

Australia Star iBurst Service Level Agreement

1. Introduction

This document describes the Australia Star Communications Pty Limited (ACN 078 222 778) (“Australia Star”) Service Level Agreement (“SLA”) for the iBurst Data & Internet Service (“Service”) if you signed the Standard Customer Agreement (“SFOA”) AFTER 1 July 2006.

2. Quality of Service

2.1 Air Interface Bandwidth

The initial implementation of the Service uses a best effort mechanism with a fairness MAC (Medium Access Controller) that allocates resources equally between users when contention occurs on the radio interface.

2.2 Performance Targets

2.2.1 Average Downlink Speed

Average downlink speed is the measured throughput from a base station to a single user where that user has reliable radio coverage that can support maximum download speed under unloaded network conditions.

As network loading increases, the average throughput that a user will experience will decrease during periods of heavy network load. This will be reflected in the user’s inability to achieve maximum download speed of 1 mbps for a certain percentage of the time over the month.

Target Metric

- 95th percentile: > 900 kbps
- 98th percentile: > 450 kbps
- 99th percentile: > 200 kbps
- 100th percentile: No measure

How is this measured?

This will be measured by the Service Assurance System that will periodically download a 1Mbyte file from a server in the Service, and measure the time taken to download this file, to calculate download speed. These measurements will be taken once every 15 minutes and recorded in the Service Assurance System database to calculate a distribution of download times over the month.

2.2.2 Average Uplink Speed

Average uplink speed is the measured throughput from a base station to a single user where that user has reliable radio coverage that can support maximum upload speed under unloaded network conditions.

As network loading increases, the average throughput that a user will experience will decrease during periods of heavy network load. This will be reflected in the user’s inability to achieve maximum upload speed of 350kbps for a certain percentage of the time over the month.

Target Metric

- 95th percentile: > 300 kbps
- 98th percentile: > 150 kbps
- 99th percentile: > 75 kbps
- 100th percentile: No measure

How is this measured?

This will be measured by the Service Assurance System that will periodically upload a 300Kbyte file to a server in the Service, and measure the time taken to upload this file, to calculate upload speed. These measurements will be taken once every 15 minutes and recorded in the Service Assurance System database to calculate a distribution of upload times over the month.

2.2.3 Average Latency

This is a measure of the delay introduced in the end to end IP connection due to the Service radio connection. As network load increases the latency will increase. During busy times, the latency may increase to a point where delay sensitive protocols such as VoIP or TCP appear to operate at reduced rate due to the increased latency.

Latency will be expressed as round trip delay, as measured by the ICMP "Ping" command distributed into different percentile bands over the month.

Target Metric

- 95th percentile: < 100 mSec
- 98th percentile: < 150 mSec
- 99th percentile: < 250 mSec
- 100th percentile: No measure

How is this measured?

Network Latency will be measured by the Service Assurance System by performing an ICMP Ping command to a server located in the Service core network from a service assurance agent located at each base station every 15 minutes. The service assurance system will record all measurements and produce a distribution report for each base station and the whole network at the end of each month.

2.3 Redundancy

2.3.1 Base Station Network

In many areas, there will be overlapping coverage from two or more base stations, so that in the event of a complete base station failure, users will be able to continue to receive service seamlessly from surrounding base stations.

The base stations themselves incorporate a high level of redundancy, with 1+1 redundant electronics for critical systems and N+1 redundancy for less critical systems, which if a single system fails, the base station will continue to operate with reduced capacity. Also, battery back up is provided to protect against short term power failures. Back haul transmission between base stations and the core network is not redundant.

2.3.2 Core Systems

All core network equipment that represents a single point of failure is provisioned with 1+1 or N+1 redundancy. This includes Layer 2 Switching, Packet Data Switching Nodes, Foreign Agent Control Nodes and Wholesale Radius systems.

2.4 Air Interface Security

iBurst uses 3 separate security protocols for base station authentication, user data encryption and user terminal authentication known as i-hap, i-sec and i-tap.

The i-hap protocol uses public key encryption and the public key of the certificate authority to transmit a digital certificate from the base station to the user terminal to ensure that the user is only accessing authorized base stations. (This prevents network spoofing). The base station signature is generated using a hashing function according to ISO 9796 and public key encryption using RSA-1024 method is used to generate the digital signature.

A shared secret is established between the user terminal and the base station which is used to encrypt all further messages (including user payload data) using a 163 bit symmetric encryption method. The identity of the shared secret is renewed every time a session is established with a base station, and is kept secret by encrypting it using the 163 bit elliptic curve private key of the user terminal.

Only authorized user terminals can access the Service. User terminal authenticity is verified by the i-tap protocol using a digital certificate based on 163 bit elliptic curve private key. The base station knows the public key of the user terminal to verify the user terminal's digital signature. The i-tap protocol prevents session theft by an unauthorized user terminal at inter base station hand over.

2.5 Coverage

Data & Internet Service coverage may only be available in selected metropolitan and regional areas and is subject to availability, geographical & technical capability and lack of capacity & faults in other telecommunications networks to which the Data & Internet Service is connected.

Please see www.australiastar.com.au or call **1300 764 765** for coverage maps indicating the estimated current availability of the Service coverage.

3. Support

3.1 Support Responsibilities

Level 1 (technical user support):	Australia Star
Level 2 (escalated user support):	Australia Star
Level 3 (network support):	Network Operator

Only calls that relate to faults within the Service and systems which hinder the normal operation of the Service modem should be escalated to the Australia Star Support team. These types of issues would include:

- Base Station availability/capacity
- General Network Availability enquiries

Issues which would be handed by Australia Star would include:

- End user installation issues
- Faulty User Terminal, e.g. User Terminal not picking up signal within coverage area
- IP traffic related issues
- General performance issues
- User name and password issues
- General Coverage enquiries

It is the responsibility of Australia Star to ensure that:

- Calls that relate to user level billing and technical support are handled by Australia Star's Support team
- A fault to be escalated to the Network Operator technical support is not reported multiple times

3.2 Contacting Australia Star Technical Support

To escalate a call to Australia Star technical support, the phone number to call is **1300 764 765**.

This number is applicable both within and outside business hours but, initially, out of hours fault reports will go to a recorded service to be dealt with the next day (see below).

For less urgent matters, problems can be reported to the help desk by email to iburstsupport@australiastar.com.au.

3.3 Australia Star Technical Support Procedure

Faults that are handled by the Australia Star help desk will be allocated to one of three categories:

- Minor
- Major
- Critical

The following sections explain the characteristics of the various fault levels as well as the target response procedures.

Note: In all cases target response times are indications of the response times that Australia Star strives to achieve. However many factors including such things as availability of parts and intractable faults may contribute to these times not being achievable.

3.3.1 Minor Faults

Characteristics:	A system has partially failed but, due to redundancy, there has been no loss of capacity.
Target response:	Rectified within the next business day
Support available:	8 AM to 6 PM Monday to Friday
Notification:	None

3.3.2 Major Faults

Characteristics:	A system has failed resulting in reduced capacity. A base station has failed but coverage is available due to overlap from adjacent cells. A fault has caused minor reduction in capacity on a link to Australia Star or the Internet. Provisioning systems have failed.
Target response:	Rectified within the next business day
Support available:	8 AM to 6 PM Monday to Friday
Notification:	Email, Phone

3.3.3 Critical Faults

Characteristics:	System or network failures resulting in loss of coverage for a significant number of users. A fault has caused significant reduction in capacity on a link to Australia Star or the Internet.
Target response:	Rectified as soon as possible
Support available:	24 hours/7 days a week
Notification:	Email, Phone