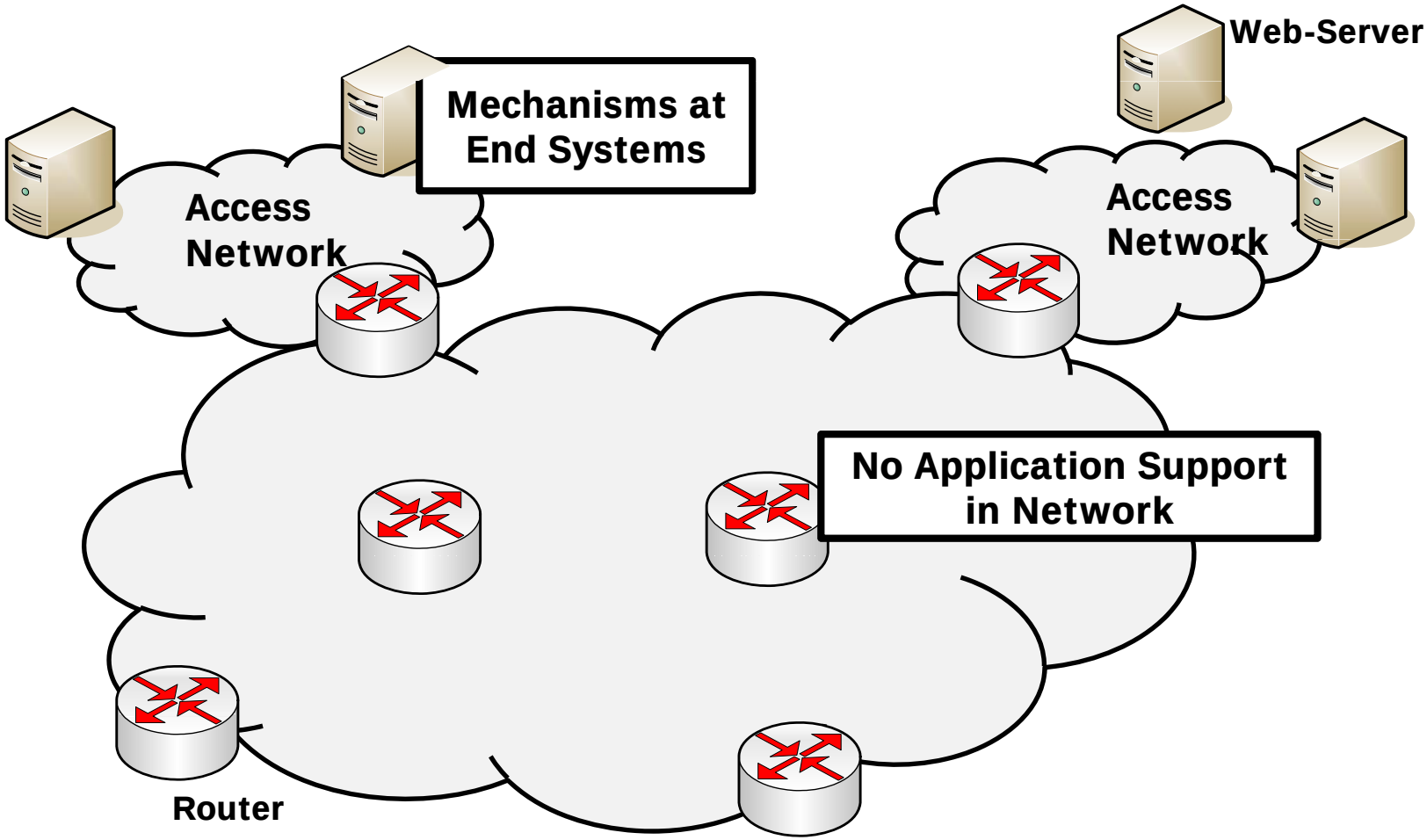
Presentation and Demo:

Flow Valuations based on Network-Service Cooperation

Tanja Zseby, Thomas Hirsch
Competence Center Network Research
Fraunhofer Institute FOKUS, Berlin, Germany

Today: End-to-End Principle



Internet Problems

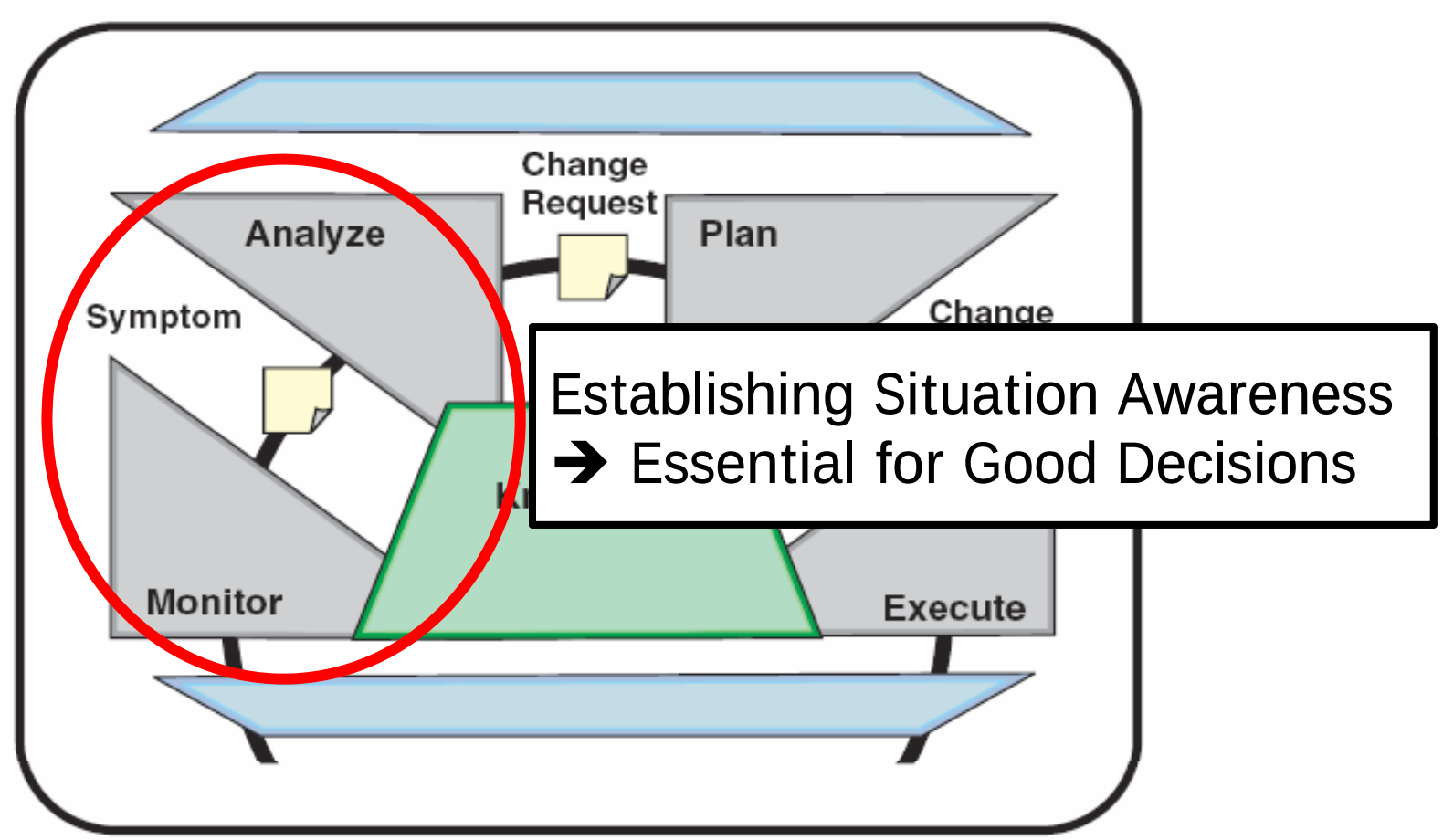
- Security Threats
  - Immense monetary loss
  - Fast adapting attack patterns
- Management costs
  - Increasing network size
  - Increasing heterogeneity (technical, administrative)
- Lack of support for users and applications
  - Quality, security levels, route options, privacy, etc.

