The testbed operations procedures

Added by Pekka Savola, last edited by Pekka Savola on May 29, 2009

Introduction

This is ICT SHOK FI deliverable DA4.1.2, giving an overview of testbed operational procedures. More information about the testbed can be found in DA4.1.1, the testbed architecture.

Administrative procedures

Ordering

Joining the testbed is coordinated by CSC at WP4. WP4 receives the requests and negotiates with the questioner. The specific needs are discussed and the possibilities to respond to the needs are investigated. The alternatives are discussed with the interested party and a suitable method is chosen. The basic facts on end point addresses, contact persons and other practical pieces of information are collected.

After this preliminary phase the request enters the normal Funet procedures for establishing customer connections. This contains agreement and contract issues, possible call for tender procedures, device procurements, installations and testing. The extent of each step varies greatly depending on a case. For example, a laboratory located in a current Funet member's campus is administratively more straightforward to handle, whereas a new organization needs a longer agreement negotiation phase.

The technical delivery time depends on whether or not fiber infrastructure is readily available from the nearest Funet PoP to the customer location. Order and delivery of a fiber connection typically takes from 12 to 16 weeks (3-4 months). A week or two should be reserved for installation. The administrative delivery time depends on the activity of the parties. It is, however, possible to manage the practicalities in comparable time frame with the technical scheduling.

Funding issues - overview

CSC has budgeted for testbed-specific equipment, connections, etc. which has 50% TEKES funding.

If a company gets a connection or equipment, the company may pay for CSC's part the "other 50%", but this payment must not use company's TEKES financing. This requires a (generic) written permission from TEKES, which we need to draft once/if it seems this will be needed. In the final report, we'll also need to show how these expenses were realized.

Public organizations can't contribute to "the other 50%" or get CSC's budget reallocated to them because this would mess up the company/public numbers. If a public organization would want to get covered to buy equipment etc., they'll need to take this into account in the next year's ICT SHOK FI budgeting.

Funding procedures for universities and companies

If an organization needs equipment for testbed connection, it's possible to shift their own budget to equipment. Informal queries to TEKES on this indicate that as long as this doesn't exceed 20KEUR, it's OK.

If CSC needs to get equipment (e.g. CWDM mux/demuxes, CWDM SFPs, a concentrator Ethernet switch) for testbed connections, this can be put under CSC's TEKES budget (equipment). It will get 50% funding and CSC will cover the other half if the equipment has wider applicability.

If a university requires a connection, the preferable approach is to make the additional cost a part of regular Funet billing, paid by the IT centre of the university. Then the IT-centre and research group can agree on how the cost is reimbursed. However, this expense cannot be covered by TEKES financing.

If a company requires a connection, the company is added to Funet billing and any expenses are a part of this. This cost can probably be financed by TEKES, but the funding percentage is 35% compared to CSC's 50% and the company will need to shift their budget.

Additionally, either the same bill will include the cost for fiber/connection (resulting in 35% TEKES funding), or CSC will pay for it (50% TEKES funding) and the company will reimburse the other 50% from their non-TEKES budget.

Contract procedures

A contract is necessary.

In a university setting, this can be covered by the regular Funet contract university's IT-centre has, so necessarily no paperwork is needed (except possibly between the research group and the IT-centre).

In a company setting (assuming the company is not a Funet member), a customized Funet contract needs to be drawn up. As company's lawyers may want to get involved, some time should be reserved to agree on it. A finalized contract is not a strict prequisite for connecting, it's sufficient that the process is under way.

Setting up connections

Customer responsibilities at delivery

Customer is responsible of purchase, installation, and configuring customer equipment. Usually there is no need to install Funet equipment in customer premises. However, in some cases a passive CWDM-mux/demux device is installed. Sometimes a media converter is also needed but usually it is acquired by the customer.

The interface towards Funet can be either fiber or copper and must be agreed. Fiber interface is usually preferred so no media converters are needed.

