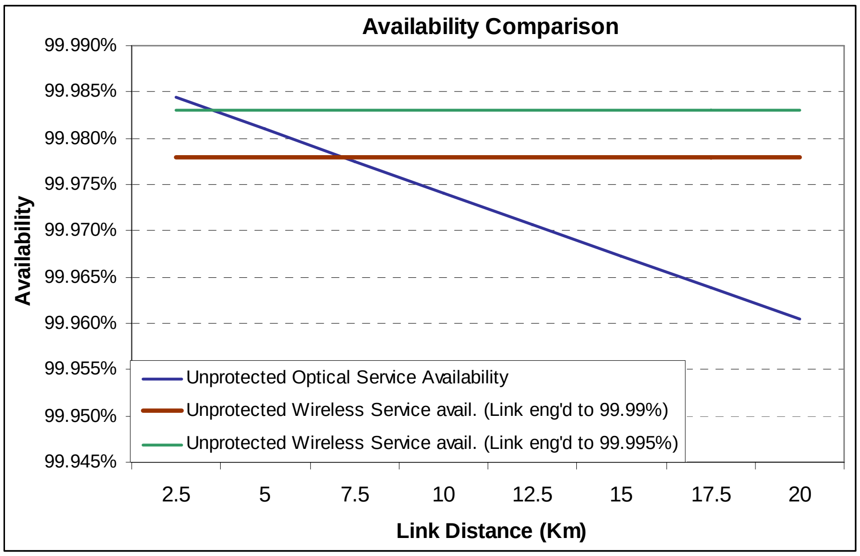
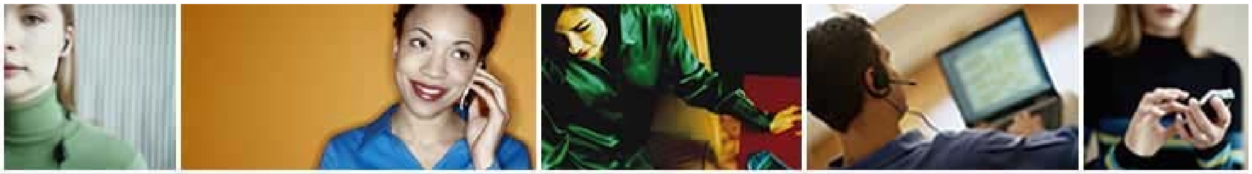


Figure 1 - Effect of Distance on Availability

4 Increasing availability through protection

The two contributing factors to wireless unavailability are the equipment and the path or air unavailability. The equipment unavailability can be avoided by using two redundant, parallel links, which protects against equipment failures. This would increase the service availability of the 99.978% service up to 99.99%, which is equal to the availability that the path is engineered to. Similarly, if the path was engineered to 99.995%, equipment redundancy will increase the service availability to also be 99.995%. For optical services, the fiber path becomes the limiting factor, with a resulting availability of 99.986%



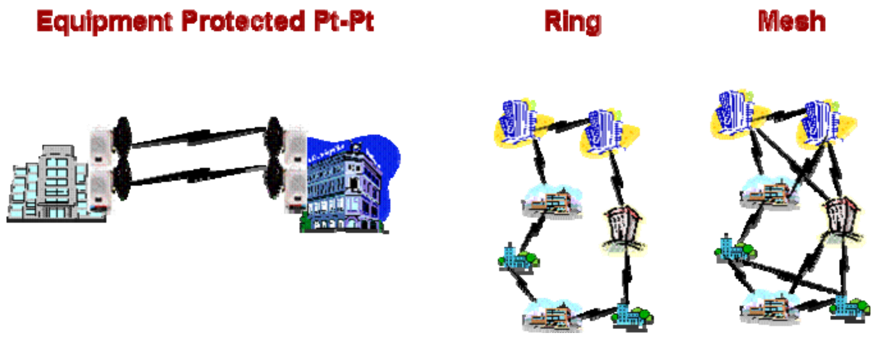


Figure 2 – Protection Options

In order to increase the service availability to 99.999%, link diversity is required. One way of doing this is to introduce a relay site on the redundant link. However, this introduces additional cost. A more efficient way of providing this diversity is to introduce a ring configuration as shown in figure 2 above. For wireless links, the major factor effecting availability is the rain, however this can be reduced by providing diverse paths. The path diversity improvement factor (PDIF) is described in [3]. It provides a measure of the joint probability of two co-joined links failing simultaneously. A PDIF of 5 or higher is quite common for a link of 10 Km. This results in the Unavailability of the link being reduced by that factor. The service availability of a 99.99% path becomes 99.995%, and the unavailability of a 99.995% path becomes 99.999%. By introducing a mesh with 3 paths out of each node, the PDIF can be increased to10, further improving availability. The effect of this and the other protection schemes is compared in Table 1.

