Yang data model for TACACS+

draft-ietf-opsawg-tacacs-yang-01

Guangying Zheng, Zitao Wang, Bo Wu(Presenting)  Huawei
TACACS+ YANG model

• Existing ietf-system.yang [RFC 7317] covers local and Radius authentication

• TACACS+ data model extends system user authentication methods to support tacacsplus authentication configuration
Current Tree

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
      |  |  +--:(source-type)?
      |  |  |  +--rw source-ip?      inet:ip-address
      |  |  |  +--:(source-interface)
      |  |  |  |  +--rw source-interface? if:interface-ref
      |  +--rw vrf-instance?
      |  |  - > /ni:network-instances/network-instance/name

  +-rw single-connection?   boolean
  +-rw timeout?             uint16
  +-ro statistics
    |  +--rw connection-opens? yang:counter64
    |  +--rw connection-closes? yang:counter64
    |  +--rw connection-aborts? yang:counter64
    |  +--rw connection-failures? yang:counter64
    |  +--rw connection-timeouts? yang:counter64
    |  +--rw messages-sent?     yang:counter64
    |  +--rw messages-received? yang:counter64
    |  +--rw errors-received?   yang:counter64
    |  +--ro sessions?          yang:counter64
Changes since -00 (IETF 105)

• Refinement to introduction text, data model design section and YANG module based on comments received from John Heasley
• Added the TACACS+ Protocol draft as normative reference
• Added Tacacs+ session counter
• Added ‘tacacsplus’ identity to allow ‘system-authentication’ enable tacacsplus authentication
Issue: system authentication order

- System-authentication can be only configured with local authentication and radius authentication.

```yang
container authentication {

  leaf-list user-authentication-order {
    type identityref {
      base authentication-method;
    }
    must '(. != "sys:radius" or ../../radius/server)' {
      error-message
      "When 'radius' is used, a RADIUS server"
      + " must be configured.";
      description
      "When 'radius' is used as an authentication method,
       a RADIUS server must be configured.";
    }
    ordered-by user;
  }
}
```

ietf-system@2014-08-06.yang
Next Steps

• Resolve remaining issues