Enabling Active Flow Manipulation In Silicon-based Network Forwarding Engines

Tal Lavian - tlavian@Nortelnetworks.com
Phil Wang, Ramesh Durairaj, Jennifer Rasimas, Doan Hoang, Franco Travostino.
Nortel Networks, Advanced Technology Labs

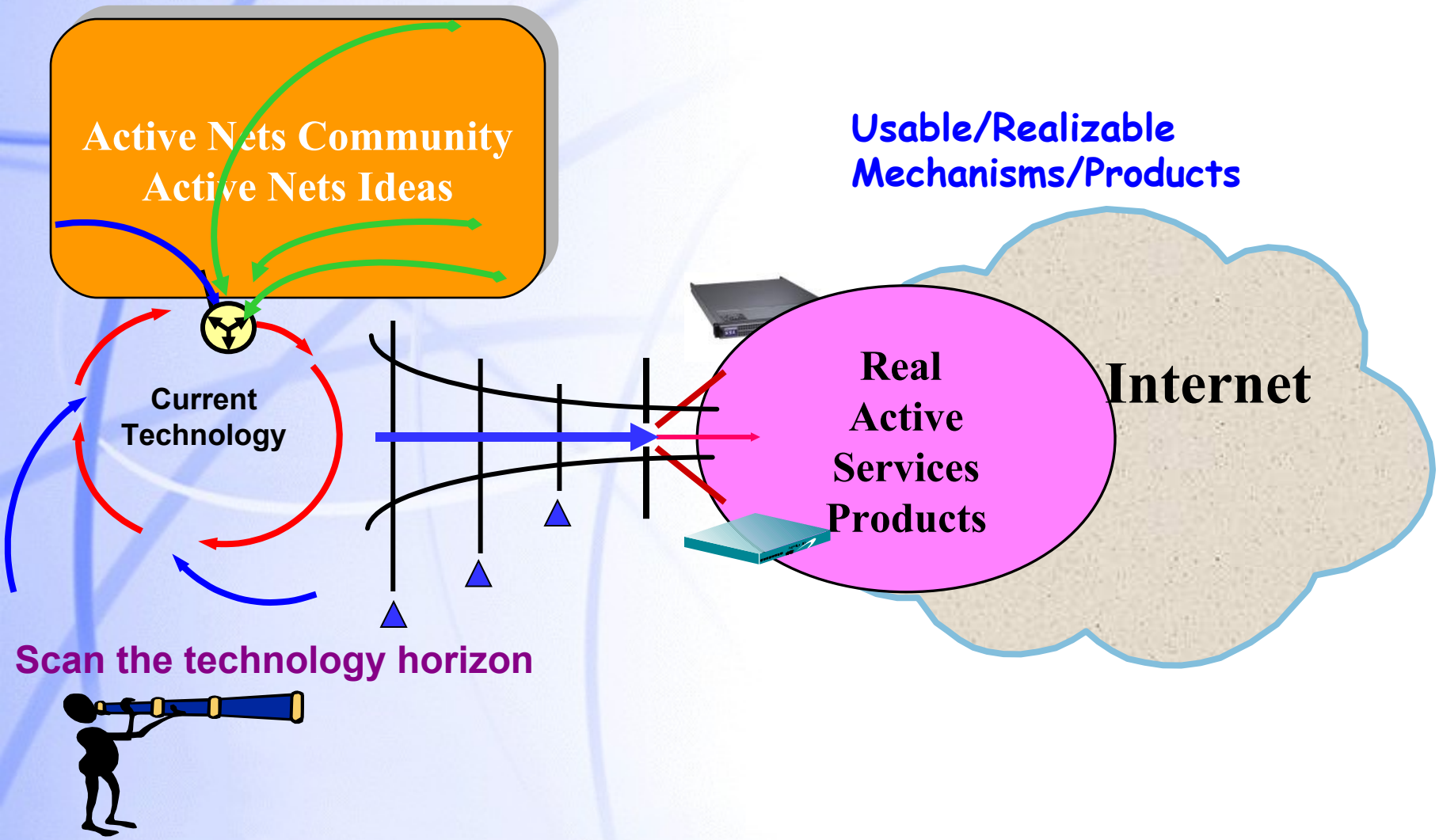
Open Source - http://www.openetlab.org

Outline of the talk

- AN technology Transfer
- Issues in the realization of AN technologies
- Main contributions of the paper.
- Commercial Active Services Platform
- Application Example 1 – SSL
- Application Example 2 – ASF
- A Demo Application
- Next Generation Active Services Platform
- Conclusion

AN Technology Transfer

Great Ideas



AN issues

Lack of industrial-strength Active Network devices that dispel major concerns:

