Control Plane Extensibility for Shared Network Infrastructure

Bushar Yousef
PhD Candidate
Advanced Research in Networking Lab (ARN)
UTS

Supervisor: Professor Doan B Hoang
Advanced Research in Networking Lab (ARN)
UTS

Co-Supervisor: Glynn Rogers
ICT CSIRO
Talk Outline

• Background:
  – Services
  – Provisioning methods

• Serviter
  – Vision
  – Architecture
  – Partitioning

• Conclusion
Services

• What is a Network Service?
  
  – Traditionally:
    • Connectivity
    • Protocol Translation
  
  – Today:
    • Connectivity with Quality of Service
    • Monitoring, Fault Detection, Auto-Recovery
    • Virtual Private Networks
    • SSL acceleration
    • Firewalls
    • Intrusion Detection Systems
    • Mobile Services (Connect Me, Find Me, Follow Me)
    • Etc…
Services

A Network Service -

*An operation performed inside the “network” that directly benefits end-users.*

More specifically,

*The network intelligence and forwarding logic which work together to perform an operation that directly benefits end-users.*
A network is composed of:
- Forwarding plane
- Control plane
- Network management protocol

<table>
<thead>
<tr>
<th>Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Management</td>
</tr>
<tr>
<td>Control Plane</td>
</tr>
<tr>
<td>Forwarding Plane</td>
</tr>
</tbody>
</table>

Services require support from all three.
Services Provisioning: Provisioning Methods

- Flexibility
- Service Deployability
- Safety
- Performance

Active Networks
Programmable Networks
Current Networks
Services Provisioning: Current Network Infrastructure

Current Networks

Status of:
- Hardware, Links, and Queues
- Packet Capture:
  - Routing Updates, Remote Config.

Boot Configurations
- Routing Protocols (RIP, OSPF, etc)
- Network Management Protocols
- Burst or Wavelength switching

Configuration:
- Routing entries, queues, firewall rules, load balancing, SSL keys, etc.
- Routing Updates

Forwarding logic (IP, MPLS)
- QoS control, SSL, Intrusion Detection
- Firewall, Load Balancing, etc.
Services Provisioning: Current Network Infrastructure

Current Networks

Black Box

Control Plane

Forwarding Plane

Proprietary Protocol

IOS/Boot Image: Preprogrammed Extensible only by manufacturer

Fixed Hardware May contain a degree of programmability
What does it take to deploy a new service?

- Manufacturer support
- Nodes upgrade
- Service configuration
- Multiple SLA
- Cost-Benefit Analysis
Services Provisioning:
Current Infrastructure drawbacks

- Cost and Rollout time

- External dependency
  - Manufacturer
  - Partner Providers

- Non-customisable services
  - Network providers provision fixed services of which a user may purchase
  - Services do not take into account needs of individuals
  - Due to the great cost of manual customisation
Services Provisioning: Provisioning Methods

- Active Networks
- Programmable Networks
- Current Networks
Services Provisioning: Provisioning Methods

- Network Management
- Control Plane
- Forwarding Plane

Extensible Software
Generic CPU and NIC
Services Provisioning: Provisioning Methods

Active Networks

Node OS
Domains
Code Library (optional)
Execution Environments
Packet Capture
TCP Stack
Generic CPU and NIC

Packets
Code / Ref # Payload

Bushar Yousef (ARN Labs UTS) - CSIRO ICT Talk 2005
Services Provisioning: Active Networks Drawbacks

• There is a consensus that Active Networks are *Not Feasible!*
  – *Drastic Scalability and Performance degradation*
  – *Security*

• Proponents argue:
  By placing Active nodes in strategic locations of a network these issues are overweighed by the benefits.

Funding for the DARPA Active Networking project had not been renewed!

The community is moving towards Adaptive Protocol Stacks.
Services Provisioning: Provisioning Methods

Active Networks

Programmable Networks

Current Networks
Services Provisioning: Provisioning Methods

Programmable Networks

Network Management

Control Plane

Forwarding Plane

- Signaling and Deployment Protocols
- Extensible Software
- Interface
- Programmable Network Processors (or FPGA)
Services Provisioning: Provisioning Methods

Programmable Networks

Network Generic Services:
- Customised Routing
- Routing Algorithms
- DiffServ Scheduling

Standardised Interfaces

Service Injection

Value Added Services

Monitoring

Extensible Software

Network Services Intelligence

Code Injection

Virtual Network Device (software representation)

Monitoring

PNP

Forwarding Microcode

Signalling and Deployment Protocols

API

API

API
Services Provisioning: Programmable Networks Drawback

- Difficult to standardise interfaces

- Performance
  - Generic hardware support can not be optimised

- Restrictive
  - Can not perform Service specific operations

- Security and Resource Management
  - Based on testbed experimentation
  - Configuration is restricted

- Non-customisable services
Serviter

Goal:

To develop a common platform for existing and new commercial modules (networking module, content directors, SSL accelerators, IDS, etc) for safe on-demand deployment and customisation of services.

Vision:

- Network providers focus only on providing new links and modules.
- Third party services providers and users purchase hardware shares.
Serviter:
Vision Explained
Serviter: Criteria

• Control Plane Extensibility

• Risk Isolation

• Scalability
  – Services
  – Partitions

• Differentiated Services

• On-demand Services in on-demand Partitions
Serviter

- Control Channels
- Extensible Control Plane
- Traditional Control Plane
- Hardware Modules
Serviter: Architecture

- Current Hardware Modules
  - Traditional Control Plane
  - System Services (Cp API)
  - User Services
  - Extensible Control Plane

Aux Hardware Support (FPGA, Secure Processors)

Provider

Third Party Partition #1
P #2
P #3
P #4
Other Advantages:

- Intelligent Monitoring, Detection, Recovery
  - Autonomic Networks
- Dynamic Network Provider management
- Adaptive Optical Network Control Plane
Extensible Control Plane:
A number of PC hosting *User Services* and other management components

Traditional Control Plane:
A Management Module with fixed IOS

Forwarding Plane:
- Layer 2/3 Switching Modules
- Content Switching Modules
- SSL Accelerators
- Firewall Modules, etc..