	Unprotected Service	Equipment Protected	Ring Protected or Relay Site Protected	Mesh Protected
Wireless Link Engineered to 99.99% Path availability	99.978%	99.990%	99.995%	99.999%
Wireless Link Engineered to 99.995% Path availability	99.983%	99.995%	99.999%	>99.999%
Optical Service	99.974%	99.986%	>99.999%	>99.999%

Table 1 - Availability Comparison

5 Other Fault Conditions

A significant contributor to outages in optical networks is maintenance and finger errors. However, they are not well documented, and therefore have not been included in these calculations. Typically, maintenance outages in optical networks occur by the wrong fiber in a bundle being disconnected, or a fiber accidentally being pulled. As the wireless system has no fibers, and can be mounted entirely outdoors, with only a single cable being brought indoors, it is likely that maintenance outages are reduced significantly in a wireless network.

Another factor that has not been included is full site outages. Some conditions, such as a lightning strike, tornado or earthquake may take out a complete site in an optical network, but are very minor contributors to service availability. This factor has also not been included in the wireless availability, but outage rates due to site failure, or tower problems are expected to be on the same order as for an optical network.

Large disasters such as earthquake or terrorist attacks have not been included in thee availability calculations as they are very small contributors. However, these types of disaster typically will take out large amounts of fiber, including the diverse portions, taking out communications for sites that aren't hit by the disaster. For wireless communications, the wireless paths are not affected, and therefore have reduced effect on service.

6 Security and other Wireless Performance Characteristics

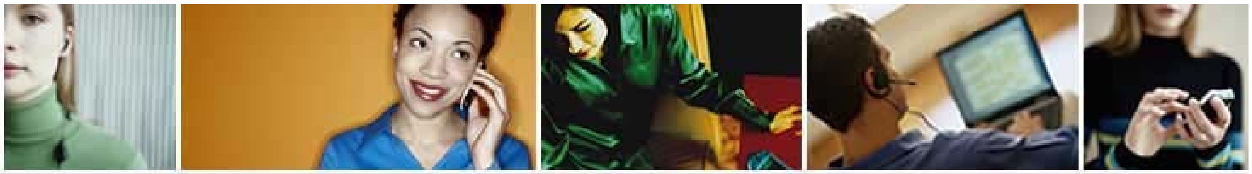
The AirPair product implements a number of security features to ensure data is not intercepted [4]. For authentication, each end of a link knows the identity of its other link end, which is factory set, and it will only communicate with that radio. Authentication is constantly verified, and data flow will stop if an alarm is raised. Additionally, DragonWave employs DES encryption. The entire frame is encrypted using a DragonWave-proprietary algorithm which encodes the entire link transmission, not just the data payload. AirPair also employs multiple security levels for management access, and transmits management traffic in-band.

In addition to all of these data security features, there are a number of physical challenges in preventing eavesdropping to the encrypted radio data. The RF Beamwidth is typically 1 – 2°, so eavesdropping requires interception of this narrow signal. Additionally, Installation on roof-tops or towers generally makes interception highly challenging. DragonWave recommends Line of sight installations, thereby precluding the existence of locations where eavesdropping can be carried out.

The AirPair system is a Point-to-Point solution which employs native Ethernet and operates its over-air interface at the same speed as the network interface port, 100 Mbps full duplex. This rids the system of all of the delay-inducing impairments. All types of IP traffic are handled without distortions due to the high speed, low delay, and low delay variability performance of this solution. The overall packet delay across an AirPair-100 wireless link is 250 us typical) depending upon packet sizes, and is further discussed in a separate document. This is independent of the wireless link distance since in-flight delay adds only ~ 300 ns per kilometer of link distance.

7 Conclusion

The availability of optical services and wireless services are very similar in most cases, and slightly better for wireless systems in many cases. In unprotected scenarios, the equipment is the major contributing factor to failure rates. The availability of



unprotected optical services is around 99.97%, and wireless availability is 99.98%. If equipment protection is introduced, fiber availability can be increased to 99.99%, and wireless availability can be improved to 99.995%. As path diversity is introduced into either of these solutions, service availability can be increased beyond 99.999%. Additional factors, especially maintenance outages are likely to affect optical systems more than wireless systems.

Wireless also performs comparable to alternatives on other key service characteristics. AirPair has a number of features and inherent characteristics to ensure secure data transmission. The latency across an AirPair system has been extensively studied, and is typically under 250us, with a maximum of 500 us.

8 References

[1] Boch, E., “Propagation Effects of Rain & Fog on the AirPair System
”, Aug 2002.
[2] Nguyen,Q., “DragonWave IDU-ODU Failure Rate and MTBF Prediction”, March 2004.
[3] Hnidson, D., “Enhanced Wireless Link Availability Derived from the DragonWave Mesh/Ring Topology”, February 2004
[4] Boch, E., “APP-048 AirPair Data Security”, October 2002.
[5] Griffiths, J., “IP Latency Across DragonWave’s AirPair 100 System”, February 2003.

DragonWave Inc.
600-411 Legget Drive, Ottawa, Ontario, Canada, K2K 3C9
Tel: 613-599-9991 Fax: 613-599-4225
www.dragonwaveinc.com