|  |
| --- |
|  |
| BT Technology |
| Interconnect  Operations and Maintenance Manual |
| Issue 7.0 |
|  |

**1 Document Control**

**1.1 Index**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Section** | | **1** | – | Document Control | |
|  | |  | | |  |
| **Sub-Section** | | **Title** | | | Page |
|  | |  | | |  |
|  | 1.1 | Index | | | 3 |
|  | 1.2 | Legal Notice | | | 5 |
|  | 1.3 | Contractual Significance Statement | | | 5 |
|  | 1.4 | Issue Control | | | 6 |
|  | 1.5 | Document History | | | 6 |
|  | 1.6 | Summary of Changes to Last Issue | | | 7 |
|  | 1.7 | Author | | | 8 |
|  | 1.8 | Document Review Procedure | | | 8 |
|  | 1.9 | Glossary | | | 8 |
|  | 1.10 | Foreword | | | 9 |
|  | | | | |  |
| **Section** | | **2** | – | Network Management | |
|  | |  | | |  |
| **Sub-Section** | | **Title** | | | Page |
|  | |  | | |  |
|  | 2.1 | Responsibilities | | | 11 |
|  | 2.2 | Real Time Network Traffic Management | | | 12 |
|  | 2.3 | Large Call Events | | | 14 |
|  | 2.4 | Isolation of Networks | | | 15 |
|  | 2.5 | Planned Engineering Works | | | 16 |
|  | | | | | |
| **Section** | | **3** | – | Fault Management | |
|  | |  | | |  |
| **Sub-Section** | | **Title** | | | Page |
|  | |  | | |  |
|  | 3.1 | Responsibilities | | | 19 |
|  | 3.2 | Fault Progression | | | 20 |
|  | 3.3 | Major Service Outage | | | 24 |
|  | 3.4 | Special Fault Investigation | | | 24 |
|  | 3.5 | Signalling Faults | | | 25 |
|  |  |  | | |  |
| **Section** | | **4** | – | Call Trace | |
|  | |  | | |  |
| **Sub-Section** | | **Title** | | | Page |
|  | |  | | |  |
|  | 4.1 | Responsibilities | | | 27 |
|  | 4.2 | Categories & Priorities | | | 27 |
|  | 4.3 | Malicious Call Trace | | | 28 |
|  | 4.4 | Network Integrity Call Trace | | | 30 |

**1.1 Index (Contd)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Section** | | **5** | – | Emergency Services | |
|  | |  | | |  |
| **Sub-Section** | | **Title** | | | Page |
|  | |  | | |  |
|  | 5.1 | Responsibilities | | | 32 |
|  | 5.2 | Planned Interruption to Service | | | 33 |
|  | 5.3 | Administrative Processes | | | 33 |
|  | | | | | |
| **Section** | | **6** | – | In-Life Switch Changes | |
|  | |  | | |  |
| **Sub-Section** | | **Title** | | | Page |
|  | |  | | |  |
|  | 6.1 | Responsibilities | | | 35 |
|  | 6.2 | Notification Methods | | | 35 |
|  | 6.3 | Change Process | | | 35 |
|  | 6.4 | Hot Switch Changes | | | 35 |
|  | | | | | |

**1.2 Legal Notice**

British Telecommunications plc “BT” provides a copy of this Interconnect Operations and Maintenance Manual “O&M” to UK Communications Providers “CPs” for their own use subject to the following conditions:

* That any revision has all references to BT removed (unless BT gives its prior written consent to the contrary);
* That in the event that the CP wishes to disclose or publish the document (or a revision thereof) other than as set out above then the prior written consent of BT shall be obtained; it will be a condition of such consent that BT is indemnified in substantially the same terms as set out in the current industry agreement;
* That the document is provided “as is” and BT gives no warranty of any kind in respect of its reproduction, content, use, fitness for purpose, third party’s rights or otherwise;
* That no licences from BT are granted or implied other than a royalty free licence under BT’s copyright in the document for the purposes of creating, reproducing and publishing a revision of the document as set out above.

Note that “BT” and the “BT Technology” logo are trademarks of British Telecommunications PLC.

**1.3 Contractual Significance Statement**

This document does not form part of any contract between BT and the CP.

However, some parts of this document may, where a ‘Standard Interconnect Agreement’ [Telephony Reference Offer: NCC Contract Schedules](https://www.btwholesale.com/help-and-support/regulatory.html#reference-offers) exists between BT and the CP, repeat certain legally binding provisions of that agreement. If that is the case, the fact that this document is not itself legally binding shall not affect any of the rights and obligations of BT or the CP under that agreement.

BT and the CP will endeavour to ensure that the information contained in this document is correct to the best of their knowledge. However, neither party warrants that such information will be free from errors.

**1.4 Issue Control**

This document is issued and maintained by BT Technology and is controlled in accordance with BT’s Quality Management System Procedures.

The Issue Number of the document will be identified by the ‘Issue’ on the front page.

The Issue Date of the document will be identified by the top entry in the table in sub-section 1.5.

The current version of this document can be located [here](https://www.btwholesale.com/assets/documents/help-and-support/voice/interconnect/operations-and-maintenance-manual/Interconnect_O_M_Manual_v5.docx).

