HELSINKI UNIVERSITY OF TECHNOLOGY

Measurement based policy creation

10.12.2002 Mika Ilvesmäki

Networking laboratory

Contents

- Policy system framework and terminology
- Users or network
  - who decides about policy
- Classification
  - what info binds the packet to the policy?
- What to measure in a network to characterize applications?
- Flow analysis
- Case: Measurement based policy creation

Traffic management

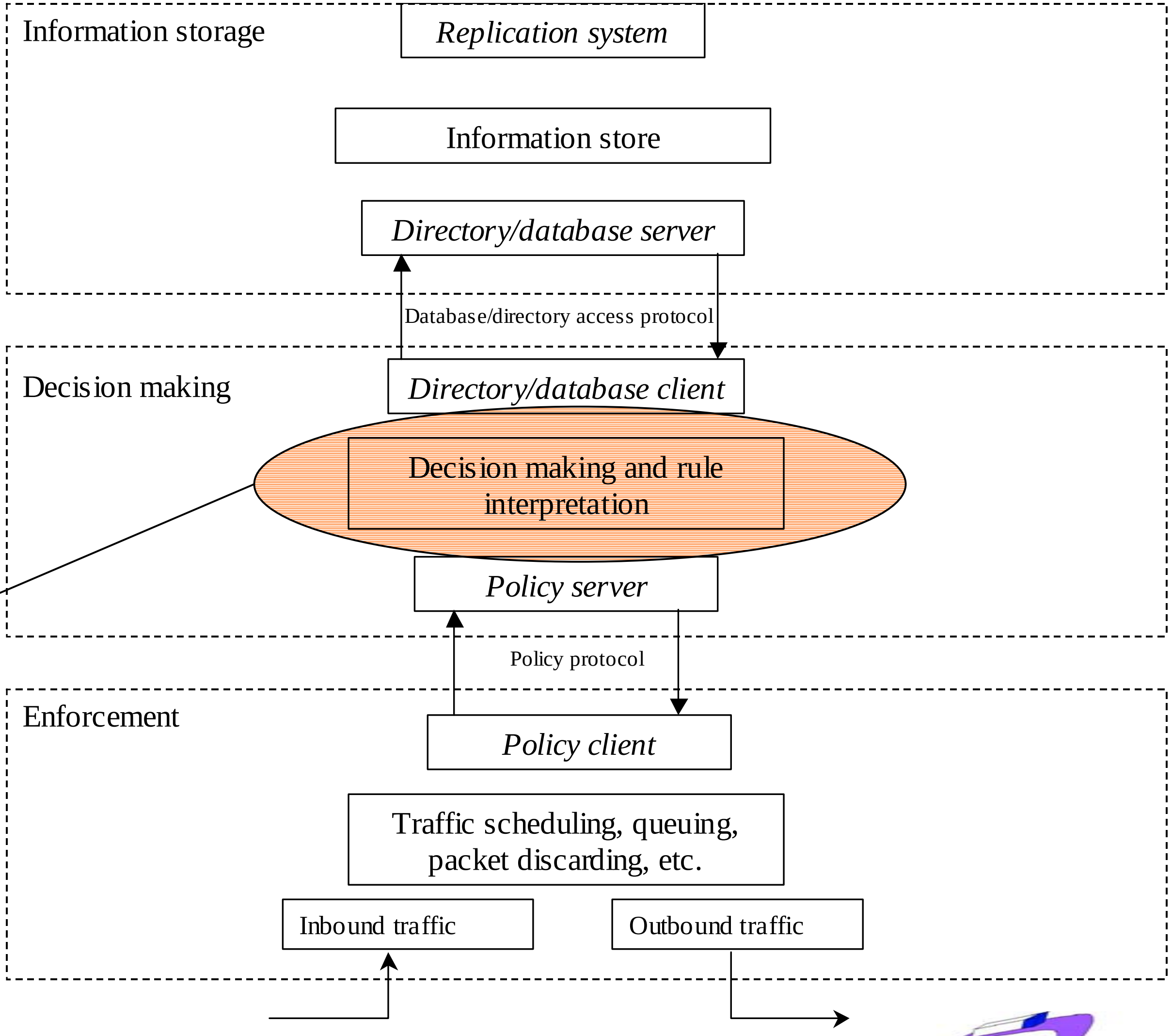
- TM systems consist of a set of high-level rules that are propagated out to enforcement points using a policy system
  - Policy must be enforced to ensure that the users are behaving properly
- Network should classify, handle, police and monitor the traffic

Terminology (RFC 3198)

- Policy is either:
  - A definite goal, course or method of action to guide and determine present and future decisions. "Policies" are implemented or executed within a particular context (such as policies defined within a business unit).
  - a set of rules to administer, manage, and control access to network resources [RFC3060].
- Policies are built with policy rules
  - Policy rule is a basic building block of a policy-based system. It is the binding of a set of actions to a set of conditions - where the conditions are evaluated to determine whether the actions are performed [RFC3060].
- Policy condition is usually a filter
  - A set of terms and/or criteria used for the purpose of separating or categorizing. This is accomplished via single- or multi-field matching of traffic header and/or payload data. "Filters" are often manipulated and used in network operation and policy. For example, packet filters specify the criteria for matching a pattern (for example, IP or 802 criteria) to distinguish separable classes of traffic.

