Tampereen teknillinen yliopisto. Tietoliikennetekniikan laitos.
Tutkimusraportti 2010:1
Tampere University of Technology. Department of Communications Engineering.
Research Report 2010:1

Karri Huhtanen, Jari Miettinen, Pekka Savola, Kaisa Haapala,
Matti Laipio & Markus Peuhkuri

# ICT SHOK Future Internet Testbed Architecture v2.0

ICT SHOK Future Internet Deliverable 4.1.1

TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

Tampereen teknillinen yliopisto. Tietoliikennetekniikan laitos. Tutkimusraportti 2010:1
Tampere University of Technology. Department of Communications Engineering.
Research Report 2010:1

Karri Huhtanen, Jari Miettinen, Pekka Savola, Kaisa Haapala, Matti Laipio & Markus Peuhkuri

# ICT SHOK Future Internet Testbed Architecture v2.0

ICT SHOK Future Internet Deliverable 4.1.1

Tampereen teknillinen yliopisto. Tietoliikennetekniikan laitos
Tampere 2010

ISBN 978-952-15-2387-8
ISSN 1459-4617

## Table of Contents

# 1. INTRODUCTION

This document is ICT SHOK Future Internet WP4 deliverable DA4.1.1, which describes the testbed architecture. This work was supported by TEKES as part of the Future Internet program of TIVIT (Finnish Strategic Centre for Science, Technology and Innovation in the field of ICT). More background and justification can be found in the Future Internet Research Agenda [FIResearchAgenda, page 19].

Most technologies and services that will form the future Internet do not yet exist or are not ready to be deployed on top of the Internet today. Some assume Internet takes an evolutionary path: the Internet will never be perfect and solutions must be developed to overcome these imperfections. Others assume a technology revolution. On top of these are the research and innovations concentrating in combining different communities, authentication federations and services into new innovative combinations. A future Internet testbed must support and encourage all of these approaches and especially the ideas and innovations, which are found by combining the developed technologies and services together.

To achieve this objective, ICT SHOK Future Internet testbed is divided to four architectural levels (Figure 1) each supporting a different kind of connectivity:

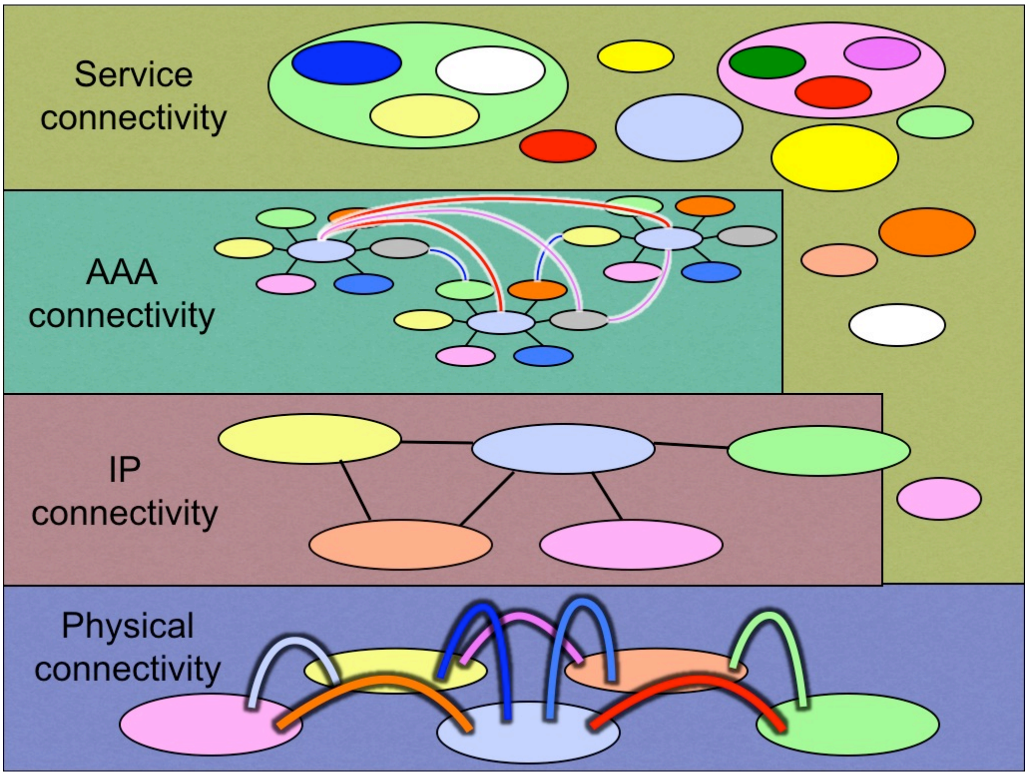

**Figure 1: ICT SHOK Future Internet Testbed Architecture**

The physical connectivity is for connecting organisations and services as well as research done below or instead of Internet Protocol (IP) connectivity. Examples of such research can be found within "next generation Ethernet" concepts and so-called Publish-Subscribe Internet Routing Paradigm [PSIRP]. The objective on this testbed level is to provide connectivity to the researchers that goes below the IP level, such as for example dark fiber backbone networks between various organisations.

The IP connectivity contains the research done to optimise and develop technologies and services to enhance and utilise IP connectivity. The technologies and services on this level include among others the optimisation of Internet routing tables, IPv6, non-firewalled connectivity, and utilisation of IP multicast and the connectivity enhancement technologies and services both in the imperfect Internet now and in the future. The objective of the testbed on this level is to provide both the ideal IP connectivity (which is not often available to the researchers) and when needed also imperfect real-world IP connectivity for testing the future Internet solutions and technologies.

The authentication, authorisation and accounting (AAA) connectivity level is based on the assumption that in the future Internet as it is already in the current Internet, there will not exist only one dominating identity provider or collaboration federation between multiple providers, but instead several different ones. Various different identity providers and federations create the need for "routing" (in this context meaning usually "database lookup") and connecting these services on the authentication level to enable authentication connectivity without the need for every service provider to make direct connections to all other identity service providers. The objective of the testbed on this level is to provide the opportunity to connect to some of the authentication federations and not to limit the utilisation of other existing ones.

The service connectivity level is perhaps the least developed level in the current Internet. In the current Internet there already exists physical connectivity in the form of light paths, IP connectivity with both IPv4 and IPv6 and authentication connectivity with OpenID, Google/Yahoo/Microsoft accounts, SAML, eduroam etc., but inter-service connectivity exists usually only within one service provider. Some of the service providers have started opening up and standardising their service interfaces for service interconnectivity, but more research and work is still needed for fully open and standardised inter-service connectivity. This is, however, from the perspective of testbed development, only part of the larger concept, where in the testbed connecting completely unrelated services and solutions should be possible for creating inter-connected combination services.

## 1.1. A high-level view of testbed potential

In the following, some illustrative examples are provided on research possibilities in the testbed; see later for longer description.

### 1.1.1. Physical connectivity

Point-to-point light paths

- Experimenting with different IP-versions, building custom routers, or other experiments that are not feasible with current IP-network
- Experiments with applications that require very high bandwidth and low jitter
- Applications that cannot be connected to the Internet due to security issues

- Use case examples include a CWDM ring in Oulu, Aalto University light paths, the physical setup of Aalto Comnet connection, and Metsahovi physical connection.

Multipoint light paths

- As with point-to-point light paths, but between more than two parties
- Possible to connect to TREX or other exchanges for extended outreach

### 1.1.2. IP connectivity

Routed IP connections:

- Test services that need to be reachable from various locations (when Funet connection is not there or cannot be used)
- Various tunneling solutions can also be used (e.g., multicast and IPv6 have been tunneled over a cellular network to an Internet tablet)

Outsourced research network / services:

- A number of players including some project partners are willing to provide testbed facilities and services.

Enhanced connectivity to mobile terminals, providing rich network access to virtual machines on user's desktop:

- Advanced connectivity to devices, hosts and networks anywhere, any time

### 1.1.3. AAA connectivity

Some examples include:

- RADIUS based roaming betweek community networks
- Peer-to-peer roaming with RadSec
- Policy-controlled integration between various identity provider federations.
- Integrating an organisation or a service provider to an existing identity federation.

### 1.1.4. Service connectivity

Service integration is the most open and flexible layer, some examples include:

- Mash-ups, "Web 2.0", service integration across service providers (e.g., Google Maps APIs).
- OpenVPN PurpleNet provisioning system with Shibboleth authentication

### 1.1.5. Collaboration

Collaboration activities is demonstrated for example with the following:

- OpenVPN connectivity suite: three different systems by three different programme participants but integrated and developed jointly
- Planet Lab experimental research systems in various testbed networks
- International light path connectivity options

## 1.2. Objectives/motivation

Physical connectivity is the basis on which higher layer connectivity services are built. The testbed has multiple options for physical connectivity so that economically and practically feasible solutions can be found for different kinds of needs. Because the goal is to have a low cost and simple solution, typically there is no redundant connectivity (e.g. in the event of fiber cut) to the end users. However, experience has shown that typically service-affecting critical problems are rare.