Running fiber to a laboratory or an end user in the campus typically requires administrative coordination and approval as the IT management usually needs to be involved (e.g. in providing cross connects). Justifying the need and getting this approval may take some time and effort. An agreement regarding responsibilities and obligations (e.g., responding to security incidents, not connecting systems to both production and test network and thus providing a "back door") may also be needed.

The customer should have at least one technical contact person who has information about single-mode fiber availability in customer premises and who can connect the equipment. The person needs to have access to necessary equipment and cross connect rooms.

The customer performs performance tests to the connection when the connection is brought up or if modifications are made. Funet has an iperf server and live CD that can be used for these tests.

Testbed operator's actions

CSC will deliver connectivity service in Funet network as agreed with the customer. If new fiber connections are needed (usually the last mile), CSC will tender and order the connections.

Details of the connection implementation are discussed with the customer. There is a checklist (in Finnish) about things to be considered that can be used. CSC will assign the necessary CWDM wavelength, provision DWDM channels and make routing configurations as needed.

CSC makes available a live CD for network performance testing.

IP addresses

Funet assigns the required address space to the customer. If the customer already has Funet routed addresses, either IPv4 or IPv6, a subnet might be used. Address range must be a CIDR block. It is recommended that separate address ranges are used for dedicated testbed connections. It is assumed that traffic between a testbed network and organisations' main Funet connection is routed through Funet. Source-address filtering is done in Funet router customer interface using uRPF. Static routing is used towards the customer assuming backup routing is not required.

Funet Hostmaster (hostmaster@funet.fi) is the contact point for requesting IP addresses. Addresses are assigned according to RIPE NCC policies from Funet PA address space.

The customer should tell how many addresses are needed and to what purpose. The information is given in in a RIPE request form. Funet hostmaster will provide assistance in filling the form if needed.

http://www.ripe.net/ripe/docs/iprequestform.html
http://www.ripe.net/ripe/docs/ipv6-assignment-request.html

The evaluation of a request takes typically a couple of days or a week. Funet hostmaster or RIPE NCC may ask additional questions or clarifications.

When the request is approved, Funet hostmaster will assign the address range and updates the RIPE database.

Customer needs to set up reverse DNS for the addresses. If this would be a challenge, Funet may be able to offer services that may help in this respect. Address block can be routed when reverse delegations are ready.

Contact information

CSC maintains a list of customer contact persons. There are three groups for different kinds of issues: administrative, technical and security. All roles must be defined but can be only one person or a centralized contact point.

Setting up services

Using existing testbed services

WP4 has collected a wiki page that lists existing testbed services that project members make available. The page is open for project participants.

The wiki page contains information about availability, cost, and contact information about each service. There are also examples of use cases of the services.

See: TestbedServices. An overview is also available in DA4.2.2, the testbed connectivity establishment report.

Offering services to project partners

WP4 has created a service template to facilitate offering different kinds of services to project participants. It has been used by project participants and also a third party to describe their offering.

While using the services may incur some cost, the primary purpose of service descriptions is to create and foster collaboration between researchers, and to enable test possibilities even if a researcher's organisation would not be able to offer services locally.

Services are available on a best effort basis unless otherwise stated.

WP4 has also created a use case template that should be used to illustrate current or potential use cases, examples, applicability, etc. of a service, possibly integrating multiple services.

Service life cycle

Providing service and discontinuing a service usually takes some time, so service providers should typically be looking at the service life cycle of at least a year. A single user will probably also use the service for at least half a year, unless the process is automatic or no registration is needed.

Service provider will fill in the service and use cases templates and WP4 will make them available. Service provider may also write a short advertisement for the new service in the next WP4 newsletter that's distributed inside the project.

Those interested in the service will contact the service provider contact directly, but WP4 may also act as a middle man if necessary. Service provider should however report if there has been interested in the service.