Reconsider Internet Design Principles

The Idea of Autonomic Networking

- Bring ***decision cycles*** in network nodes
  - Establish situation awareness
  - Enable decision processes beyond routing
- Objectives:
  - Support for Applications in the network
    - Flexible levels for quality, security, etc.
  - Self-Management
    - Reduction of human intervention
  - Self-Protection
    - Protection of network and applications

Decision Cycle

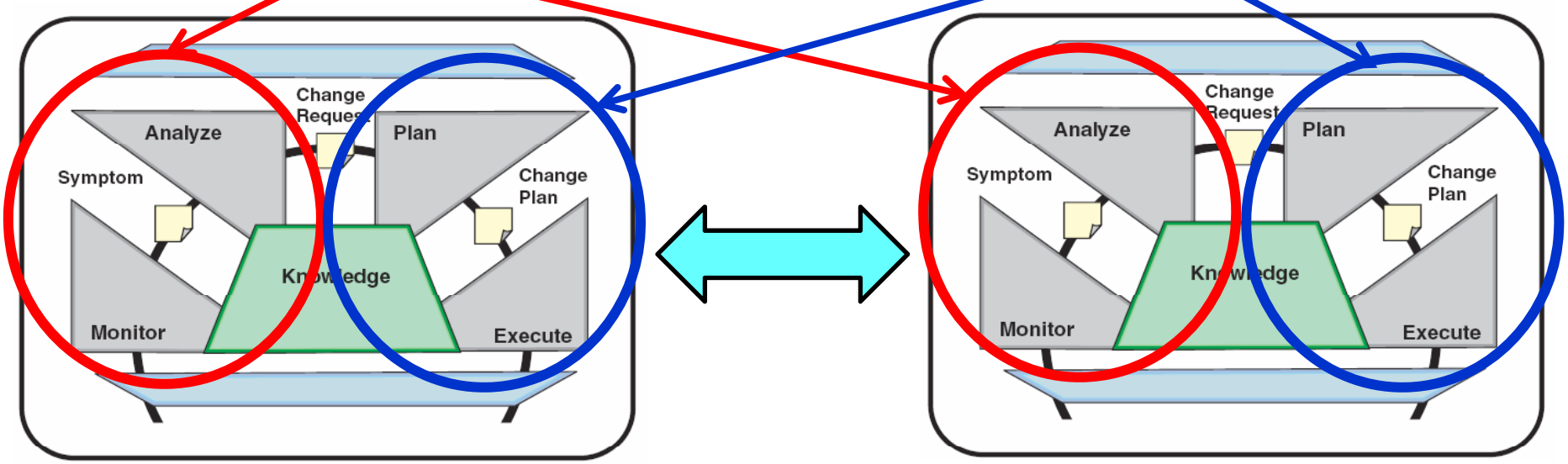


Autonomic Computing [IBM]: MAPE
Monitor-Analyze-Plan-Execute

Enabler: Node Collaboration

Improve
Situation Awareness

Enforce
Joint Strategy

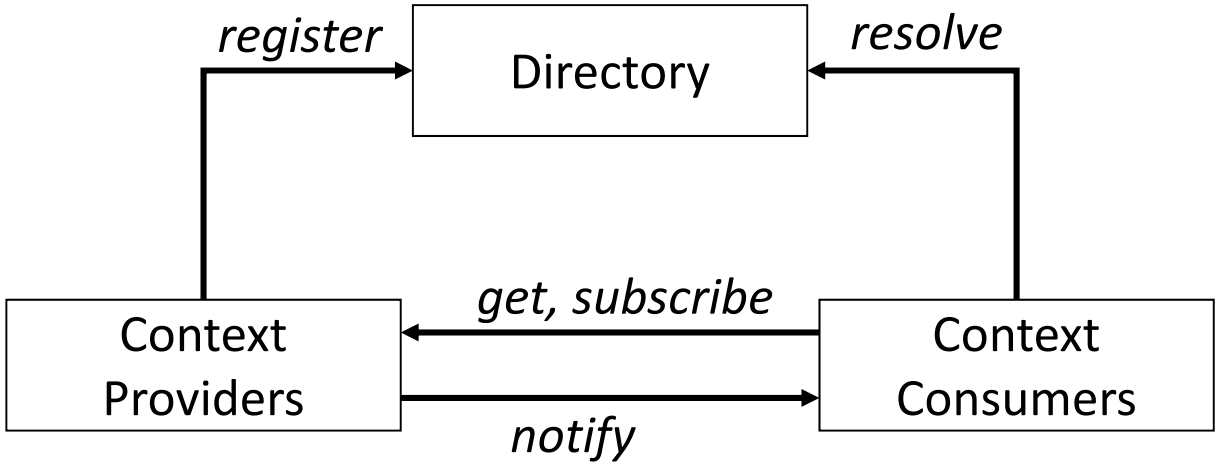


Provide Different Viewpoints

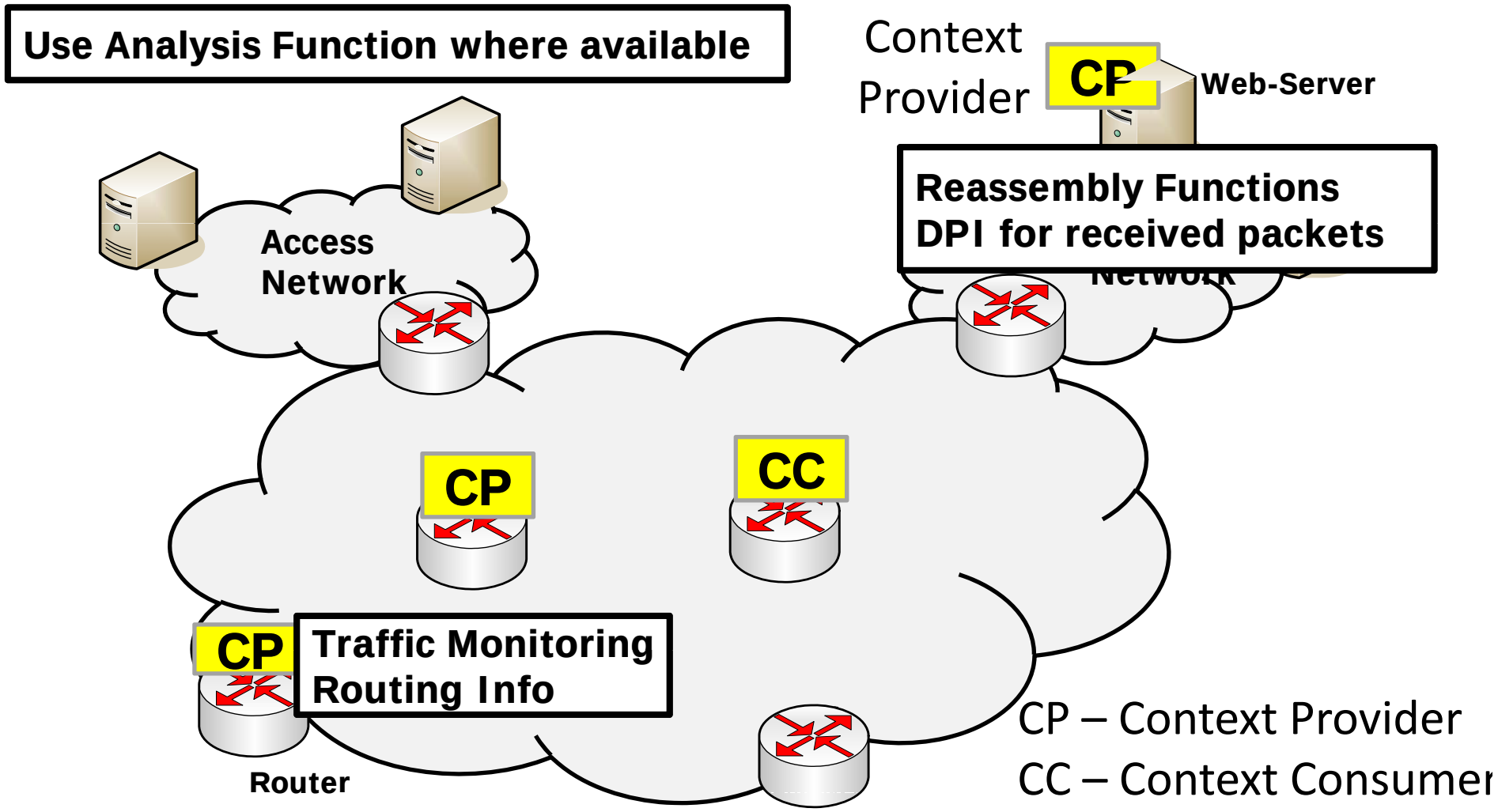
Learn from Others

Node Collaboration System (NCS)

- Nodes that want to collaborate
