SERVICE DEFINITION

BROADBAND SERVICE

For Heathrow Airport

Author: Alexandr Lichy
Creation Date: 11th July 2013
Last Updated: 12th July 2013
Version: 0.3

Contents

Version Control

Date	Author	Version	Change Reference
11th July 2013	Alexandr Lichy	0.1	Initial version based on the document for airlines
12th July 2013	Alexandr Lichy	0.2	Removed section 8.2 and the AOC references

Glossary

Acronym/Terminology	Description
Active Infrastructure	All equipment, typically but not limited to, routers and switches used in conjunction with Passive Infrastructure to provide a service between any two or more Demarcation Points.
Airport	Heathrow Airport
APOC	Supplier Operations Centre
Authorised Users	Those personnel, or third party vendor personnel named by the Customer, authorised to contact the IT Service Desk.
BGP	The Border Gateway Protocol is the core routing protocol of the Internet
Business Change Control Periods	To ensure that the IT Infrastructure and operational business activities are protected during times of increased volume of passengers. Any Change, that is planned for implementation during a Business Change Control Period and has an operational impact on the Airport, will require Supplier approval before it can be progressed.
Change	Any variation or amendment requested by the Customer to the Services including requests for: (a) additional capacity (Demarcation Points); and/or (b) new technology
Common Passive Infrastructure	Means all elements of cabling, be they fixed cables and or patch leads, patch panels, cabinets and distribution points including consolidation points, tertiary cabling, all trays, supports, ducts and physical routes within and between buildings.
Demarcation Points	Any two outlets between which the Passive Infrastructure connects. The exact point of demarcation is the male/female connection of the Passive Infrastructure to which a subsequent connection is made (Commonly referred to as the channel for CAT 6 cabling). The following are examples only and are not limitations Example 1: an RJ45 outlet in an office is the demarcation point, into which the Customer's patch lead connects. Example 2: in a comms room where the infrastructure continues beyond the patch panel and includes a patch lead with a male RJ45 connector or fibre connector which is the demarcation point, which then plugs into the Customer's switch at Access or Distribution layer.
DHCP	Dynamic Host Configuration Protocol, used to configure devices connected to a network for the communication via the IP
DNS	Domain Name System, used to translate the numerical IP addresses to the domain names
Emergency / Fix On Fail Works	Emergency / Fix On Fail works are system changes that need to be made immediately to resolve operational problems.

Acronym/Terminology	Description
Incident	Any event which is not part of the standard operation of the Common Infrastructure, which causes, or may cause, an interruption to, or reduction in, the quality of the Common data Infrastructure.
IT Service Desk	The service desk provided by the Supplier for the receiving and logging of calls from Authorised Users relating to: (a) Incidents; (b) Change requests; and (c) Patching Requests. Please refer to section 5 for contact details
Internet Protocol	Internet Protocol (IP) is an essential technology used for the communication via Internet
Known Errors	A Problem that is successfully diagnosed and for which a workaround is known.
LAN	Local Area Network.
Planned Works	Planned works are system changes that are scheduled in advance, following the Supplier's change management process.
Problem	The unknown underlying cause of one or more Incidents.
Operational Location	Can be any location such as Check-In (both dedicated and common use), Gate Rooms, Transfer Desks, Baggage Reclaims, Baggage Make-up Areas, Lost and Found, and similar operational areas / functions where there is one or more end user devices connected to the HAL Managed LAN Service
Resolve	The restoration of the Services affected by an Incident to normal operating status and includes any temporary workaround and "Resolution" shall have a corresponding meaning.
Response	The time taken by the Supplier to diagnose the fault and initiate remedial action, including determining the total resolution to a fully restored service, or an acceptable work around until full restoration can be effected and where necessary the dispatching of an engineer to site. It also includes reporting back to the call initiator or their service provider.
VLAN	Virtual Local Area Network, providing isolation between the data of the different Customers transmitted on the common infrastructure.
WLAN	Wireless Local Area Network, a wireless network service provided by Supplier
WPM	Working Practices Manual

1. Purpose

The purpose of this document is to detail the scope of the Broadband Service being provided to the Customers at the Airport and the Service Levels applying to that service.

The Service Levels within this Service Definition document define the minimum levels of service that the Supplier shall deliver to the Customer in provision of the Broadband Service.

