Deliverable D4.1.2
The 2nd version of testbed backbone operations procedures

Pekka Savola, Jari Miettinen, Kaisa Haapala

ICT SHOK Future Internet Programme
(ICT SHOK FI)

Phase 2: 1.6.2009 – 31.12.2010

Tivit, Yritysten tutkimus- ja kehittämisrahoitus, Päätös 516/09, 29.5.2009, Dnro 560/31/09

TKK, Tutkimusrahoituspäätös 40212/09, 29.5.2009, Dnro 925/31/09

www.futureinternet.fi

www.tivit.fi

This work was supported by TEKES as part of the Future Internet programme of TIVIT (Finnish Strategic Centre for Science, Technology and Innovation in the field of ICT).

The testbed operations procedures

Added by Pekka Savola, last edited by Pekka Savola on May 26, 2010

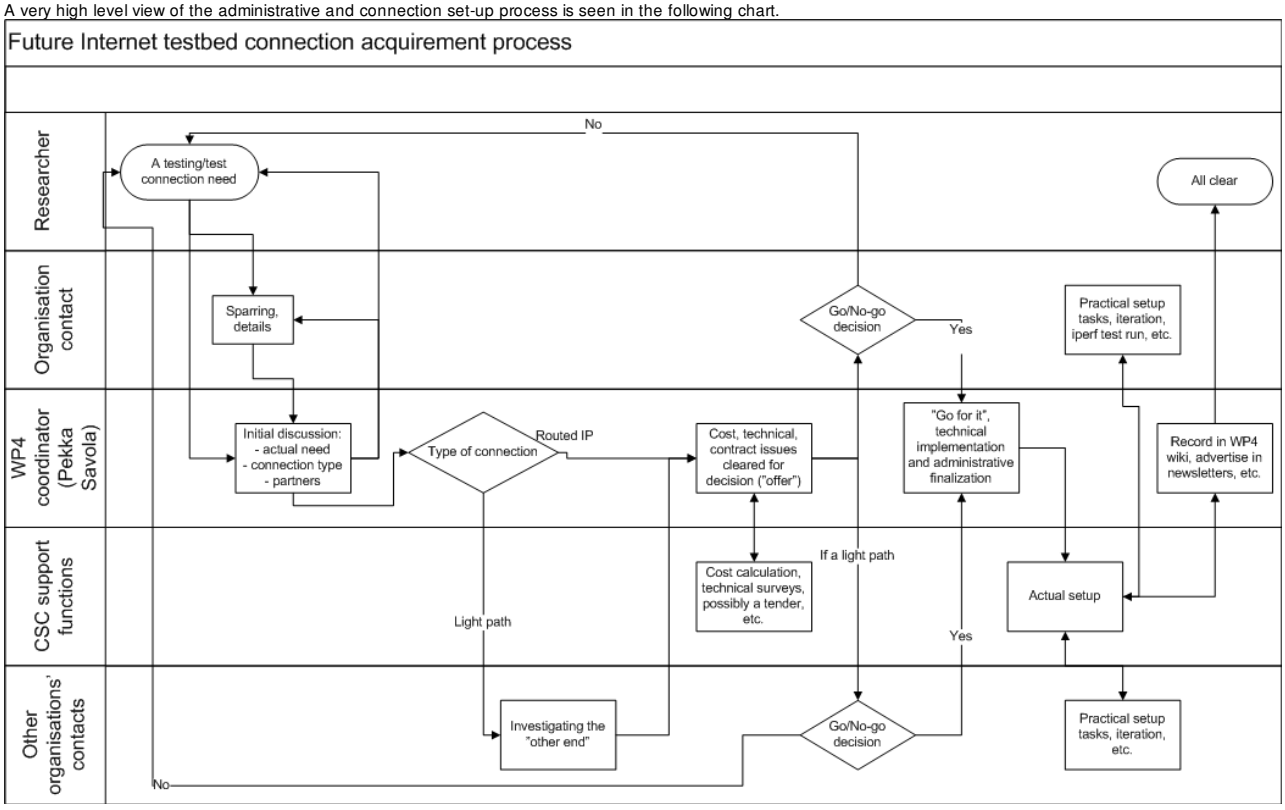
Introduction

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

The operations procedures gives an overview on the use of the testbed for a researcher. The document contains essential information to anyone interested in practical testing in the Future Internet programme. It covers the ordering, setting up and deploying the connection. The operational period is covered by describing the ways to install own services and telling what kind of monitoring and support services are available. The operational and security areas of responsibility are described and the users are given sources for further information.

ICT SHOK FI work package four (WP4) is acting as a coordinating body which serves the project with practical testing capabilities. WP4 relies on the services provided by CSC and other project partners for delivering the testbed to the researcher's fingertips.

A very high level view of the administrative and connection set-up process is seen in the following chart.



Administrative procedures

This section covers ordering, funding and contracting the testbed connection. It is assumed that the administrative needs may be tedious, so it is recommended to make an early contact to WP4. It is the intention that the administrative tasks could be done in parallel to practical actions. When completed the researcher's home organization will have a solid contractual relationship with the testbed operator.