**This manual becomes uncontrolled when printed or after being downloaded.**

**1.5 History**

|  |  |  |
| --- | --- | --- |
| **Issue** | **Date** | **Summary Of Changes** |
| 7 | 29/10/19 | Fault templates updated, all links to documentation on BT Wholesale portal updated and checked. |
| 6 | 31/07/18 | Update to BT Technology, copyright dates etc. |
| 5 | 31/03/12 | Full Working Issue. Minor text changes from Draft B (see Section 1.6) |
| 30/11/11 | Draft B - Text amendments (see Section 1.6)  Draft A - Inclusion Of Waiver & Equipment Change Processes; Update of Fault Classification Criteria; Review of all sections; conversion to single document |
| 31/08/11 |
| 4 | 03/10/05 | Major review; Target Restoration Timescales removed |
| 3 | 30/09/04 | Issued in standard document format, contact details corrected |
| 2 | 30/11/01 |  |
| 1 | 30/04/98 | Initial Version of document |

**1.6 Summary of Changes to Last Issue**

|  |
| --- |
| **Section 1 - Document Control** |
| Links to the Standard Interconnect Agreement (SIA) updated |

|  |
| --- |
| **Section 2 - Network Management** |
| Links to the Provisioning Manual updated. |

|  |
| --- |
| **Section 3 - Fault Management** |
| This section has been updated to include the latest fault reporting documentation and links to the BT wholesale website to enable the latest copy to be obtained.  Links to the Provisioning manual, test & integration manual have been updated. |

|  |
| --- |
| **Section 4 - Call Trace** |
| Note: This section was previously titled ‘Maintenance’  No changes This section has been completely reviewed although the key processes have not changed |

|  |
| --- |
| **Section 5 - Emergency Service** |
| No Changes This section has been completely reviewed although the key processes have not changed |

|  |
| --- |
| **Section 6 - In-Life Equipment Changes** |
| Note: The items previously found in this section have been moved to Sections 2 & 3  Links to the Provisioning manual, test & integration manual have been updated. |

**1.7 Author**

The author of this document can be contacted for enquiries or comment via e-mail by clicking [here](mailto:ix.support@bt.com?subject=Interconnect%20Operations%20and%20Maintenence%20Manual%20Enquiries).

**1.8 Review Procedure**

The document will be reviewed biennially by the author.

Should amendments or additions be required, the proposed changes will be communicated to industry via interconnect notification and/or briefing via the Standard Contract Forum as appropriate.

Comments or proposed amendments to this document should be forwarded to the Author.

**1.9 Glossary**

ASR Answer Seizure Ratio

BT British Telecommunications plc

CLI Calling Line Identity

CP Communications Provider

CRM Customer Relationship Manager

CSP Customer Service Plan

CSI Customer Sited Interconnect

CTC Call Trace Co-ordinator

Egress Outgoing traffic from the CP network

EA Emergency Authority

FRP Fault Reporting Point

GOS Grade of Service

Ingress Outgoing traffic from the BT network

ISI In-Span Interconnect

MI Momentary Interruption

MSO Major Service Outage

NTM Network Traffic Management

NMF Network Management Facility

NNG National Number Group

NSA Non Service Affecting

NSI Network Special Investigations

OSCC Operator Service Contact Centre

PEW Planned Engineering Work

POC Point of Connection

SA Service Affecting

SDH Synchronous Digital Hierarchy

SIA [NCC] Standard Interconnect Agreement (‘Contract’)

SC Switch Connection

SFI Special Fault Investigation

SRM Service Review Meeting

SS7 ITU-T Signalling System 7, aka C7

**1.10 Foreword**

In this document, a signatory to the Interconnect Agreement will be referred to as a ‘party’, unless it is necessary to be specific, whereby reference will be made to either ‘BT’ or ‘CP’ as appropriate. Where it is necessary to refer to an entity providing ‘operator services’ such as directory enquiries, the word ‘Operator’ will be used.

The manual details the responsibilities, methods and procedures to be employed for the operation and maintenance of the interconnect between the PSTN telecommunications networks operated by BT and the CP. The manual is intended to support and align with the Standard Interconnect Agreement (SIA) between the two parties and in the event of any dispute the SIA shall take precedence.

Any procedures not covered in this manual which are specific to individual parties will be   
documented in the relevant Customer Service Plan (CSP) and any such procedures in the CSP will take precedence over those in this manual.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  | **End of Section 1** |  |

**2 Network Management**

**2.1 Responsibilities**

2.1.1 General Conditions

In the Ofcom ‘General Conditions of Entitlement”, Condition 3 (Proper and Effective Functioning of the Network) requires the CP “to take all necessary measures to maintain, to the greatest extent possible:

(a) The proper and effective functioning of the Public Communications Network provided by it at all times, and

(b) In the event of catastrophic network breakdown or in cases of force majeure the fullest possible availability of the Public Communications Network and Publicly Available Telephone Services provided by it, and

(c) Uninterrupted access to Emergency Organisations as part of any Publicly Available Telephone Services offered.”

In terms of the agreement between the parties, which this manual supports, this requires that both parties are required to ensure that interconnect between them is jointly managed to comply with this condition at all times.

2.1.2 Network Management Facility

Each party must establish a distinct Network Management Facility and make available 24 hour contact details which should be recorded in the CSP.

Each party’s Network Management Facility (NMF) must have the ability and authority to monitor and control the flow and routing of traffic to maximize the effective use of available capacity.

Parties must co-operate at all times to achieve efficient and effective Real Time Traffic Management relating to the traffic routes linking their respective networks.