The testbed is a part of research infrastructure that enables long term pilot services deployment and development. New applications, concepts, and technologies can be tested and piloted that are not yet feasible in common Internet.

While the duration of individual tests may vary and be typically rather short, it is recognised that the need for a testbed connection is more permanent in nature. For example, research work aiming at a doctoral thesis takes at least three to four years.

From architectural point of view it is essential that physical connectivity infrastructure does not set strict limitations to the available bandwidth or protocols. Data intensive research can be carried out without affecting other traffic.

Tunneling can be used as a means to deliver all the features of a service over any network in between. However, the drawbacks of a tunnel cause performance degradation that can be easily demonstrated with e.g. IPTV, can't offer high bandwidth reliably or without impacting other traffic, and other limitations like lowering the MTU.

## 1.3. Implementation (tools and methods)

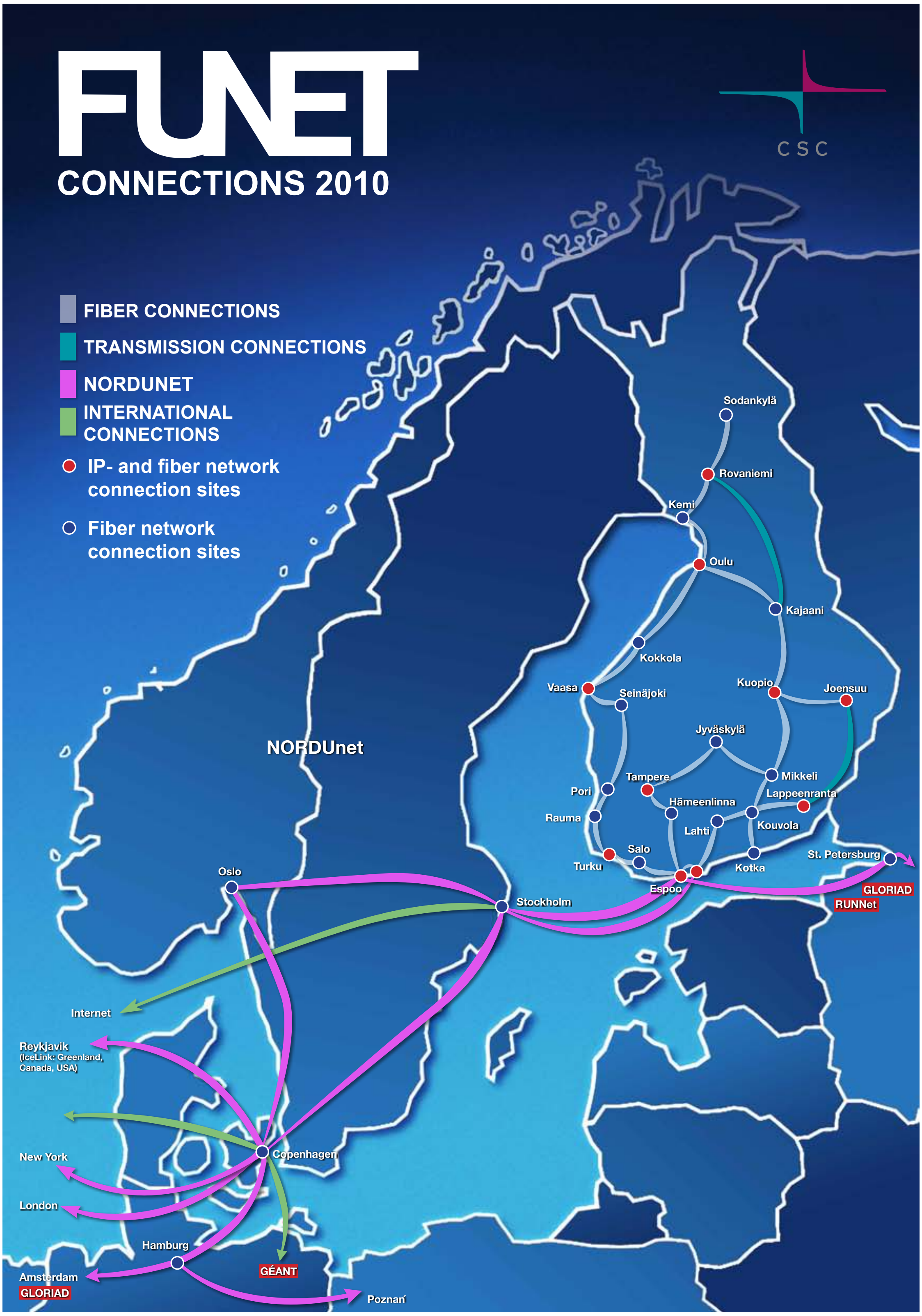

**Figure 2: Funet DWDM physical connectivity, May 2010**

Figure 2 shows the availability of light paths in May 2010.

### 1.3.1. Introduction to light paths

Light paths are OSI layer 1 or 2 connections between end sites. They are implemented in the test bed using Wavelength Division Multiplexing (WDM) technology. It has two variants, coarse (CWDM) and dense (DWDM). Because DWDM is finer grained than CWDM also finer tuned equipment is needed. While a CWDM system might be 2 rack units (10 cm) in height, a DWDM system might take a whole rack. The unit price and price per channel on DWDM system is also higher.

The setup allows the use of point-to-point and point-to-multipoint topologies in a geographically wide area. The end sites see each other as a member of the same local area network. In a typical usage case two or more research groups involved in a joint project interconnect, forming a private network.

The physical connectivity is based on fiber infrastructure where a single wavelength is transported through the system. In an ideal case no wavelength frequency change is needed. However, as the capabilities of the transmission systems are limited, few signal amplifications are performed. The light path constructing method minimizes the amount of devices in the path, which gives advantages in several ways such as maintainability, mean time between failures, fault analysis, and service independence.

The technical implementation enables the usage of non-standard framing. Thus the researchers are not limited to e.g. the use of traditional TCP/IP or Ethernet, but can explore completely new ways of communication.

The Funet light path service is gradually providing optical connectivity in Finland. The Funet DWDM network is interconnected to the Nordic NORDUnet DWDM network. This enables the scientists and researchers to achieve light path connectivity for research purposes very easily in the Nordic area. In addition, the European co-operation in the field of research and education network gives similar opportunities to the rest of the European countries, the United States and beyond.

### 1.3.2. Implementing light paths with passive CWDM

Passive CWDM devices are simple pure optical prisms. They combine typically eight different wavelengths in a single fiber pair. CWDM is a very cost-effective way to deploy WDM and it can often installed quickly in a matter of weeks as well. Typical installation is done so that a gigabit connection that previously ran on top of fiber is replaced with CWDM and multiple connections on the same fiber.

The passive nature of the CWDM limits the usage to metropolitan (often 20 km or less) or local area networks. In the longer links the signal degrades and becomes unusable. The end equipment are normally routers or switches which use so called colored optical transmission modules. Colored modules are widely available from most manufactures and other suppliers. Some vendors require optics modules to be their own brand and reject everything else. This may require replacing equipment, using "vendor-branded" 3rd party optics or using a media converter. Gigabit speed is regularly used. 10 Gigabit Ethernet optics with CWDM spacing have also recently become available. The pure optical approach allows any framing if wavelength is not altered.

The relatively low optical multiplication rate gives freedom in the quality of the fiber infrastructure. This means that also the older generation of the fiber infrastructure is usable, which may be a major asset in the campus environment.

From the operational perspective passive optics add an extra layer to the connection. This may cause fault scenarios, which are hard to debug and fix. Fortunately because the systems do not require electricity, failure rate is low. On the whole the deployment of a CWDM system does not remove the need to carefully plan, measure and implement the overall structure.

The testbed connections, which use CWDM, are either connected to the Funet DWDM backbone or the Funet IP service. In a metropolitan area a case of a direct path may also emerge.

The current CWDM equipment is a feasible and advisable tool, and it fits many purposes. The system can be built in relatively short delivery (week or two) and installation times (1 hour). On the other hand, the small amount of multiplied wavelengths is quickly used, which results in the need of a more complex WDM system or additional fiber pairs. However, the limited complexity of a eight wave system is an operative benefit, as the complexity remains at a reasonable level.

### 1.3.3. Implementing light paths with DWDM

DWDM technology is used in the testbed core to connect cities. There are two bands of 40 DWDM channels that are multiplexed to one fiber pair.

Client signal is usually connected to a transponder card on a DWDM system. Transponders are used to make wavelength conversion and power adjustment to be able to inject the signal to the multiplexed line. Wavelength conversion is done with OEO (optical-electrical-optical) regeneration so the transponder needs to support the line protocol. In line optical amplifiers are used to reach longer distances. The connections can be for example 600 kilometers without regeneration.

In principle any kind of optical signal can be injected in the DWDM network as long as it's on the correct wavelength and within allowed power range. A client that is connected directly to the line interface without a transponder is called "an alien wavelength". Too high optical power in one channel might disturb optical amplification.

Chromatic dispersion and polarisation mode dispersion (PMD) in the fiber limit the distances. Chromatic dispersion can usually be compensated but the PMD cannot. This sets strict requirements to the quality of the fibers.