  - Register with directory
  - Provide location of information they can offer (context provider)
  - Can get location of network information from others (context consumer)



Node Collaboration System

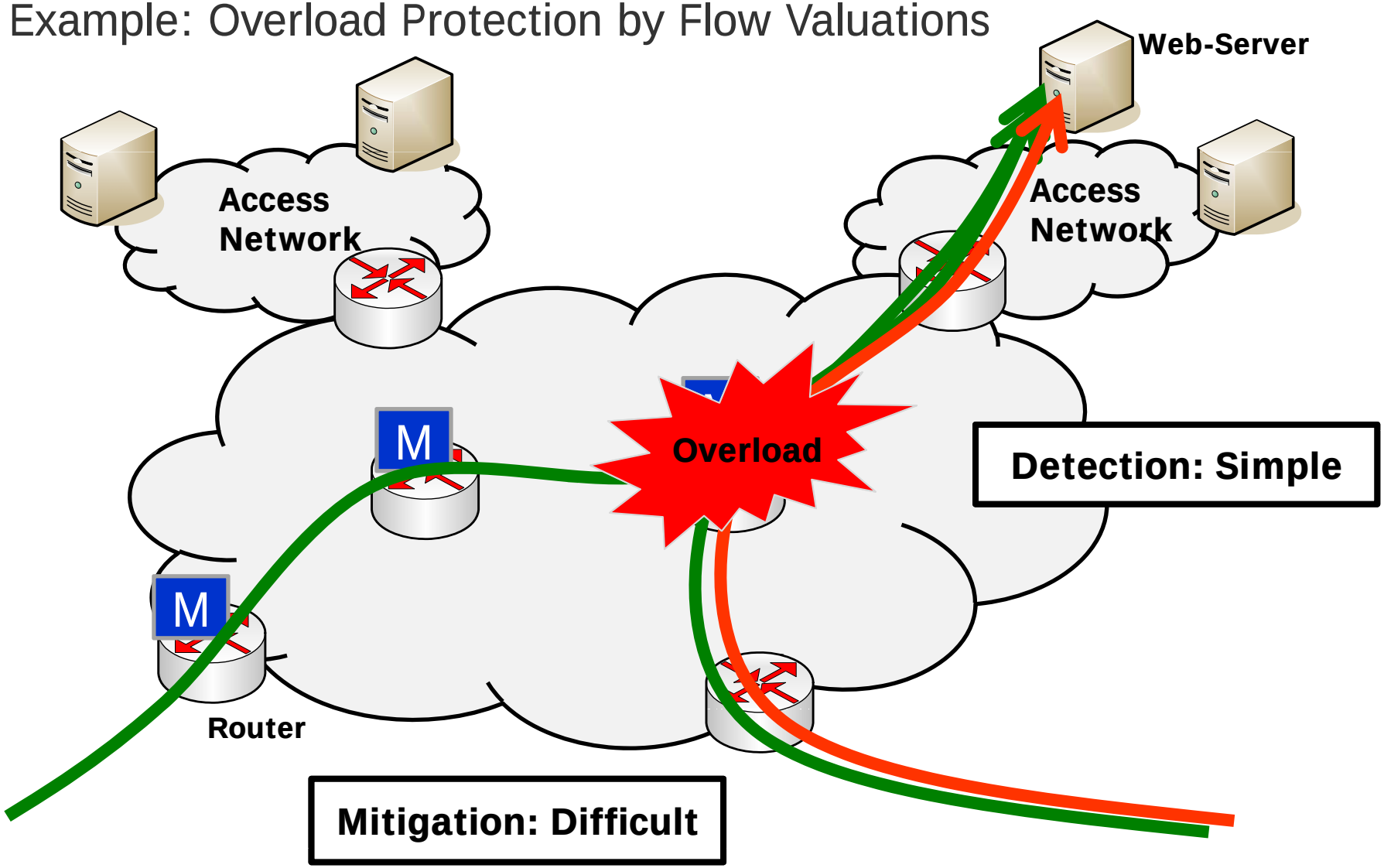


Implementation

- Registration and Resolve
  - HTTP–like Protocol
  - Unified Resource Identifier for addressing info
- Actual Information transfer with different protocols
  - Push (subscribe to CP) or pull (explicitly request info)
  - IP Flow Information Export (IPFIX)
- Additional support for
  - Invoking new measurements
  - Artificial context providers (situation generation for assessing new decision algorithms)

J. Tiemann, D. Witaszek: Context Coordination and Dissemination System – Architecture and Basic Implementation, FOKUS Technical report TR-2008-0303-CCDS-Basics