Next steps in services management

For smoother communication with those organisations that are not ICT SHOK FI programme partners, to reduce project specificity, and to manage the life cycle of services in the event that FI programme ends, the long term vision is to move testbed-related activity to its own site where access can be granted to the interested third parties as well.

Network monitoring and reporting

Funet NOC operations

Funet NOC (= Network operations Center) duty officer is reachable by phone and email on working days from 8.30 to 16.00. Funet NOC uses network monitoring systems to monitor the status of network services and customer connections. Funet NOC may also contact the customers if there there are interface errors, output drops, abnormal traffic or some other anomalies.

Routed IP connections are monitored with http://im.funet.fi system. The system uses ICMP ping to test customer connections. Target addresses are chosen with the customer from customer network when the connection is set up. The im.funet.fi system has a public view for monitoring data.

Unless otherwise agreed, alarms related to testbed connections are not processed outside office hours.

Currently Funet NOC has limited means to monitor light path connections. Light path customers can run monitoring software in their own devices.

Availability

Network services are offered on a best effort basis. The connection typically has no redundancy and is terminated at a single edge device, and therefore a problem or service break in the last mile or in the equipment will cause some non-availability.

Funet AUP can be found from the CSC's public web pages: http://www.csc.fi/english/institutions/funet_en/about/ethics

Fault reporting

Contact point for all operational issues is Funet NOC: http://www.csc.fi/english/institutions/funet_en/networkservices/usersupport/noc

Security issues

Responsibilities

Responsibility for the information security at the end site belongs to the project partner. The requirement of using information systems which are maintained according to best current practices and accepted standards is remarkably important if the partner requests an internet connection, as opposed to e.g. point-to-point light paths, which, by their very nature, are closed circuits and thus less prone to external threats.

CSC does not offer generic firewall service or port filtering as this is seen as a drawback and a possible source of anomalies in research use. Because no filtering (except uRPF) is performed, it is very important that the site's security practices are in order and it has filtering and anomaly detection capabilities of its own.

The project partners are required to respond to and act on any contact made by the Funet network and security administration.

CSC, as a member of the project, is responsible for the transmission connection. For example, in IP-based connection cases CSC takes care of the information security of the router network and in the case of light paths the security of the optical transmission system.

Incident reporting

In case of a security incident, the connected project members are required to report the incident to Funet CERT. Funet CERT is an internationally acknowledged and trusted computer security incident response team, tasked with improving network information security for Funet constituents and the network itself, as well as handling and responding to detected security incidents.

Instructions for reporting an incident can be found on the Funet CERT webpage (http://www.cert.funet.fi/). The reporter is asked to provide, at a minimum, basic information concerning the incident, and optimally a more thorough succession of events and related evindence, such as system logs and discovered artifacts.

Reports of detected security incidents may also originate from Funet CERT or other parties, as compromised systems and anomalous traffic may be noticed before the project member is aware of the situation.

Incident handling and response

The customer is expected to handle security incidents through all the phases of incident response. This may require thorough analysis of and several system administration tasks on the affected systems. Funet CERT can provide assistance in coordination and analysis if requested.

Extreme cases

Finnish Communications Regulatory Authority (FICORA) requires that internet operators must take responsibility for the general availability and functionality of their public information networks. This requirement, the responsibilities to our customers, and the international co-operation bodies enforce CSC to maintain the stable production state in the network.

If a project partner acts irresponsibly, CSC will take measures to minimize the harm to other network users. In extreme cases the testbed connection will be shut down and the agreed arrangement terminated. Deliberate malicious activity and/or gross negligence of established best current systems, network and security administration practices may also result in legal consequences.

Legal considerations

Handling of personally identifiable information must be taken into consideration and actions must comply with requirements set forth in current legislation and regulations.

Reference materials

RFC2196 - Site security handbook
RFC2350 - Expectations for computer security incident response
RFC3013 - Recommendations for ISP security services and procedures
RFC2142 - Mailbox names for common services, roles and functions
RFC3227 - Guidelines for evindence collection and archiving