Bushar Yousef (ARN Labs UTS) - CSIRO ICT Talk 2005
Serviter:
Security and Resource Management overview

Services Compete for Computational Resources
Interfere with each other

BUS/Switching Fabric

Control CE

Bottlenecks

Services May configure operations on traffic of others
Extensible Control Plane Resources: What to Manage?

- **Internal Router Resource Allocation:**
  - Computational
    - CPU time, Memory Pages, I/O operations, Harddisk space
  - Communication
    - Computation resource consumed outside of VM
    - Managing bottleneck fairly:
      - Bus/Switching fabric bandwidth
      - Control-CE

- **CE Resource Monitoring**
- **Balancing the load across CEs**
Serviter: Computation Elements

- CE Management
  - User Services
  - System Services
    - Resource Management Interface
    - Operating System
  - Hardware
Serviter: Computation Elements
Class-based Kernel Resource Management
ckrm.sourceforge.net
Internal Comm. Resource Partitioning: Dispatcher Structure

CE

User Services

Service Dispatcher

RE Dispatcher

System Dispatcher

CE Dispatcher

Bus Channel Allocation DB

NI

Control CE

NPU

Flow Access Restriction
Internal Comm. Resource Partitioning: Dispatcher Structure

Fix Size queue

UserVM Source 1
UserVM Source 2
. . .
. . .
UserVM Source N

GOLD
SILVER
BRONZE
B. E.

Weighted Scheduler

Verification (and any execution)

Routing

Destination Service

Next Dispatcher

BUS
Serviter:
Forwarding Plane Partitioning

Flow Access Restriction Module

- Source Classifier
  - Invalid Users
    - Ignore
    - Invalid Commands
  - Valid Users
    - Command Verifier
      - Valid Commands
      - Control-CE
    - Update
  - User Privileges DB

Commands

Bushar Yousef (ARN Labs UTS) - CSIRO ICT Talk 2005
Conclusion

Add Extensible CP
Add Resource Management
Add Risk Isolation

Current Networks

Active Networks
Programmable Networks
Current Networks
Lessons Learned

- Interfaces Standardization:
  - User Services -> System Services
  - System Services -> NI

- To what extent can NIs be programmable?
- How this be specified and Discovered?

- Traditional CP Bottleneck
- Move toward a fully distributed extensible control plane.
<table>
<thead>
<tr>
<th>NI Capabilities: Specification and Discovery</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Layer 7</strong></td>
</tr>
<tr>
<td>Classification:</td>
</tr>
<tr>
<td>Regular Expression on:</td>
</tr>
<tr>
<td>- Protocol Type</td>
</tr>
<tr>
<td>- HTTP header data</td>
</tr>
<tr>
<td>- Packet payload data</td>
</tr>
<tr>
<td>Manipulation:</td>
</tr>
<tr>
<td>- HTTP header field substitution</td>
</tr>
<tr>
<td>- SSL</td>
</tr>
<tr>
<td>Forwarding:</td>
</tr>
<tr>
<td>Load Balancing for:</td>
</tr>
<tr>
<td>- Manipulation NIs</td>
</tr>
<tr>
<td>- Web servers</td>
</tr>
<tr>
<td>- Firewalling</td>
</tr>
<tr>
<td><strong>Layer 4</strong></td>
</tr>
<tr>
<td>Regular Expression on:</td>
</tr>
<tr>
<td>- TCP header data</td>
</tr>
<tr>
<td>- UDP header data</td>
</tr>
<tr>
<td>- QoS fields</td>
</tr>
<tr>
<td>Substitution of:</td>
</tr>
<tr>
<td>- TCP header fields</td>
</tr>
<tr>
<td>- UDP header fields</td>
</tr>
<tr>
<td>- QoS fields</td>
</tr>
<tr>
<td>Queue configuration and monitoring</td>
</tr>
<tr>
<td>NI status monitoring</td>
</tr>
<tr>
<td>Routing table modification</td>
</tr>
<tr>
<td><strong>Layer 3</strong></td>
</tr>
<tr>
<td>Regular Expression on:</td>
</tr>
<tr>
<td>- IP header data</td>
</tr>
<tr>
<td>Substitution of:</td>
</tr>
<tr>
<td>- IP header field</td>
</tr>
<tr>
<td>Route using new header</td>
</tr>
<tr>
<td><strong>Minimum Level</strong></td>
</tr>
<tr>
<td><strong>Layer 2</strong></td>
</tr>
<tr>
<td>MAC addresses</td>
</tr>
<tr>
<td>Ingress or Egress NIs</td>
</tr>
<tr>
<td>Substitution of:</td>
</tr>
<tr>
<td>- MAC addresses</td>
</tr>
<tr>
<td>Internal Redirection</td>
</tr>
<tr>
<td>Mirror Drop</td>
</tr>
<tr>
<td>Switch Normally</td>
</tr>
</tbody>
</table>

Bushar Yousef (ARN Labs UTS) - CSIRO ICT Talk 2005
Thank You

ARN Advanced Research in Networking
Faculty of IT, UTS
http://research.it.uts.edu.au/arn/