

Yang data model for Terminal Access Controller Access Control System Plus

draft-zheng-opsawg-tacacs-yang

Guangying Zheng

Zitao Wang

Bo Wu

Huawei Technologies

Recap

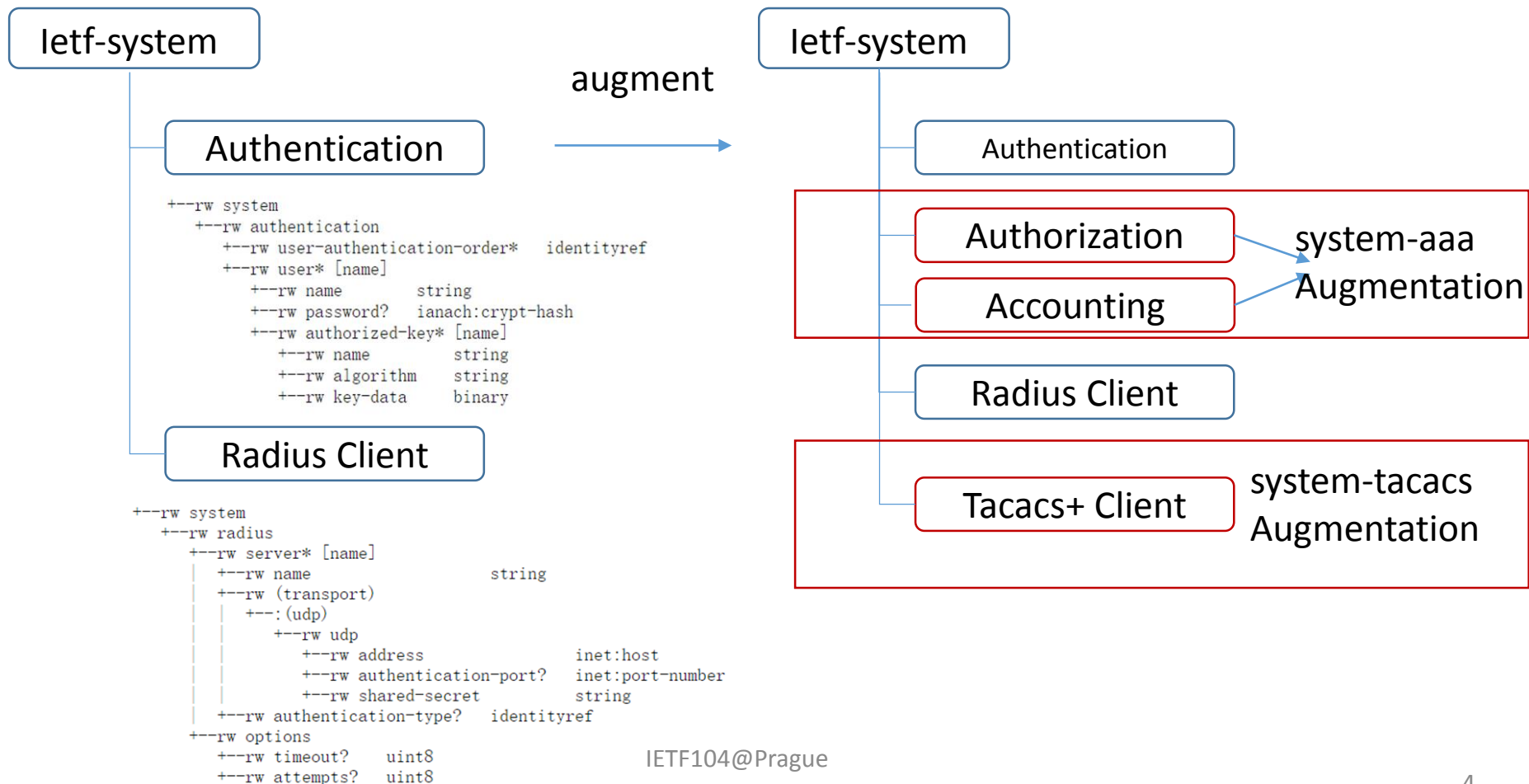
- This draft initially defines a YANG data model for the tacacs+ client
 - allows the configuration of network element for centralized Authentication, Authorization and Accounting
- At 103 IETF meeting, the WG suggested to extend the system-aaa model to make device management AAA complete, thus supporting the full functionality of tacacs+.

Updates since last IETF 103

- Change the tacacs+ client YANG structure
 - Align the tacacs+ YANG structure to system(RFC 7317) Radius client
 - Change major tacacs+ properties to be configurable for per tacacs-server
- Extend the system user authentication to make tacacs+ authentication enabled via the authentication-method configuration
- Add the system user authorization and accounting model as the system model augmentation to support the additional device management AAA configuration

Draft Overview

- Augments RFC 7317 (system management)
- The data model for configuration of the TACACS+ client and updated system-aaa has the following structure:



Model Overview

- ietf-system-tacacs
 - Be consistent with system radius client configuration
 - NMDA compliant
- ietf-system-aaa
 - Extend user authentication to support tacacs+ authentication method configuration
 - Add User Authorization and user accounting

```
module: ietf-aaa-tacacs
augment /sys:system:
  +--rw tacacs {tacacs}?
    +--rw server* [name]
      +--rw name string
      +--rw server-type? enumeration
      +--rw address inet:host
      +--rw port? inet:port-number
      +--rw shared-secret string
      +--rw source-ip? inet:ip-address
      +--rw single-connection? boolean
      +--rw network-instance? -> /ni:network-instances/
    +--ro statistics
      +--ro connection-opens? yang:counter64
      +--ro connection-closes? yang:counter64
      +--ro connection-aborts? yang:counter64
      +--ro connection-failures? yang:counter64
      +--ro connection-timeouts? yang:counter64
      +--ro messages-sent? yang:counter64
      +--ro messages-received? yang:counter64
      +--ro errors-received? yang:counter64
  +--rw options
    +--rw timeout? uint16
```

Per tacacs+ Server type configuration
Server type: Authentication, Authorization, Accounting

Parameters applied to all servers

```
module: ietf-system-aaa
augment /sys:system:
  +--rw authorization {authorization}?
    +--rw user-authorization-order* identityref
    +--rw events
      +--rw event* [event-type]
        +--rw event-type identityref
  +--rw accounting {accounting}?
    +--rw user-accounting-order* identityref
    +--rw events
      +--rw event* [event-type]
        +--rw event-type identityref
        +--rw record? enumeration
  +--rw authentication
    +--rw user-authentication-order* identityref
```

Open issues

- Make system-aaa to be a separate draft?
 - Alan DeKok commented to add radius to system-aaa extension module, but current radius client configuration in RFC 7317 only support user authentication.

Next Steps

- Solicit more comments and improve document
 - Your comments and suggestions are welcome!
- Seeking WG adoption