Policy system structure

- Policy systems as such are pretty straightforward
  - Policy clients at routers ask the policy parameters from the policy server
  - Policy servers get the policy data from the information store
- Key question rarely given thought: How do you *create* the policy rules and the corresponding actions?
  - Static choices
  - Guesses
  - Dynamically
    - based on what?


Information storage
Replication system
Information store
Directory/database server
Database/directory access protocol
Decision making
Directory/database client
Decision making and rule interpretation
Policy server
Policy protocol
Enforcement
Policy client
Traffic scheduling, queuing, packet discarding, etc.
Inbound traffic
Outbound traffic

Traffic classes

- Based on experience and scalability studies the easiest way to bring service differentiation into the Internet is to use a limited amount of traffic classes (DiffServ).
  - But how many? 2, 3, 8 or more?
- Different traffic classes represent different priority levels
  - How do you know what packets go to which classes?

Network decisions

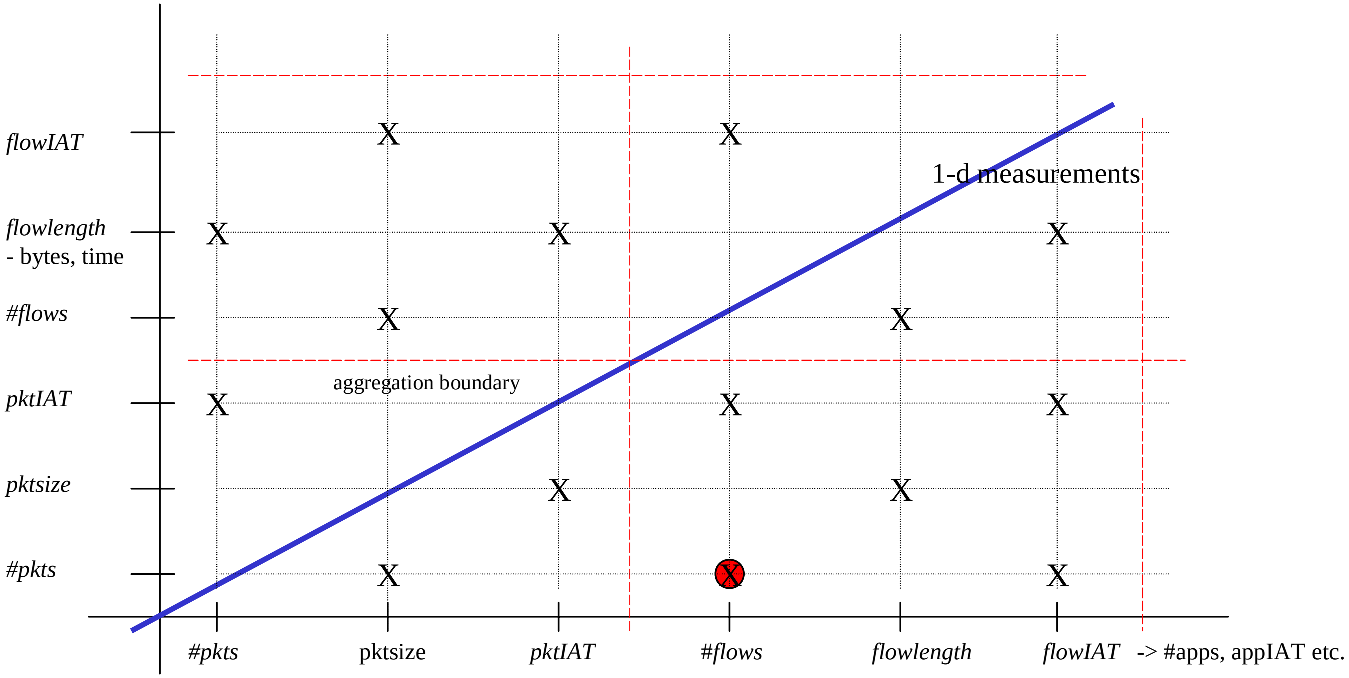
- Network determines the service level (class) of the packet
  - feedback from the use of resources
    - SLAs should not (and do not) promise anything absolute in terms of network service
  - AAA (Authentication, Accounting and Administration) guarantees the service levels to appropriate users
- If network decides individual packet treatment it should know what kind of packet it is classifying
  - This requires knowing the application characteristics
    - by examining the packet headers and/or content
    - by information obtained from other network devices that know the packet’s type