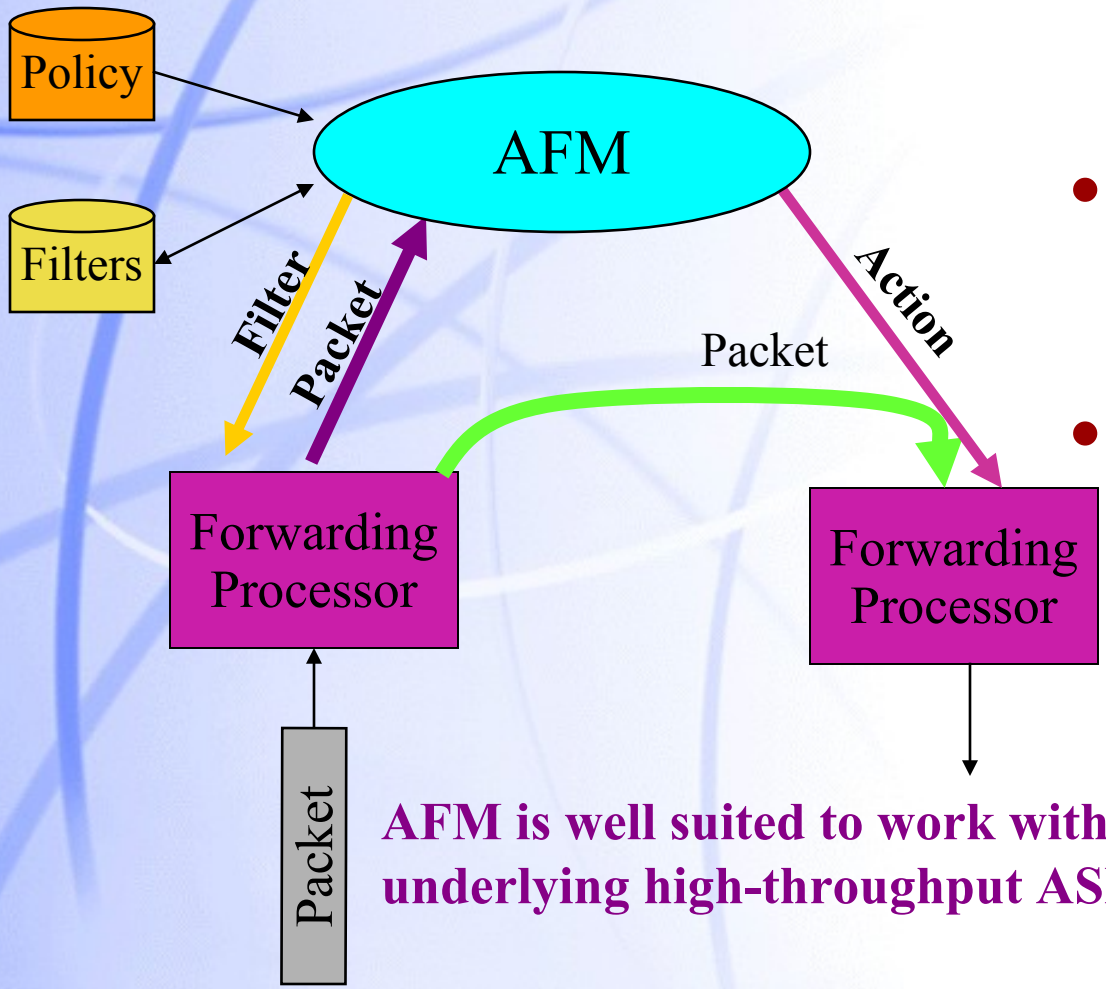
- AN requires substantial supports from a NOS
- AN introduces substantial software component, hence delay on the data path
- AN lacks adequate measures to addressing integrity and security of network devices.

Main contributions of the paper

Dynamically control *ASICs* and *MEMs*

- **Active Flow Manipulation Concept**
  - Flow abstraction
  - Actions on Flows
  - Control/Data separation
- **Openet Platform**
  - Commercial Network Devices
  - Runtime Environment
  - Active Services
- **Applications**

Active Flow Manipulation



AFM is well suited to work with underlying high-throughput ASICs

- **A key enabling technology of Openet**
- **Two abstractions**
  - Primitive flows
  - Primitive actions
- **Customer network services exercise active network control**
  - Identifying specific flows
  - Apply actions to alter network behavior in real-time

Dynamic L2-L7 Filtering

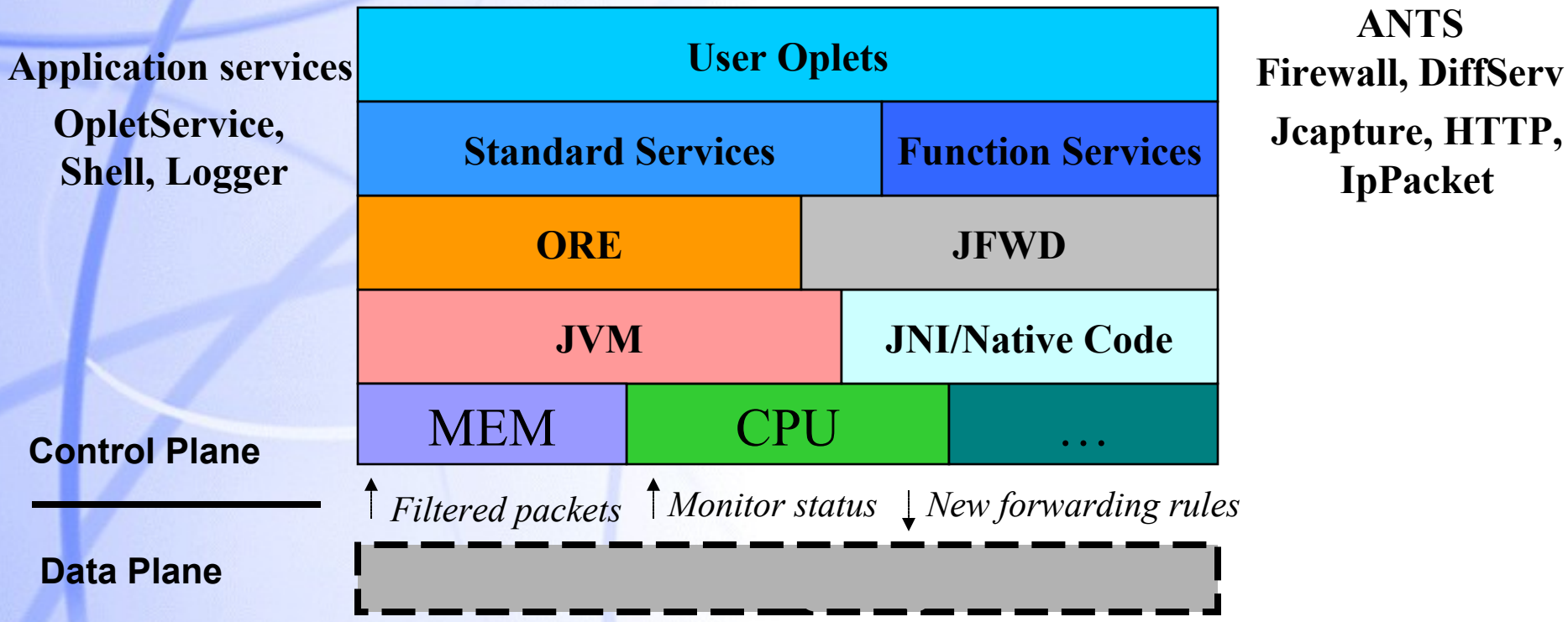
L2-L7 Filtering Capability

- Source Address
- Source Port
- Destination Address
- Destination Port
- Protocol
- VLAN
- Diffserv Code Points
- Content Filtering
- Cookies Filtering

Active Flow Manipulation

- Flow redirection
- Stop/Forward flow
- Change DSCP field
- Set VLAN priority
- Adjust priority queue
- Modify session table
- Parsing request header
- Parsing application contents

