Tampereen teknillinen yliopisto. Tietoliikennetekniikan laitos. Tutkimusraportti 2009:2
Tampere University of Technology. Department of Communications Engineering.
Research Report 2009:2

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

ICT SHOK Future Internet Testbed Architecture v1.0

ICT SHOK Future Internet Deliverable 4.1.1

Tampereen teknillinen yliopisto. Tietoliikennetekniikan laitos
Tampere 2009

ISBN 978-952-15-2293-2 (printed)
ISBN 978-952-15-2294-9 (PDF)
ISSN 1459-4617

Table of Contents

1. INTRODUCTION

This document is the 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, the ICT SHOK Future Internet testbed is divided to four architectural levels (Figure 1) each supporting a different kind of connectivity:

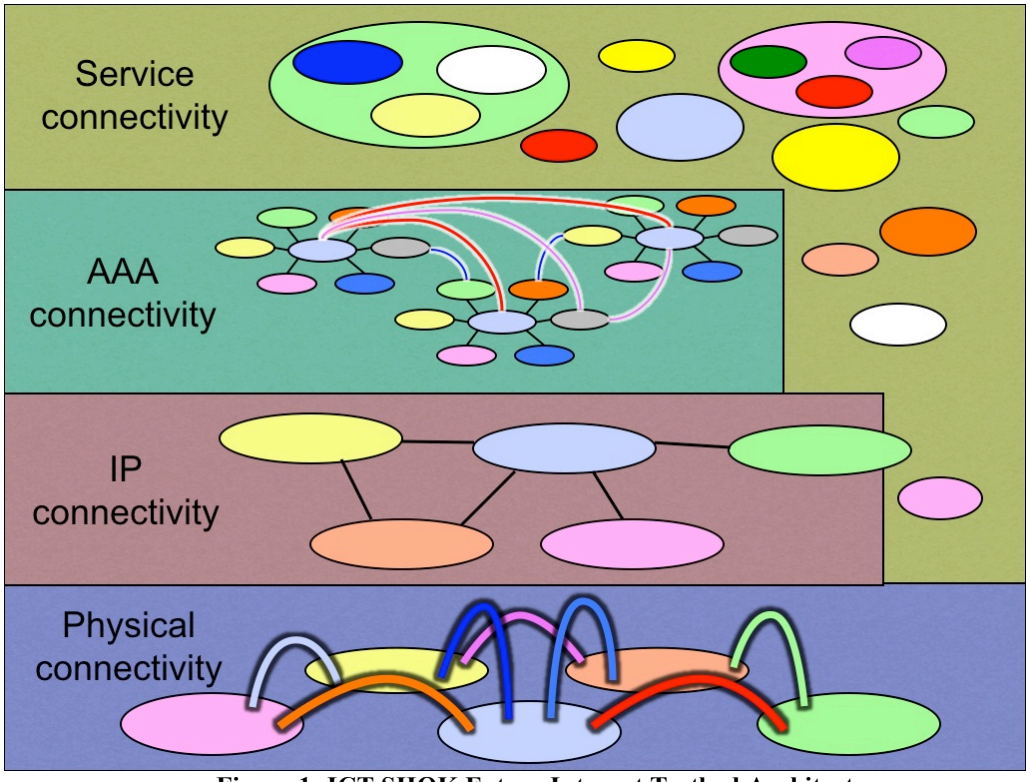

Figure 1: ICT SHOK Future Internet Testbed Architecture

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 connectivity options across the layers

Only some illustrative examples are provided; see later for longer description.

1.1.1. Physical connectivity

Point-to-point light paths

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

Multipoint light paths

- As with point-to-point light paths, but between more than two parties
- May be restricted to Ethernet
- Possible to connect to TREX or other exchanges

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.

1.1.3. AAA connectivity

Some examples include:

- 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).

2. PHYSICAL CONNECTIVITY

2.1. 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.

2.2. Implementation (tools and methods)

Figure 2: Funet DWDM physical connectivity, April 2009

Figure 2 shows the availability of light paths in April 2009.

2.2.1. Introduction to light paths

Light paths are OSI layer 1 or 2 level 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 multiple 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.