Provisioning new DWDM light paths is relatively fast in a couple of days, if no equipment needs to be installed. Order and delivery of new equipment takes months. 1 Gbps and 10 Gps transponders are available and 40 Gbps is also possible.

### 1.3.4. Last mile

Setting up a light path requires optical fiber infrastructure end to end. Potential challenges are on the last mile from network edge towards the customer. The use of CWDM allows optimising the use of existing fiber infrastructure on the last mile. Even if the testbed connection uses the same fiber connection as production traffic they have entirely distinct channels with no interference.

Fiber availability may be limited in some areas due to lack of demand or competition. Regulation of dark fiber has recently started in some areas (e.g. local loops) but it typically only applies to service providers. Some commercial providers have policies to rather offer capacity services than dark fiber. A few also offer CWDM wavelengths. Delivery times may also be long, especially if delivery requires building (digging in) new fibers. Delivery times are often 3-4 months even if no new fiber is needed. The length of the contract period usually has an effect on pricing. For example a period of 60 months might have a reasonable price.

When fiber to the customer premises is available, it's still not obvious that inside cabling reaches the customer device. The number of single-mode (SM) fiber pairs is often limited. Inside cabling may also be multimode (MM), and using it requires a media converter; best would be to avoid having to use MM fiber completely. Optical characteristics and length of the fiber connections must be measured for link budget calculation. This is especially important if there is more than one CWDM hop on the path.

If the customers' edge device doesn't have an optical interface, a media converter is needed.

Wireless access to the testbed is implemented with access points connected to customer access networks.

## 1.4. Use cases

### 1.4.1. Comnet Connection

#### Introduction

CSC provided a Routed IP connection to Aalto University (Comnet). This was implemented using CWDM technology.

#### Problem

Comnet required a routed IP connection for their research network needs. There was existing fiber to Aalto University campus in Otaniemi. However, it was already used for another purpose. The new connection had to be established in a cost-effective and operationally robust manner.

#### Solution

Two CWDM mux/demux devices were installed at CSC and HUT. Devices consist of prisms and band pass filters. These require no electricity or maintenance, reducing the likelihood of downtime. Each can support up to 8 light paths (GE or 10GE) on a fiber pair. Existing fiber-pair was connected to CWDM muxes. New Comnet connection was added using a "coloured SFP" on both ends utilising 1590 nm CWDM wavelength. From Otakaari 1, an internal HUT fiber path was used to Comnet premises.

After Comnet installation, a number of other light paths have been added to the same devices.

The setup is depicted in the Figure 3.

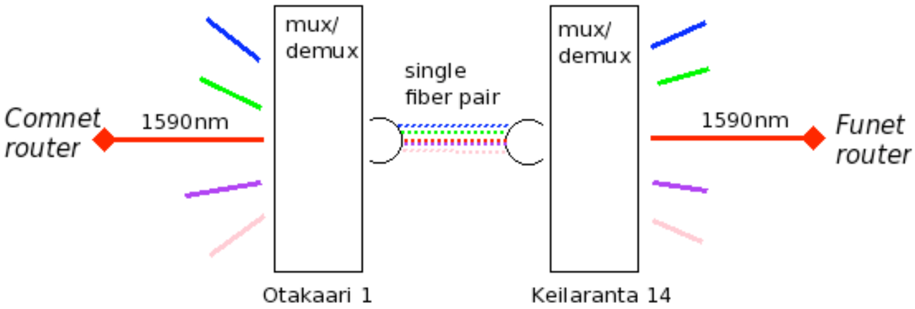

**Figure 3: Comnet connection setup**

### Requirements

Dark fiber availability or possibility to convert existing fiber connection to CWDM. A couple of units of rack space at each site for CWDM muxes. Coloured SFPs at each end.

- Utilised testbed services
- Dark fiber
- Light path service

## 1.4.2. Aalto lightpaths

### Introduction

CSC has provided light paths to Aalto University for connecting their internal network at seven locations across Finland. This was done using CWDM and DWDM technology. This is described as a use case to demonstrate the applicability also in the testbed context.

### Problem

HUT had a number of campuses, and the number grew with the foundation of Aalto University. Reliable and high capacity network was required between the sites. VPN technology was deemed insufficient, and IP routing would have required complicated IP re-addressing and high-end, expensive routers.

### Solution

Metro networks in Helsinki region were built primarily using CWDM technology. Longer spans were implemented using DWDM technology, and CWDM as applied in the last mile as needed. Major sites used multiple fibers and equipment so that the network would automatically recover in the face of a fiber cut of equipment failure. Backup paths were configured in DWDM system to be distinct from the primary paths for redundancy reasons. The setup is depicted in the Figure 4: Aalto lightpaths.

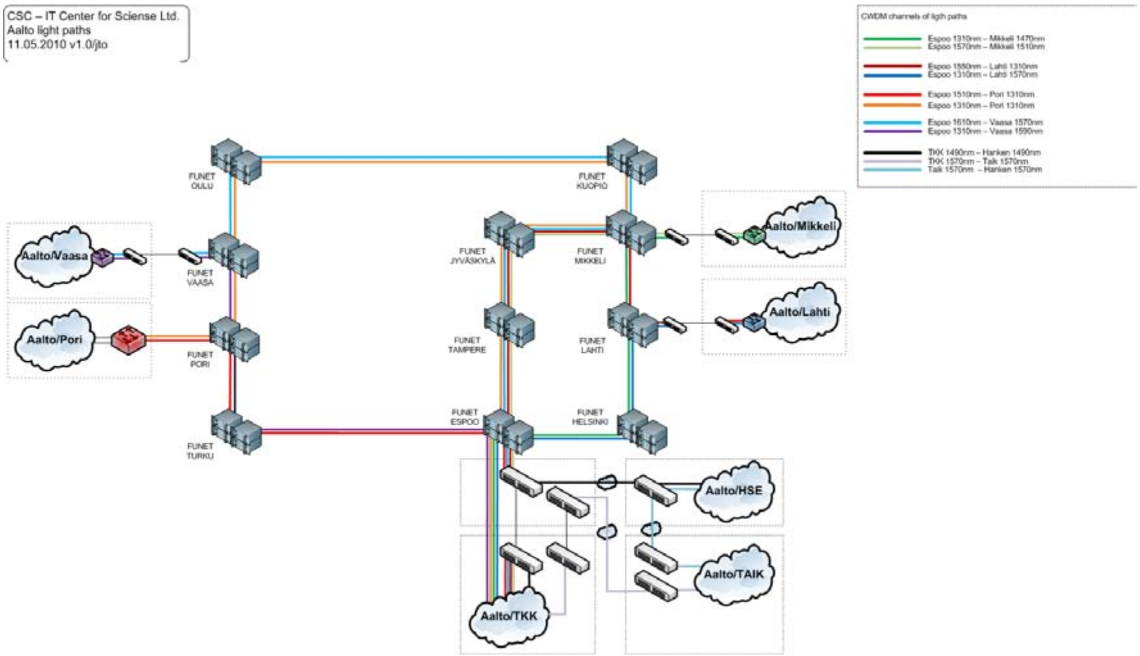
CSC – IT Center for Sciense Ltd.
Aalto light paths
11.05.2010 v1.0/jto
CWDM channels of ligth paths
Espoo 1310nm – Mikkeli 1470nm
Espoo 1570nm – Mikkeli 1510nm
Espoo 1550nm – Lahti 1310nm
Espoo 1310nm – Lahti 1570nm
Espoo 1510nm – Pori 1310nm
Espoo 1310nm – Pori 1310nm
Espoo 1610nm – Vaasa 1570nm
Espoo 1310nm – Vaasa 1590nm
TKK 1490nm – Hanken 1490nm
TKK 1570nm – Taik 1570nm
Taik 1570nm – Hanken 1570nm
FUNET OULU
FUNET KUOPIO
FUNET JYVÄSKYLÄ
FUNET MIKKELI
FUNET VAASA
FUNET TAMPERE
FUNET LAHTI
FUNET PORI
FUNET ESPOO
FUNET HELSINKI
FUNET TURKU
Aalto/Vaasa
Aalto/Pori
Aalto/Mikkeli
Aalto/Lahti
Aalto/HSE
Aalto/TAIK
Aalto/TKK

Figure 4: Aalto lightpaths

### Requirements

Dark fiber availability or possibility to convert existing fiber connection to CWDM. A couple of units of rack space at each site for CWDM muxes. DWDM availability at physical sites. Coloured SFPs at each end.

Utilised testbed services

- Dark fiber
- Light path service

## 1.4.3. Oulu CWDM Ring

### Introduction

CWDM technology allows multiple channels to be multiplexed into one fiber pair. Passive multiplexing is very cost efficient over short distances.

### Problem

Connectivity services were poorly available and rather expensive. Adequate capacity was not available at a reasonable price and commercial providers were reluctant to develop their products. Information of technical details was not available which made it difficult to assess the performance or reliability of the services.

### Solution

A CWDM ring was built in Oulu area. Ring topology was chosen so that redundant connections are possible when needed.