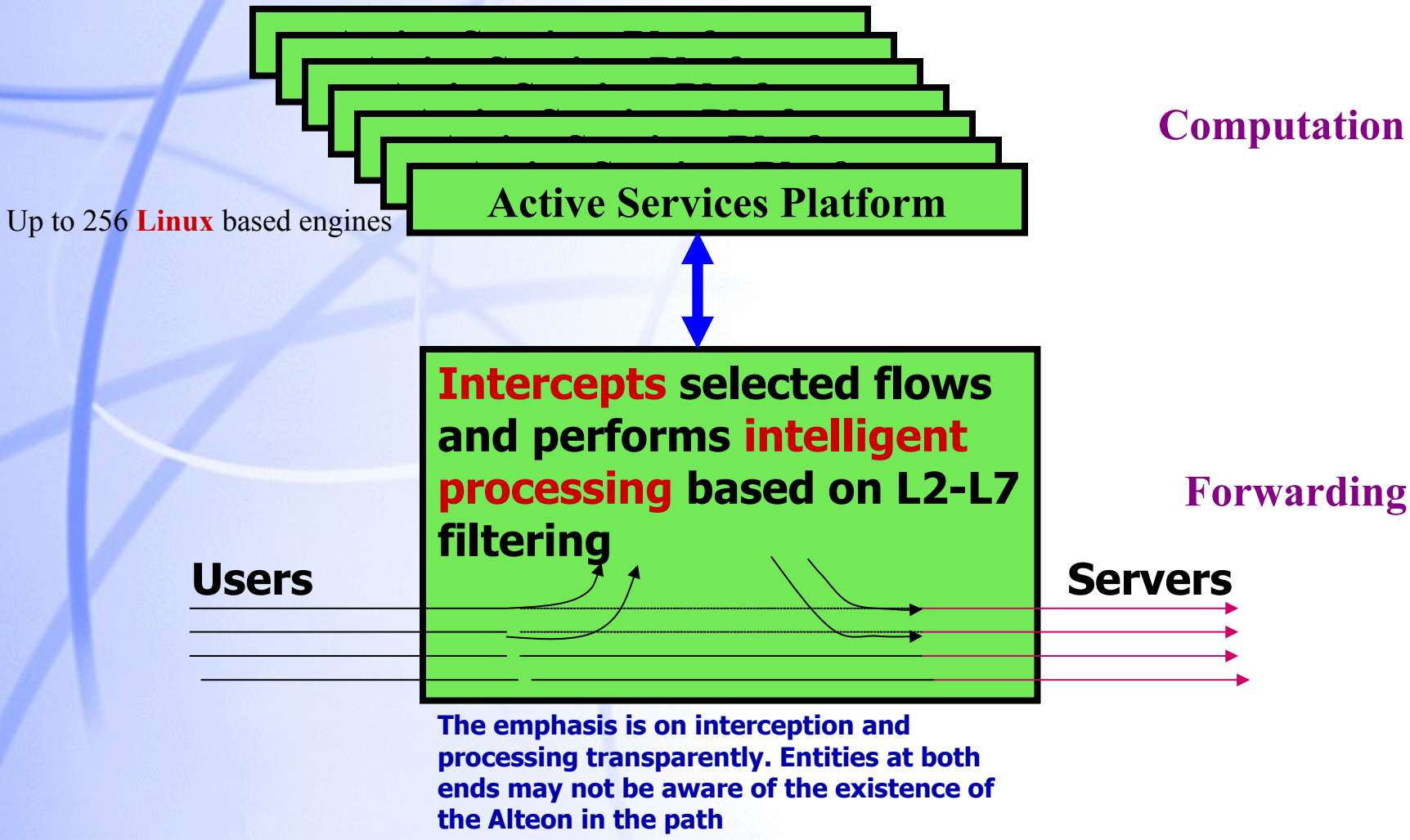
Openet: An active service platform



Nortel Networks' contributions to Active Services

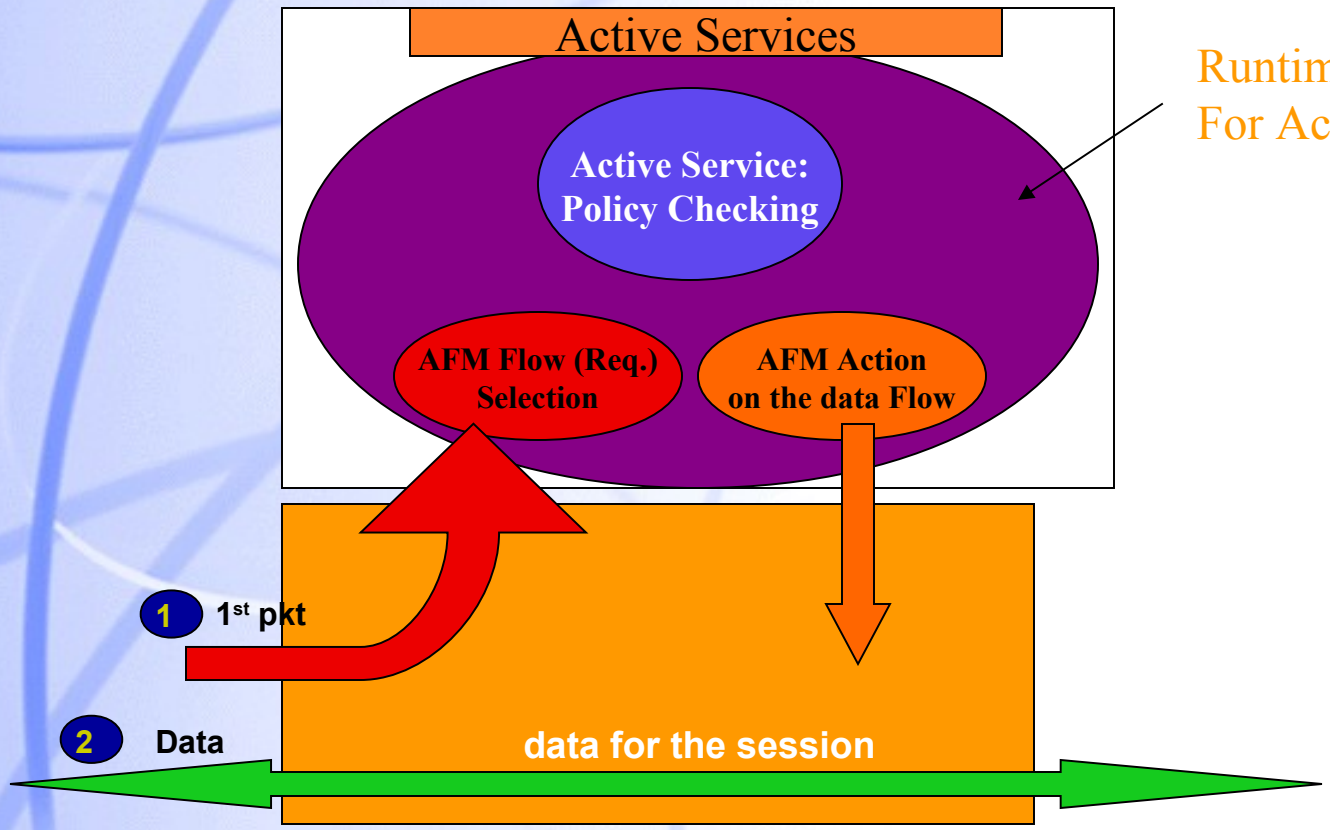
- **Practical Active Services Architecture on real network device.**
- **Commercial Active Services platform.**
  - ASF - Product
  - SSL – Product
  - Open Active Architecture for more product
  - Alteon+iSD as a research platform
  - L3 programmable routing switch PP8600 – used by research community
  - Photonic Switch – Early prototype
- **Identify Active applications** (more than Ping☺)
  - Active VPN – Carrier A
  - Active fault diagnostic – Carrier A
  - Active SLA reliability
  - Active Extranet on Demand – CeNTIE- Media post production industry
  - Early stages in disaster recovery and fault tolerant networks