Example: Overload Protection by Flow Valuations



Objectives

- Protect access links and servers
  - Detect and mitigate overload situations in the Network
  - Mitigate before access or servers are affected
- Reduce collateral damage
  - Important traffic should be protected
  - Unimportant or malicious traffic can/should be filtered
- Mitigation as close to the originator as possible
  - Protect core from unwanted traffic

- Avoid:
  - Providers to decide about importance of traffic (net neutrality)
  - Deep Packet Inspection (high effort)

Challenge

- Overload may be originated by
  - Legitimate traffic (Flash Crowds)
  - Abusive DDoS
- Goal: Reduce traffic to prevent overload
  - Cause may be unknown
  - But: reduce collateral damage

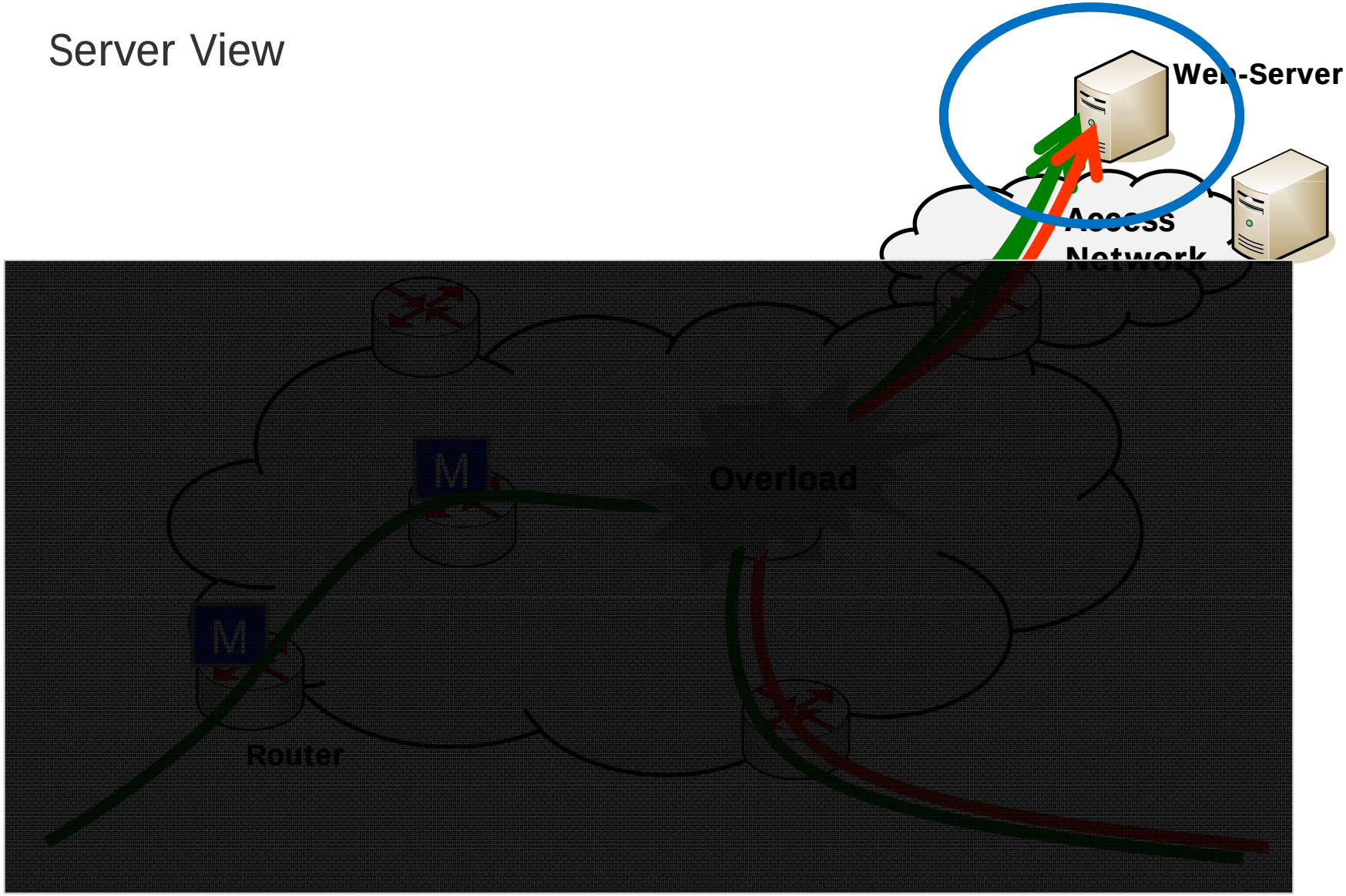
Challenge: Which flows should be blocked?

Conventional Solutions

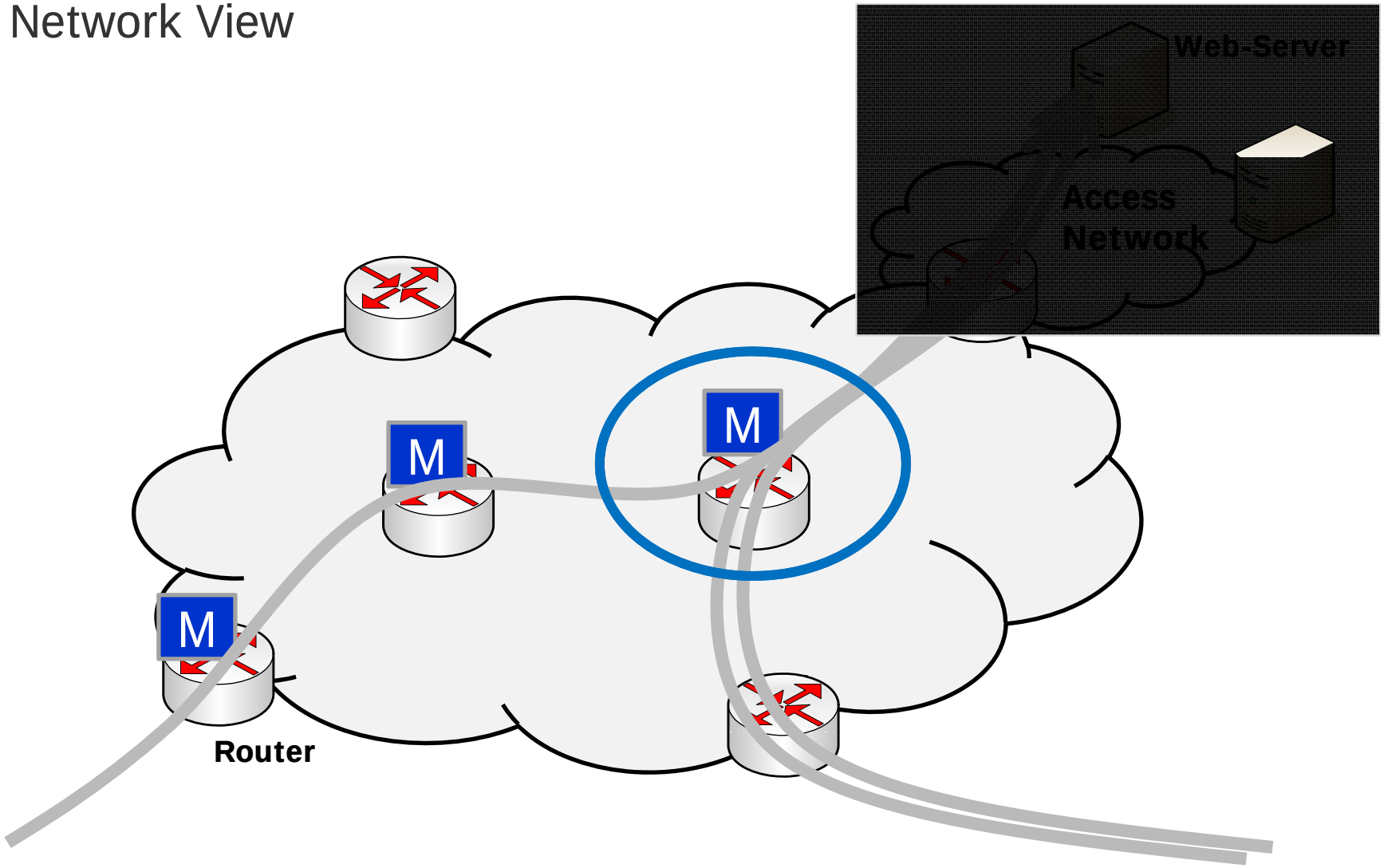
- Random Filtering
  - No separation between good and bad packets
  - Problem: High collateral damage (blocking of legitimate users)
- Intrusion detection systems
  - Attempt to separate good and bad packets by Inspection (DPI)
  - Problem: High Effort in Network

