Office of the Director of
Telecommunications
Regulation

CONSULTATION PAPER

Network Resilience

Document No: 01/77

Date: 27th September 2001

Oifig an Stiúrthóra Rialála Teileachumarsáide
Office of the Director of Telecommunications Regulation
Abbey Court, Irish Life Centre
Lower Abbey Street, Dublin 1, Ireland
Tel. +353 1 804 9600 Fax. +353 1 804 9680 E-mail info@odtr.ie

Contents

Foreword

The delivery of quality services to consumers is one of the benefits arising from the liberalisation of the telecommunications market. Fundamental to the quality aim is that consumers have reasonable level of assurance around the continuity and security of the service being provided.

Liberalisation has also lead to an increase in the number of operators seeking to interconnect their networks and the resulting greater complexity in arrangements that are necessary to facilitate this.

Resilience of both individual and interconnecting networks is therefore becoming increasingly important from a quality of service perspective. In light of this I would like to obtain views from a wide range of parties as to how best network resilience can be assured.

Etain Doyle
Director of Telecommunications Regulation

1 Introduction

1.1 Background

The Director of Telecommunications Regulation ("the Director") is responsible for the regulation of the Irish telecommunications sector in accordance with national and EU legislation.

One of the key benefits of competition is that consumers can enjoy greater choice of operators providing a wider range of services. However, at a more fundamental level it is also critical that consumers can have a reasonable level of assurance as to the continuity and security of the service being provided whether it is a fixed, mobile or data service. On the one hand as competition develops consumers should expect a greater degree of assurance arising from the fact that there is more than one network. However, it is also true to say that with this expansion, interconnectivity and interoperability of networks becomes increasingly important, particularly having regard to the overall resilience of networks and assurances around the continuity of quality services. Therefore resilience is an issue not just for individual networks but also because of the increased potential for problems arising from the interdependence of networks. This includes, for example, the interrelationship between mobile and fixed networks. It is from this perspective that the issue of resilience is important in regulatory terms.

The Director's responsibilities in relation to network availability and security are clearly set out in EU and national law. A summary of the legal basis for this consultation is set out below. The Director is concerned that more attention needs to be paid to the issue of network resilience. With increasing traffic volumes and interdependence of networks it is essential that adequate precautions are taken by operators to ensure permanence and availability of service. We have, in the past, experienced a number of outages which have caused serious disruption to users resulting in economic and financial loss. While in some 'force majeure' situations a temporary loss of service may be unavoidable it is essential that all reasonable precautions are taken to ensure continuity of service. In this consultation the Director wishes to seek views from a wide range of parties, including network operators and user groups, as to how best network resilience can be assured. This consultation is exploratory at this stage and, depending on the outcome, may be followed by a more detailed approach on specific issues. In summary therefore the purpose of this consultation is as follows:

- To assess what network resilience is and why it is important
- To examine ways in which network resilience can best be assured
- To assess, at a general level, the existing arrangements for ensuring network resilience
- To explore whether further action at a regulatory or operator level may be required including, for example, greater co-operation between operators.

The ODTR has already conducted a number of interviews with major network operators on the subject of resilience. The results of these meetings in so far as they are operator specific and individual operator plans are confidential are not discussed in this paper. However, some of the general conclusions of these meetings are included for discussion in the Paper.

1.2 Legal background

Under current EU and Irish legislation operators have obligations to protect their networks and ensure service to users is maintained. The Director of Telecommunications Regulation has a range of powers to ensure networks and services are protected by operators. The most relevant legislation pertaining to these powers is;

- European Communities (Interconnection in Telecommunications) Regulations, 1998, SI No. 15 of 1998, Regulations 10 and 11.

- European Communities (Leased Lines) Regulations, 1998, SI 109 of 1998, Regulation 9.

- European Communities (Voice Telephony and Universal Service) Regulations, 1999, SI No. 71 of 1999, Regulation 17

- Postal and Telecommunications Services Act 1983, SI No. 24 of 1983, Section 111.

