NETCONF Access Control

draft-bierman-netconf-access-control-02
IETF 78, July 2010

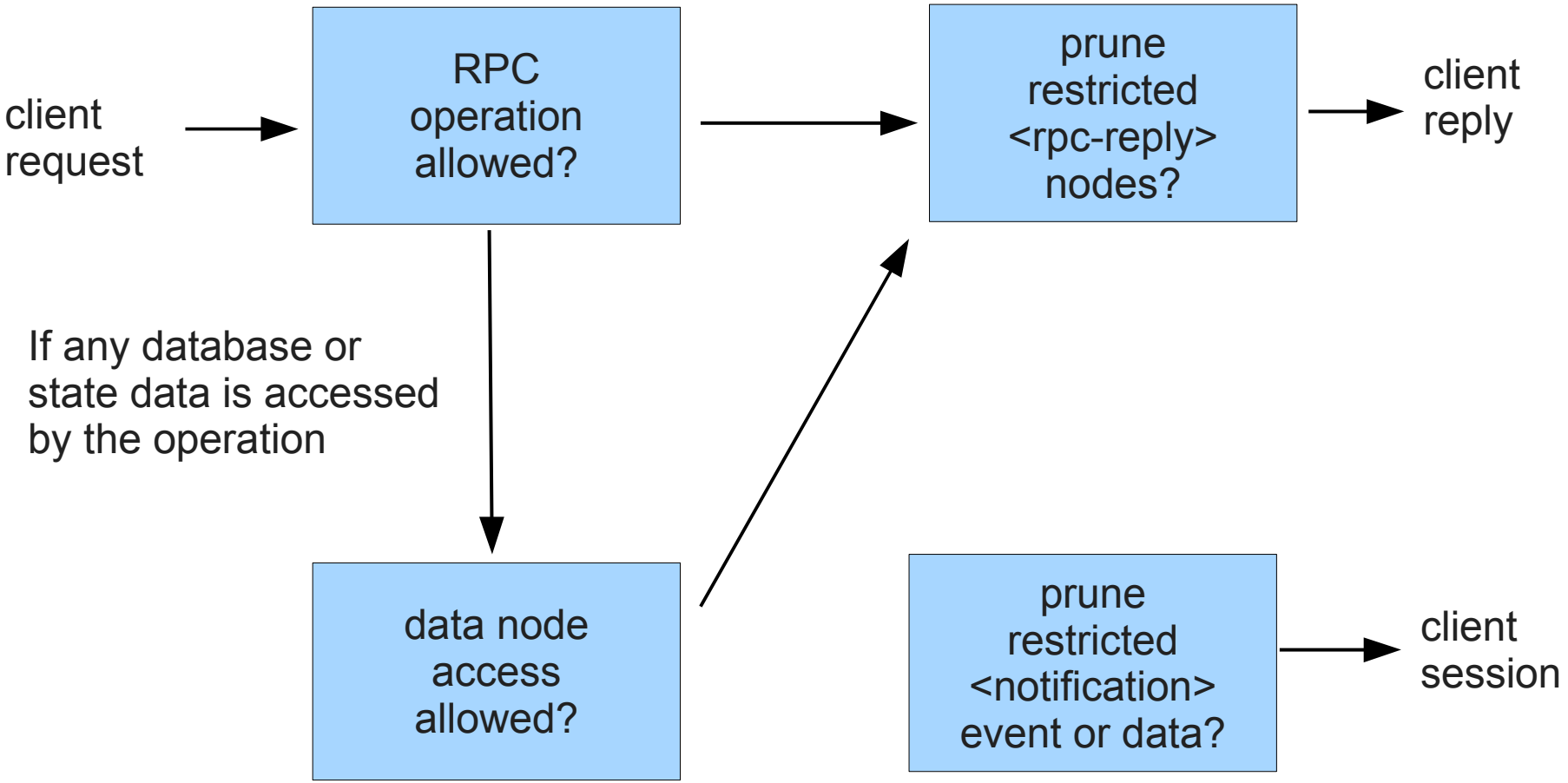
Andy Bierman
ietf@andybierman.com

Martin Bjorklund
mbj@tail-f.com

Agenda

- NACM Overview
- Changes to NACM Data Model
- Proposed Charter Text
- Open Issues