- Alternative: Network-Service Cooperation
  - Cooperate to establish situation awareness
  - Utilize analysis functions at application level
  - Combine information from multiple cooperative sources
  - Combine preferences to form a joint decision

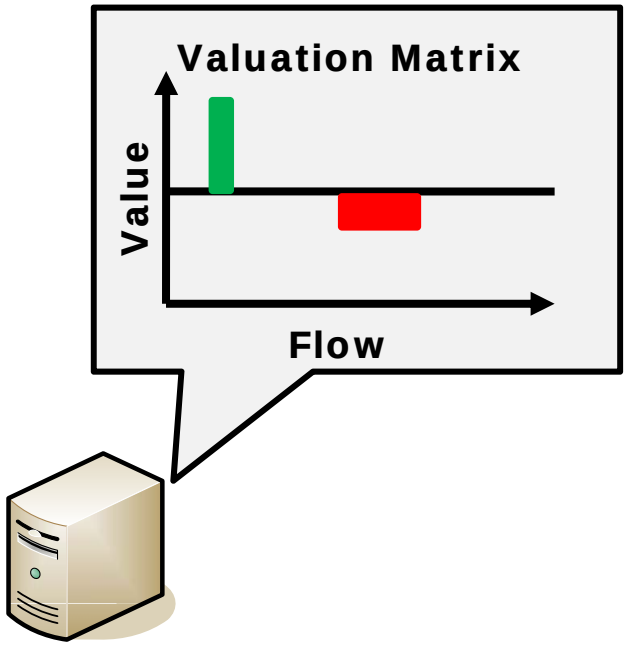
Server View



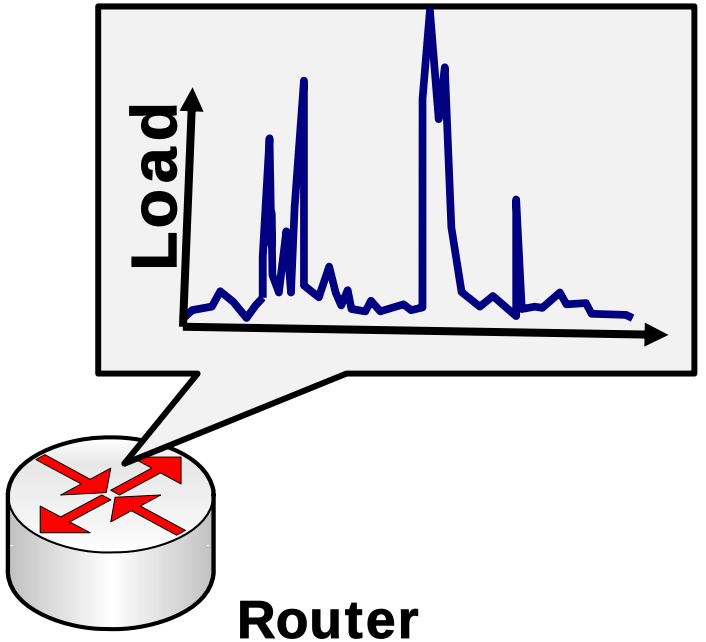
Network View



Approach: Network-Service Cooperation



Server

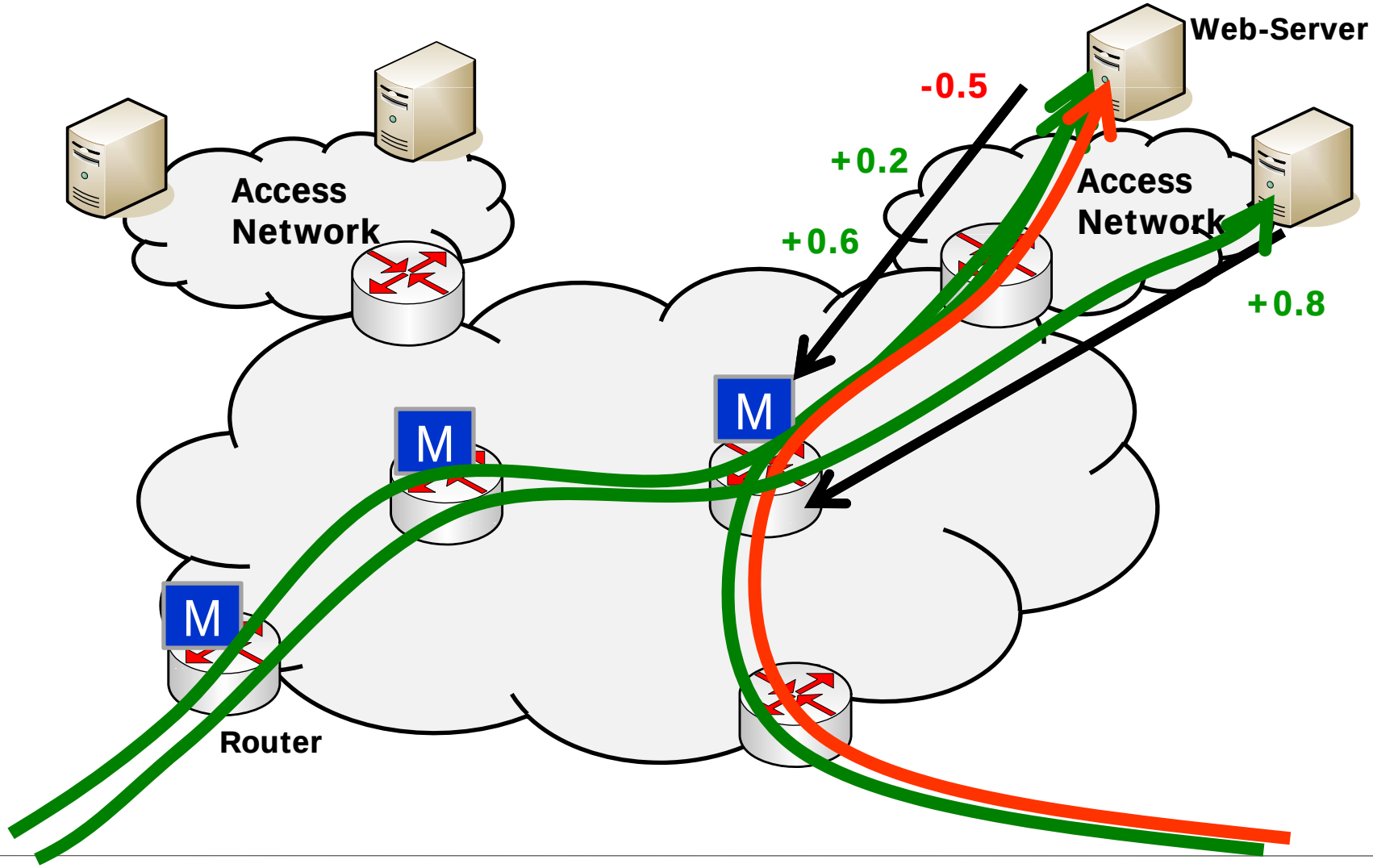


Router

Servers
- know the value of their user traffic

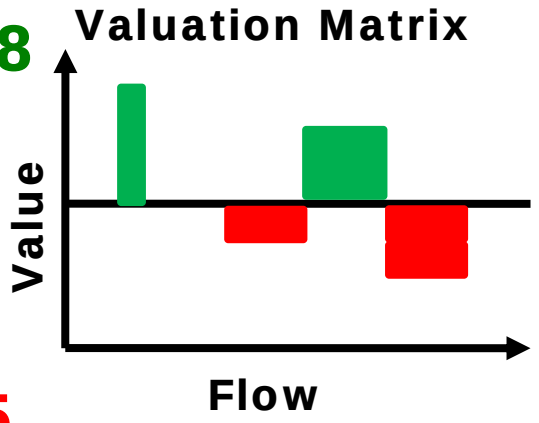
Routers
- Can detect overload
- Can filter before traffic enters access links
- But don’t know the traffic value