This is a consultation document only and does not constitute legal, commercial or technical advice. The Director is not bound by it. The consultation is without prejudice to the legal position of the Director or her rights and duties to regulate the market generally.

2 Network Resilience

2.1 Why protection is necessary

Modern telecommunications networks are complex systems that have gained so strong a reputation for reliability that very substantial business systems are utterly dependent on them. This makes it very important to review network resilience periodically to ensure its adequacy. Networks may be vulnerable to a range of failures or unusual patterns of calls. Failures can result from a variety of reasons ranging from software problems to catastrophic external events such as fire. Unusual demand profiles may result from failures in other networks or external events such as a major disaster or televoting. Problems can be further exacerbated by callers' propensity to re-dial calls when they fail. Hacking, data security and sabotage are also concerns. Without adequate protection mechanisms (network resilience) the impact of a major or even minor problem can quickly spread through the network leading to a serious or, in the worse case, total degradation or cessation of service for users. Such a failure could represent a major cost to telecommunications users.

Operators themselves will need to protect the service for their own customers, but as will be explained in section 3 of this document other factors of a cross-industry nature also come into play.

Therefore telecommunications networks are inherently vulnerable to internal failures or external changes in demand. Internal failures cover a wide variety of problems including (as a short selection only) the following:

- Physical damage of cables.
- Power outages.
- Catastrophic loss of switches through fire.
- Corruption or loss of routing data within switches.
- Other software problems.

These problems may arise through a variety of causes ranging from entirely unavoidable problems such as flooding or accidental damage (often of external plant by other contractors) to deliberate sabotage or hacking. They may also result from inadequate internal systems such as poor maintenance, poor design, inadequate operational procedures, or testing.

Some faults such as power loss (without backup) of a local switch or a break in local access cables can mean the complete loss of service to a small number of customers. Others will have a less direct impact resulting in a more general but less intense degradation of service.

External events have an impact when they cause demand on a network to change substantially from the ‘normal’ load that it was designed to handle. These may include predictable events such as higher calling at Christmas, a concentrated inbound telemarketing campaign or televoting event. Unpredictable events are myriad but those perhaps of greatest concern are those where many people are concerned about the safety of friends and relatives or where an interconnected network itself fails.

Unfortunately demand and supply are linked in a way that tends to exacerbate the original problem of overload. This is because when a call fails people (especially when that call is important to them as would be the case if they were concerned about a relative’s safety) redial the number. Phones with redial buttons make the problem even more acute. For data calls similar effects are observed as failed packets (for example) are retransmitted automatically according to the rules of the protocol. Furthermore, a higher number of calls will put pressure on network resources that can result in even more calls failing. Without remedial action, a vicious spiral can then ensue that may eventually result in such severe overload that callers do not even get dial tone when they lift the handset or the throughput of a data network slows to such an extent that it is largely unusable.

Different problems will occur with different probability and will have different impact. Network designers have to plan how to handle a combination of a failure with unusually high demand or the combination of two or more failures.

Q. 1. **Respondents are invited to comment on the above. Are there other significant circumstances that pose a threat(s) to continuity of service on a national or more localised basis? If so please explain**

2.2 Approaches to Providing Protection

Resilience is the ability of a network to withstand internal failures and external events at best without effect to traffic or at worst with a managed reduction in service level. Remedial action can range from measures to prevent problems occurring in the first place; through measures to alleviate the symptoms of a problem whilst it is occurring; and on through to good procedures to repair or replace faulty equipment as quickly as possible.

Physical security of buildings and facilities, software firewalls, scheduled maintenance, the use of well-designed and well-manufactured equipment, fire protection and duplication of power supplies by battery and/or generator are examples of measures taken to prevent problems occurring in the first place. Such arrangements are good business practice and are not the focus of this paper

For similar reasons, the repair of failed facilities is not considered further. Neither are disaster planning and recovery procedures. Such plans would be activated if for example a fire destroyed a major switch.