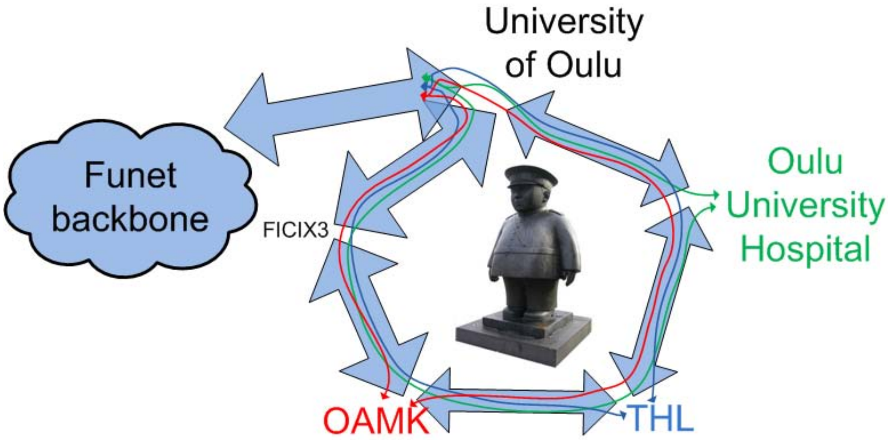

**Figure 5: Oulu CWDM ring**

The ring (Figure 5: Oulu CWDM ring) has five add-drop sites that are connected to each other with dark fiber. Two passive CWDM-mux/demux devices were installed per site one for each line direction. Each site is also equipped with a media converter chassis that is used for wavelength conversion and regeneration when necessary. The ring covers all Funet members in Oulu area.

### Requirements

Dark fiber availability via two separate physical routes to all relevant locations is required. Also a couple of units of rack space at each site and electricity for the media converters is requires.

### Utilised testbed services

- Dark fiber connection.

## 1.4.4. Metsähovi Radio Observatory

### Introduction

Metsähovi radio observatory is an institute of Aalto university with premises in Kirkkonummi, approximately 35 kilometers from the main campus. The scientific work at the observatory, e.g. VLBI research requires powerful communicatations capabilities to sister observatories. The communication is used for real time tuning and directing the telescopes in real time for simultaneous measurements.

The observatory is an example of a research instrument that uses a data communication network to process results in a significantly more efficient way. More information is at the following CSC press releases and publications:

- Metsähovi connected with 10 Gbps [Metsähovi2006]
- Funet network rate more than 8 Gbps - MetsähoviRadio Observatory sets world record [Metsähovi2008]

### Problem

The observatory site is located far from the main campus with limited infrastructure and settlement. This is a planned situation due the requirement to limit the radio noise in the millimeter and microwave band. The fiber distance is also considerable for affordable optical equipment.

### Solution

A fiber optical link was built between the Metsähovi site and the Aalto campus at the Otaniemi. Part of the link utilised leased connections in the existing network but the last mile required digging a new cable. The site was connected to the Funet access routers. High power long range optics modules were deployed to nullify the need for in between amplifiers.

### Requirements

Dark fiber availability near the end site and either dark fiber or light path capacity is required. Optical transmission equipment is pocket sized but needs a proper installation for reliable service.

### Utilised testbed services

- dark fiber connection, a CWDM connection or a light path
- the testbed connectivity

# 2. IP CONNECTIVITY

## 2.1. Objectives/motivation

Currently most of the Internet services are developed and built on top of IP connectivity. These services as well as IP connectivity will still be part of the future Internet. The IP connectivity today is less than ideal and varies vastly by each implementation. Several levels of firewalls, network address translations (NAT), lossy, congested and, in essence, barely working best effort networks bring old and new challenges for services and applications running on top of them. IPv4/IPv6 transition brings also new challenges.

On the IP layer, the future Internet testbed must both the research for ideal solutions and the research for solutions overcoming the limitations and imperfections of the current Internet. The testbed must also provide means for researchers and research organisations to easily gain access to the IP networks, which represent both the actual Internet connectivity today and the ideal or non-ideal connectivity in the future. To realise this, we must develop testbed services for delivering this connectivity as a service, between networks and to the desktop of a single researcher.

## 2.2. Implementation (tools and methods)

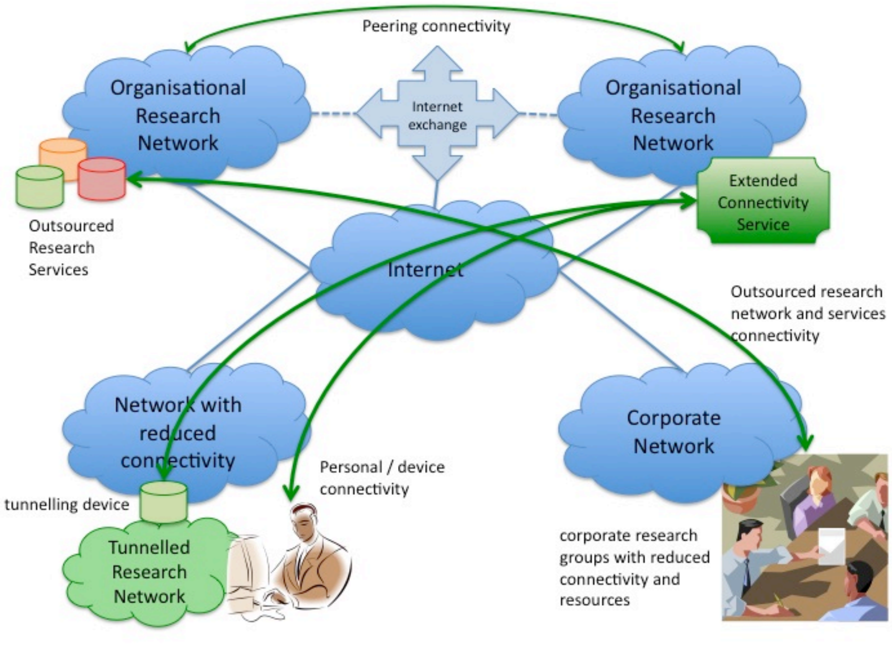
Peering connectivity
Organisational Research Network
Internet exchange
Organisational Research Network
Extended Connectivity Service
Outsourced Research Services
Internet
Outsourced research network and services connectivity
Network with reduced connectivity
Corporate Network
Personal / device connectivity
tunnelling device
Tunnelled Research Network
corporate research groups with reduced connectivity and resources

**Figure 6: ICT SHOK Future Internet Testbed IP Connectivity Architecture**

To cover the testbed IP connectivity requirements the testbed IP connectivity architecture (Figure 6) must be divided to the following kinds of IP connectivity:

- Regular IP connectivity
- Peering connectivity
- Outsourced research network and services connectivity
- Extended connectivity via connectivity clients and devices

### 2.2.1. Regular IP connectivity

The regular IP connectivity is the connectivity provided to the organisation by the service providers. It usually includes at least IPv4 connectivity and when service provider's network is advanced enough, also IPv6 and multicast connectivity. The regular IP connectivity may include Internet transit or peering but with the distinction that both are production level services without opportunity for peering or transit related research.

The regular IP connectivity is available from the commercial Internet service providers or from research network service providers such as CSC/Funet (see Use Case: Routed IP connection)

### 2.2.2. Peering connectivity

Peering connectivity is the connectivity provided by research oriented Internet exchange points, which often includes the opportunities for Internet peering, transit and routing protocol research. Often these kinds of Internet exchanges can also provide physical level interconnections in the form of switched virtual LANs.

Peering connectivity can also be defined as a research access to full Internet routing tables and private peering with other organisations. In these kinds of use cases also research network service providers may provide access to full Internet routing tables and private peering arrangements.

### 2.2.3. Outsourced research network and service connectivity

Often corporate and organisational networks are designed, segmented and optimised only for the production or business application use. Researching, developing and in production testing new networking technologies and services is usually not recommended and may even be forbidden. This creates a need for separate research networks. Creating separate research networks however requires resources and corporate or organisational policy development, which can sometimes take more time and resources than is currently available. Local network administration is often also overworked, not being able to address other than the most critical production needs.

Outsourcing the research network and the researched services may then provide a cost efficient opportunity to conduct networking research and partner with other research organisations. Usually these kind of outsourced research network services are offered in research cooperation projects between research organisations (such as TUT and HIIT) and corporate research partners. Completely outsourced research networks and services i.e. without research cooperation projects are not usually available.

This kind of connectivity provides opportunity for companies regardless of their size to gain access to the research organisations' network resources and partner in developing new network technologies. In ICT SHOK Future Internet Testbed at least Tampere University of Technology (see use case: Outsourced research network and service connectivity) and Helsinki Institute of Information Technology offer outsourced research network services for programme participants.

### 2.2.4. Extended connectivity via tunneling

Providing connectivity and technologies beyond the resources, capabilities and competencies of organisations' IT support may often be difficult to achieve. To make it easier for both the researchers and their employers, the architecture for extending ICT SHOK Future Internet testbed to mobile terminals, research workstations and organisation research networks was defined.