Strong computation power inside network device.

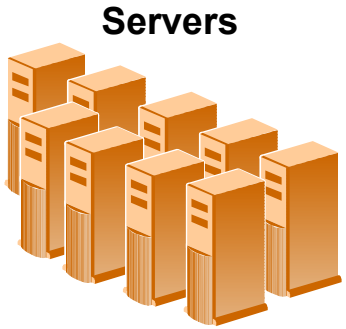


The emphasis is on interception and processing transparently. Entities at both ends may not be aware of the existence of the Alteon in the path

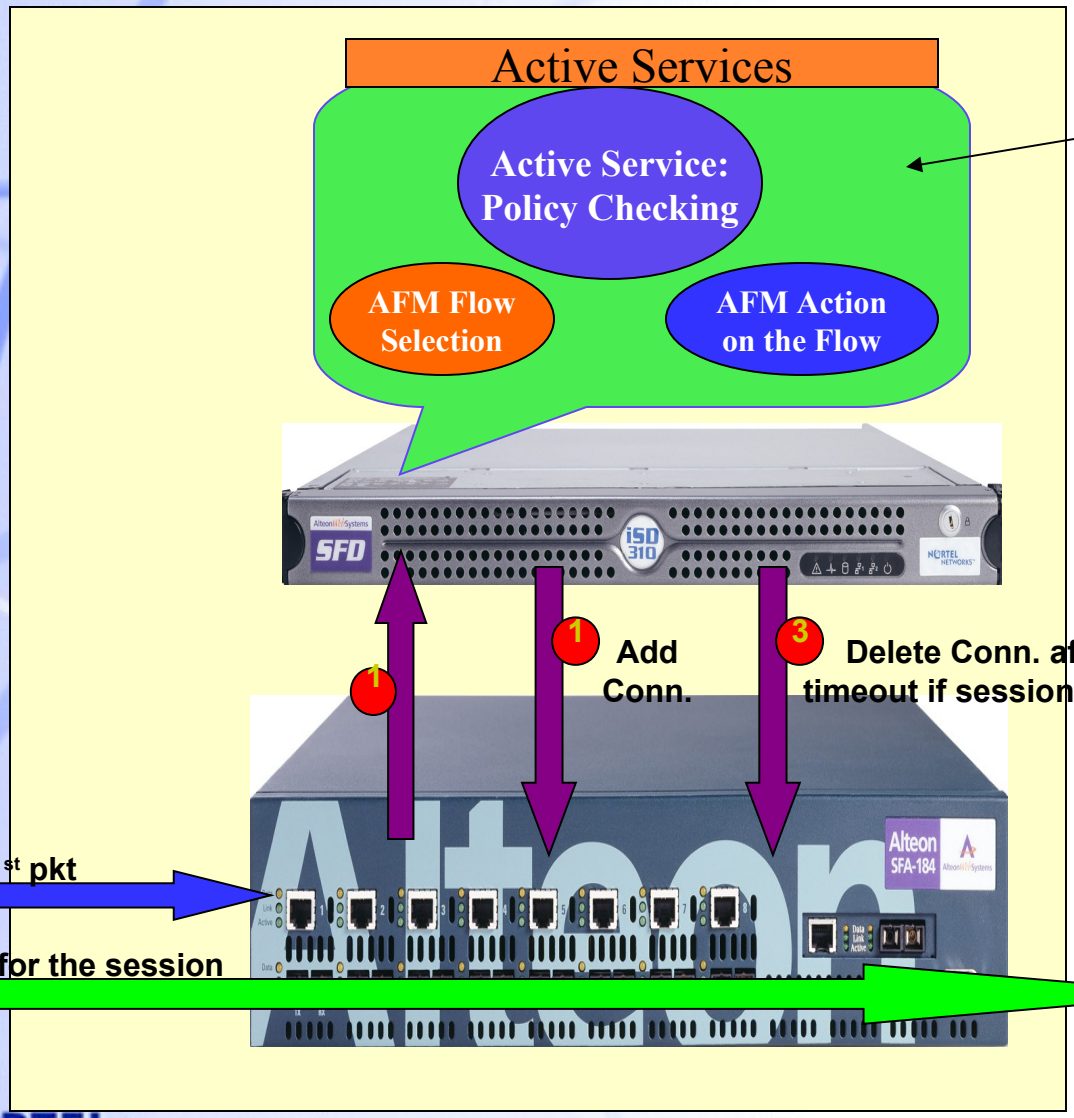
Alteon Switched Firewall (ASF)
A Real Product