This paper concentrates on approaches aimed at mitigating the impact of a problem whilst it is occurring. The methods of providing resilience are similar for both internal and external events, but differ in detail. Essentially there are two approaches. First is the ability to use equipment that is deliberated kept as backup, or is otherwise unused at the time of the fault, as efficiently as possible to circumvent the problem. Second, if the first cannot be done, is to contain the problem so as to prevent the effects from spreading.

Broadly, internal events (mostly equipment failures, either hardware or software) are usually catered for by providing multiple alternative physical and logical routes for traffic – whether voice or data. This is known as diversity. In addition, switching and transmission capacity – particularly in the upper layers of the network – which can be flexibly accessed by a range of traffic streams, is incorporated into the design of voice networks, so that the network is to an extent self-healing. Such equipment may be provided more plentifully than typical (ie problem free) circumstances might dictate. Many data network protocols include this self-healing ability by allowing messages to be routed ‘around the problem’. The same is true of SDH rings. On some key national or international routes, unused capacity is often kept ‘on stand-by’ to allow a severed route to be fully by-passed.

If this approach is not sufficient, or if an external traffic-stimulating event occurs, network management action is taken. Software allows even voice switches to be reconfigured quickly. Different traffic routes exhibit natural and random variations in loading at different hours of the day. This means that there is often some spare capacity in the network even when the network is at its busiest. This 'temporary' spare capacity is exploited so that an alternative route bypassing the problem or increasing capacity can be introduced while the fault is repaired, restoration occurs or demand remains unusually high.

If it is not possible to 'reroute' traffic, approaches tend to resort to containment rather than restoration by isolating the problem. One example of this would be the case of unusually high demand to a single area or even telephone number (for example where a enquiry line number is published after an accident). Another example would be blocking all attempts as early as possible to reach a network that is known to have failed. In such circumstances network management actions aim to ensure that those calls that will not be successful do not affect calls to unaffected numbers, areas or networks.

Q. 2. Do you consider that there are there other approaches to providing network protection? If so please outline.

2.3 Commercial Concerns

A network can never be entirely protected and very high levels of protection only come at a commensurately high level of cost. Combinations of failures can occur with serious consequences but may occur at a probability that is so small as to be considered negligible. The additional cost in planning for this 'negligible' risk would need to be recovered through higher end user tariffs which may not be acceptable to the majority of users. Clearly some users want and are willing to pay for the highest levels of protected services possible. However the majority, has the right to expect a good level of protection without profligate 'gold plating' above reasonable expectations. A completely fail-safe network would not appear to be justified as the norm for all calls. However neither is one with no protection.

Operators therefore aim – relying as appropriate on international standards or best practice – to achieve a balance between the cost of protection and the likelihood and potential impact of the failure and concentrate their effort and resources at the most critical components with the greatest risk of failure.

There is a clear commercial incentive for operators to pay adequate attention to protecting their own networks. In an ideal world, operators and their customers would agree the level of protection required and the charges that would apply. Some customers do require assured service, others will be happy to buy a 'cheap and cheerful' service with no guarantees. In a fully competitive market different product offerings are likely to be developed to cater for these different needs. However the telecommunications supply industry does not yet have this level of choice and so average expectations are considered.

Q. 4. What do operators consider to be best international practice for network resilience? Do operators comply with that standard?

Q. 3. Do you consider that the level of protection as currently offered is sufficient to protect customers' interests?

2.4 The Cross-industry Dimension

The commercial importance of a resilient network may suggest that regulatory intervention is not required. However, there are many potential problems that arise due to the fact that the 'national network' nowadays comprises several networks operated by different companies and the interactions between these companies and the interfaces between them raise their own resilience problems. Potential concerns include but are not limited to the following:

- Network failure or overload in one network leading to problems in those connected to it. For example problems on the mobile network affecting calls on the fixed network.
- Inadequate resilience on interconnection circuits themselves.
- A failure of an interconnection circuit leading to a distorted traffic pattern for the receiving network.
- An operator that has a reduced network discriminating against interconnection traffic in favour of its own retail traffic.

