Management Challenges for Different Future Internet Approaches

Iris Hochstatter and Gabi Dreo Rodosek

Information Systems Laboratory, Universität der Bundeswehr München
Werner-Heisenberg-Weg 39, D-85577 Neubiberg, Germany
iris.hochstatter@unibw.de, gabi.dreo@unibw.de,

EMANICS (European Network of Excellence for the Management of Internet Technologies and Complex Services) has organized a workshop on the topic "Vision and Management of the Future Internet"[1]. Selected experts from within and outside EMANICS had been invited to discuss possible scenarios for the future Internet and their management implications. Three main scenarios have been discussed: first, the replacement of the current Internet with a "clean slate" design, second, many federated networks and generic inter-networking mechanisms, and third, evolution happens around IP, while IP stays almost as it is.

Does a clean slate design for the future Internet imply a clean slate design for the management? Do we need to rethink existing management approaches and architectures? And if the evolution happens around IP, do we need to change anything wrt. management concepts at all?

1 Revolutionary Approach: Clean Slate Design

An all optical Internet core will consist of hundreds of core routers with (nearly) full connectivity and cover the whole world similar to tier-1 providers. There will be five to ten operators that provide enough fiber capacity for all ongoing communications worldwide. The main costs are for transmit and receive equipment and not all fibers/lambdas will be used initially.

This scenario implies three main management challenges. First, **configuration management** includes the path planning and provisioning and indicates when to establish and release paths. Inter-domain path request handling will be a necessary feature and resilience has to ensure that there are different physical paths available. This management technology is well-known, such as TL1, SNMP, GMPLS and others.

Second, **monitoring** is needed for provisioning as well as for security reasons. The main question is what to monitor as Tbps of data will flow through those networks. Monitoring ports are needed for lawful interception / data retention and each country on the path may have different requirements thus monitoring has to be possible at intermediate optical switches. And third, **access control** has to protect the core from the access networks and vice-versa. Sites with unwanted content or which perform attacks have to be blocked. Thus, high-speed firewalls will be needed as current firewalls may not scale.

[1] http://emanics.org/content/view/131/135/

2 Evolutionary Approach: IP remains as it is

The main characteristics of the evolutionary approach are that there will be sufficient bandwidth available in the core network by assuming optical network technologies. The operator of the core network offers a simple data forwarding interface and does not want to expose management capabilities to its customers. The bandwidth of the access network may vary, e.g. in the case of a wireless access network. And additional functionality is needed for a node to operate adequately in such an environment, e.g. with resource constraints, or changes in connectivity in a wireless environment. The scenario implies requirements on relationship between layers:

- There is management below the IP layer, e.g. managing a Metro-Ethernet, or managing wireless access networks.
- There is management at the IP layer. This management must be aware of what happens below.
- There is management of functionality above the IP layer. This management must be aware of what happens below.

Those requirements impose that management of each layer should be aware of management of the layer below and in some cases, management of one layer also has to be aware of information of a layer above. For example, information relevant for security, e.g. spam-related information (from application layer) is relevant for network layer.

Besides the layering requirements on management, we expect new management features in the future Internet. First, **automation:** having static logic in an algorithm that specifies how to handle different situations. This is programmed by humans. The programmed logic fits to previously understood scenarios. Second, **self-management:** A device should be capable of configuring itself based on specific guidelines. End user and access network devices equipped with autonomic capabilities, i.e. with information sensing, decision making and enforcement. Decision making is based on programmability not restricted to the manufacturer of a device.

3 Real Challenge: Services and Content

We assume that the future Internet will be driven by content and services. Ubiquitous connectivity will allow everybody to access content and services anywhere and anytime. Networked sensors will provide computer-usable information about the real world in all situations. The current trend of user-generated content will evolve into the possibility for everybody to create her own services, supported by general service frameworks and mesh-ups. Some of those services will change the way we work and live (similar to how the Internet changed our lives).

This scenario will imply that not managing networks but managing the data is the main future management challenge. Management will also act like an "Internet life guard" as it has to prevent serious damage in any "connected"

situation and will resolve conflicts between users. Privacy management and its easy applicability will be a key enabler and major challenge. All data has to be protected and securing connections will diminish. Also, privacy management will be provided as a service. Identity management will play a very important role, too. The technology needed for this scenario includes e.g. context models for different services, semantic service descriptions and mesh description languages.

4 Conclusions

The different approaches taken by the three groups lead us to the following preliminary conclusions:

- The future Internet will have an all optical core, consisting of a few hundred optical switches, which provide end-to-end optical paths.
- Therefore we argue that the role of IP is diminishing; IP will become only an access technology.
- Future Internet = Content + Services. Since the users will perceive the future Internet in terms of contents and services, the user should no longer be bothered with details such as IP addresses, firewalls etc.
- Access to a mass of sensor data surrounding the users lead to new services that we cannot image today.
- Security and privacy management will become increasingly important.
- We have to automate management to get the humans as far as possible out of the loop.
- The focus moves from network management, via service management to information and content management.
- Although we believe that the core routing infrastructure of the Internet will be replaced by an all optical switched network (which can be considered as clean-slate design), the focus of research on the future Internet should be on services and the content (which will not need a clean-slate design).

Acknowledgements

The contents of this abstract have been jointly produced by the participants of the EMANICS Workshop on "Vision and Management of the Future Internet", in particular: Aiko Pras (University of Twente, The Netherlands), Burkhard Stiller (University of Zurich, Switzerland), David Hausheer (University of Zurich, Switzerland), Gabi Dreo Rodosek (Universität der Bundeswehr München, Germany), Georg Carle (TU München, Germany), Iris Hochstatter (Universität der Bundeswehr München, Germany), James Won-Ki Hong (POSTECH Korea), Javier Rubio-Loyola (UPC, Spain), Juergen Quittek (NEC Europe Limited, Germany), Juergen Schoenwaelder (Jacobs University Bremen, Germany), Marinos Charalambides (University College London, UK), Marc Fouquet (Universität Tübingen, Germany), Spiros Spirou (Intracom Telecom, Greece).