Possibilities of measured properties

- Of any phenomenon one can measure
  - the phenomenon occurence (#pkts)
  - the quantitative measures of the phenomenon (size, length)
  - temporal relations of the phenomena (pktIAT)
    - Grouping the measurements per some field(s) in the packet header (masking) we get packet sets (flows, for instance) that may also be measured etc.
      - #flows, flowIAT, flowLength, flowSize (in bytes)

Increasing the dimensionality of the measurements

- Packet phenomena may be better described if new, preferably orthogonal, measured properties are added
  - However, the curse of dimensionality may follow. Be careful!



Measurement analysis methods

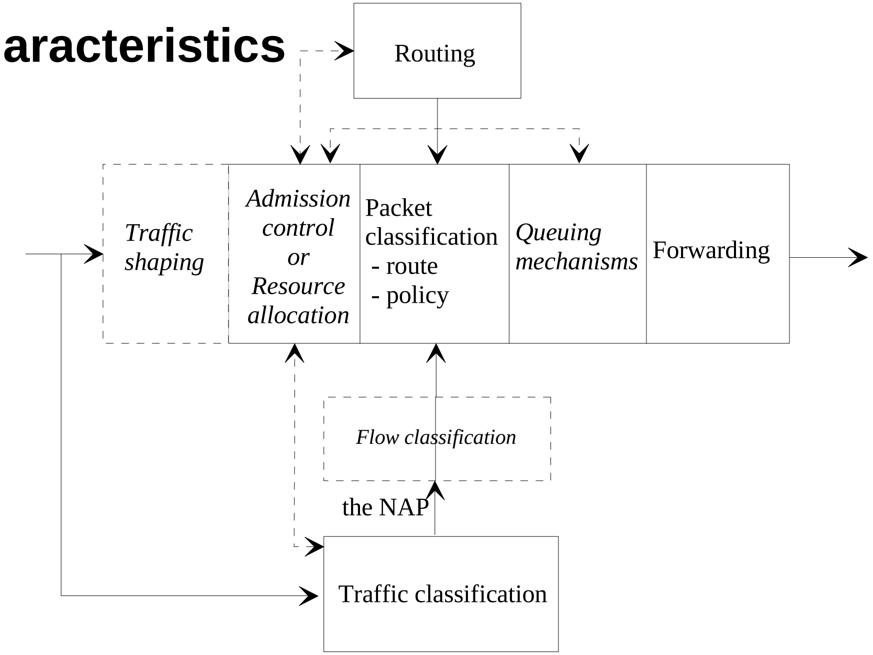
- Measurements may be further analyzed
  - averages, variances etc.
  - distribution modeling
- The measured/analyzed properties may be sorted, or otherwise analyzed against
  - absolute boundaries (particular packet sizes, certain variance limits)
  - each other (all packets smaller/larger than the average packet size are classified/not classified)
- Multidimensional data may be clustered and classified
  - SOM, LVQ (if pre-classified samples are available) and other classification/cluster identification mechanisms

Design guidelines #1, #2 and #3

1. Do not associate port numbers to QoS classes (-> potentially 65535 classes)
   - Analyze traffic, get port number lists and bind the contents of the list to DiffServ Codepoints (DSCP), for instance.
     - Port number have nothing to do with QoS identification whereas DSCP is designed just for that
2. Do not imply policy within design
   - Use as value-neutral design as possible and leave room for freedom of choice
3. Preserve end to end principle: ”If possible do everything at the edges.”
   - Profiling and marking should be done and used at the edges of the network
     - although measurements may, of course, be done anywhere in the network

Measurement based policy creation

- Policy creation supports a QoS capable network
  - It co-exists with other functional blocks in the packet path and its basic task is to:
    provide info on application characteristics



Evaluation of the policy creation system

- Evaluate the network (element)
  - Use of transmission capacity, architecture dependent router resources (connection setup / class, packet forwarding / class etc.)
- Evaluate the effect on user
  - What applications are classified to priority
    - Relevance, application type, application count
    - Stability of the application set

Summary

- Policy is a definite goal, course or method of action to guide and determine present and future decisions in the network.
- As far as packet handling is concerned it might be smart to create policies (semi-) automatically, based on measurements.
- Measurements should be done on the packet level concentrating on the packet header infromation (and arrival information of the packet)
- Analysis of measurements is an upcoming field of research.