2.2.2. 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 is degraded 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 are not available yet. 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.

2.2.3. 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.

2.2.4. 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 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. In addition, there is no regulation for the dark fiber market. Some commercial providers have policies to rather offer capacity services than dark fiber. 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 base stations connected to customer access networks.

2.3. Use cases

2.3.1. Metsähovi Radio Observatory

Metsähovi Radio Observatory is an example of a research instrument that uses a data communications 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 [Metsahovi2006]
- Funet network rate more than 8 Gbps - Metsähovi Radio Observatory sets world record [Metsahovi2008]

2.3.2. 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.

The 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.

3. IP CONNECTIVITY

3.1. 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.

The future Internet testbed must support on the IP level 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.

3.2. Implementation (tools and methods)

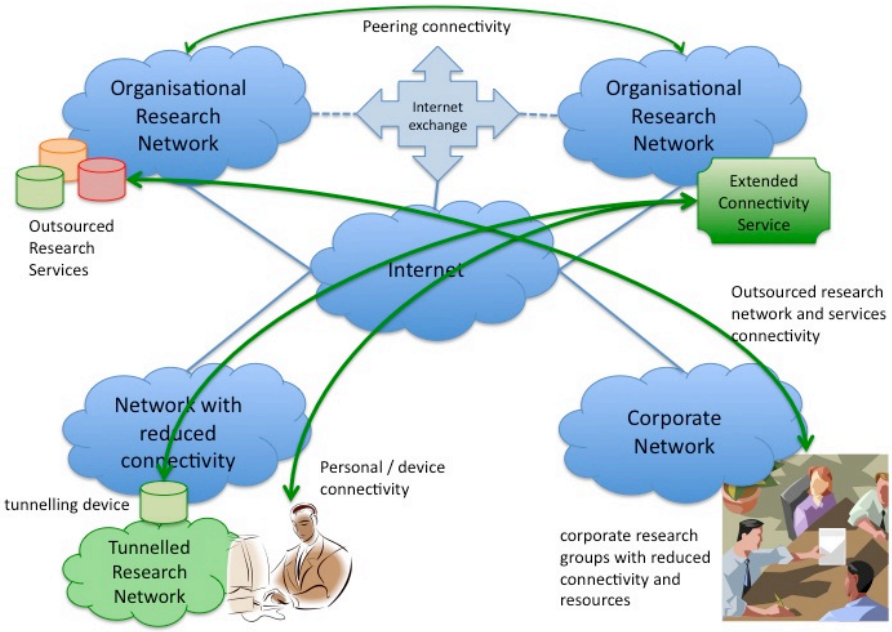

Figure 3: ICT SHOK Future Internet Testbed IP Connectivity Architecture

To cover the testbed IP connectivity requirements the testbed IP connectivity architecture (Figure 3) 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

3.2.1. 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 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 (see Use Case: Routed IP connection)

3.2.2. 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.

3.2.3. Outsourced research network and services connectivity

Often corporate and organisational networks are designed, segmented and optimised only for the production or business application use. Researching, developing and testing new networking technologies and services in this kind of networks 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.

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 this 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 services connectivity) and Helsinki Institute of Information Technology offer outsourced research network services for programme participants.

3.2.4. 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 the 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 already 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 3.

The second one is to utilise a virtual machine image on the researcher workstation. The virtual machine is configured to build the 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 3, personal connectivity).

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

With these three options the 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 the 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 practical reasons for creating the virtual research network connectivity. 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.

3.3. Use cases

3.3.1. 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. In TUT Research Network 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 TUT Research Network requires a research contract with Tampere University of Technology.

Utilised testbed services

- TUT Research Network Service(s)
- Another provider: Spidernet (Jyväskylä Polytechnic) [SpiderNet]

3.3.2. 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 internet exchange points in Finland and to the Internet and Geant via NORDUnet.

Problem

The current Internet service providers concentrate mainly to provide reliable and 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-art network technologies and connections for research purposes creates a need for separate research network providers such as for example CSC.

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. IPv6 routing and multicast are available.