2. Introduction

The Active Infrastructure comprises all equipment, typically but not limited to, routers and switches used in conjunction with Passive Infrastructure to provide a service between any two or more Demarcation Points.

The Common Passive Infrastructure, comprising both fibre and copper cabling, has been designed based on British and European Norm standards and best practices to enable various communications protocols to be supported by the common cabling infrastructure.

The Broadband Service will be accessible via the Active Infrastructure, the Common Passive Infrastructure, and the WLAN Infrastructure (as selected on the Order Form) and will be available from the Customer's Demarcation Points, including the Supplier network switches.

The Customer's equipment will be located within the space occupied by the customer at the Airport and will not be located within the Supplier's communications rooms.

Note 1: Border Gateway Protocol (BGP) is the only dynamic routing protocol that the Supplier will allow Customers to use to connect 3rd party routers.

Please refer to the Working Practices Manual (WPM) for the low level process detail.

Please refer to Appendix A for LAN port security details.

3. Services

3.1 Broadband Service

(1) The Supplier shall provide a "Broadband Service" during the relevant service hours set out in section 5 of this Schedule that:

a) Will provide connectivity for the Customers to the public Internet through separated VLAN;

b) will provide a bandwidth speed selected by the Customer;

c) will provide DHCP and DNS;

d) Is based on British and European Norm standards and best practices to enable various communications protocols to be supported by the Common Infrastructure.

3.2 Support and Maintenance Services

The Supplier shall provide the following support and maintenance services ("**Support and Maintenance Services**") during the relevant service hours set out in section 5 of this Schedule, and according to the Service option selected by the Customer:

(1) Maintenance

The Supplier shall:

a) Use all reasonable endeavours to conduct all planned works ("Planned Works") on the Common Infrastructure between the hours of 23:00 and 03:00 each day ("Maintenance Window"), when required. All planned changes will be subject to *last flight / first flight* considerations;

b) Notify the Customer and/or any that may be affected at least 10 Working Days prior to any Planned Works, and make allowances for any Customers' concerns over the scheduled period and to take all reasonable steps to mitigate any such concerns, where there is an expected impact to the Services for that Customer. Such notification is to include the impact on the Services and the duration of any associated outage. All reasonable endeavours will be

made to notify Customers where the Supplier is required to carry out emergency / fix-on-fail works;

c) Develop a regression plan for the Planned Works, with appropriate go/no go decision points;

d) Notify the Customer if they are required to participate in the implementation of the Planned Works and to test for correct operation following the completion of the Planned Works;

e) Use all reasonable endeavours to ensure that any outage caused by the Planned Works will not impact on the Services; and

f) Notify the Customer of the completion of the Planned Works.

(2) Incident Management

The Supplier shall:

a) Provide and adequately staff the IT Service Desk to receive and log calls from the Authorised Users relating to Incidents;

b) Accept and log Incidents from Authorised Users;

c) Respond to and Resolve Incidents as appropriate to this SLA;

d) Provide the Authorised User with regular progress updates;

e) Escalate Incidents in accordance with the Escalation Matrix set out in section 9; and

f) Liaise with and co-ordinate all Supplier internal teams and any third party suppliers in order to Resolve an Incident.

(3) Problem Management

The Supplier shall:

a) Evaluate Incidents with significant impact or repeat Incidents to identify and record a Problem if relevant;

b) Perform problem and/or root cause analysis;

c) Evaluate and agree the viability for implementing permanent solutions over workarounds based on time, effort and likelihood of occurrence;

d) Recommend and implement permanent solutions to Known Errors; and

e) Engage and manage third party suppliers as necessary to resolve Known Errors.

3.3 Change Management Services

(1) The Supplier shall, during the relevant service hours set out in section 5 of this Schedule:

a) Receive, log and coordinate a Change request received by phone via the IT Service Desk (option 2);

b) Allocate a reference number to each Change on receipt of the Change request;

c) Ensure that all Change requests, including costs and timescales, are authorised by the Customer;

d) Implement all Changes authorised by the Customer.

e) Contact the originator of the Change to confirm receipt of the request and, if appropriate, arrange a project initiation meeting.