Normal Operation: Servers provide Valuation Reports

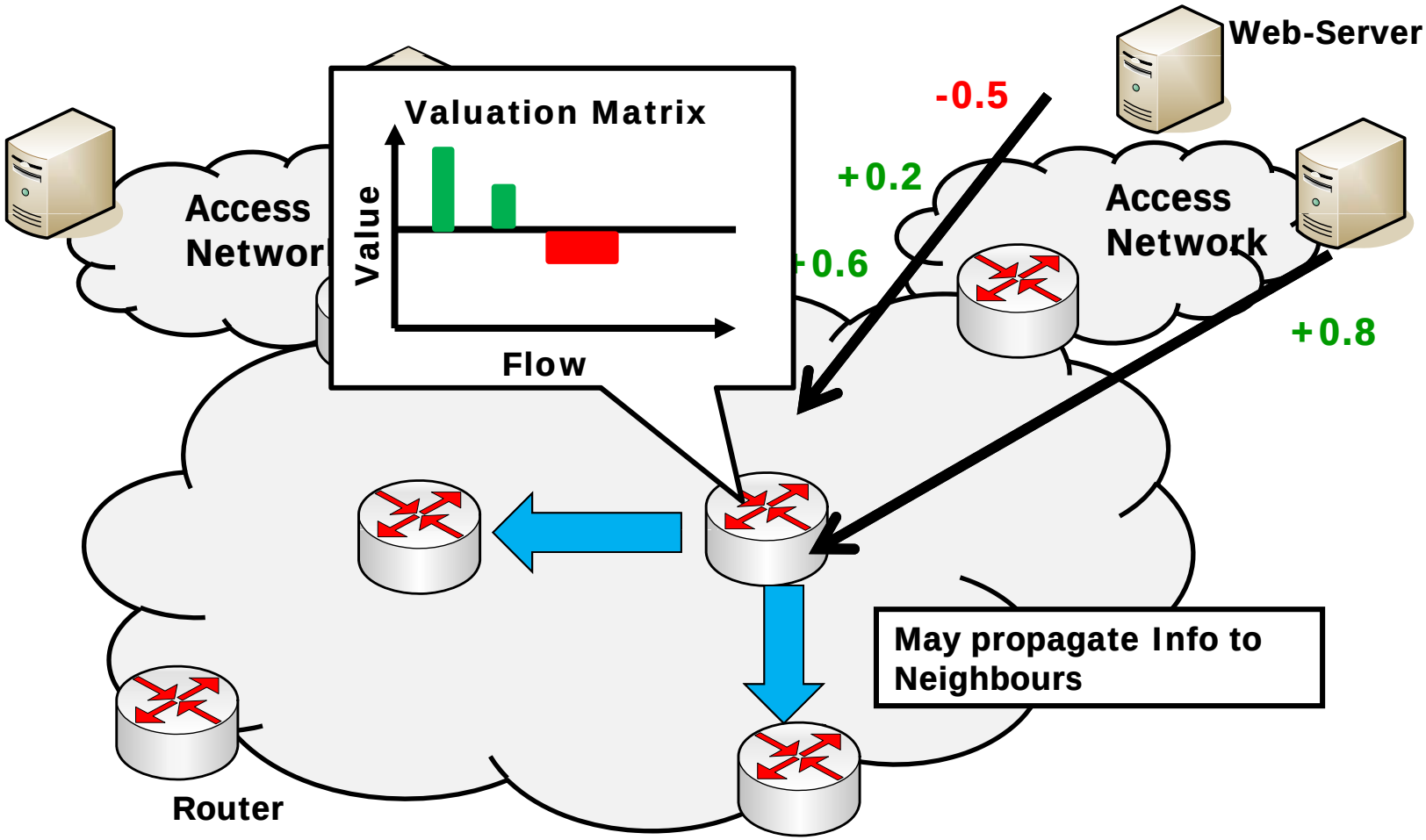


Flow Valuations

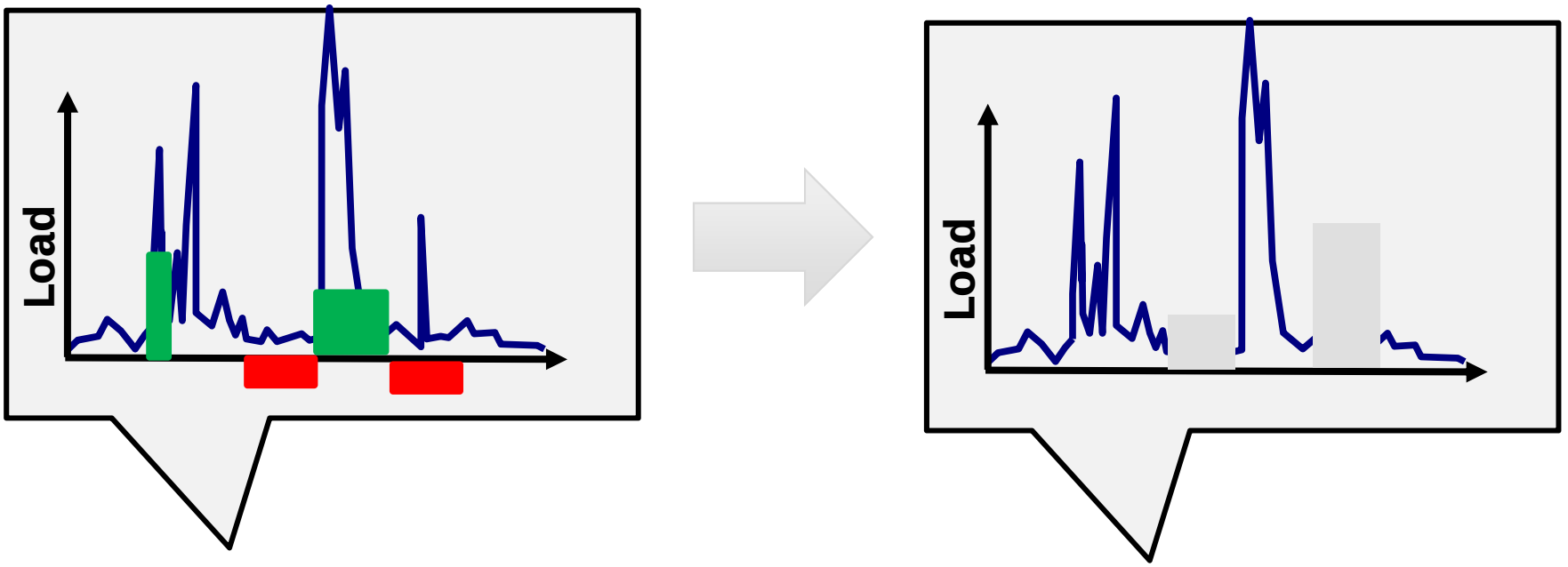
- Assessment of user traffic with simple system
- Example valuations
  - User logged in with password → **+0.8**
  - Regular browsing pattern → **+0.5**
  - Customer completed buying → **+1.0**
  - Failed login attempt → **-0.1**
  - Repeatedly loading single site → **-0.5**
  - Attempt to log into database server → **-0.9**