- Under forecasting of interconnection traffic leading to a network operator failing to make adequate provision in its network. This in turn results in reduced resilience

Furthermore, commercial best-practice alone may be insufficient to protect the wider national interests. In the language of economic regulation concerns of this type are known as externalities. An externality occurs when the cost to an operator (of in this case a network failure) is less than the cost to consumers of the service whether they be wholesale or retail customers. For example, an operator will lose revenue during an outage and may have to pay certain compensatory charges to customers. But the loss of a deal to a competitor by that customer who has lost phone service may cost a great deal more than any compensation received. Externalities would be avoided if customers could choose the level of protection (and charge) they required. However while an average expectation is used regulation should ensure externalities are contained.
For these reasons, the Director concludes that there are certain circumstances where a cross-industry approach to network resilience is necessary.

3 Existing industry arrangements

ODTR has undertaken a brief review of resilience in the Irish market. The following summarises the findings.

3.1 Infrastructure resilience

3.1.1 General

Eircom as the former incumbent and as the operator with the most extensive network has a central role in preserving national integrity. The picture that emerged was that the eircom network is key to the connectivity of operators systems within Ireland. Some operators have network links to other operators which are not dependent on eircom switching services but which still use eircom transmission capacity. Other links, notably international services, are duplicated with separate operators providing the service and physically separated routes to each operator.

3.1.2 Power

Operators appear to have good provision for dealing with power failures: the major sites are provided with standby generators (large local switches and all switches in the upper levels of the hierarchy); minor sites (small local switches and mobile base stations) are usually reliant on battery backup only (generally configured for about 10 hours service). This is in line with normal best practice in the industry. Certain key mobile base stations are also provisioned with generator backup so that some network connectivity can survive a prolonged (greater than the standby battery capacity) power failure.

3.1.3 Network Management

Major operators indicate that they have separate network management centres with separated (from the main business network) data networks used for management and control. They seek to ensure that external access to these control networks is minimised and strictly controlled. Some operators have more elaborate controls in place than others. Data backup and recovery procedures are in place. Operators indicate that they have a prepared alternate site and arrangements with vendors to deal with the loss of their management centres.

3.1.4 Switched Networks

There appears to be good diversity within mobile networks. Operators appear to have significant resilience built into their switching networks. In each case this consists of dual parenting of switches into the network hierarchy, multiple logical routes and multiple physical routes usually provided over fault tolerant links (using SDH ring transmission systems). Additional switching capacity is provided in each of the networks to allow for switch failures and traffic surges.

eircom's network also consists of dual parented primary level switches and a multiple physical and logical route structure with redundant switching capacity. eircom's provisions appear to be in line with best practice. There is concern, nevertheless, about eircom's ability to respond to rapid and unpredicted changes in traffic flows especially ingress traffic from other networks.

3.2 Conclusion

The telecommunications infrastructure in Ireland appears to be capable of continuing to provide service (although possibly at a slightly degraded level) in the event of a single failure or traffic surge. As indicated earlier, rather less thought appears to have gone into considering the implications of multiple networks and possible multiple failure. The ODTR's particular concerns are as follows:

- The tendency to plan for only a single failure (or event) in the operators own network.
- The apparent lack of information passing between operators - especially those not directly connected with one another (e.g. transiting via eircom).
- The reliance on a single network for the majority of interconnectivity (eircom).
- A low level of resilience in inter network links.
- The potential susceptibility of eircom's network to failures of external networks producing major changes in traffic flows.

Question 4. Do you agree with the above analysis?

Question 5. Are there other risks that need to be considered?

Question 6. Are current measures adequate to guard against these risks?

4 Options to improve situation

ODTR believes that in general commercial factors should be sufficient discipline to ensure that adequate protection is provided to an operator's own retail customers. However for the reasons set out in section 2.4, ODTR is concerned that certain matters of a cross-industry impact need fuller consideration.