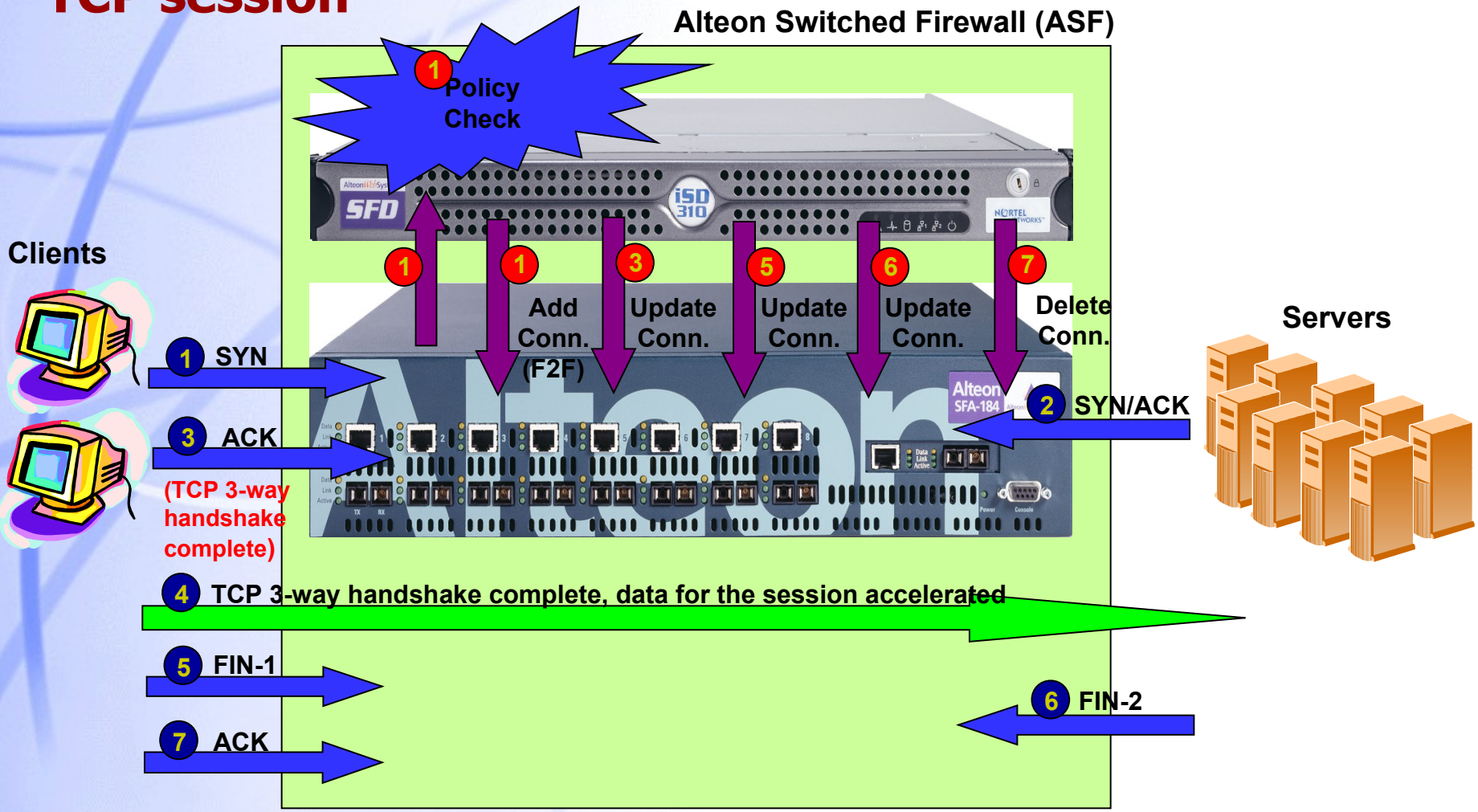
Runtime Environment
For Active Services



Alteon Switched Firewall (ASF)
A Real Product



Secure XL & NAAP in Action
TCP session

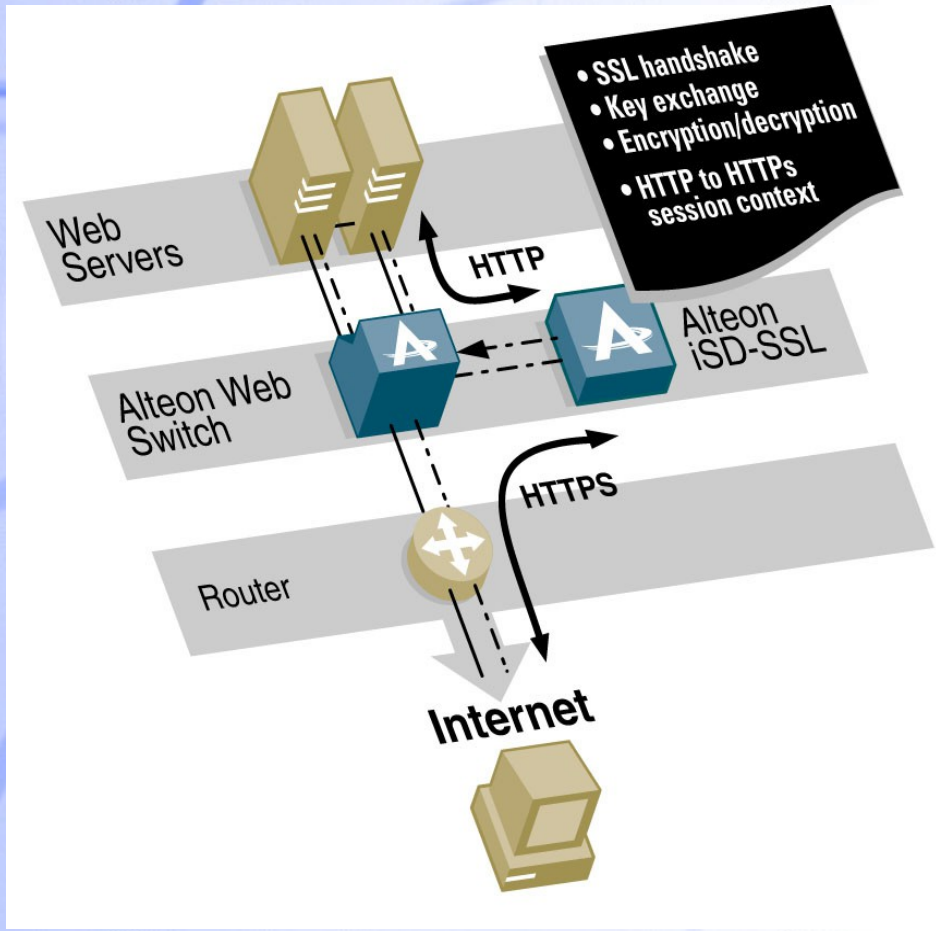


ASF as an Active Service Technology

- The Alteon selectively redirects new connection requests to the Alteon Switched Firewall Director to perform policy checking.
- The Director runs the Check Point FireWall-1 engine as an Active Service.
- The Active Service manages the connection table, specifies rules for handling packets in the session, passes the connection table to the Alteon Switched Accelerator.
- 90% of traffic is accelerated, supporting a throughput of 3.2 Gbps.

