

TCP YANG Model – Update

Michael Scharf

Vishal Murgai

Mahesh Jethanandani

With contributions from Simon Bauer and Martin Mager

TCPM @ IETF 111

Scope and status

- **YANG model** for TCP configuration with **narrow scope**

1. TCP basic statistics (optional)
2. TCP connection list
3. TCP-AO and TCP MD5 with TCP-AO being strongly RECOMMENDED

} Established by TCP MIB
} For instance, for use in draft-ietf-idr-bgp-model

- Keepalives from draft-ietf-netconf-tcp-client-server

- Use in BGP YANG model

- **draft-ietf-idr-bgp-model-11** import of TCP-AO definitions

```
import ietf-tcp {  
  prefix tcp;  
  reference  
    "I-D.scharf-tcpm-yang-tcp: Transmission Control Protocol (TCP)  
    YANG Model.";  
}
```

draft-ietf-idr-bgp-model-11

```
choice option {  
  case ao {  
    uses tcp:ao;  
    leaf ao-keychain {  
      type key-chain:key-chain-ref;  
      ...  
    }  
  }  
  description  
    "Uses TCP-AO to secure the session. Parameters for  
    those are defined as a grouping in the TCP YANG  
    model.";  
  reference  
    "RFC 5925 - The TCP Authentication Option.";  
}
```

draft-ietf-idr-bgp-model-11

- Stable TCP-AO YANG model needed by **end of 2021**

Compete tree diagram

```
module: ietf-tcp
  +--rw tcp!
    +--rw connections
      | +--rw connection*
      |   [local-address remote-address local-port remote-port]
      |   +--rw local-address      inet:ip-address
      |   +--rw remote-address     inet:ip-address
      |   +--rw local-port         inet:port-number
      |   +--rw remote-port        inet:port-number
      |   +--rw common
      |     +--rw keepalives!
      |       | +--rw idle-time      uint16
      |       | +--rw max-probes     uint16
      |       | +--rw probe-interval uint16
      |       +--rw (authentication)?
      |         +--:(ao)
      |           | +--rw enable-ao?    boolean
      |           | +--rw send-id?     uint8
      |           | +--rw recv-id?    uint8
      |           | +--rw include-tcp-options? boolean
      |           | +--rw accept-key-mismatch? boolean
      |           +--:(md5)
      |             +--rw enable-md5?   boolean
      +--ro statistics {statistics}?
        +--ro active-opens?          yang:counter32
        +--ro passive-opens?         yang:counter32
        +--ro attempt-fails?         yang:counter32
        +--ro establish-resets?      yang:counter32
        +--ro currently-established? yang:gauge32
        +--ro in-segments?           yang:counter64
        +--ro out-segments?          yang:counter64
        +--ro retransmitted-segments? yang:counter32
        +--ro in-errors?             yang:counter32
        +--ro out-resets?            yang:counter32
        +--x reset
          +--w input
          | +--w reset-at?   yang:date-and-time
          +--ro output
          | +--ro reset-finished-at? yang:date-and-time
```

Connection list

Keepalives from draft-ietf-netconf-tcp-client-server

TCP-AO (and TCP MD5)

Stats

draft-ietf-tcpm-yang-tcp-02

→ Relatively straightforward model

Diff between -02 and -01

- **Write access to connection list:** List must be writable due to YANG semantics
 - Expanded description: “List of TCP connections with their parameters. **The list is modelled as writable, but implementations may not allow creation of new TCP connections by adding entries to the list. Furthermore, the behavior upon removal is implementation-specific. Implementations may support closing or resetting a TCP connection upon an operation that removes the entry from the list.**”
 - Issue reported by Simon Bauer and Martin Mager
- **Client/server imports:** Removed from model
 - Discussed during last meeting
 - Issue reported by Simon Bauer and Martin Mager
- **Reset RPC for statistics:** No change as compared to -01, but additional explanation
 - New text: “**Note that the TCP MIB does not include means to reset statistics, which are defined in this document. This is not a major addition, as a reset can simply be implemented by storing offset values for the counters.**”
 - Suggestion by Richard Scheffenegger and Michael Tuexen
- **TCP-AO modeling:** Clear description of how to set send-id and recv-id
 - Expanded description: “The SendID is inserted as the KeyID of the TCP-AO option of outgoing segments. **The SendID must match the RecvID at the other endpoint.**”
 - Feedback from Melchior Aelmans and Greg Hankins