Normal Operation: Router aggregates Valuations

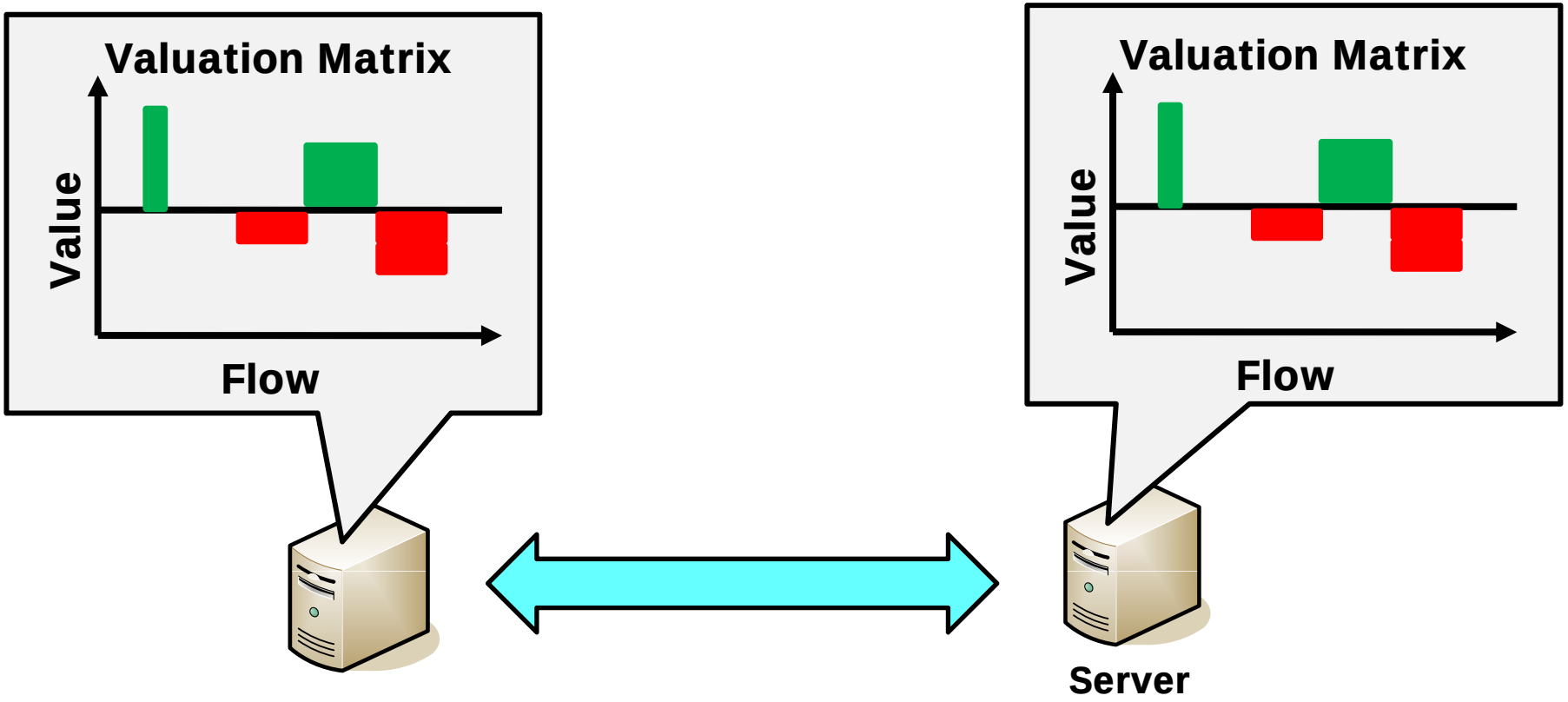


Overload Situation: Correlate Information



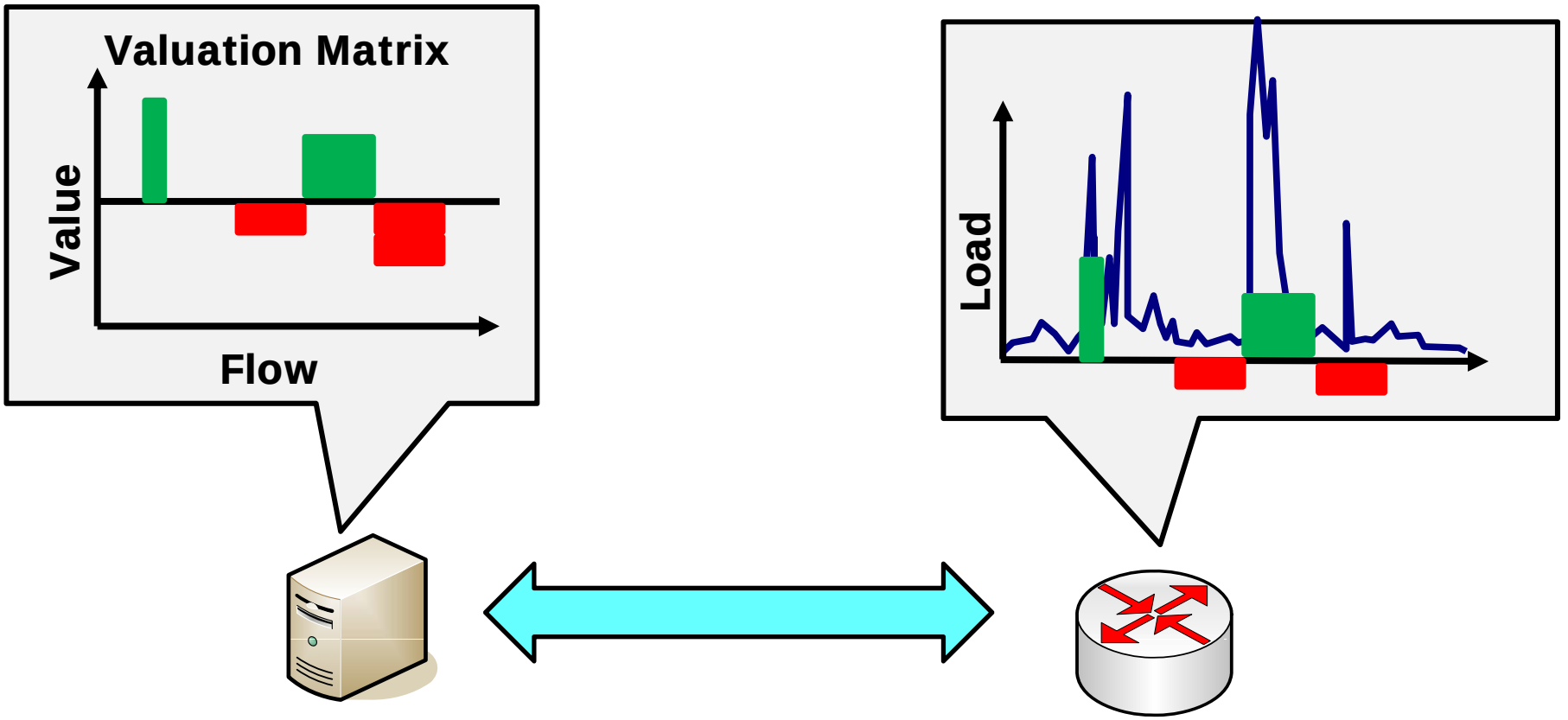
Blocking Decision based on aggregated valuations

Good: Collaboration of Nodes

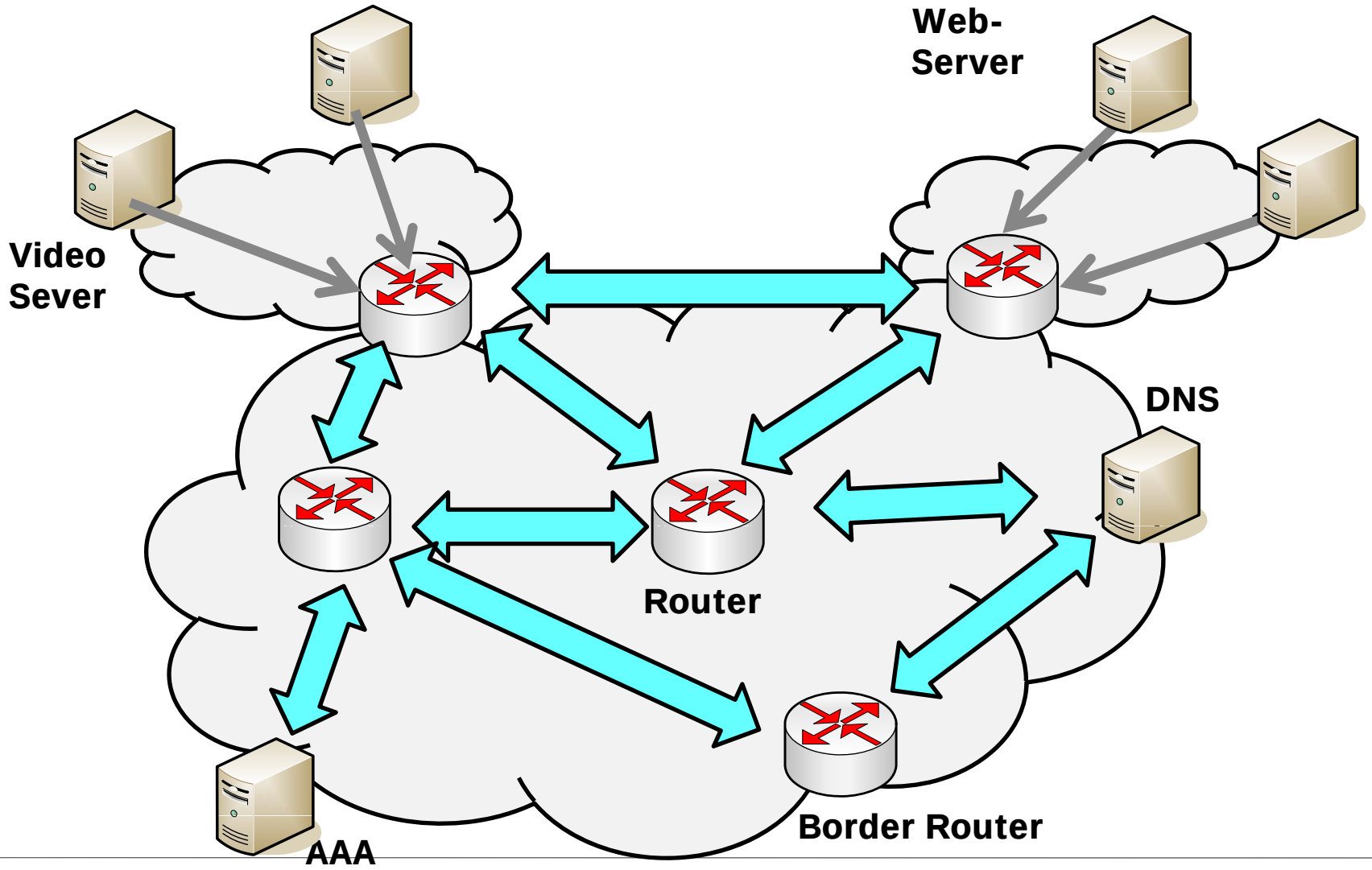


Learn about traffic value

Better: Collaboration of Different Nodes



Unbeatable: A Heterogeneous Collaborative Team



Status and Future Work

- Node Collaboration System for Flow Valuations
  - Implemented on Cisco AXP routers
  - Using IPIFIX for information transfer
- Cooperation Incentives (in progress)
  - Incentives to provide information
  - Inter-domain exchange
- Integration of further sources
  - Information from sophisticated sources (IDS, AAA,...)
  - Worm detection information from enhanced DNS

Thank You!

Contact: *tanja.zseby@fokus.fraunhofer.de*

Fraunhofer FOKUS