Ordering

Joining the testbed is coordinated by CSC at WP4. WP4 receives the requests and negotiates with the customer (requester). The specific needs are discussed and the possibilities to respond to the needs are investigated. The alternatives are sought with the interested party and a suitable implementation 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, testing, and documentation. The extent of each step varies greatly depending on the 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 and installation phase.

The technical delivery time depends on whether or not fiber infrastructure is readily available from the nearest Funet point of presence (PoP) to the customer location. The ordering 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 a budget for testbed-specific equipment, connections, etc. which has 50% TEKES funding. This constitutes a method to ease the building process as it is subsidized. The will of TEKES is to promote the testing activity.

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 the TEKES financing of the company. 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 versus public figures. 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

Some fundamental ways to arrange funding for test hardware and connections can be identified. The prime methods and known rules for each organization types are the following:

1. If any project organization needs equipment for the testbed connection, it's possible to shift their own budget to the equipment. Informal queries to TEKES on this indicate that as long as this doesn't exceed 20KEUR, it's acceptable.
2. 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 center of the university. Then the IT center and research group can agree on how the cost is reimbursed. However, this expense cannot be covered by TEKES financing.
3. If a company requires a connection, the company is added to the Funet billing and any expenses are a part of this. This cost can probably be financed by TEKES, but the company funding percentage is used (e.g. 35%) compared to CSC's (e.g. 50%) and the company will need to shift their budget.
4. 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 equipment budget. It will get 50% funding and CSC will cover the other half if the equipment has wider applicability.
5. Additionally, either the same bill will include the cost for fiber/connection (resulting in e.g. 35% TEKES funding), or CSC will pay for it (50% TEKES funding) and the company will reimburse the rest from their non-TEKES budget.

Contract procedures

A written contract is always required for testbed setups. CSC will assign a small negotiating group which will go through the process from the early conversations to a signed contract. Agreement templates exist which can be utilized. The goal of the contracting is to find a solution which fits well to the test needs and which can be sustained for the time necessary to achieve good results. An existing contract can be expanded to cover multiple connections and sites.

If the other party is an university, a contract can be covered by the University IT center's regular Funet contract. This means, that in some cases only very limited paperwork is needed. However, it may be that the research group and the IT center may want to make a separate contract between themselves, but this is the university internal issue.

If a company is willing to have a testbed connection a customized Funet contract needs to be drawn up. As the negotiations may be more versatile some time should be reserved to agree on it. A finalized contract is not a strict prerequisite for initiatiating the practical steps. It's sufficient that the process is under way.

Setting up connections

This section clarifies the situation when the testbed connection or connections are installed and put into use. After passing the setup phase a functioning testbed connection is activated and operational.

Customer responsibilities at delivery

Customer is responsible of the 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 needed on-site. Sometimes a media converter is also needed but usually it is acquired by the customer.

The demarcation with Funet can be either fiber or copper and it has to be defined in advance. Fiber interface is usually preferred so that no media converters would be needed. Avoiding conversion equipment removes one possible source of malfunction.

Running fiber to a laboratory or an end user in the campus typically requires local administrative coordination and approval. The IT management usually needs to be involved e.g. in providing cross connects in the campus. Justifying the need and getting this approval may take some time and effort. An internal agreement regarding responsibilities and obligations may also be needed. Typical issues to be agreed on are e.g., rules of operation, the responding to security incidents and rules for connecting systems to the production and test network without providing a "back door".

The customer should have at least one technical contact person who has knowledge about single-mode fiber availability in customer premises and who can connect and operate the equipment. The person needs to have access to necessary equipment and cross connect rooms. This special person can also act as a named technical contact (see section "Contact information").

The customer performs performance tests to the connection when the connection is brought up or if modifications are made.

Testbed operator's actions

CSC will deliver connectivity service in Funet network as agreed with the customer. If new fiber connections are needed CSC will tender and order the connections. The usual needs emerge in the last mile fiber connections.

There will be a site meeting where details of the connection implementation are discussed with the customer. In the meeting a check list (in Finnish) is filled about things to be used. CSC will assign the necessary CWDM wavelength, provision DWDM channels and make routing configurations as needed.

CSC provides a bootable Linux live CD for network performance testing. The CD contains end-user friendly tools to check the features of the connection and a reporting function to send the results to CSC immediately when finished. It is also possible to consult the experts while testing and tune the systems jointly.

IP addresses

Funet assigns the required address space to the customer organization. If the organization 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. For security and legal reasons, source-address filtering is done at Funet router's customer interface using strict unicast RPF feasible paths mode. 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 indicate how many addresses are needed and for what purpose. The information is submitted 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. When practical, Funet can offer services that may help in this respect. Address block can be routed when reverse delegations are ready. When the testbed use and the connections are terminated the address space returns to CSC.

IP routing

The customer is required to have a router as a demarcation device unless a light path is used. Static routing is used unless there is a good justification otherwise. A BGP session may be provided based on need (e.g. study of BGP dynamics).