Requirements

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

Utilised testbed services

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

3.3.3. 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 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 what the service provider does not yet support. Also researching the services provided by 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. The terminals are capable of utilising technologies such as IPv6 and multicast with the help of tunnelling even in cellular networks. The terminals are also capable of providing terminal based services such as content sharing via mobile WWW servers etc. This enhanced connectivity was possible by running a 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

4. AAA CONNECTIVITY

4.1. Objectives/motivation

Extending physical and IP connectivity are not the only ways to expand both the impact and coverage of the 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 or 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.

4.2. Implementation (tools and methods)

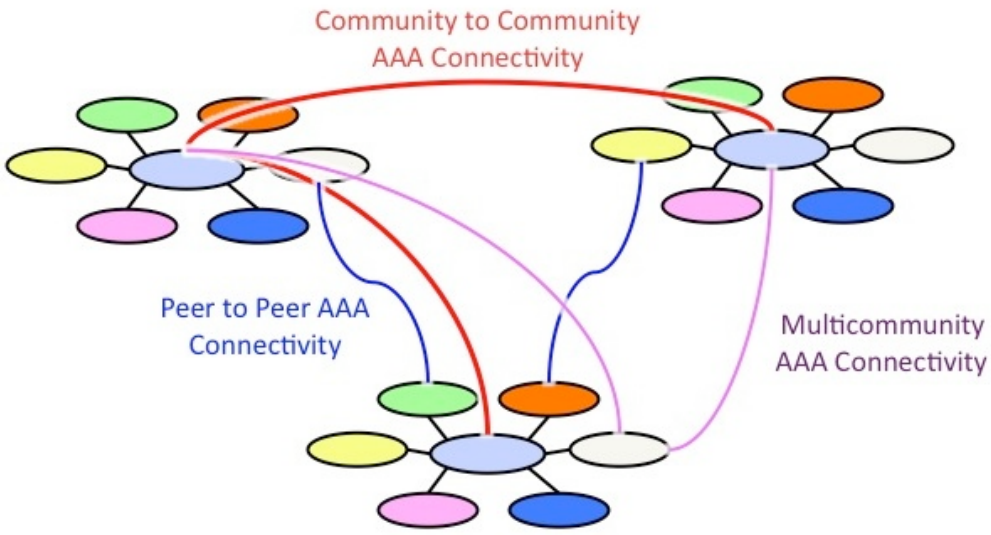

Figure 4: AAA Connectivity Architecture

In defining the AAA connectivity architecture for the 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 4 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 4 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 communites and organisations utilsing 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.

The technologies mentioned (DIAMETER, RADIUS, SAML2 [SAML2], Shibboleth) can already all be utilised within and interconnecting with the 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 in the Internet with Shibboleth/SAML2 handling the single sign on for services.

4.3. Use cases

4.3.1. 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 a 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, the organisations 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

4.3.2. 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 can could be used to provide research-related services to this user base.

An example of this is a WWW interface for university libraries, which all students can use. There are numberous other examples (see beyond the link below for more).

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

5. SERVICE CONNECTIVITY

5.1. Objectives/motivation

Increasing 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 trying and researching 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 the way they can be easily and openly connected, which means the services and technologies must have open interfaces for inter-service communication.

5.2. 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 use of 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 beginning.

In the actual service creation and research this kind of combining services and technologies can be encouraged by ensuring the used or developed technologies and interfaces are interoperable and preferably open for integration with other services. The current Internet with open interfaces and 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.

6. FUTURE DIRECTIONS

Once ICT SHOK Future Internet programme closes, the expectation 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.

Connecting participants from outside the program will also underline the need to move substantial parts of the testbed activity under a more generic framework that is available to a wider audience. Another reason is that ICT SHOK Future Internet programme participants over the years will also likely change.

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 using a service template. The number of offered services is likely to increase slightly over the years.

Figure 5: Funet DWDM network (12/2009 coverage lighter color)

Figure 5 shows Funet DWDM network coverage in April 2009 (darker color), and the expected coverage at the end of 2009 (lighter color). Arbitrary testbeds and testbed connections can be easily deployed using the network.

7. REFERENCES

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

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

[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

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

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

[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)

[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

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

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

[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

[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

[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