Q. 7.	**Under what circumstances may commercial factors be insufficient? Should ODTR audit performance?**

4.1 Discrimination in the event of abnormal events

Discrimination by an SMP operator between its downstream retail divisions and OLOs seeking interconnection is illegal. This should be the case whether or not an abnormal event is occurring unless discrimination is necessary to protect network integrity or is a direct result of a failure by the OLO. This latter point is discussed below.

Question 8.	**Do you agree that existing measures avoid discrimination whilst adequately protecting network integrity?**

4.2 Co-ordination

ODTR believes that consumers and industry as a whole would benefit from greater exchange of information requiring network management intervention. This would be necessary during both the planning stage and when actionable events are occurring. ODTR believe that a sub-group of the O&M forum may be an appropriate mechanism to provide this co-ordination.

Question 9.	**Do you agree with the need for an industry co-ordination forum? If so what should be included in its terms of reference?**

4.3 Service Level Agreements

ODTR is of the opinion that SLAs within interconnection agreements would be an appropriate mechanism for ensuring that interconnection providers and seekers achieve adequate clarification of protection arrangements in place. This would include penalties for failure to meet obligations. This is attractive technically and economically. Technically, operators can plan with greater certainty, economically operators can consider better the true cost of failure and plan accordingly.

ODTR recognises that responsibilities exist in both directions. Interconnection providers can expect accurate information for planning purposes and should have the right to ensure that access seekers do not export their problems. Access seekers should expect that their traffic streams are adequately protected.

ODTR believes that operators should in the first instance attempt to develop an appropriate framework that is of mutual benefit. If this process fails, ODTR notes its willingness to intervene and impose changes that might be necessary.

Questions 10. Do you believe that SLAs or specific terms and conditions around in-service performance are a useful mechanism for ensuring adequate protection?

Question 11. If not, what other mechanisms might be appropriate? If yes, how might SLAs be created/modified ? Also if yes, what process and timescales would be appropriate for developing the new framework?

4.4 Interconnection Links

ODTR believes that interconnection links must be available that allow adequate protection in the event of failures in the transmission path. ODTR is not yet convinced that this is done cost effectively (for example self-healing rings are not supported) and believes that there are circumstances where OLOs are disadvantaged. In particular, ODTR feels it is necessary to define a resilient interconnection product that better meets market needs.

ODTR would expect SMP operators to respond to requests for such a product quickly. It would also be willing to intervene directly if progress was not occurring or conflicting requests were received.

Question 12. Do you agree that there is a need to review the resilience of interconnection links? What concerns do you have in this regard? What protection might be necessary for each party?

Question 13. Do you agree that access seekers should prepare product definitions in the first instance?

5 SUBMITTING COMMENTS

All comments are welcome, but it would make the task of analysing responses easier if comments were referenced to the relevant question numbers from this document.

The consultation period will run from 27 September, 2001 to 9th November, 2001 during which the Director welcomes written comments on any of the issues raised in this paper. Having analysed and considered the comments received, the ODTR will review the responses received and publish a report in December on the consultation which will, *inter alia* summarise the responses to the consultation. In order to promote further openness and transparency the ODTR will publish the names of all respondents and make available for inspection responses to the consultation at her Offices.

The Director appreciates that many of the issues raised in this paper may require respondents to provide confidential information if their comments are to be meaningful. Respondents are requested to clearly identify confidential material and if possible to include it in a separate annex to the response. Such information will be treated as strictly confidential.

"All responses to this consultation should be clearly marked "Reference: Submission re ODTR [01/77]" and sent by post, facsimile or e-mail to:

Mr. Kevin Kennedy
Office of the Director of Telecommunications Regulation
Irish Life Centre
Abbey Street
Dublin 1
Ireland

Ph: +353-1-8049600 Fax: +353-1-804 9680 Email: kennedyk@odtr.ie
to arrive on or before 5.30pm on 9th November, 2001.

Office of the Director of Telecommunications Regulation
27th September, 2001