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 one person may have multiple roles. A technical centralized helpdesk type contact point ("NOC contact") can also be provided. An administrative contact should have authorization to most contractual matters related to the testbed. A technical contact should have the capabilities to perform operations in the own testbed hardware. A security contact should be authorized to handle and process security incident material.

Operating the local testbed network

This section covers the operational time frame of the testbed use and advises researchers in testing. Acceptable use policies are described, daily procedures, and best practises are referred to.

Acceptable user policy (AUP)

Funet AUP can be found from the CSC's public web pages: http://www.csc.fi/hallinto/funet/esittely/etiikka. The information is in Finnish.

The AUP recognises primarily the Finnish law with some examples. In addition, it raises some issues which can be regarded as unethical or unwanted behaviour. The following are examples of bad behaviour:

- the reservation and excessive use of the resources
- aggressive, intrusive and careless behaviour
- the neglect of network safety precautions

The conduct of the AUP depends on the nature of the test setup. If the testbed connectivity is implemented as a Routed IP connection the AUP is in effect. Special care should be taken and negotiations with the Funet NOC are recommended if excessive use of resources is expected. However, if light paths are used there is a lot more freedom because all communication is private. The security issues are discussed in a separate chapter (see section "Security issues").

Daily procedures

The researchers are expected to use the testbed safely and in good faith. No daily communication or reporting is needed to the Funet NOC. Only the operations directly affecting the physical testbed connections are suggested to be informed in advance for avoiding false alarms. The researchers can use and connect any equipment they want within the AUP.

Best practises

The information systems are growing increasingly complex. This means that the administration and configuration will also get more burdensome. Some work time lost in solving operational issues can be saved to research work with the use of best practise documents.

There exists plenty of material for easing the deployment and operations in Internet. The information contains both technical solutions and administrative guidance. The reliable sources are the standardization bodies, vendors and governmental agencies. A set of security references to further reading is collected under "Security issues" section. Examples of other documents include the BCP and Informational series of Internet Engineering Task Force (IETF) documents, available at http://www.rfc-editor.org/bcp-index.html.

Setting up services

Researchers can utilize the testbed for any subjects they want. In addition, there exist services supporting their work. If interested the researchers can also provide services to the project themselves.

Using existing testbed services

WP4 has collected existing testbed services that are available on the TestbedServices ICT SHOK Wiki page. The page is in open use 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. The services are meant to ease and speed up the researcher's deployments, as work duplication is avoided. In some cases the existing services can be combined with the researcher's own services.

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

Offering services

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 offerings.

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. In a special need it is recommended to contact the service provider and WP4. E.g. in some test scenarios the time zones may cause a collision with service hours.

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. The use case format explains clearly the problem faced, how it was unraveled and on which services the solution was based on.

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. It is recommended that a service would be available for the life span of the Future Internet SHOK project.

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 and disseminate if necessary. However, service provider should report to CSC if there has been interest in the service.

Next steps in services management

The WP4 long term vision is to move testbed-related activity to its own or a more widely available context. This would enable a smoother communication with those organisations that are not ICT SHOK FI programme partners, i.e. third parties like other SHOKs and Finnish development projects. Also the project specificity is wanted to be limited. The life cycle of services must be managed in the event that FI programme ends. The goal can be achieved with a content site where access can be granted to the interested third parties as well.

Network monitoring and reporting

This section covers the support information for the service period. The Funet NOC is presented and fault reporting procedures described.

Funet NOC operations

Funet Network Operations Center (NOC) duty officer is reachable by phone and email on working days from 8.30 to 16.00. Funet NOC uses network monitoring systems (NMS) to monitor the status of network services and customer connections. Funet NOC may also contact the customers directly 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. A typical target is located well within the network. 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. This is due their pure optical type. The improvements are being investigated with the transmission system vendor. Light path customers can run monitoring software in their own devices.

Availability

Network services are offered on a best effort basis. The basic connection has no redundancy and it 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.

The quality and availability are constantly being developed. Due to the end-to-end nature of the network quality measurement system the local area network problems constitute a part of the service breaks. However, the typical figures for the best 50 percent of the Funet network customers is at least 99.99% (a 2008 figure). This means there are hardly any noticeable breaks. The current measurement system is built for validating five nine availability (99.999).

Fault reporting

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

Security issues

The network security responsibilities and reporting methods are described in this chapter. Some advice and references to further information is given.

Responsibilities

Responsibility for the information security at the end site belongs to the researcher's home organization. The requirement of using information systems which are maintained according to best current practices and accepted standards (see references below) is remarkably important if the customer 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 the 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 sufficient filtering and anomaly detection capabilities of its own.

The customers 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. Reports are kept confidential by Funet CERT.

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, the 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 organization 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 customer 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 agreement 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. This general rule also applies in research context. One primary example of personally identifiable information are IP addresses. For example packet traces including IP addresses cannot be shared between research groups without due consideration.

Security reference materials

VAHTI - Finnish ministry of finance security guidelines (Finnish)
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