2.1.3 Grade of Service

Grade of Service requirements for interconnect routes are detailed in the SIA Annex A Section 5.3 and both parties are jointly responsible for ensuring that the appropriate Grade of Service is maintained on all interconnect routes.

2.1.4 Call Performance Measurements

Call Performance Measurements requirements are detailed in the SIA Section 16.2 of Annex A and both parties should exchange and agree Call Performance Measurements on a monthly basis unless agreed otherwise.

Call Performance Measurements should be used to manage capacity needed in excess of forecasts and/or reconfiguration of either party’s network to rebalance traffic on the interconnect routes.

Call Performance Measurements should normally be made available or updated within one month of opening of a new route or change of capacity on an existing route.

Where either party is unable to provide Call Performance Measurements, then that party accepts and agrees that the Call Performance Measurements provided by the other party may be used in their place.

Where provided, parties will also supply a definition of terms used in the Call Performance Measurements provided to the other party.

Distribution contact points for Call Performance Measurements will be detailed in the relevant Customer Service Plan (CSP).

**2.2 Real Time Traffic Management**

Real Time Traffic Management (RTTM) is defined as the real-time surveillance and control of traffic flow on a telecommunications network, with the aims of both maximising the effective use of available capacity for call completion during periods of overload and maintaining the defined Grade of Service.

2.2.1 BT’s Network Protection Policy

To enable BT to discharge its responsibilities in relation to the General Condition 3, there may be occasions, e.g. during high profile media phone-in events or during a disaster scenarios, where call gapping measures need to be implemented to protect network components from excessive overload, both within the BT network and connected CP networks.

During excessively high profile media events, which terminate in BT’s network, BT will liaise with the other parties as appropriate to request the application of overload controls on the incoming interconnect routes and likewise for events terminating on the network of another party, BT will, when requested, apply reasonable overload controls to provide protection to that network.

This ensures that all reasonable steps have been taken to maintain the effective functioning of the public telephone network including uninterrupted access to emergency services.

2.2.2 Traffic Controls

To protect its own network each party’s NMF may apply controls within its own network without necessarily gaining agreement from the other party, even though traffic destined for that other party’s network may be affected. In these circumstances the other party’s NMF will be consulted, whenever possible in advance, and given advice of the application and subsequent removal of the controls.

Any issues can be resolved by using the normal escalation procedure, using the contact points as documented in the CSP.

2.2.3 Traffic Control Methods

There are three main types of real time traffic control, in order of preference:

*Automatic*

Use of in-built bilateral automatic switch overload controls on UK-ISUP routes following the Automatic Congestion Control protocol as defined in NICC UK Standards document [ND1007](http://www.niccstandards.org.uk/publications/public-net.cfm).

*Expansive*

Use of alternative traffic routing to temporarily move traffic away from the affected switch(es) (dependant on the available network architecture).

A re-route control may mean that the affected traffic will be temporarily carried over the originator's network for a greater distance than normally expected before being offered to the other CPs network. The NMFs will have responsibility for activating and removing the re-route options for each incident.

*Protective*

Protective controls prevent equipment elements being put in jeopardy due to excessive call attempts, problems and overloads in the other party’s network.

The protective call-gapping control would mean that traffic destined for the other party’s network may be restricted by the application of the control. This control will normally, although not necessarily, be applied on the receipt of a formal control request.

Liaison between NMFs to query real time network traffic status and to consider application of controls should not be made via Fault Reporting Points (FRPs) unless a preceding fault identified the traffic problem, in which case the ‘lead’ FRP should be updated on an hourly basis.

2.2.4 Traffic Control Requirements

1. Both parties must jointly implement Automatic Congestion Control (ACC) functionality on UK-ISUP routes where testing has shown their equipment supports it. Section 10 of the Interconnect [Provisioning Manual](https://www.btwholesale.com/help-and-support/voice/interconnect.html#interconnect-provisioning-manual) refers.
2. Both parties must use reasonable endeavours to ensure that its end-users do not plan large 'Phone-in' type events without prior consultation. In circumstances where large amounts of traffic are expected both parties will liaise and agree the application of any controls giving at least two days’ notice.
3. When a party detects an unplanned event the other party should be advised using the agreed channels as quickly as practicably possible.
4. Both parties must liaise and endeavour to assist each other to overcome traffic management issues in the other party’s network in a real time basis.
5. Any applicable controls must be applied by both parties in reasonably short timescales.
6. In normal circumstances, both parties will communicate as necessary to achieve a co-ordinated traffic management effort.
7. Where appropriate, each party will notify the other in a timely manner when major problems occur that are likely to affect interconnect traffic.
8. Each party may operate controls within its own network in response to perceived problems in either party’s network. Where there is a direct effect on the other party’s service the initiating party will advise the other party when such action is taken detailing the scope, cause, impact and likely duration of the problem. The initiating party will also notify the other party of removal of any controls.
9. If either party considers that the use of traffic controls by the other party is acting to the detriment of its own network's performance, both parties agree to discuss the concerns using appropriate escalation contacts as defined in the relevant CSP. Any issues arising should be addressed at the service review process as documented in the CSP.
10. Traffic information relevant to an existing or perceived problem must be provided as quickly as practical by to the other party on request. Under no circumstances will either party be required to provide commercially sensitive information, nor shall the information supplied be used for any other purpose than traffic management purposes.

**2.3 Large Call Events**

2.3.1 Requirements

Both parties must make every effort to ensure that their service providers inform them prior to large call events which may cause network congestion. Liaison between the respective service providers and the two parties should be part of normal business practice.