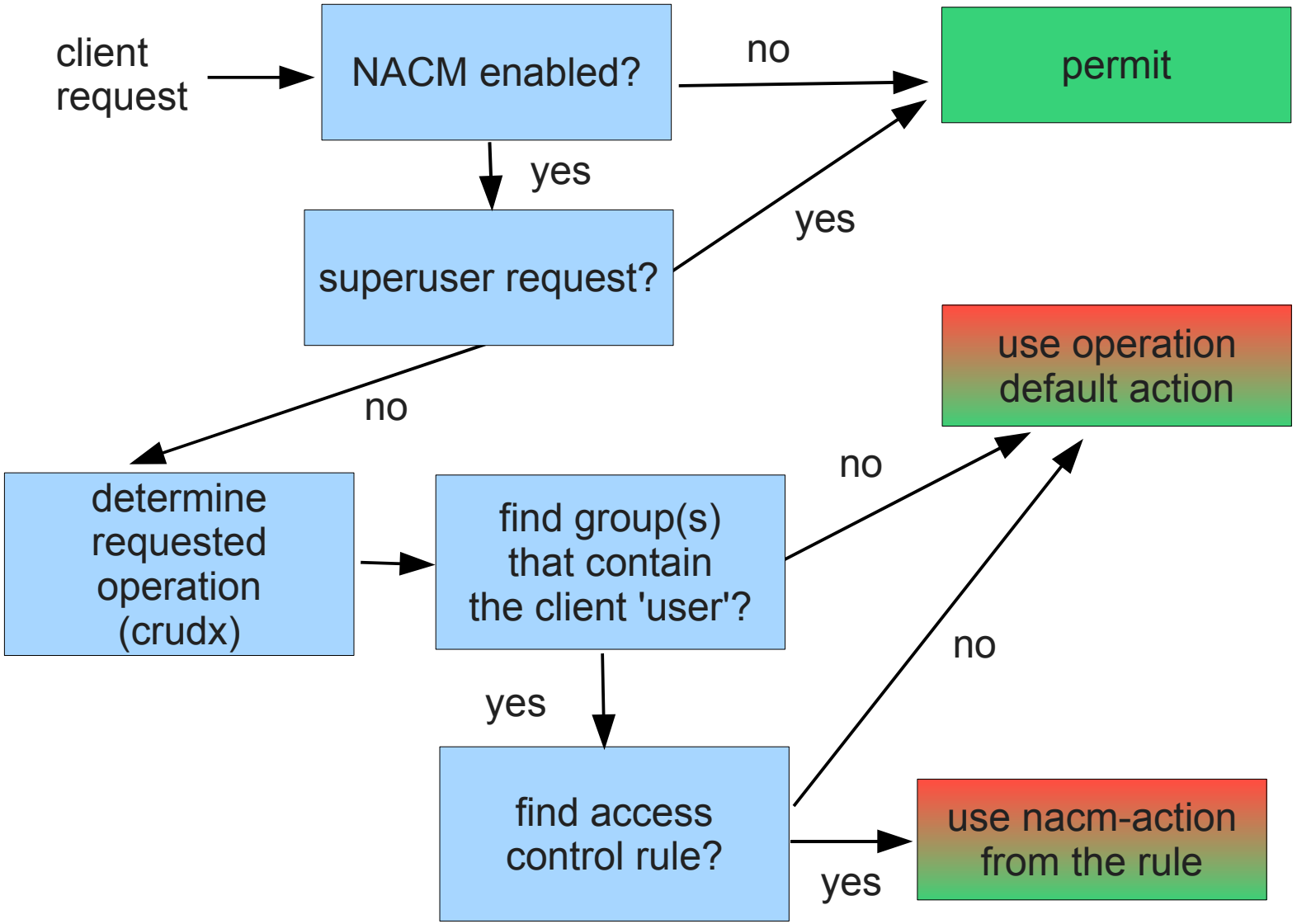
Conceptual Message Model



NACM Authentication Methods

- Three authentication methods defined:
  - publickey for local users over SSH
  - password for local users over any transport
  - password for RADIUS users over any transport
- Additional methods may be defined by other standard documents or by vendors.
- Optional to implement (YANG features)

Conceptual Authorization Model



NACM Rules Overview (1)

- Simple access control rules are provided:
  - <module-rule>
    - access to an entire YANG module.
  - <rpc-rule>
    - access to a specific RPC operation.
  - <data-rule>
    - access to a subset of all conceptual data nodes, available for a <get> operation.
  - <notification-rule>
    - access to a specific notification event type.

NACM Rules Overview (2)

- NACM access control rule common fields:
  - <rule-name>
    - arbitrary name for user-ordered list insertion.
  - <allowed-rights>
    - bits containing zero or more permissions granted by this rule (wildcard '*' == all bits set)
  - <allowed-group>
    - leaf-list of all the group names that are affected by this rule.
  - <nacm-action>
    - Action (permit or deny) for this rule
  - <comment>
    - user comment to store along with this rule.

Changes to NACM module (1)

- Addition of wildcard mechanism:
  - string '*' will match all existing <allowed-group> instances
  - string '*' will match all possible <nacm-rights> bit values
- Addition of <nacm-action> to each rule type:
  - The <nacm-rights> parameter is now part of the match procedure, instead of determining the rule outcome
  - <nacm-rights> now determines the rule outcome (permit or deny)

Changes to NACM module (2)

- Groups are now identified with strings, not YANG identities (less complexity)
- Global controls now use nacm-action-type instead of boolean data type
- <allowed-rights> changed from 3 bits (rwx) to 5 bits (crudx)
- <allowed-rights> now optional (and ignored) for rules where it is irrelevant (rpc and notification)

Changes to NACM module (3)

- <authentication> container added:
  - leaf-list <user-authentication-order>
  - container <radius>
    - list server
      - key <address>
      - leafs <port> and <shared-secret>
  - list <user>
    - key <name>
    - leafs <password>, <ssh-dsa>, and <ssh-rsa>

Proposed Charter Text

There is a need for standard mechanisms to restrict NETCONF protocol access for particular users to a pre-configured subset of all available NETCONF operations and content.

The WG will produce a document which identifies the access control requirements specific to the NETCONF protocol, as defined in [4741bis]. This document will also provide a standard YANG data model which addresses these requirements.

It is possible that the WG will not reach solution consensus on every possible requirement identified in the document. In this case, it is expected that the solution will evolve over time to meet these requirements.

Open Issues

- More complex data rules and wildcard mechanisms?
- What to do about <copy-config> leaving out unauthorized data?
  - Should backup/restore only be done by a user with full access, or should the server violate the NETCONF operation and pretend the unauthorized data was not removed?
- Is an <access-denied> notification event needed?