TeraBit Lan Networking: TeraControl

www.science.uva.nl/~delaat

Cees de Laat

SURFnet

EU

University of Amsterdam

SARA
TI
TNO
NCP
Simple service access

Pitlochry, Scotland - Summer 2005
Token Based Networking

Access Control, Resource Management and Path Selection in Optical Networks using Tokens


- Separation of (slow) authorization process and real time usage.
- Binding to many different types of attributes: user, time, resource, etc.
- Policy Decision to be abstracted from Policy Enforcement Point.
- Anonymous usage
- Resource Management

Tokens performing Path Selection and Access Control at Optical Inter-Connection Points

- Economic Link Owners to assign usage rights without routing changes.
- Recognition at Inter-Connection Points (Optical Exchanges). When authentic and valid, token marked traffic will use the Link Owners path.
- Implementations that support different business models
- Hardware (NPU based) recognition rate expected to be a 10 Gb/s.
Authorization Sequences*

**PULL Sequence**
- User
- Service
- Authority

1. User requests service
2. Service requests authority
3. Authority responds to service
4. Service receives authority

*Internet Dail-in, RSVP*

**AGENT Sequence**
- User
- Service
- Authority

1. User requests authority
2. Authority responds to user
3. User requests service
4. Service receives authority

*Bandwidth Brokers Lightpath provisioning*

**PUSH Sequence**
- User
- Service
- Authority

1. User requests service
2. Service requests authority
3. Authority responds to service
4. Service receives authority

*(2/3) Tokens, Tickets Attribute Certificates, SAML Assertions*

* According to RFC 2904 / GFD.38
Token Switch Function at Interconnection Point

Available Link Advertisement

Link Access Request

Request to other brokers or authorities

Link Admission Policies from Stakeholders

Ingress Switch

Token-key

Link Reservation Request

Token-based Switch

Switch Function at Interconnection Point

Stakeholder X connection

Stakeholder Y connection

BGP Router

InterConnection Point A

To Transit Network
Token Switch Principle

IP HEADER  DATA  CRC

MASK

AES-XCBC-MAC-96 algorithm

Token Key

Token

IP HEADER  Options  DATA  CRC
Implementation: Network Processor Units

Features:

• The IXP 2850 is able to perform packet functions at 10 gb/s
• 16 programmable Micro Engines to allow parallel dataplane processing.
• Two crypto units support bulk security algorithms (AES, DES, 3DES, SHA1)
• Designed for IPSec, however is general enough to do other things.
• Supports Cypher Block Chaining in combination with MAC.
• Expected to be usable within a Content Monitoring & Action Device (CMAD)
Intel® IXP2850 Network Processor Block Diagram

The IXP2850 network processor implements the same store-and-forward design as the IXP2800, including 16 multi-threaded microengines in the dataplane and a high-performance Intel XScale core for control plane functions. The IXP2850 adds two cryptography blocks.
Principle points in TBN

- Decoupling of Authentication and Authorization from provisioning
- Real Time
- In band vs out of band signalling
- Out of band just in time provisioning
The StarPlane project addresses two concerns in optical networks:

1. The Basic StarPlane Management Infrastructure

   StarPlane allows applications to take advantage of the increased bandwidth and potential flexibility in optical networks by letting them create their own network topology in a simple way.

2. The Applications and Their Needs

   StarPlane will discover how this new freedom to manipulate the network will benefit the applications.

StarPlane will use the physical infrastructure provided by SURFnet 6 and the distributed supercomputer DAS-3. Hybrid optical networks such as SURFnet 6 allow network administrators to partition the network and to create multiple overlay networks, each with a different logical topology. The novelty of StarPlane is that it does give this flexibility directly to the applications by allowing them to choose the logical topology in real time, ultimately with subsecond switching times.

Staff members of the research team:
- Prof. dr. ir. H.E. Bal, VU professor
- Prof. dr. ir. C.T.A.M. de Laat, UvA associate professor
- Prof. dr. ir. P.M.A. Sloot, UvA professor

Parallel programming
- Computer networks
- Internet and Grids
- Computational science

DWM network provided by SURFnet

SURF.net

Funded by NWO in the GINCE program
StarPlane Goals

Goals in the proposed StarPlane project:
1. fast, application-specific allocation of the network resources with deterministic characteristics;
2. application-specific composition of the protocol stack that is used to control the resources;
3. low-level resource partitioning (and, hence, no interference);
4. high-level requests (whereby policies and inference are used to assist the user).
GRID-Colocation problem space

Extensively under research

New!
Common Photonic Layer (CPL) in SURFnet6

~5000 km
StarPlane
DWDM
backplane

SURFnet

university
WS+AAA

CPU's

switch

NOC
DAS Cluster

head node

Local interconnect

Fast interconnect

32 compute nodes

To University

To SURFnet

1 Gbit/s Ethernet

10 Gbit/s Ethernet lanphy
Resource Brokering: Your Ticket Into NetherLight

Application architecture:

Lambda networking allows the creation of application specific light paths.

Lambda networking facilities empower users to request services and provision end-to-end light paths if and when they need it.

NetherLight, located in Amsterdam, The Netherlands, is one of such facilities.

The Amsterdam LightHouse is a joint research laboratory of the UvA and SARA.

Resources in the LightHouse can be used by collaborators to prove the concepts of hybrid networks.

Lightpath setup components:

- Topology information
  We make use of semantic web techniques. The description of the network is contained in RDF files.

- Reservation system
  We provide web services interfaces to the client for: resources and path inquiries; reservation handling.

- Management system
  We provision the paths on the LightHouse equipment.

Semantic web
The Network Description Language, an RDF Schema, describes networks in a standard, interoperable way.

Web Services
A WSDL file describes the interfaces to the service available to clients. Clients can interact with the service directly or via a portal.

Our SC'05 demonstration
We show the setup of dynamic connections between two computing nodes through the LightHouse/NetherLight Optical Exchange.
Transport of flows

For what current Internet was designed

Needs more App & Middleware interaction

Full optical future

GLIF Future?

# FLOWS
Thanks to:

- Kees Neggers, SURFnet
- Tom DeFanti, UIC & iCAIR
- Joel Mambretti, CANARIE
- Bill St. Arnaud, CANARIE
- Freek Dijkstra, VL-team
- Hans Blom, Bas van Oudenaarde
- Leon Gommans, VL-team
- Arie Taal, VL-team
- Pieter de Boer, VL-team
- Bert Andree, VL-team
- Fred Wan, VL-team
- Jeroen van der Ham, VL-team
- Karst Koymans, VL-team

Partially complete list:

- Caas Chase Cess Case Caas Chase Cess Case

The END