Both parties must ensure that they have adequate NMF capability available to assist during major incidents and planned large phone-in type events. In circumstances where large amounts of traffic are expected, both party’s NMFs will liaise directly and agree appropriate traffic management actions

There are two scenarios each with differing timescales for advising the other party:-

1. Planned Phone-in type events - minimum two working days notice is required
2. Unplanned traffic flow problems or congestion during normal operations – controls normally to be applied within 30 minutes or as soon as operationally possible

The availability of such controls and degrees of selectivity and possible speed of implementation shall be agreed in advance and documented in the CSP.

2.3.2 Requesting / Notifying Implementation of Controls

Where it is necessary for one party either to implement controls which will affect the other party’s traffic, or request reduction of traffic from the other party, then that party must notify the other party in line with the time scales in 2.3.1.

The requesting / notifying party must use the ‘Traffic Management Controls Request Form’ attached.



2.3.3 Traffic Management Controls Request Form Process

All fields should be completed. Any known related fault references should be included in the ‘reason’ section of the form. All communications will be logged and given a unique reference number by both parties for tracking and reference purposes.

Confirmation of actions, either taken or requested, should be given by the requesting party by completing Section A of the form and sending it to the other party, as per the agreed communication method.

The party receiving the request will either note or apply the controls and confirm by completing Section B of the form and return it to the originating party via the agreed method.

The originating party, on seeing that the problem has cleared, will either inform the other party of the removal of controls, or request removal of controls by completing Section C of the form and again passing it to the other party via the agreed method.

Finally the appropriate party will either confirm removal of the controls, or acknowledge receipt of notification of the controls, and conclude the process by completing Section D and returning the form to the other party.

**2.4 Isolation of Networks**

It is possible that a problem emanating from within either network may place the BT or CP switch in jeopardy. If this situation arises the course of action will depend upon the assessment of the impact by the NMF owning the switch.

*Before any isolation of an interconnect route by disconnection of the signalling is considered necessary, investigations must take place to determine if that route carries 999/112/18000 emergency calls. If this is the case then the decision to isolate the route should be escalated within both parties (with a working alternative routing to be confirmed as minimum requirement prior to disconnection).*

*Potential Switch Failure*

Where there is no immediate threat of failure to either party’s switch, NMFs should continue to monitor and take no further action. The situation should be actively monitored by both parties and potential mitigations should be agreed should the situation worsen.

Potential mitigations to be considered include:-

1. Reduction in traffic - e.g. application of call gapping traffic re-routing
2. Reduction of capacity (out of servicing some E1s on the routes)

Either party may consider that unilateral action is warranted and will advise the other NMF as appropriate. In this case a fault must be raised and the BT and CP FRPs will then direct actions within their respective networks.

*Imminent Equipment Failure*

If a switch is considered to be in a critical position then the interconnect between the parties must be isolated immediately by disconnecting the signalling.

The BT or CP NMF has the responsibility for isolation / disconnection of the interconnect route where there is NO DOUBT that the interconnect route is causing the switch to be in a critical position.

Details of the circumstances known at the time plus actions taken must be communicated to both party’s FRPs. The situation will then be managed between each party’s FRP in terms of fault clearance and each party’s NMF in terms of any modifications to the actions taken.

**2.5 Planned Engineering Works**

Each party will inform the other of any foreseen work it finds necessary to carry out within its own network which may affect interconnect arrangements or standards of performance between the networks as perceived by the parties or their customers. The request for deferment of a planned outage by the other party will be subject to negotiation and agreement with each case taken on its merits as documented in the planned engineering process documentation

Any foreseen / emergency work falls into one of two main categories:-

1. Work performed directly on transmission that carries the interconnect route(s)
2. Work on equipment terminating the interconnect or work within each network which will have a direct bearing on the perceived performance of the connectivity.

The notification contact points and the escalation contact points must be detailed in the CSP.

2.5.1 Planned Works on Transmission

Such work may take one of the following forms:-

1. Changeover from MAIN to STANDBY working by the use of high speed switching equipment.
2. Momentary Interruptions (MI's) which may be of maximum duration of 1 minute during "Preferred" hours.
3. Out of service interruptions - where a "make good" route does not exist, a "Scheduled Outage" will be necessary.

Times when Change-Overs, MI's and out of service interruptions may be scheduled by either party will be agreed by use of the designated contact points.

Both party’s notification contact points are identified in the CSP.

It is essential that checks are carried out in both networks to ensure service access is maintained throughout the duration of the planned work. This should include the impact of any currently applied network management controls or other current activities that limit the availability of alternative means of access. It may be necessary for additional alternative means of access to be arranged. This should be requested before the planned work is agreed between both networks.

It will be assumed that the work was completed as planned unless the originating party advises otherwise.

2.5.2 Other Planned Works

If either party intends to carry out a planned work in this category then the originating party will notify the other and will provide the following information: -

1. The originator’s contact details
2. Date the planned work was originated
3. Planned work reference number
4. Equipment or unit affected
5. Interconnect route(s) affected (to include BT and CP Equipment designations)
6. Break type, i.e. HSS, MI or scheduled outage
7. Date, time and duration of the planned work
8. Any other pertinent information

2.5.3 Notification Timescales

At least 3 days notice is expected for planned works.

*Both parties MUST agree the scope and timing of any planned work.*

If the receiving party is unable to agree to the interruption to service then they must promptly contact the originating party to discuss and agree an alternative.