The extended connectivity can be achieved with three different options.

The first one is to have a connectivity client pre-installed in the terminal and utilise it to connect to the connectivity services residing within some organisation's research network. This option provides the device connectivity presented in Figure 6.

The second one is to utilise a virtual machine image on the researcher workstation. The virtual machine is configured to build a connection to the research network of the organisation providing the connectivity services, thus making it possible to have a sandboxed research network environment straight on the researcher's fixed or mobile desktop (Figure 6, personal connectivity).

The third option is aimed for tunneling a segment of a research network between organisations and can be realised by either setting up regular tunneling or utilising a specifically designed tunneling device designed and implemented by Helsinki University and Helsinki Institute of Information.

With these three options ICT SHOK Future Internet testbed is able to provide both layer 2 (below IP level) and layer 3 (IP level) research network connectivity even to networks and researchers otherwise incapable of utilising ICT SHOK Future Internet testbed networks and services.

The first implementations of these three options utilise OpenVPN [OpenVPN] for creating the network funnels. If the three option model and architecture proves to be efficient, the extended connectivity options may be expanded to cover for example IPSEC [RFC4301] and HIP [RFC4423]. Programme participants are welcome to contribute to both the extended connectivity solutions as well as to the open source project developing OpenVPN based extended connectivity architecture (e.g. [PurpleNet], [OpenVPNVirtual].

# 2.3. Use cases

## 2.3.1. Outsourcing the research network services

### Introduction

When own organisation or service provider's capabilities and services start to limit research opportunities there might be a time to consider outsourcing the research network or services to a research partner.

### Problem

The larger the organisation, the harder it is to deploy new network technologies and services for research purposes in the organisation network. Deploying research services, which require extensive amount of bandwidth or new network technologies such as native IPv6, is even more difficult because the organisations or service providers and their equipment may not support the technologies or have enough capacity with reasonable costs.

### Solution

Tampere University of Technology solved these limitations by creating a TUT Research Network concept [TUTRDNet], which enables the departments to conduct their networking research flexibly and cooperate efficiently with external research partners. During ICT SHOK Future Internet program, similar research networks have been deployed in Aalto University and Helsinki Institute of Information Technology. With the help of these kinds of research networks the research partners gain access to the newest IP technologies and university-grade capacity and reliability in the network connections provided by CSC/Funet. Services can also be deployed easily on virtual hosts which run on VMWare virtualisation software.

### Requirements

Utilising research network resousrcs requires a research or cooperation contract with the service providing organization.

### Utilised testbed services

- TUT Research Network Service(s)
- Spidernet (Jyväskylä Polytechnic) [SpiderNet]
- Aalto Comnet research network
- HIIT research network

## 2.3.2. Routed IP connection

### Introduction

A routed IP connection allows all IP-routed testbed members to connect to each other and to the rest of Funet network. Funet is connected to four internet exchange points in Finland and to the Internet and Geant via NORDUnet. Implemented examples of this are Aalto University Comnet and University of Helsinki/HIIT connections.

### Problem

The current Internet service providers concentrate mainly to provide already field-tested Internet connections with clearly defined business cases. This usually means that the technologies utilised are, from viewpoint of Internet research, old and sometimes even obsolete. The lack of service providers providing state-of-the-art network technologies and connections for research purposes creates a need for separate research network providers such as for example CSC/Funet.

### Solution

A connection to Funet router network is typically a Gigabit Ethernet interface that is connected to a Funet router. The network is reliable and has sufficient bandwidth also for somewhat demanding needs. Native IPv6 connectivity and multicast are available.

### Requirements

A contract between the customer and CSC is required. The customer network needs to have sufficient firewall filtering capabilities and an interface to be connected.

### Utilised testbed services

- Dark fiber connection, a CWDM channel, or light path

## 2.3.3. Enhanced connectivity for mobile terminals

### Introduction

With the help of the testbed OpenVPN connectivity services mobile terminals can gain enhanced two-way connectivity even if the access networks between the terminals do not support all the technologies used.

### Problem

Especially in cellular access networks the mobile terminals can normally use only the network technologies available from the service provider and only make terminal initiated connection to the Internet. This makes it difficult to research new network services, which the terminals would be capable of utilising, but which the service provider does not yet support. Also researching the services provided by a terminal to the Internet or other terminals is difficult as service providers' firewalls generally prevent connections from Internet to the terminal.

### Solution

In Tampere University of Technology we have utilised OpenVPN to provide enhanced dual-way Internet connectivity to Maemo-based Internet tablets regardless of the access network used. With the help of tunnelling the terminals are capable of utilising technologies such as IPv6 and multicast even in cellular networks. The terminals are also capable of providing terminal based services such as content sharing via mobile WWW servers. This enhanced connectivity was possible by running an OpenVPN server in TUT Research Network and OpenVPN clients in terminals.

### Requirements

Terminal must be capable of running OpenVPN client to utilise the service.

### Utilised testbed services

- OpenVPN Connectivity Service
- TUT Research Network

## 2.3.4. Providing advanced network access to virtual machines on user's desktop

### Introduction

VPN for virtual machines allows rich networking to machines local to user even if local network infrastructure does not support advanced networking. From user desktop a VPN tunnel is created and this tunnel has other end in research network supporting advanced networking features.

### Problem

Research topics may require network access that is not possible within local network because of network policy or because some networking technologies (like IPv6 or multicast) is not implemented. Although some research tasks could be run in remote machines, this is not a good solution for task related to video and other media.

By running a test environment in virtualised computer without access to local network it is possible to test experimental applications and services without putting security of campus network into risk.

This would provide possibilities to study advanced networking in student projects. In a typical home ADSL or cable modem access the service is just basic IPv4 without multicast and some services limited. If students are provided with access to research network, they would have a possibility to study advanced networking.

## Solution

The solution will have three components:

- Virtual machine and OpenVPN software installed into desktop computer
- OpenVPN server at research network
- User authentication and certificate distribution server

For the researcher ("user") desktop computer a virtualisation software and OpenVPN client is installed. This can be done by support personnel, if required by organisation policy. The user logs into authentication server using Haka federated authentication and can download OpenVPN configuration files and certificate.

Using certificate provided, user can create OpenVPN connection to a OpenVPN server at resesarch networks and have provide her virtual machine a research network access.

It is possible that there exists multiple gateways in different networks, which will make possible for a user to study e.g. multihoming.

There may be multiple user authentication servers or then one using federated authentication. The user needs to authenticate only once to get certificate. The lifetime of certificate is limited (6 months for students, a year for researchers). The certificate can be put on blacklist if terms of service in research network is violated.

## Requirements

User must be member of HAKA federation unless separate authentication (based on local or radius accounts) is established.

## Utilised testbed services

- OpenVPN Connectivity Suite
- Haka federation [Haka]
- (PurpleNet OpenVPN management software) [PurpleNet]

# 3. AAA CONNECTIVITY

## 3.1. Objectives/motivation

Extending physical and IP connectivity are not the only ways to expand both the impact and coverage of ICT SHOK Future Internet testbed. Already, several other organisations and communities provide networks and services to their own members as well as to their visitors and partners. By introducing and implementing AAA (Authentication, Authorization, Accounting) connectivity architecture, the testbed impact and coverage can be expanded via AAA interconnectivity to, for example, other testbeds, network communities, community and municipal networks etc.

## 3.2. Implementation (tools and methods)

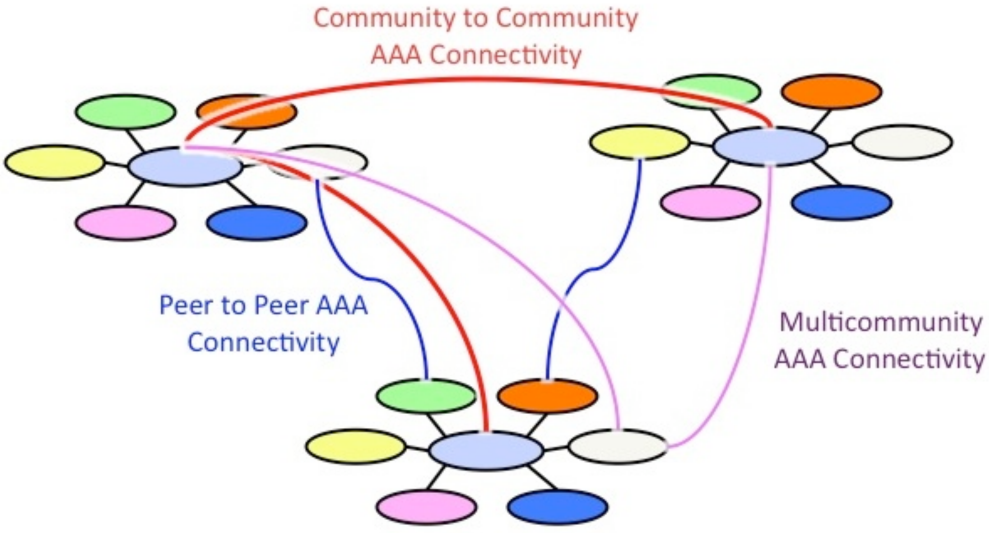

**Figure 7: AAA Connectivity Architecture**

In defining the AAA connectivity architecture for ICT SHOK Future Internet, at least the following three variations to implement the interconnectivity should be considered.