4. Roles & Responsibilities

The Customer will adhere to the Customer obligations defined in section 7 of this Service Definition. Failure to do so may mean that the Supplier cannot be held to the terms of these Service Levels that are directly affected by that failure on the Customer's part.

Any failure caused by malfunction of Host Computer(s) or associated third party network communications are excluded from these Service Levels.

4.1 The Supplier's Service Level Manager

Responsibilities of the Service Level Manager shall include, amongst other things, the following:

- Is the primary single point of contact between the Customer and the Supplier for service issues. Note that the IT Service Desk is the single point of contact for incidents.
- Shall be aware of, manage and report on, all and any aspects of the Managed Broadband Service, or its maintenance and support in the Suppliers,
- Has the ability to escalate and need to acquire, assign or manage other Supplier resources to work on any aspect of the service provided in the Airport.
- To attend scheduled and ad-hoc meetings with Customer(s) as reasonably required.
- Shall provide regular status reports to the Customer

5. Service hours and contact details

The following service hours apply to the provision of the Services:

Service	Service Hours	Service Days	Critical Business Periods
Support and Maintenance	00.00 – 23.59	Mon – Sun	24*7*365
Change Management service	08.30 – 16.30	Mon - Fri	N/A

A change request itself must be made in the stated time frames; the actual work may be carried out at other times.

IT Service Desk contact details:

- Faults : 0845 602 7793 Option 1
- Patching Requests : Email itservicedeskrequest@baa.com (primary contact); or
  : Phone 0845 602 7793 Option 2
- Change Management : Email itservicedeskrequest@baa.com (primary contact); or
  : Phone 0845 602 7793 Option 2

6. Service Levels

The following Service Levels will apply to this service:

a) To resolve the underlying cause of an Incident

b) To provide additional connections

c) Service availability

(a) Service Levels to resolve the underlying cause of an Incident

The Service Levels given relate to the time that the Supplier will respond to a failure of the Broadband Service. Within this time, the Supplier will log the call and provide appropriate resource and effort to actively resolve the fault according to the impact the issue has on the Customer. If both parties agree that insufficient information has been given for the Supplier to commence analysis of the Incident, then an appropriate amount of time will be deducted from the timings. This deduction of time will take account of the period whilst the information was lacking.

Impact		Service Response (Active and Passive)	Service Restoration (Active Network Failure)		Service Level
Standard Description	Service Example		Standard Service	Premium Service	
Down for all Customer users	Failure for all end users	Within 30 minutes	Remote fix within 24 hours	Remote fix within 8 hours	95%
Down for some Customer users	Failure for some end users	Within 2 hours	Remote fix within 24 hours	Remote fix within 8 hours	95%
Down for one Customer user	Single end user failure	Within 2 hours	* Please see note below	* Please see note below	95%

Note: The above service levels for a single end user failure quote a 2 hour response time and no resolution time. However, the Supplier will take all reasonable steps to restore service within 8 hours. This will be dependent on the time taken to make the area safe, to gain appropriate access to the faulty equipment, and to rectify the failure at the supplier.

For all faults, time spent completing the following will not be counted towards the Service Levels:

- Secure a permit for entry or works to any part of the cable run. This could include an ATP for a baggage area, road closure(s) or airfield area(s).
- Make safe a public area to gain access to the faulty cabling.
- Gain access to non Supplier offices and equipment cabinets.
- Resolve Health & Safety issues prior to, or during, resolution works.
- Install replacement cabling.

The Incident Restoration time will be calculated on a monthly basis. The Incident Restoration time is an aggregate percentage measure calculated as follows:

(a) Total number of Incidents logged in the month = M

(b) Total number of Incidents where the Restoration exceeded the Service Level = L

(c) 100 – (L/M x 100) = percentage of Incidents meeting the Service Level

(b) Service Levels to provide additional connections

Additional New Network Ports	Request Completion Service Level
Acknowledgement of request by IT Service Desk	Within 30 minutes
Project team to arrange survey	Within 3 working days
Provide scope and cost	Within 5 working days of request (subject to Standard Installation Request (as defined below), Customer providing

	sufficient details, availability of Customer to discuss and the Customer arranging access for survey)
Commencement of works	Within 5 working days of Customer providing the Airport with a Purchase Order to proceed with scope and cost

A Standard Installation Request is defined as:

- Demarcation Point within 90m of existing network switch with available capacity
- Cabinet and containment is available and has spare capacity
- No external change control or Authority to Proceed (ATP) is required e.g. from Health & Safety, Engineering, Baggage, etc
- No specialist works are required e.g. asbestos inspection/removal, diamond drilling, etc

(c) Service availability

Service availability shall be at least 99.85% over each calendar month (i.e. non-availability should not exceed 65 minutes). This will be measured at device level and not port level.