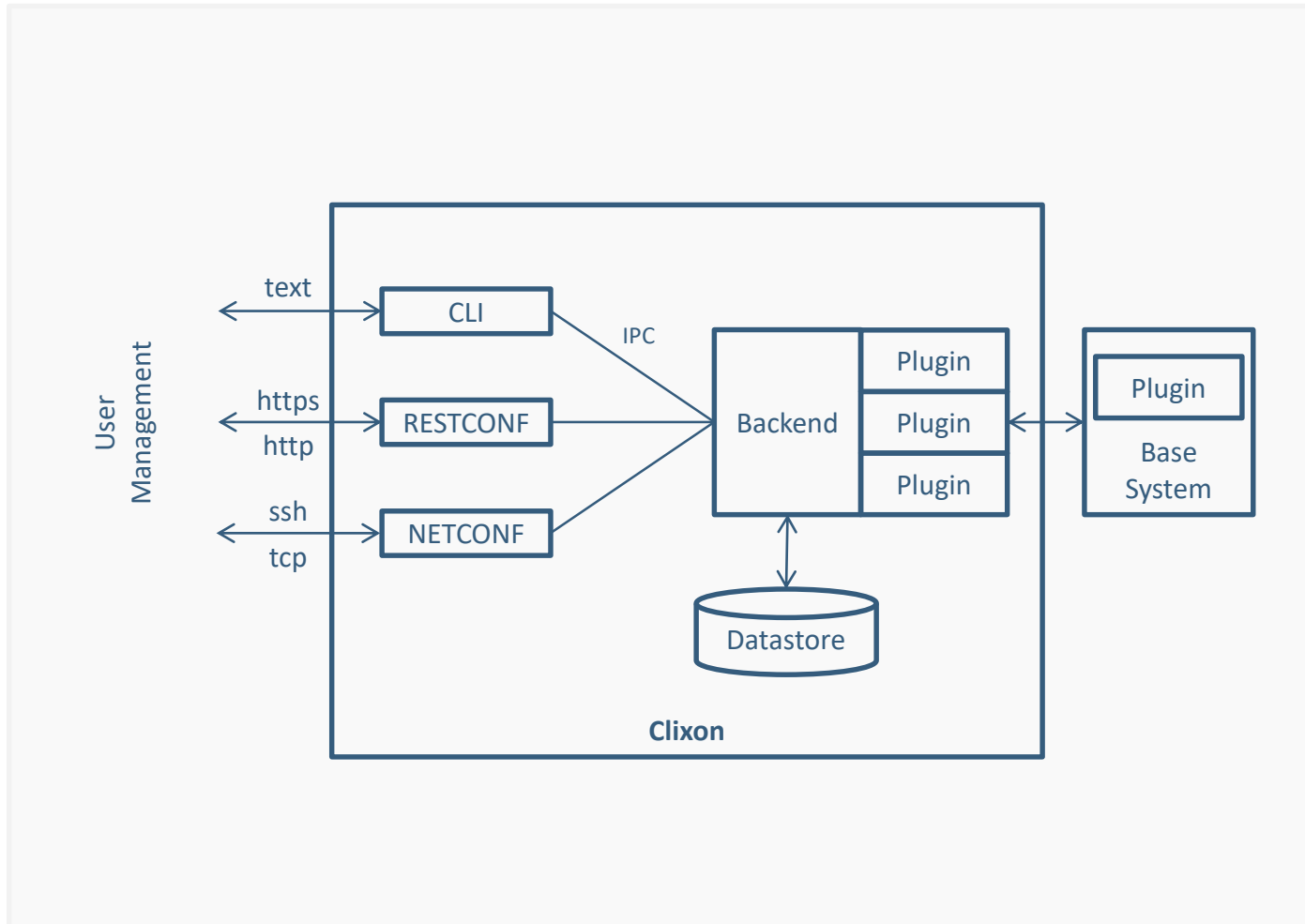
→ Only minor changes between -02 and -01

Prototype

- **Software prototype** for draft-ietf-tcpm-yang-tcp
 - Student research project at Hochschule Esslingen – University of Applied Sciences
 - Developers: Simon Bauer and Martin Mager
- **NETCONF server based on open-source software “clixon”**
 - Clixon source code at <https://github.com/clixon/clixon>
 - Clixon supports NETCONF, RESTCONF, and CLI interfaces
 - No builtin NMDA support (so far)
- **Initially supported functions** in draft-ietf-tcpm-yang-tcp
 - Connection list
 - Stats

