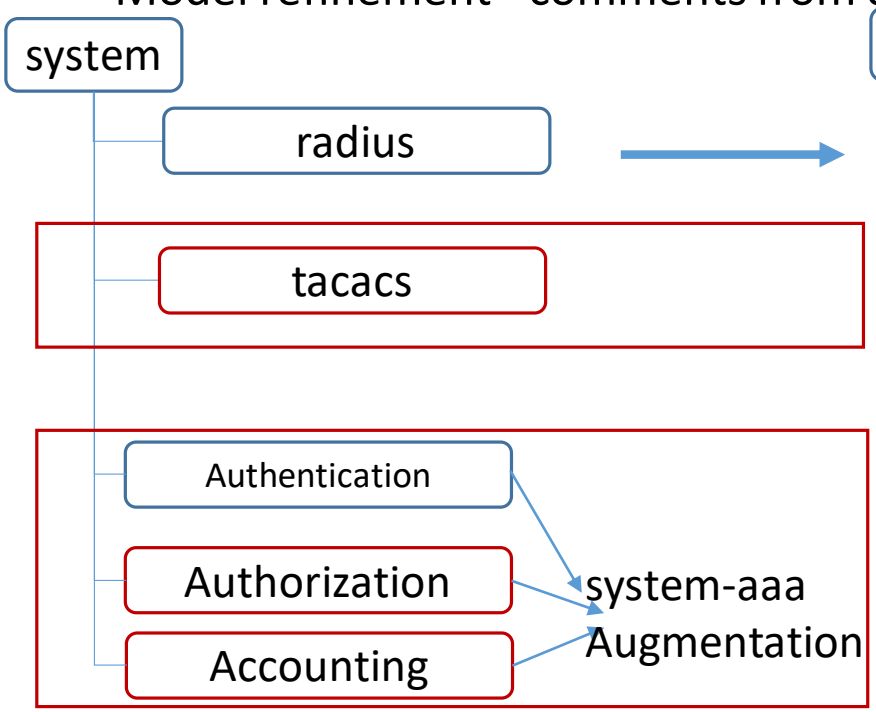
Yang data model for TACACS+

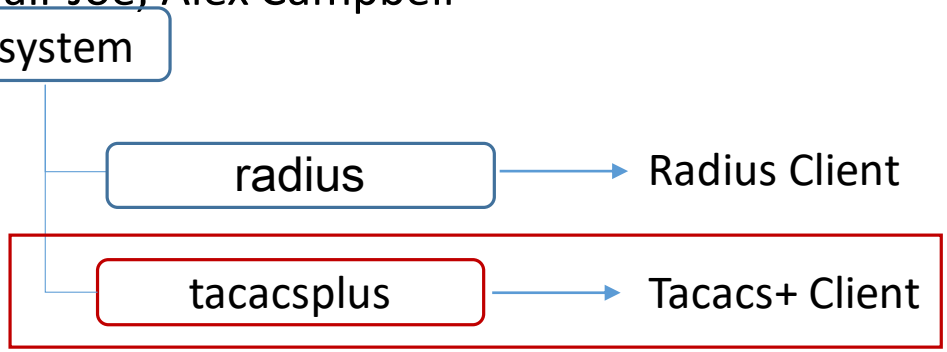
draft-ietf-opsawg-tacacs-yang-00

Guangying Zheng, Zitao Wang, Bo Wu(Presenting) Huawei

Overall changes

- Keep only the "tacacsplus" model – comments from chair Joe and Alan DeKok
- Model refinement- comments from chair Joe, Alex Campbell






```
module: ietf-system-tacacsplus
  augment /sys:system:
    +--rw tacacsplus {tacacsplus}?
       +--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-type)?
          |  +--:(source-ip)
          |  |  +--rw source-ip?              inet:ip-address
          |  +--:(source-interface)
          |     +--rw source-interface?       if:interface-ref
          +--rw single-connection?            boolean
          +--rw timeout?                      uint16
          +--rw vrf-instance?
          |       -> /ni:network-instances/network-instance/name
          +--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
```

Issues 1-
Downref TACACS+ Protocol

- Eliot’s comment
  - If this draft is targeted as a standard track and needs to downref TACACS+ protocol(current version is informational) , based on RFC 8067, this requires the chairs and Ignas' discussion

Issues 2-
Model extension for TACACS+ / TLS

- Eliot's comment
  - Does TACACS + / TLS affect model structure?
- Options
  - Next revision: an augmentation or even a bis to this model
    - The current model defines the state and configuration of the TACACS+ connection and is unlikely to change too much.
    - Or add a transport choice for flexibility

```
+--rw (transport)
|  +--:(tcp)
|     +--rw tcp
|        +--rw address                inet:host
|        +--rw port?                  inet:port-number
|        +--rw shared-secret          string
```

Issues 3- ietf-system “user-authentication-order”

- Ebben’s comment
  - System-authentication can be only configured with local authentication and radius authentication. If add tacacsplus authentication,
    - 'tacacsplus-authentication‘ feature
    - 'tacacsplus' identity
    - system-authentication: user-authentication-order
- Two options:
  - Propose a system-aaa augmentation draft in Netmod WG?
  - Add a section to give example for augmentation?

Issues 4- Session counter

- Comment from John Heasley
  - Tacacs+ session counter is different from “connection-opens” counter. If single-connection, a single-connection tacacs+ connection may be >1 sessions
- Add “sessions” counter?

Next Steps

- Resolve the comments from John Heasley.
- Further comments and suggestions are welcome.

Model augmentation option

- ietf-system-tacacsplus
- Ietf-system-aaa
  - Extend user authentication to support tacacsplus authentication method configuration
  - Add User Authorization and user accounting

```
module: ietf-system-tacacsplus
  augment /sys:system:
    +--rw tacacsplus {tacacsplus}?
       +--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-type)?
          |  +--:(source-ip)
          |  |  +--rw source-ip?           inet:ip-address
          |  +--:(source-interface)
          |     +--rw source-interface?     if:interface-ref
          +--rw single-connection?          boolean
          +--rw timeout?                    uint16
          +--rw vrf-instance?
          |       -> /ni:network-instances/network-instance/name
          +--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
```

Per tacacs+ Server type configuration

Server type: Authentication, Authorization, Accounting

```
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 accouting {accouting}?
       +--rw user-accouting-order*   identityref
       +--rw events
          +--rw event* [event-type]
             +--rw event-type    identityref
             +--rw record?       enumeration

+--rw authentication
   +--rw user-authentication-order*   identityref
```

'tacacsplus' that is base off ietf-system:authentication-method