SSL Acceleration

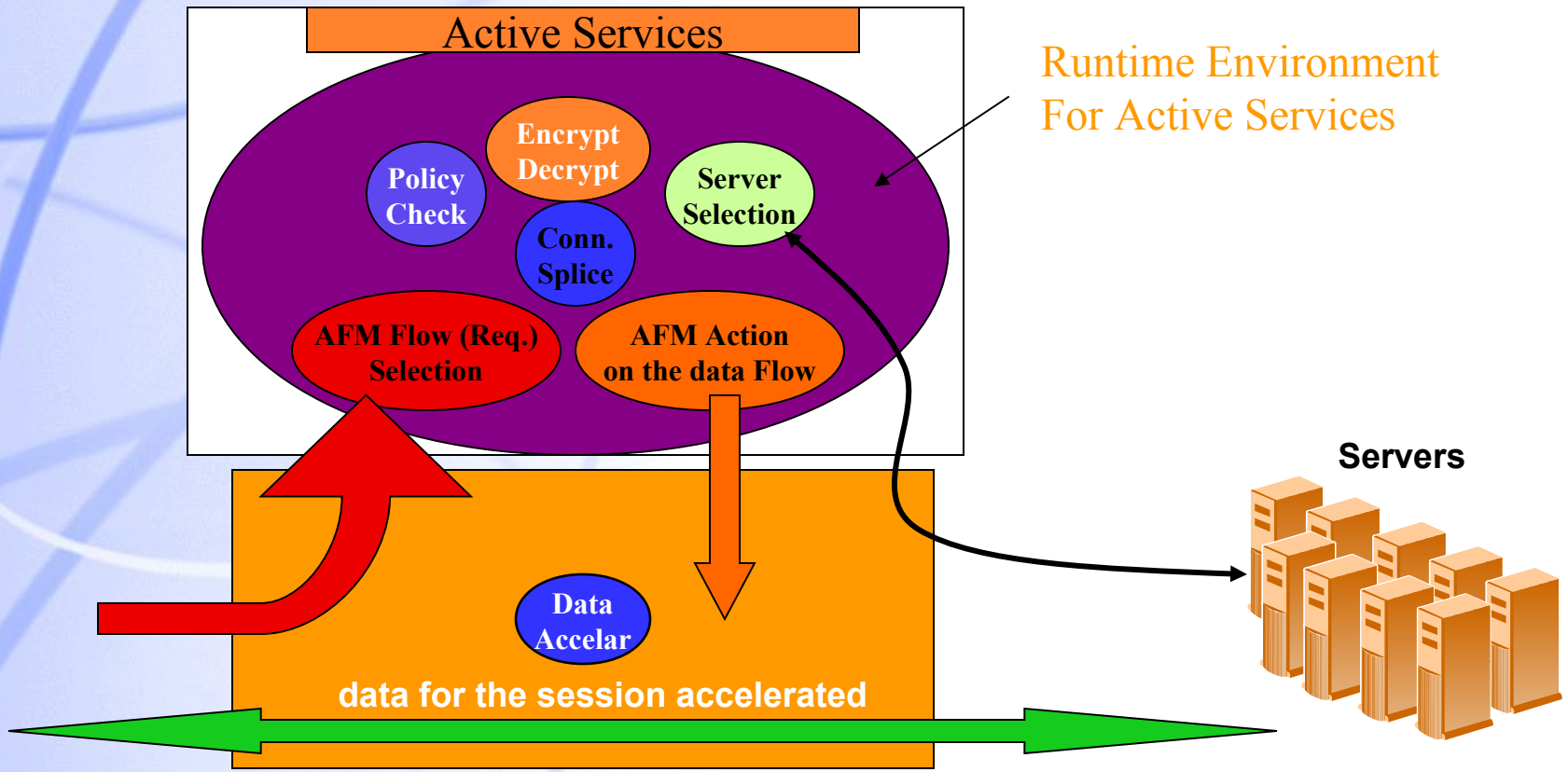
How Does the iSD-SSL Accelerator work?



- **Client sends an HTTPS request**
- **Switch redirects request on port 443 to iSD-SSL**
- **iSD-SSL completes SSL handshake**
- **iSD-SSL initiates HTTP connection to server on port 80**
- **Switch selects real server based on configured LB policy**
- **Server responds to HTTP request and replies to the iSD-SSL**
- **iSD-SSL encrypts session and sends HTTPS response to client**