If interruption of service cannot be agreed then the originating party must contact the relevant escalation contact point.

A reduction of the notification timescales should be allowed only under exceptional circumstances and each occurrence will be treated as an Emergency Planned Work. Emergency Planned Works must not become ‘business as usual’ practice.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  | **End of Section 2** |  |

**3 Fault Management**

**3.1 Responsibilities**

3.1.1 Fault Procedures

Each party must establish a distinct Fault Reporting Point and make available 24 hour contact details which should be recorded in the CSP.

Each party’s Fault Reporting Point (FRP) will have the ability to identify and repair (using appropriate means) faults within its network and will work with the other party to clear faults on the interconnect equipment.

Each party will have an escalation path which will be documented with 24 hour contact points recorded in the CSP.

The party with the fault in its network will be will be responsible for fault progression (including internal escalations and arranging co-op with the other party where necessary) and the subsequent reporting of clears.

Each FRP will meet reasonable requests to provide diagnostic assistance from the other party even if no formal fault exists.

Any issues with the fault progression should be resolved with the escalation procedure, using the contact points as documented in the CSP.

Prior to reporting the fault the reporting party will ensure that a genuine fault exists that reasonable steps have been taken to prove the fault away from their own network, i.e. beyond the Point of Connection (POC).

3.1.2 Transmission

Each party is responsible for the equipment on its side of the Point of Connection (POC).

For CSI based transmission, where terminating equipment is accommodated at the CP premises, BT maintenance teams must be permitted access to the equipment for service restoration purposes. Requests for access to the CPs premises by BT maintenance will be made by the BT FRP.

For ISI based transmission and unless otherwise agreed (and documented in the CSP), the party which has provided, or has utilised a third party supplier’s transmission line plant to provide, the greatest proportion of the transmission line plant which makes up the interconnect link will have full controlling end responsibility for :-

a) Authorising all work on the connectivity

b) Its removal from service for routine maintenance and testing

c) Ensuring dangerous voltages (if any) are removed/locked-off on power feed systems

d) Ensuring that lasers are removed/locked-off on fibre optic systems

e) Restoration of the connectivity back into service

Where a 3rd party is involved, the controlling party must arrange suitable procedures with that party to support (a) to (e) above. Where service on the connection is likely to be affected the notification of Planned Engineering Works (PEWs) procedures (Section 2.6) must be adopted.

3.1.3 Health and Safety

Health and Safety matters are covered by legislation in force at the time of access to which all organisations and individuals must adhere.

It is the responsibility of each individual, under the terms of the Health and Safety at Work Act, to ensure the safety of their working environment and to work in a safe manner. Appropriate use of risk assessments should be used and the building owners must be prepared to accept questions and comments regarding safety issues and to take the appropriate action where necessary. Visitors shall accept directions regarding safety and safe working practices from the building representative.

Should any dispute arise about access being unsafe, work should cease and the matter escalated immediately to the representatives of each party to their central point for management decision.

When working with lasers, guidance as per latest version of IEC specification 60825 Parts 1 (Equipment Classification, Requirements and User Guide) and 2 (Safety of Optical Fibre Communication Systems) must be followed.

**3.2 Fault Progression**

3.2.1 Link & Network Fault Definitions

Faults reported between the parties will be defined as either ‘Link’ or ‘Network’ faults.

Link Fault: *A fault affecting an identifiable E1 (aka ‘circuit’ or ‘2Meg’ or ‘system’)*

Network Fault: *Any fault that cannot be specifically identified as a link fault*

3.2.2 Structured Questions

The following structured questions should be used by the reporting party to gather information about the fault BEFORE it is reported to the other party. The party receiving the fault report should also use the questions in order to ensure that all the relevant data is captured at the initial fault reception.

|  |  |
| --- | --- |
| *Link Faults* | *Network Faults* |
|  |  |

To check for the latest version of the link and network fault documents, use the following link:

[Interconnect - Fault Templates](https://www.btwholesale.com/help-and-support/voice/interconnect.html#interconnect-faults-templates)

3.2.3 Priority Marking

The parties will jointly agree the fault priority based on the information captured in the structured questions.

*Classification*

Priority 1 faults (Service Affecting) will be progressed by both parties until they are cleared, regardless of the time of the day.

Priority 2 faults (Non Service Affecting) will only be progressed during normal working hours (usually 8am - 6pm GMT/BST) unless agreed otherwise and documented in the appropriate CSP.

Except in exceptional circumstances, Priority 1 should only be adopted where the reporting party confirms that:

a) The fault has been proved away from their network and

b) Co-op will be available AT ALL TIMES out of hours

At any time whilst it is open and where both parties agree, a fault may be re-classified to a different priority.

The party fixing the fault report may lower the priority if the party originating the fault is subsequently unable to provide co-op.

3.2.4 Priority Criteria

*Link Faults*

Priority 1 (Service Affecting)

The agreed Grade of Service is not being met at the time of report (or is likely not to be met during the upcoming busy traffic period)

#### Priority 2 (Non Service Affecting)

Any other link fault falling outside the Priority 1 criteria

The following may also be considered by both parties when deciding on link fault priority:-

a) Any other outstanding link faults affecting the route

c) Any network controls or temporary traffic re-routes already applied

d) Any active or Planned Engineering Works (PEWs) or planned media events

e) Whether the fault should be classified as a ‘Major Service Outage’ (MSO)

*Network Faults*

Priority 1 (Service Affecting)

a) Total loss of access by either party to pass calls between the two networks

b) Total loss of access to one or more of the number groups or ranges owned by either party

c) Total loss of access to one or more of the number groups or ranges owned by a third party when calls are transited via either party’s network

d) A loss of any service deemed as ‘business critical’

e) Any loss of emergency service access

#### Priority 2 (Non Service Affecting)

Any other network fault falling outside the Priority 1 criteria

3.2.5 Reporting

The party raising the fault will raise the fault to other party’s FRP using the method and contact details provided in the receiving party’s CSP.