The first variation is the currently most common one. A community-to-community AAA Connectivity presented in the Figure 7 with red lines. This variation assumes that the communities are formed hierarchically and without overlapping members belonging to several communities at once. In this variation the community interconnections also form a hierarchy without multiple authentication paths between communities and community members. The most common examples of these kind of communities are the RADIUS protocol based WiFi community networks and federations such as current eduroam [eduroam], Fon [Fon], Funet WLAN roaming [FunetRoaming], Haka federation [Haka], Kalmar confederation [Kalmar], Sparknet [Sparknet], Wippies [Wippies] and Wireless Tampere [WirelessTampere].

The community member requirements for connecting simultaneously to more than one community and having this way multiple authentication routes leads to the second variation of AAA connectivity. This is presented in the Figure 7 with the organisation connecting to two different communities (the violet lines). Also the communities may connect to each other in a way, which also requires handling, selection and prioritisation of multiple authentication routes. Example of this approach are the selection of the federation to be utilised in the Shibboleth [Shibboleth] authentication and the realm lists used in organisations belonging both to the Funet WLAN roaming and Wireless Tampere community networks. While some of the issues can be solved by applying Internet routing solutions also to the authentication routing, this kind of of AAA interconnectivity offers still an area for additional research both in ICT SHOK programme and in general.

The third variation is approaching the solution for multicommunity interconnectivity from the decentralised perspective. The peer-to-peer AAA Connectivity is based on the assumption that AAA interconnections can be made dynamically between communities and organisations utilising technologies such as DNS service discovery and X.509 certificate infrastructure for finding and securing ad hoc authentication connection points. This kind of peer-to-peer AAA connectivity has been mentioned as a use case for DIAMETER [RFC3588] protocol, but also solutions utilising RADIUS [RFC2865] and DNSSEC [RFC4641] have been proposed. The success and utilisation of peer-to-peer AAA connectivity model would eliminate some of the problems in multicommunity AAA connectivity and enhance reliability by removing the need for centralisation from the architecture.

All the technologies mentioned (DIAMETER, RADIUS, SAML2 [SAML2], Shibboleth) can already be utilised within and interconnecting with ICT SHOK Future Internet testbed. For network level interconnections technologies such as RADIUS roaming and optionally Diameter are recommended, while Shibboleth and SAML2 can handle the application level authentication interconnectivity and federations. Already with these technologies, the authentication interconnectivity can be extended from WiFi networks to operator cellular networks and even over the Internet with Shibboleth/SAML2 handling the single sign on for services.

# 3.3. Use cases

## 3.3.1. RADIUS based roaming between community networks

### Introduction

Via Funet WLAN roaming service, ICT SHOK Future Internet Testbed now connects not only research and education organisations but also companies, consumers and other members of community networks such as SaiNet, Sparknet and Wireless Tampere. The members of these community networks are now able to utilise the combined coverage of all these community networks combined to the coverage provided by research and education organisations around Finland.

### Problem

Often community and other Wi-Fi networks are their own islands with their own access control and user databases. The users are typically restricted to utilise their credentials within the same community network without the ability to roam to other networks at least without additional costs. This can lead to a situation where community network service providers try to expand their coverage even on areas, where there might be already existing coverage provided by another service provider. Deploying several independent Wi-Fi networks on top of each other creates interference and reduces the quality of the already existing networks. A cooperation model is needed for community networks to extend their coverage cooperatively.

### Solution

By utilising RADIUS based roaming infrastructure, such as Funet WLAN roaming, these community networks can be connected to provide collaborative coverage instead of each community service provider building their own one on top of each other. In ICT SHOK Future Internet Testbed this has been already demonstrated by joining Funet WLAN Roaming, SaiNet, Sparknet and Wireless Tampere federations and community networks with a common RADIUS roaming root service [Cooperation]. Funet WLAN roaming also supports new RadSec based roaming [RadSecRoaming].

### Requirements

- RADIUS server and its configuration, VPN tunnel connections if needed
- In EAP authentication, a routable outer EAP identity
- Roaming agreement to join/utilise the Funet WLAN roaming community
- Wi-Fi guest or community network to be shared with other participants

### Utilised testbed services

- Funet WLAN Roaming Service

### 3.3.2. Peer-to-peer roaming with RadSec

#### Introduction

Current roaming models between service providers are based on the fixed hierarchical RADIUS connections and the routing of authentication messages is based on a certain prefix or suffix (usually called realm or domain) added before or after the username. A peer-to-peer roaming is a new distributed architecture where roaming participants can create the roaming connections between authenticating servers dynamically without the need for fixed connections or hierarchies.

#### Problem

A hierarchical model requires fixed configuration of roaming connections, which makes it inflexible for ad hoc connections. This also creates challenges in ensuring that the hierarchy's functionality is ensured and single points of failure are avoided. RADIUS as a authentication protocol does not yet in itself support encryption of the authentication data or verification of the authentication server validity with anything other than pre-shared secrets making the protocol insufficient for dynamic authentication connections. DIAMETER already has some of these already defined, but is not widely supported in network access control devices.

#### Solution

A peer-to-peer roaming architecture utilising DNS for authentication server discovery [P2PRadSec], TLS for traffic encryption and certificates for server validation can be utilised. This can be used either to provide hybrid architecture supporting both hierarchical and peer-to-peer-roaming [RadSecRoaming] or in the future completely replace hierarchical roaming. Similar architecture models have been already validated in implementing other distributed communication architectures such as XMPP [XMPP] based instant messaging and Google Wave [GoogleWave]. With the help of DNS discovery based peer-to-peer roaming architecture it is possible to enable organisations and companies build free form identity federations dynamically without the need for single coordination points or authentication server hierarchies.

#### Requirements

- RadSec server, a free open source implementation called radsecproxy [RadSecProxy] can be used for this
- A DNS server or ability to modify necessary records (A, SRV and NAPTR)
- Test or existing certificates from roaming service provider
- RADIUS server and its configuration. RADIUS and RadSec server can be combined.
- In EAP authentication, a routable outer EAP identity
- Roaming agreement to join/utilise the Funet WLAN roaming community
- Wi-Fi guest or community network to be shared with other participants

#### Utilised testbed services

- Funet WLAN Roaming Service

## 3.3.3. Mobile authentication in access networks

### Introduction

With the help of Funet WLAN roaming / eduroam(tm) hierarchy, the area for multimode terminal related mobility and authentication research can be extended to include eduroam(tm) and Funet WLAN roaming community networks in several universities around Finland.

### Problem

Modern cellular terminals have the ability to utilise both WiFi and cellular networks for data connections. However the automatic authentication to password protected WiFi networks has been a problem since it usually requires user interaction. Also Most WiFi networks do not have roaming agreements or even a common roaming root server to make it possible to utilise home organisation credentials wherever the user connects to the network.

### Solution

Funet WLAN roaming / eduroam(tm) hierarchy makes it possible for external participants to join as an organisation to the WiFi roaming community and utilise both WWW and WPA/WPA2-authenticated WiFi networks in several cities around Finland. The choice of mobile authentication method (such as EAP-SIM, EAP-AKA, EAP-TLS) is not limited as long as the authentication can be routed through hierarchy to home organisation's RADIUS server. By joining the Funet WLAN roaming federation, an organisation can now utilise WiFi networks in various universities and education organisations around the Finland to do mobility related research in cooperation with any of the participating research institutions.

### Requirements

- RADIUS server and its configuration, VPN tunnel connections if needed
- in EAP authentication, a routable outer EAP identity
- research agreement to join/utilise the Funet WLAN roaming community

### Utilised testbed services

- Funet WLAN Roaming Service

## 3.3.4. Web service authentication utilising Haka federation

### Introduction

User authentication can be a tedious process. Casual users usually aren't very interested in creating a new user account for new services. In case the user is already identified by a trusted organization, this user authentication can be used to authorize users. Haka identity federation includes most higher education students, researchers, and other staff could be used to provide research-related services to this user base.

An example usage is a WWW interface for university libraries, which all students can use. There are numerous other examples on Haka federation pages.

### Problem

User authentication and managing user accounts is difficult. Users don't want to sign up, but if the service is such that completely anonymous access is unacceptable, some authentication is necessary.

### Solution

Join Haka identity federation as a service provider to get user authentication and authorization without having to deal with signups, account management, etc.

### Requirements

- if you're already a Haka member, just deploy the service provider software to enable service.
- if not, sign up with Haka first.

### Utilised testbed services

- Haka Authentication Service

# 4. SERVICE CONNECTIVITY

## 4.1. Objectives/motivation

Increasing the number of Internet innovations are currently found by connecting technologies and services together, instead of building completely new services and technologies from scratch. To encourage trial, experimentation and research of this kind of service connectivity, the testbed must provide ways to find out the new services and technologies already available for use. These technologies and services must also be developed in a way they can be easily and openly connected, which means that the services and technologies must have open interfaces for inter-service communication.