HTTPS, SMTP-S, POP3-S and IMAP-S services

SSL Acceleration Cont



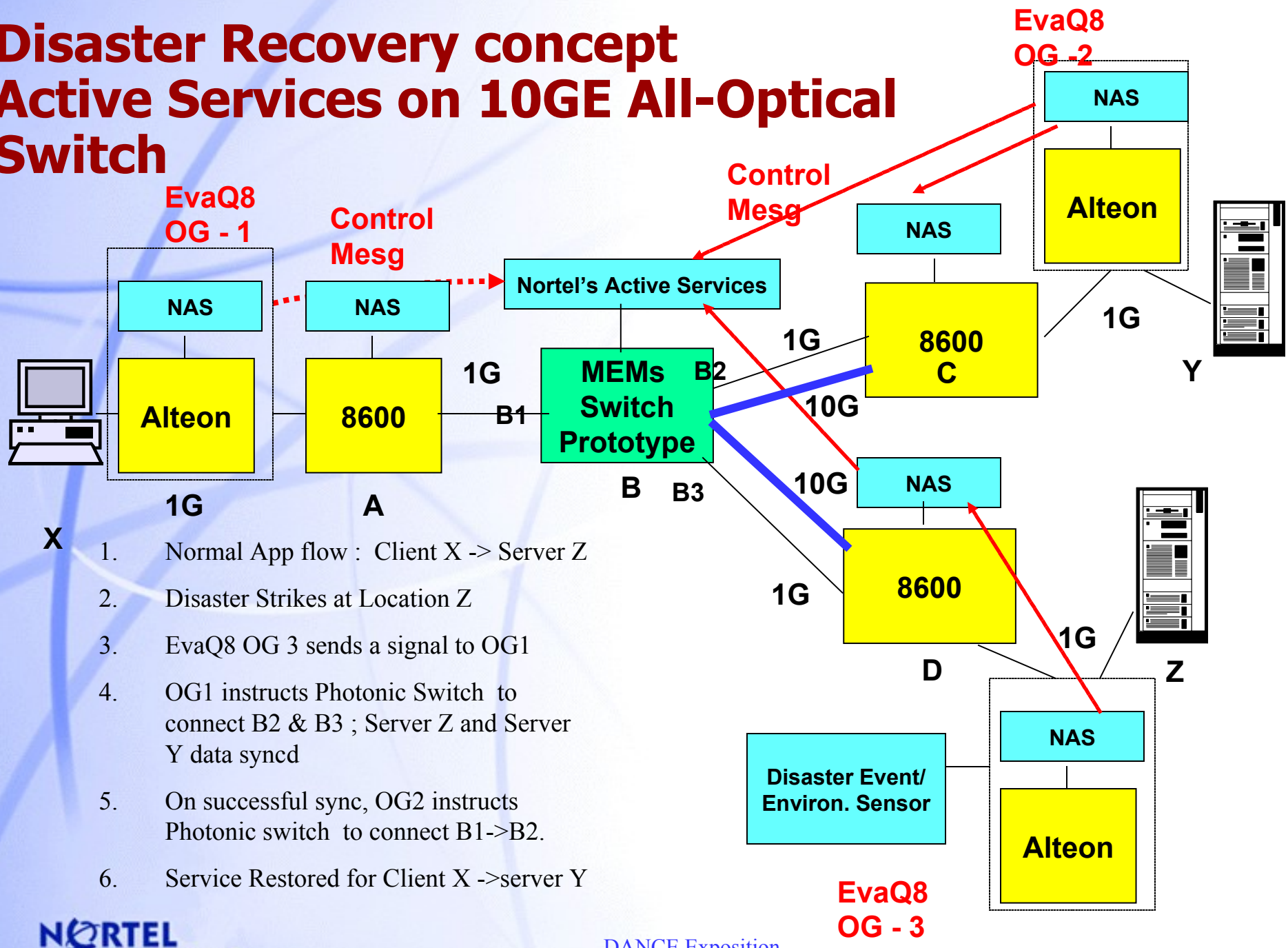
Active Services: Surviving Disasters

Active Service Creation: With the right service platform and APIs, we were able to set the prototype in just few weeks

When a disaster strikes, there are a few seconds left to evacuate any and all data out of the disaster area. A huge bolus of data drops unannounced at the network edge

- **Data Evacuation**
  - Data collection (e.g., data since last backup, sensor data, top-secret data)
  - Automated network setup and data transport
    - Disaster sensor acts as service trigger
    - Policy elements (e.g., what, where to)
    - Secure data carriage
  - Active control of both legacy and optical networks
    - Cannot have all circuits to all potential disaster areas pinned all the time!
    - Fast route setup, end-to-end. Bandwidth on demand
    - Secure access to exclusive high-priority service (akin to GETS in telephony)
- **Data Recovery**
  - Service restoration from the safe site
  - Active control of both optical and legacy networks
    - Fast re-route setup
    - Bandwidth and priority

Disaster Recovery concept Active Services on 10GE All-Optical Switch



1. Normal App flow : Client X -> Server Z
2. Disaster Strikes at Location Z
3. EvaQ8 OG 3 sends a signal to OG1
4. OG1 instructs Photonic Switch to connect B2 & B3 ; Server Z and Server Y data syncd
5. On successful sync, OG2 instructs Photonic switch to connect B1->B2.
6. Service Restored for Client X ->server Y

AN Collaboration: CeNTIE – CSRIO- Nortel

Center for Networking Technologies for Information Economy (CeNTIE) - a CSIRO-led consortium including Nortel Networks, Amcom Telecommunications, the UNSW, UTS and the WA Interactive Virtual Environments Centre (IVEC).
www.centie.net

Tele-Health Focus Group

- Royal Australian College of Surgeons
- Medic Vision
- University of Sydney
- NSW Health
- Royal Prince Alfred
- Interactive Virtual Environment Centre (IVEC).
- Centre for Medical and Surgical Skills (CTEC).

Media Systems Focus Group

- **Fox Studios**
- **Animal Logic**
- **GMD**
- **Film Industry Broadband Resource**
- Ambience
- Enterprise (FIBRE)
- WAM!NET
- Australian Broadcasting Corporation (ABC)
- ScreenWest

Summary of Our Work

- We have inspired ourselves to active networks concepts
- **Capable of dynamic monitoring, controlling and modification of ASICs and MEMs**
- Demonstrate Active Networks technology transfer through Nortel Active Services platform.
- We have implemented programmable Gigabit Routing Switch (backplane 256 Gbs)
  - New Active Services platform: Openet + Alteon + iSD
- Active Services in the control plane (slows down in the data plane)
  - AFM abstraction
- The granularity is streams and not packets
  - Short time granularity (part of apps and not human intervention, keyboard, telnet, cli, snmp)