The Network Management System used by the Supplier provides advanced tools, processes and techniques to reduce unplanned outages to extremely low levels and allows the Broadband to achieve high availability levels.

Calculation of actual availability will be:

$$\% \text{ Availability} = \frac{\text{NSST - NSDT}}{\text{NSST}} \times 100$$

Where NSST = Network Switch Service Time
= (Number of Network Switches x 24 x 60 x Number of days in month)
- (Planned down time in minutes x Number of Network Switches impacted)

and NSDT = Network Switch Down Time
= for each Incident (Downtime in minutes x Number of Network Switches impacted)

7. Customer obligations

People/Management

7.1 The Customer shall:

(a) Ensure that any use of the Broadband Services by its employees, agents or sub-contractors, is compliant with the design of the services.

(b) Be responsible for their own user/access security and network access.

(c) Provide a point of contact for management/escalation of Service issues;

Provisioning

7.2 The Customer shall:

(a) Ensure that all Change requests are filtered and prioritised prior to logging with the IT Service Desk.

(b) Only request business critical Changes to be implemented during the Supplier's Business Change Control Periods. The Business Change Control Periods will be notified to the Customer in advance at the Service Review. All changes requested during this period will require Supplier approval.

(c) Use only such Customer's Equipment as approved by the Supplier, per the instructions given at the time of Service installation.

Fix/Support Process

7.3 The Customer shall:

(a) Use reasonable endeavours to diagnose a fault reported to it by clients and only raise Incidents with the IT Service Desk if the Customer believes there is a fault with the Broadband Service.

(b) Within a reasonable time of the Customer becoming aware that an Incident has occurred, notify the Supplier of the Incident and, if required, or deemed necessary, provide the Supplier with all reasonable assistance to resolve the Incident.

8. Service Management

8.1 Service Reviews

Service Review meetings shall be held at least half yearly between key representatives from the Supplier and a nominated Customer representative. Attendees from the Customer shall be agreed by the parties. Other stakeholders may be invited to these reviews as required. These meetings shall include, but not be limited to:

a) A review of performance against Service Levels;

b) A review of any Planned Works; and

c) Discussion of any new Change requests received by the Supplier.

A review of Schedule 2 (Service Definition) shall take place annually at the same meeting, during the term of the Agreement. This annual review shall cover:

a) The scope of the Services; and

b) The Service Levels.

Any changes to Schedule 2 (Service Definition) arising from the annual review, or arising from the half yearly review, shall not be effective unless agreed by all parties in writing.

9. Dispute resolution and escalation process

The hierarchical escalation path for a Priority 1 Incident is as follows:

Escalation level	Supplier	Customer
1	IT Service Desk	
2	Incident Manager	
3	EMC Manager (or Crisis Manager out of hours)	
4	Head of IT Services	
5	Chief Information Officer (CIO)	

Within the Supplier, hierarchical escalation for a Priority 1 Incident will take place from one level to the next at the discretion of the escalating Manager.

