Janet availability
How Jisc maintains key network services

1. Introduction

We use a number of third party service providers to build the Janet network, and while we value the close working relationships we have with a number of our suppliers, we are not their only customers and may certainly be a relatively small part of their customer base.

Occasionally, this leads to unavoidable conflicts of interest when suppliers plan maintenance work at times that are inconvenient for our members and customers. This is especially true when maintenance occurs at critical periods such as during Clearing.

This document explains the steps taken by Jisc to minimise the risk of service disruption throughout the year, and especially during critical periods.

2. High availability by design

Janet is designed from the bottom up to be highly available, so that wherever possible, no single fibre break, power failure or equipment malfunction should disrupt the network service.

2.1. Infrastructure Design

Designing diversity and resilience into a network is vitally important. Too little resilience can result in a catastrophic failure of a network backbone, but care must also be taken not to introduce too many levels of resilience, to the point where inherent complexity causes more problems than it solves, and costs escalate.

The Janet national backbone and regional backbones are designed to be resilient. Each network is built from diversely routed dark fibre or managed circuits to ensure that no single circuit failure can take down a backbone. Regional networks are diversely connected to the national backbone, and the national backbone has many separate and diverse connections to the Global Internet.

In particular, we have worked with suppliers to ensure that our global Internet connectivity:

- Is provided by two separate, Globally connected Tier-1 carriers
- Is provided in multiple diverse locations on the Janet backbone
- Does not rely on a single transatlantic cable route
- Is available in locations other than London using routes which do not pass through London

2.2. PoPs

The premises we use to house key backbone points of presence (PoPs) are themselves designed to provide very high levels of availability for the equipment located within them. They have multiple connections to the electricity supply and power to each of our racks is fed from at least two diverse power feeds, each of which is backed up by separate UPS and generator. Fibre routes into these locations are also physically diverse.

Access to PoP locations is strictly controlled, with security measures in place to ensure that only authorised staff can enter the suites where Janet equipment is located. Our racks are locked and monitored.

2.3. Equipment

The optical switches and core routers at the heart of our national and regional networks are chosen as much for their reliability as their traffic handling capabilities. All have multiple power supplies and control systems and can operate perfectly well on a single CPU and with a reduced number of power supplies.
We take care to ensure operating systems are stable and rarely upgrade system software to new releases until that release has been operating reliably elsewhere. We do, of course, perform upgrades where security vulnerabilities exist.

We ensure that we have out of band access to all key equipment. This enables us to communicate with the system over a network that is independent of Janet, in case its connection to Janet has failed. Access to the control interfaces of our equipment is restricted by a number of systems and controls, which ensure that only authorised members of staff can connect to equipment in order to make changes to configurations.

3. Monitoring

We have a number of Network Management Systems (NMS) which monitor the availability and performance of the network, and of individual network devices. These systems provide us with near real time visibility of the network and will alert us to circuit or equipment failure. We also monitor alarms and logs to look for indications of emerging problems, so that they can be fixed during a maintenance period, before they cause a failure at a critical time.

We also monitor to help with capacity planning, to ensure that call our network connections, from member circuits to core backbone routes, have sufficient capacity to meet demand. These systems predict traffic growth based on historical usage, so we also need to engage in regular conversations with our members, to understand any emerging requirements they might have, which would require capacity in excess of their predicted growth.

4. Maintenance

Janet continually evolves, to ensure that it meets the present and future needs of our members. Change that might disrupt services to members is performed during routine maintenance sessions. Change can include installing hardware to provide new services, upgrades to existing services or the replacement of suspect components before they fail.

4.1. Routine maintenance

Routine maintenance is performed on the network on Tuesday mornings, from 07:00 until 09:00. In practice, work is planned to be completed by 08:00, allowing sufficient time for testing and providing an opportunity to undo the changes if they don’t work, without exceeding the maintenance window. Routine maintenance is advertised two weeks in advance, in email trouble tickets published by the Jisc Service Desk. Where maintenance can’t be completed within the standard window, we normally schedule the work for weekends.

Where maintenance has to be performed in an emergency, we provide as much notice as possible, and balance the disruption caused by the maintenance, against the disruption, or potential disruption that not performing the maintenance would cause.

The diversity designed into Janet means that it is possible to perform most maintenance without disrupting the service to organisations which themselves have multiple connections to the network.

4.2. Maintenance freezes

We don’t perform routing maintenance over the extended Christmas holiday. During the month of August, we have a maintenance freeze, to ensure that the network is stable and available during the release of A-level results and throughout clearing. We will however, perform emergency maintenance in order to resolve an emerging problem, rather than risk a fault occurring during business hours, which would have a more disruptive effect. During August, we operate at a heightened state of awareness, to minimise the response and fix times should faults or third-party maintenance cause services to our members to fail.
We try to manage the relationships with our suppliers, so that their planned maintenance avoids August as far as possible, however it is not possible to postpone all third-party maintenance. Where maintenance is unavoidable, we work with suppliers to try and schedule interruptions to minimise the impact on members.

5. Providing the service

5.1. The Jisc Service Desk

The first port of call for requesting services or reporting services failures is the Jisc Service Desk (JSD). This is our first level support centre with shifts of experienced technical staff who monitor the network for problems. They are proactive and will often identify and respond to incidents before members contact us to report them.

The JSD takes ownership of all faults and orchestrates our response to network incidents. They can call upon Major Incident response teams, made up of specially trained staff, to oversee our response to incidents which severely disrupt services to a large number of member organisations.

5.2. The Network Engineering Group

Members of the Network Engineering Group (NEG) provide second level support for solving network problems. NEG engineers are also responsible for managing our regional networks, for field engineering, and running over 600 managed routers, which provide a standard interface between a member network and Janet.

5.3. Core Architecture Team

Members of the Core Architecture Team are our most experienced and knowledgeable engineers. They are responsible for designing and implementing our core network and provide third line support for incident management.

5.4. 24-hour support

We manage and support the network 24 hours a day, every single day of the year, without exception. Members may report incidents at any time of the day, or night and will get a response from our engineering team. Outside of business hours, we have second and third level engineering support on-call and the JSD is staffed between 07:00 and midnight during the week and from 09:00-19:00 at weekends.