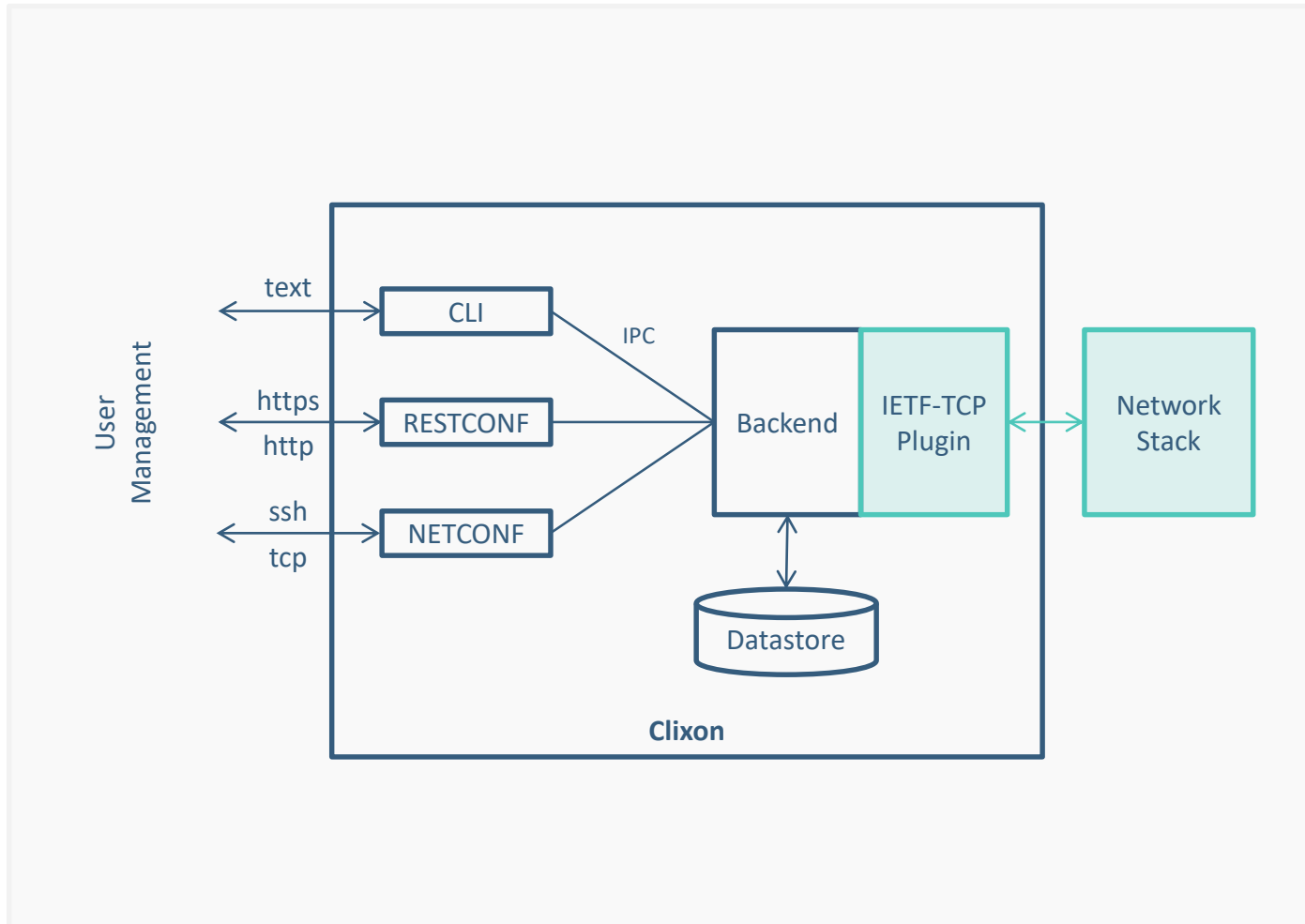
} Challenge: Lack of open source TCP-AO implementation
- **Used operating systems**
 - **Ubuntu Linux** as example for desktop/server
 - **QNX** as example for embedded networking hardware
- **No further issues in YANG model identified**
 - Network stack can be accessed by OS-specific APIs (netstat, /proc, etc.)
 - Most development work elsewhere (e.g., chunked framing support by clixon)
- **Open-source release TBD**

Prototype NETCONF Server Architecture with clixon



Source: Simon Bauer, Martin Mager, Evaluation eines modellbasierten Managements in verschiedenen Systemumgebungen, Hochschule Esslingen – University of Applied Sciences, 2021

Prototype Plugin for IETF TCP YANG model



Source: Simon Bauer, Martin Mager, Evaluation eines modellbasierten Managements in verschiedenen Systemumgebungen, Hochschule Esslingen – University of Applied Sciences, 2021