The party receiving the fault report will provide a unique reference to the other party and this reference will be used during all communications regarding the fault.

3.2.6 Progression

The party fixing the fault will be responsible for providing updates and offering information to the other party during the progression of the fault and must also ensure that adequate jeopardy monitoring mechanisms are available to ensure faults are repaired within acceptable timescales.

If the party fixing the fault requires co-operation with the other party’s repair teams it must be requested via the other party’s FRP.

Fault progression may be deferred to out of normal working hours if the problem is perceived to be due to faulty equipment common to other traffic routes on the equipment, as the effective working of those routes will be adjudged to be in jeopardy. In such cases the marking will be Priority 2 and the faulty equipment repaired out of hours.

3.2.7 Clearance & Closure

When the fault has been located, and remedial action to restore has concluded, the party fixing the fault must notify the other party’s FRP.

Once the other party has been notified, the fixing party may mark the fault as cleared.

After 24 hours, unless notified otherwise by the reporting party, the fixing party may close the fault.

The fixing party must notify the other party that the fault has been closed, using a method agreed between the parties.

Once the fault is closed, any subsequent report of failed re-test will be treated by the party which fixed the fault as a new (repeat) fault.

If either party is dissatisfied with any aspect of the fault clearance it should be discussed via the agreed service review process between the two parties (as documented in the relevant CSPs).

3.2.8 Escalations

When the reporting party is dissatisfied with the ongoing restoration progress they may escalate using the timescales detailed in the table below to the contacts outlined against the stated levels in the fixing party’s CSP.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Recommended Fault Escalation Timescales** | Minimum Time (Hrs) to Escalate to: | | | | |
| *First Level* | *Second Level* | *Third Level* | *Fourth Level* | *Fifth Level* |
| Priority 1 (Service Affecting) | 4 | 8 | 12 | 16 | 20 |
| Priority 2 (Non Service Affecting) | 24 | 32 | 40 | 48 | 56 |

3.2.9 Performance

Both parties will monitor the repair performance of the respective parts of the interconnect to which they have visibility by carrying out analysis of fault records and use this data to reduce future fault occurrence.

Where requested by the other party, shortly after the end of each calendar month the other party will generate a report which will identify the faults cleared by that party within the previous month. The report will usually detail fault reference, fault type, priority and reporting, clear type and clear and close times. In addition, other data such as that to identify any fault trends or black spots etc. may also be requested.

3.2.10 Service Review

The parties should hold regular Service Review Meetings.

The meetings will be used to analyse the output of the reports detailed above to identify any failure trends, in particular those relating to recurrent faults (to identify route causes), faults reported in error (i.e. fault not found) and faults reported where the clear is subsequently found in the reporting party’s network.

**3.3 Major Service Outage**

Faults relating to Major Service Outages (MSOs) are service affecting by definition and therefore will be marked a Priority 1. However, where applicable, an MSO related fault will take priority over any other Priority 1 fault.

An MSO is defined as the presence of a fault which results in the inability of the available links on an interconnect route/routes (including where applicable any agreed alternative overflow route/s) or either party’s internal network to carry the calls presented to it, and is perceived to have a major impact on the service offered to either party’s end-users. These faults will generally be of the following nature:

1. A major external lineplant failure
2. A switch failure

MSOs detected by either party will be identified to the other party’s FRP. It is important that as much information as possible is provided to enable action to be taken quickly to prevent as much traffic loss and/or network congestion by either party.

When requested, updates of progress should be given by the party owning the MSO and confirmation that the MSO has been cleared must also be given as soon as practicable by the owning party.

**3.4 Special Fault Investigation**

There may be occasions when both parties will need to set up a Special Fault Investigation (SFI) to resolve problems of a complex nature. Either party may request an SFI during the real time life of the fault via other party’s FRP. The problem clear, including any issues identified resulting from the SFI, should be reviewed at a Service Review Meeting if required.

There may be occasions where SFI liaison is required with several parties in order to assist the localisation of complex problems, e.g. when all parties need to liaise together with the necessary test equipment and expertise to discover the source of the problem. This form of liaison will generally be required on an exceptional basis when all other attempts to re-create / localise the problem using normal procedures has proven unsuccessful.

These types of problem can be of:

1. A national nature - where calls originating from one party, transits via one or more other parties networks to a destination party network
2. An international nature - where calls originating from one party transits via one or more other party’s international networks to an overseas network

The party requesting the SFI liaison is responsible for organising the necessary level of liaison with all other parties. The parties involved must provide reasonable assistance to each other in setting up the liaison which will include a reasonable lead time.

**3.5 Signalling Faults**

Prior to the introduction of an interconnect route, interconnect testing takes place which will ensure that the signalling (as well as the various call types) between the parties is operating as per the appropriate UK NICC standards.