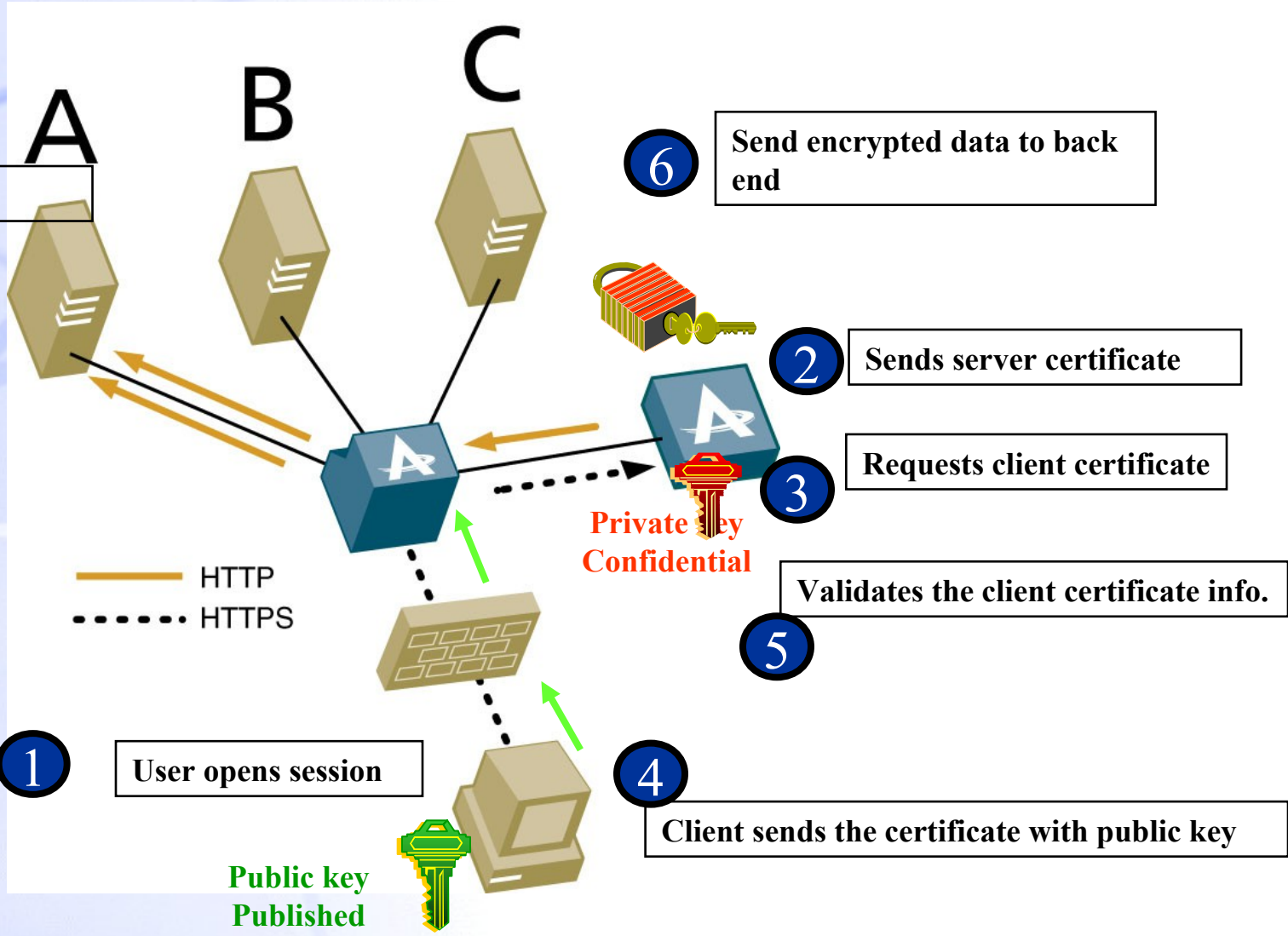
Summary of Our Our Work (cont.)

- **Enabling New Types of intelligence on programmable network device to handle Infinite Bandwidth resources, Wire speed routing capability, and nontrivial Streaming media application.**

OpenetLab – Nortel Networks: http://www.openetlab.org/

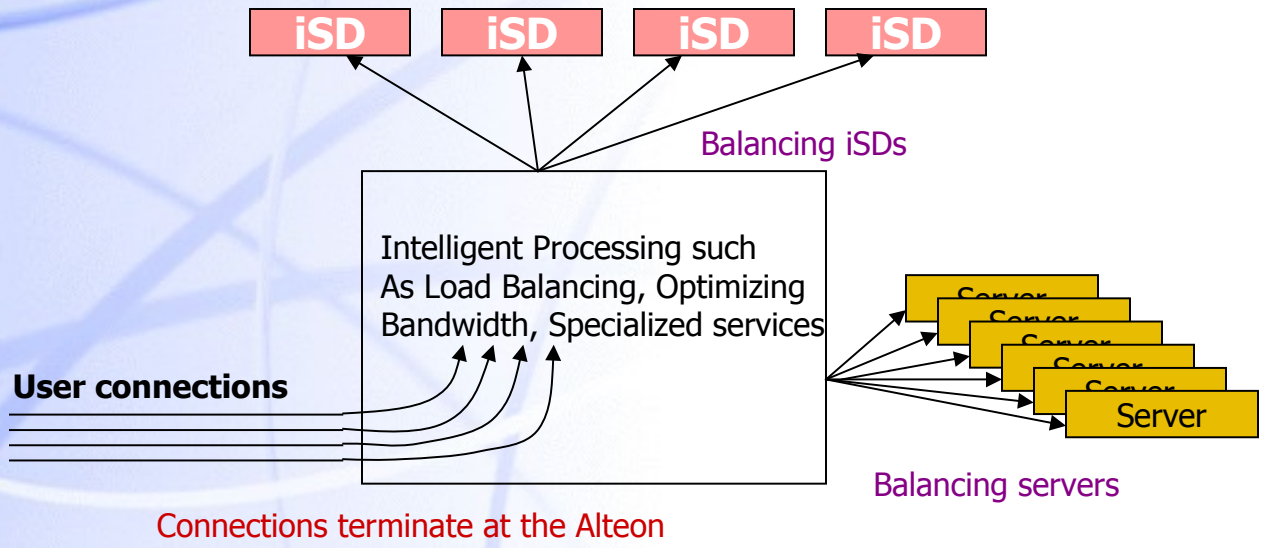
Q&A

Client And Server Authentication



Strong computation power inside network device.

Load balance of iSDs (and servers)



Balancing can be based on

- **load, or**
- **Functionality**

Powerful generic processors do not have the filtering capability of the Alteon. That is if they have to do the same thing as the Alteons, they have to do filtering in software, hence slow.

- **An API is needed for exploring this filtering capacity**

Content Re-route

- **Resource optimization (route 2)**
  - Alternative lightpath
- **Route to mirror sites (route 3)**
  - Lightpath setup failed
  - Load balancing
  - Long response time
    - Congestion
    - Fault