## 4.2. Implementation

The testbed services index and use cases both present and demonstrate actual and potential use cases for combination of the testbed services. Every programme participant is encouraged to write and publish a service description and a use case on the testbed wiki pages about a service or technology they are willing to offer for the other participants. This way it is possible to easily find, connect and cooperate with partners working on complementing technologies and services, without wasting research resources in developing, for example, needed infrastructure services from the ground up.

In actual service creation and research combining services and technologies can be encouraged by ensuring that the used and developed technologies and interfaces are interoperable and preferably open for integration with other services. The current Internet with open interfaces and an increasing number of service mashups proved this approach to be useful in finding completely new kind of services and technologies just by combining existing ones.

## 4.3. Use cases

### 4.3.1. PurpleNet user management with Shibboleth

**Introduction**

PurpleNet [PurpleNet] is a web user interface for OpenVPN tunneling servers aimed to make it easier to control, manage, deploy OpenVPN based connectivity services to the end users and devices. This kind of connectivity services can be utilised, for example, to provide secure VPN connectivity as well as in general providing better access and connectivity to the network services offered by the service provider.

**Problem**

Web service user account provisioning and management varies from one organization to other. Some use user synchronization scripts, some SQL databases, some LDAP directory servers, and some have deployed Single-Sign-On services. Often web services decide to implement one or only few of the methods to make the scalable intergration to existing user database possible. In the PurpleNet development TUT had very limited resources so a novel solution utilising testbed authentication services was selected.

### Solution

The PurpleNet user and role management was solved by implementing support for Shibboleth authentication and authorisation more commonly used in Haka federation. With Shibboleth the user and corresponding role information was easily accessible and made it possible to integrate the PurpleNet directly to the existing authentication and authorisation database.

### Requirements

- Working Shibboleth deployment in a organisation
- PurpleNet

### Utilised testbed services

- Shibboleth
- Haka federation

# 5. COLLABORATION

## 5.1. Objectives/Motivation

ICT SHOK Future Internet WP4 coordination and collaboration activities exist to provide contacts between project partners and providing leads to other national or international contacts. The work aims to find practical partnerships between researchers and different research groups. Open participation and communication is seen as a tool to get better results to all.

SHOKs are aiming to create new service prototypes, which should be refined to near production quality. At best this can be done together which will be make development more cost-efficient. The testbed platform provides a means to perform almost any field trial possible as well as concept tests. A wider view to the development gives room for service innovations through combining services and frameworks, which can result e.g. in federated interconnected applications.

## 5.2. Implementation

The basic form of co-operation is investigation and testing of a shared research topic. Eventually all testing will result in field phase where some shared connectivity is an advantage in most cases. The partners can be found naturally in the work packages but the program contains a means to find interested parties in an independent fashion. In addition, some special topics are highlighted as official cross-issues. The cross-issues provide an easy path for interaction.

The project administration acts as the formal communication channel. This is complemented by coordination services, which aim for better information dissemination. The focus is inside the program but also external dissemination is performed according to joint policies.

Testing and provisioning facilitation is performed using multiple methods. Contacting and exploitation of the resources have been made easy. Among others, a testbed contact person has been named. A project internal newsletter is published monthly, which include test partner calls and recent results. The accumulated information is stored in a cohesive manner and it is available for all program members. The bilateral discussion and correspondence is done with interested parties. The program test needs have also been mapped with a survey.

Future Internal SHOK external outreach has been concentrated to demonstration activities at Tivit SHOK events. On the international level the goals and achievements of Future Internet SHOK have been presented e.g. the NORDUnet 2009 and Terena 2010 networking conferences. Some articles have also been published for general audience.

The practical work in coordination and collaboration consist of finding the active parties, providing support in practical issues and finally delivering the requested testbed services. Maturing ideas from early phases to results may take a considerable time and it is heavily dependent on the existence of compatible activities and research agenda. Making time tables fit is also a concern, as some requests may be long-lasting to carry out.

# 5.3. Use cases

## 5.3.1. OpenVPN Connectivity Suite

### Introduction

Creating the extended connectivity to testbed via tunneling (Section 2.2.4) required coordinated effort to define, design and implement a suite of connectivity solutions to cover the use cases ranging from single researcher to whole organisations requiring access to network services. This suite was put together under coordination of Tampere University of Technology (TUT) by TUT, Aalto University, Helsinki Institute of Information Technology (HIIT). The OpenVPN Suite consisted of PurpleNet [PurpleNet] OpenVPN provisioning and management software by TUT, OpenVPN virtual Image [OpenVPNVirtual] and OpenVPN gateway device by HIIT.

### Problem

Combining a suite of software from completely separate software or developing solutions to single use cases leads usually to interoperability issues or developing overlapping solutions for example for configuration/user management and provisioning. Also when single use cases are used to define solutions, these kind of solutions usually only fit to specific problems making them hard to use it in a more general environment.

### Solution

The development effort for creating the OpenVPN connectivity suite was distributed based on interests and resources available from TUT, Aalto University and HIIT. The components were developed invidually, but coordination  and collaboration between organisations ensured that connecting and interoperating between components was taken into account during design and development.

### Requirements

- a joint interest
- coordination and development resources
- will to cooperate

### Utilised testbed services

- Coordination
- Collaboration
- Wiki

## 5.3.2. Planet Lab in Finland

### Introduction

PlanetLab [PlanetLab] is a widely spread collaboration network which aims to support the development of new network services. The organizations interested to join the activity are expected to sign a consortium agreement. Technically the partners are expected to host two or more servers for the collaboration network, which is shared with others. Users can be authorized by their home organization to run their own programs in the server network. This enables them to test e.g. server-client type of applications in a planetary scale.

The known PlanetLab consortium members are Aalto University (COMNET and HIIT) and Tampere University of Technology. All are active in Future Internet SHOK WP4.

### Problem

The PlanetLab server is by definition used by other partners, which may be from e.g. foreign academic or commercial organizations. This may be a hard requirement if the home organization local area network doesn't support alien services by design or policies. The server needs a safe access method for both home organization and partner users.

The highly experimental nature of the PlanetLab usage requires non-firewalled access to common networks or academic internet. If this is not supported some of the testing is effectively banned and this is why the filtering is prohibited in the PlanetLab hosting requirements. A valid IP address is also required with full forward and reverse DNS service.

### Requirements

Routed IP connection to a router or a research network. As means to implement routed IP connection, dark fiber availability or possibility to convert existing fiber connection to CWDM is preferable.

### Utilised testbed services

- Funet Routed IP connection
- Funet Light path service (optional)
- testbed coordination

## 5.3.3. International light path connectivity

### Introduction

Some ideas for Future Internet development require non-IP based experimentation. Destructive or unexpected behavior of the components may also produce harmful effects to other users in existing shared networks. In some occasions the requirements are high for minimum interference to the measurement results. There also exist applications or intended usage scenarios where all the available resources in the communication system are exploited. In any of these cases it may be justified to deploy optically separated test network, which is built on top of light paths.

Academic research networks have built optical capacity since early 2000. In early 2010 the early trials have matured in an optical service, which has spread to all major continents. The most comprehensive connectivity is available in the U.S. and Europe. In the Nordic countries NORDUnet, the joint Nordic research backbone, is providing the service. CSC provides access to the international light paths in Finland.

### Problem

An example from data-intensive research: two research laboratories are located in different countries. They are willing to create a joint research environment, which contains massive data transfers. The current external network connections are not suitable as they limit the usage intentions and patterns considerably.

Help is needed for setting up the connectivity and finding possible other interested parties.

### Solution

The Finnish party contacts the coordination service. The practical details are surveyed and an implementation plan is delivered for examination. If accepted the coordination service initiates the construction of the private optical channel, the light path.

A light path is configured between the nearest optical points of presence (PoP) of both national research and education networks. The last mile fibers are either leased or built. Compatible transmission optics are installed to the both ends. The connection is wired into desired devices.

A small survey is performed to find known parties with similar setups and it is delivered if permitted.

The connected organizations need to agree mutually on the use, policies and fees concerning the arrangement. The similar setup can also be built between multiple sites or for working over multiple light paths.

### Requirements

Dark fiber availability or possibility to convert existing fiber connection to CWDM is required.

### Utilised testbed services

- Funet Light path service
- testbed coordination

# 6. SUMMARY

ICT SHOK Future Internet Testbed is a collaborative concept for implementing a testbed for Internet research both for academic and industrial partners. The concept design and development was done in cooperation between CSC, Tampere University of Technology, Aalto University and Helsinki Institute of Information Technology. Once ICT SHOK Future Internet programme ends, the objective is that the testbed and its services will remain substantially the same as before, and will continue to be used for new services and Internet research in Finland. This objective is pursued by introducing and offering ICT SHOK Future Internet Testbed as a cross-programme testbed for Tekes. Utilising a single collaborative testbed would benefit both the testbed and several research programs requiring its services

It is expected that the number of testbed connections and the amount of testing performed will rise at a steady rate in the future. Demonstrations, dissemination and activity with relevant subject matter researchers will speed this up. Testbed participants are encouraged to offer services on the testbed. The offered services can be described and advertised by using service templates and wiki pages. The coordination activity continues to support the developers and testbed adopters on the route to the future networks.