Testing requirements are defined in Section 4 (and repeated in Section 5) of the [Provisioning Manual](https://www.btwholesale.com/help-and-support/voice/interconnect.html#interconnect-provisioning-manual) and the testing requirements are defined in the [Integration & Operational Testing Manuals](https://www.btwholesale.com/help-and-support/voice/interconnect.html#interconnect-testing-manuals).

However, due to the complex nature of the signalling interface, changes of build, interworking between signalling variants etc., problems may arise which were not apparent during the testing stage. These problems may be of a more general nature but may affect many interconnect routes and/or calls, so while not critical in nature in terms of network integrity signaling problems may affect a significant number of end-users and/or call revenues.

When such problems are identified, the relevant party must raise the problem as a network fault as per the procedures detailed in Section 3.2.

3.5.1 Waiver

Some fixes to signalling faults may require a software patch and/or build change to be implemented, and where this is the case, it may take long timescales to develop, test and implement the resolution. Where this is the case (and the problem is not deemed to be service affecting), the parties may agree a Waiver which will clearly detail the proposed resolution, owners and time scale for resolution.

The waiver process is documented in Section 4.3.10 or 5.3.10 of the [Provisioning Manual](https://www.btwholesale.com/help-and-support/voice/interconnect.html#interconnect-provisioning-manual).

The waiver form is contained in Appendix 34 of the [Provisioning Manual](https://www.btwholesale.com/help-and-support/voice/interconnect.html#interconnect-provisioning-manual).

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  | **End of Section 3** |  |

**4 Call Trace**

**4.1 Responsibilities**

Both parties are responsible for providing Call Trace assistance to the other party in relation to the following contractual / operational criteria:

1. Emergency Calls (see Section 5)
2. Network Integrity (see Section 4.5)
3. Telecommunications Fraud (including AIT)

Both parties must also assist Police Authorities when they are carrying out investigations in relation to Malicious Communications Offences as defined in the Section 127 of the Communications Act 2003:

1. Malicious Call Trace (see Section 4.3)

And additionally assist the relevant ‘Agencies with Investigative Powers’ (as defined in Regulation of Investigatory Powers Act 2000) in the following crime related criteria:

1. Missing Persons
2. Serious & Non Serious Crime
3. Terrorism
4. Nuisance Calls
5. Social misdemeanour

Both parties must establish a Call Trace facility which will assist the other party, Police Authority or Registered Agency ‘Single Point of Contact’ (SPoC) in lawful call trace activities including the establishment of a *Call Trace Co-ordinator* (CTC).

Both parties must supply a list of the relevant CTC contact(s) in their organisations responsible for dealing with call trace requests in the relevant CSP, and, additionally, both parties must also provide the Police Authorities with a list of contacts responsible for dealing with relevant types of call trace request.

**4.2 Categories & Priorities**

Call traces are categorised into the following types:

1. Real time - where a trace has been requested when a call is in progress
2. Pre-planned - where prior warning has been given of (an) incoming call(s) to a particular number
3. Retrospective - where a call has been completed prior to a trace request

*Priority must be allocated in the order of category specified above and within Category 1 the priorities are, in order, a), e) and d) in the criteria as defined in Section 4.1.*

**4.3 Malicious Call Trace**

When requested, the each party’s CTC must supply the Police Authority with the following information (where and as appropriate):

1. The originating/preceding network’s name (and contact information if requested)
2. The terminating/succeeding network’s name (and contact information if requested)
3. The calling end-user’s details (based on the CLI information in the signalling)
4. The called end-user’s details (based on the Destination Number in the signalling)
5. The time, date and duration of the call(s)

It is then the responsibility of the Police Authority to contact the other networks, e.g. the party which owns the originating/terminating end-user, and/or preceding/succeeding network.

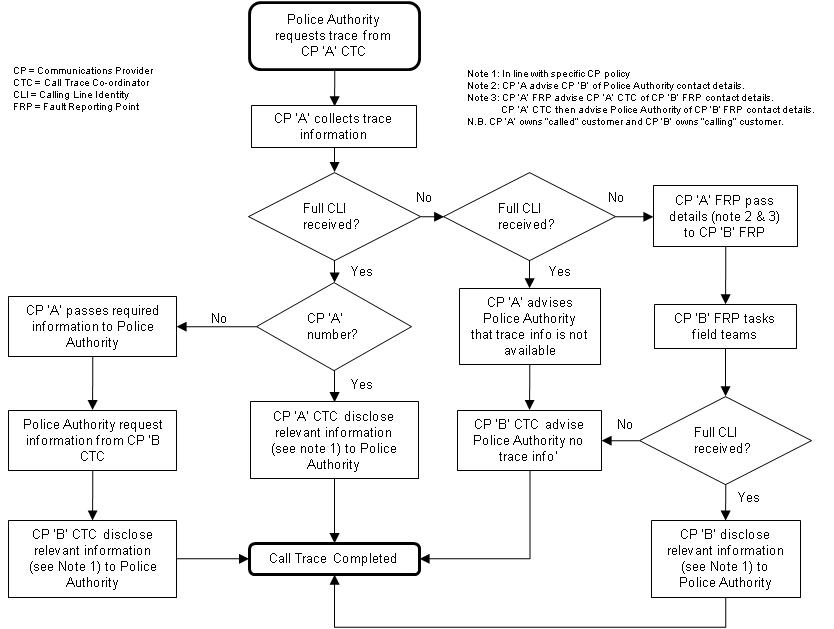
*End user information must* ***never*** *be exchanged directly between the parties.*

If the full CLI is not passed in the signalling message then the party owning the called end-user must liaise with the other networks to assist the Police Authority in identifying the calling end-user’s details.