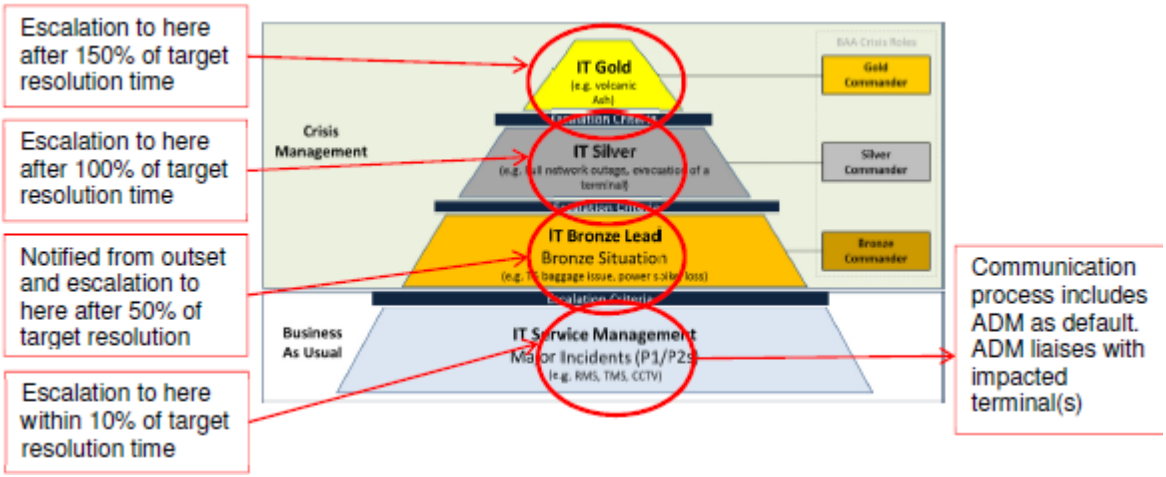
Any service disputes in relation to the provision of the Broadband Service shall be escalated as follows:

Escalation level	Supplier	Customer
1	IT Service Desk	
2	Service Level Manager	
3	Service Performance Manager	
4	Head of IT Services	
5	Chief Information Officer (CIO)	

At each level, the roles noted above shall use all their reasonable endeavours to resolve any dispute related to the delivery of the Services as soon as practicable after the date on which the dispute was allocated to that level. If the dispute has not been resolved by the level 1 roles within 10 Working Days after the date in which the dispute arose then, at the discretion of both roles, the dispute shall be referred to level 2. Escalation to subsequent levels shall take place within 10 Working Days after the date in which the dispute was allocated to the current level, at the discretion of both

9.1 IT Crisis Management & Major Incident Management

The standard communication process includes the Major Incident Manager notifying the Authorised User by default for all P1 & P2 incidents. The Authorised User then liaises with the operational lead for the affected Terminal(s). The Authorised User is kept updated according to the service level matrix – P1: every 30 minutes/P2: every 60 minutes. As this process is embedded into Heathrow command and control structure then it will evolve over time i.e. with the development of the APOC.



Appendix A: Supplier access port configuration

Background – Supplier employs a number of logical methods, in order to protect the LAN from an issue caused by clients connected to the access layer – either maliciously in unintentionally. The purpose of this statement is to share the methods – but for security reasons – not the detail of the configuration.

Port Security – this feature enables a logical restriction as to how many MAC addresses can be associated to a switch port. As an example, if a user adds a hub or a switch and the MAC address count exceeds the configured maximum the port can be configured to automatically shutdown. This condition also sends an alter to the fault management system so that further action can be taken.

Traffic Storm Control – such a condition occurs when a large number of broadcast, unicast, or multicast packets are received on a port. Forwarding these packets – as per normal operation - could cause the network to slow down or to time out. Storm control is configured operates on a per-port basis and uses rising and/or falling thresholds to block and then, after manual intervention, restore the forwarding of broadcast, unicast, or multicast packets. As with port security this condition also sends an alter to the fault management system so that further action can be taken.

Spanning tree – for an Ethernet network to function properly, only one active path can exist between any two stations, this of course has obvious implications when operating a resilient infrastructure. Spanning tree or STP is a link management protocol that provides path redundancy while preventing loops in the network. Within the configuration for spanning tree a number of protection measures can be implemented, these are as follows:

- *Portfast - t*his feature allows immediate transition of the port into STP forwarding state even if there are any loop conditions as a result the port will go into STP blocking mode.
- *Bpduguard* - In a valid configuration, Portfast enabled ports do not receive BPDUs. Receiving a BPDU on a Port Fast- enabled port signals an invalid configuration, such as the connection of an unauthorized device (such as a hub, switch), and the BPDU guard feature puts the port in the error-disabled state.

Guard root – this feature ensures that the port on which it is enabled is the designated port. If the switch receives superior STP Bridge Protocol Data Units (BPDUs) on a root guard-enabled port, the port is moved to a root-inconsistent STP state, which is like a listening state and no traffic is forwarded across the port