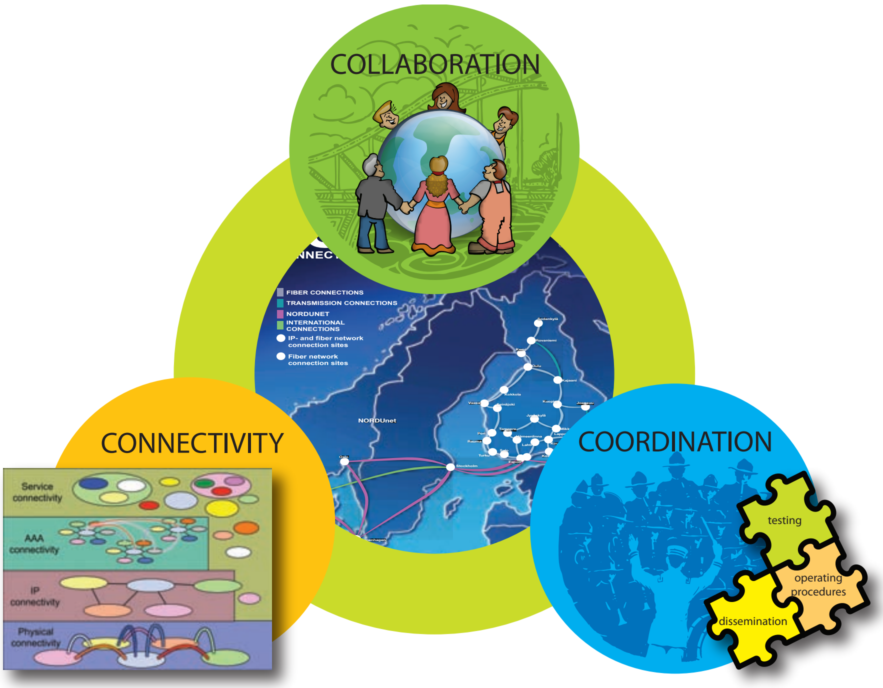

**Figure 8: ICT SHOK Future Internet Testbed**

First of the testbed's major benefits and one of its primary architecture design principles is its collaborative nature. Instead of designing and deploying overlapping testbed infrastructure, ICT SHOK Future Internet is designed to connect and provide existing research networks and services to a wider audience reducing this way operating and deployment costs. These existing services are then complemented with new testbed services such as dark fiber connectivity and enhanced IP connectivity services.

Enhanced connectivity is the second major benefit. In ICT SHOK Future Internet testbed the connectivity is provided on multiple levels from dark fiber to service interconnectivity. In between are the new, developed IP connectivity enhancements bringing the research network services on every academic or corporate researcher's desktop and reach. On an AAA level eduroam, Funet WLAN Roaming and Haka are utilised to provide cross-organisational authentication.

Collaboration and cooperation always need also coordination. The design and development of the concept was coordinated by CSC with Tampere University of Technology taking a lead role in architecture design and OpenVPN connectivity suite development coordination. CSC also coordinated and encouraged the testbed service adoption as well as facilitating testing and service provisioning.

ICT SHOK Future Internet testbed provides a cost-efficient collaborative testbed concept and architecture aiming at enhanced connectivity between academic and corporate research and development as well as providing an open innovation platform for new innovations combining both the existing and new services developed in Finland and abroad.

# 7. REFERENCES

[Cooperation] Funet network roaming being extended - CSC maintains a national and international network roaming service. CSC press release 22nd of June 2009. http://www.csc.fi/english/csc/news/news/funet_network_roaming

[eduroam] Wierenga K., Florio L.: Eduroam: past, present and future. Computational Methods in Science and Technology, Volume 11, Issue 2, 2005. 169-173.

[FIResearchAgenda] ICT SHOK Future Internet – Research Agenda, http://www.futureinternet.fi/publications/ICT_SHOK_FI_SRA_Research_Agenda.pdf , October 2007

[Fon] Fon, WiFi Community WWW site. http://www.fon.com/ . Visited 16th of November 2009.

[FunetRoaming] Keski-Kasari S., Huhtanen K. and Harju J.: Applying Radius-based Public Access Roaming in the Finnish University Network (FUNET), Proceedings of the TERENA Networking Conference 2003, Zagreb, Croatia, May 19 – 22, 2003, (CD-ROM)

[GoogleWave] Google Wave Federation Protocol. http://www.waveprotocol.org/ Visited 18th of May 2010.

[Haka] Linden M.: Organising Federated Identity in Finnish Higher Education. Computational Methods in Science and Technology, Volume 11, Issue 2, 2005. 109-118.

[Kalmar] Linden M., Simonsen D., Solberg A., Melve I., Tveter W. Kalmar Union, a Confederation of Nordic Identity Federations. Terena Networking Conference 2009, Málaga, Spain, 8 -- 11th of June 2009

[Metsahovi2006] Metsähovi connected with 10Gbps. CSC press release 31st of August 2006. http://www.csc.fi/english/csc/news/news/metsahovi_2006-8-31

[Metsahovi2008] Funet network rate more than 8 Gbps – Metsähovi Radio Observatory sets world record. CSC press release 7th of August 2008. http://www.csc.fi/english/csc/news/news/funet_metsahovi

[OpenVPN] OpenVPN Technologies WWW site. http://www.openvpn.net/. Visited 2nd of October 2009.

[OpenVPNVirtual] Use Case: Virtual Machine Network, http://www.netlab.tkk.fi/tutkimus/fi-shok/usecase.html Visited 19th of May 2010.

[P2PRadSec] Winter S., McCauley M., NAI-based Dynamic Peer Discovery for RADIUS over TLS and DTLS. RADIUS Extensions Working Group, Internet-Draft, March 5 2010. Expires September 6, 2010. http://tools.ietf.org/html/draft-ietf-radext-dynamic-discovery-02 Accessed 15th of April 2010.

[PlanetLab] PlanetLab, an open platform for developing, deploying, and accessing planetary-scale services. http://www.planet-lab.org/ Visited 18th of May 2010.

[PSIRP] Publish-Subscribe Internet Routing Paradigm, http://www.psirp.org/, October 2009

[PurpleNet] PurpleNet, OpenVPN User Interface. http://purplenet.sourceforge.net/ Visited 18th of May 2010.

[RadSecRoaming] Vatiainen H., Keski-Kasari S., Huhtanen K., Harju J. Implementing the multi-federation and peer-to-peer roaming on the eduroam federation level. Terena Networking Conference 2010, 31 May - 3 June, Vilnius, Lithuania. http://tnc2010.terena.org/schedule/presentations/show.php?pres_id=62

[RFC2865] Rigney C., Willens S., Rubens A., Simpson W. IETF RFC 2865: Remote Authentication Dial In User Service (RADIUS). June 2000. http://tools.ietf.org/rfc/rfc2865.txt

[RFC3588] Calhoun P., Loughney J., Guttman E., Zorn G., Arkko J. IETF RFC 3588: Diameter Base Protocol. September 2003. http://tools.ietf.org/rfc/rfc3588.txt

[RFC4301] Kent S., Seo K. IETF RFC 4301: Security Architecture for the Internet Protocol. December 2005. http://www.ietf.org/rfc/rfc4301.txt

[RFC4423] Moskowitz R., Nikander P. IETF RFC 4423: Host Identity Protocol (HIP) Architecture. May 2006. http://www.ietf.org/rfc/rfc4423.txt

[RFC4641] Kolkman O., Gieben R. IETF RFC 4641: DNSSEC Operational Practices. http://www.ietf.org/rfc/rfc4641.txt

[SAML2] SAML V2.0 Executive Overview. Committee Draft 01, 12 April 2005. http://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf

[Shibboleth] Shibboleth, Federated Single Sign-On Software. http://shibboleth.internet2.edu/ . Visited 16th of November 2009.

[Sparknet] Sparknet network WWW site. http://www.sparknet.fi/ . Visited 16th of November 2009.

[SpiderNet] SpiderNet, a Data Network technology laboratory of Jyväskylä University of Applied Sciences. http://student.labranet.jamk.fi/?page_id=121 . Visited 16th of November 2009.

[TUTRDNET] Tampere University of Technology Research Network. http://www.rd.tut.fi/. Visited 26th of November 2009.

[Wippies] Wippies community WWW site. http://www.wippies.com/ Visited 16h of November 2009.

[WirelessTampere] Huhtanen K., Vatiainen H., Keski-Kasari S., Harju J. Utilising eduroam architecture in building wireless community networks. Campus-Wide Information Systems, Volume 25, Issue 5, 2008. 382-391.

[XMPP] XMPP Standards Foundation. http://xmpp.org/ Visited 18th of May 2010.

Tampereen teknillinen yliopisto
PL 527
33101 Tampere

Tampere University of Technology
P.O.B. 527
FI-33101 Tampere, Finland