4.3.1 Procedures

Interconnect call trace procedures are documented in the flow diagram on the next page and must be adopted by both parties.

N.B. the process assumes that there are only two parties involved and the calling and called parties reside on these networks. Where third party networks are involved in the call, the process should be adapted appropriately.

****

**Call Trace Flow Diagram**

**4.4 Network Integrity Call Trace**

There may be exceptional circumstances where calls are being made on either party’s network, where Police Authority intervention is not required.

The following criteria are acceptable circumstances for such call traces:

1. An adverse effect on the calls that are made by either party’s end-users
2. Perceived to have a potential impact on the integrity of either network

Following initial investigations by either party’s call trace co-ordinator the other party’s co-ordinator should be approached to assist in completing the investigation.

Where deemed necessary, the appropriate Police Authority may subsequently be involved by either party.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  | **End of Section 4** |  |

**5 BT Emergency Service**

**5.1 Responsibilities**

The contacts information mentioned in the following section must be detailed in the appropriate BT/CP CSP.

5.1.1 CP

The CP must provide an *Emergency Contact* (CPEC) in order to give real time assistance to the BT Operator Service Contact Centre (OSCC), the BT FRP and the Emergency Authority (EA).

The contact must be accessible by telephone with priority answer and be available 24 hours a day.

‘Hotline’ realisation by direct lines is preferred by BT to ensure access to the CP. Where this is not possible, access via the PSTN or other types of network, e.g. mobile will be a suitable alternative. For security of access it may be necessary to provide alternative back-up arrangements.

*BT OSCC to the CP Emergency Contact*

The BT OSCC may contact the CPEC for the purpose of providing one or more of the following functions:-

1. Call Trace which comprises interrogation of the CLI to determine CP end-user and/or network details in cases of display difficulty. The OSCC will contact the CPEC to obtain this information on behalf of the EA
2. Ad-hoc fault liaison if network information is not present, incomplete or no EA connect-to numbers available, or if CLI is incomplete or unrecognised
3. Occasional requests from EAs for name and address of telephone user. The OSCC will contact the CPEC to obtain name and telephone number to pass onto EA

#### *BT FRP to the CP Emergency Contact*

Used for emergency line fault reports and liaison.

#### *EA to the CP Emergency Contact*

A telephone number agreed between the CPEC and the EA to be used for co-operation with the CP in identifying the location of a caller. Such requests will be authorised by the appropriate senior level within the EA.

5.1.2 BT

*FRP*

If during any fault investigation it is found that the fault is affecting the level of Emergency Service then BT FRP will advise the CP FRP.

*OSCC*

The BT OSCC will report any faults or a reduction in the quality of the Emergency Service to the BT FRP for onward cascade.

In addition, the OSCC may also have direct contact with the CPEC via the Hotline.

**5.2 Planned Interruption to Service**

Each party must inform the other of any foreseen work it finds necessary to carry out within its own network which may affect the standards of performance of the Emergency Service.

Three working days notice is required for any Planned Work. The procedure defined in Section 2.6 should be followed. Direct contact may be required via CSP contacts as the PEW process will not normally cater for this work.

**5.3 Administrative Processes**

5.3.1 Changes to Number Ranges

The CP must advise the BT Data Delivery Team Manager of the introduction of any new number ranges or relevant network identifiers so that the appropriate call routing tables can be built in the call handling system. The BT Commercial Interface Team (CIT) will be responsible for agreeing and documenting the proforma used.

5.3.2 Customer Complaints or Other Service / Quality Matters

The BT 999 Product Manager will act as the focus for BT investigations on these matters.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  | **End of Section 5** |  |

**6 In-Life Switch Changes**

6.1 Responsibilities

When either party wish to make changes (in relation to software or hardware) to a switch after it has been brought into service they must, as a minimum:

1. Inform the other party using the methods outlined in sub-section 6.3
2. State whether the change is likely to affect the services or signalling provided by it
3. Perform testing to demonstrate compatibility with existing equipment comprising the existing switch and the services in place via it (testing based on current BT testing recommendations as defined in the [Integration & Operational Testing Manuals](https://www.btwholesale.com/help-and-support/voice/interconnect.html#interconnect-testing-manuals)
4. Implement a single change (i.e. on one switch) and allow this to be assessed before implementing further changes.
5. Provide a schedule of implementation detailing the affected routes.
6. Be prepared to perform reverse engineering to resolve issues.

The change must be notified to the other party at least 3 months before the planned initial change.

6.2 Notification Methods

BT will initially notify industry of any changes to its switches by means of Interconnect Briefings.

CPs must use the Switch Change Notification [SCN] form, which is located in Appendix 11 of the [Provisioning Manual](https://www.btwholesale.com/help-and-support/voice/interconnect.html#interconnect-provisioning-manual)

6.3 Change Process

The process is contained in Section 4 (repeated in Section 5) of the [Provisioning Manual](https://www.btwholesale.com/help-and-support/voice/interconnect.html#interconnect-provisioning-manual)

6.4 Hot Switch Changes

Where equipment changes are to be implemented using a short break of service (hot change) method, the additional provisions relating to hot switch changes included in Section 4 (repeated in Section 5) of the [Provisioning Manual](https://www.btwholesale.com/help-and-support/voice/interconnect.html#interconnect-provisioning-manual) must be followed.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  | **End of Section 6** |  |