YANG based Config for MAC Privacy 802.1AEdk Granularity of Privacy Configuration

Don Fedyk (dfedyk@labn.net)
Outline

• Proto Config for MAC Privacy
• Considering Control of MAC privacy
Forward

• This presentation is for a discussion on detailed config.
• It may contain errors/omission and should be consider a work in progress.
• An updated version the presentation will be posted after discussion to correct it, but it will remain a work in progress.
Instance Diagram for MACSec and MAC Privacy
MACsec and MAC Privacy

- Mainly 2 New Modules
  - ieee802-dot1ae
    - ieee802-dot1ae-types
  - ieee802-dot1ae-pry

Depends on:
- ietf-yang-types
- ietf-inet-types
- iana-if-type
- ieee802-dot1q-bridge
  - ieee802-dot1q-bridge
- ieee802-dot1x
  - ieee802-dot1x-types
- ietf-interfaces
- ietf-system
- ieee802-types
Adding MAC Privacy is similar
Yanglint JSON output for a VLAN Bridge with MACsec

```json
{ "ieee802-dot1q-bridge:bridges": { "bridge": [ { "name": "bridge1", "address": "10-10-10-10-10-10", "bridge-type": "customer-vlan-bridge", "component": [ { "name": "cv1", "id": 1, "type": "c-vlan-component" }, { "name": "cv2", "id": 2, "type": "c-vlan-component" } ] } ] }, "ietf-interfaces:interfaces": { "interface": [ { "name": "eth0", "type": "iana-if-type:ethernetCsmacd", "ieee802-dot1q-bridge:bridge-port": { "bridge-name": "bridge1", "component-name": "cv1", "port-type": "c-vlan-bridge-port", "pvid": 1 } }, { "name": "eth1", "type": "iana-if-type:ethernetCsmacd", "ieee802-dot1q-bridge:bridge-port": { "bridge-name": "bridge1", "component-name": "cv2", "port-type": "c-vlan-bridge-port", "pvid": 1 } } ] }, "ieee802-dot1x:pry": { "mac-privacy": "enabled", "user-priority-to-pry": [ { "user-priority": 0, "privacy-type": "none" }, { "user-priority": 1, "privacy-type": "frame-a" }, { "user-priority": 2, "privacy-type": "express-channel" }, { "user-priority": 3, "privacy-type": "express-channel" } ] }, "ieee802-dot1ae:secy": { "controlled-port-number": 1, "verification": { "validate-frames": "strict", "replay-protect": true } }, "generation": { "max-transmit-channels": 16, "max-transmit-keys": 16, "protect-frames": true, "always-include-sci": true, "use-es": true, "use-scb": true, "user-priority-to-ec": [ { "user-priority": 0, "traffic-class": 0, "access-class-de0": 0, "access-class-de1": 0 }, { "user-priority": 1, "traffic-class": 1, "access-class-de0": 1, "access-class-de1": 1 }, { "user-priority": 2, "traffic-class": 2, "access-class-de0": 2, "access-class-de1": 2 } ] }, "ieee802-dot1ae-pry:pry": { "mac-privacy": "enabled", "user-priority-to-pry": [ { "user-priority": 0, "privacy-type": "none" }, { "user-priority": 1, "privacy-type": "frame-a" }, { "user-priority": 2, "privacy-type": "express-channel" }, { "user-priority": 3, "privacy-type": "express-channel" } ] }, "ieee802-dot1ae:secy": { "controlled-port-number": 1, "verification": { "validate-frames": "strict", "replay-protect": true } }, "generation": { "max-transmit-channels": 16, "max-transmit-keys": 16, "protect-frames": true, "always-include-sci": true, "use-es": true, "use-scb": true, "user-priority-to-ec": [ { "user-priority": 0, "traffic-class": 0, "access-class-de0": 0, "access-class-de1": 0 } ] }, "ieee802-dot1ae-pry:pry": { "mac-privacy": "enabled", "user-priority-to-pry": [ { "user-priority": 0, "privacy-type": "none" }, { "user-priority": 1, "privacy-type": "frame-a" }, { "user-priority": 2, "privacy-type": "express-channel" }, { "user-priority": 3, "privacy-type": "express-channel" } ] } ] }
```

Note Abbreviated TC table is 8 priorities 4 are shown etc

To be added a "None" type
Yanglint JSON output for a VLAN Bridge with MACsec

```
"privacy-channel": {
    "pc": "default-channel",
    "max-per-second-bitrate": "10000000000",
    "max-mppdu-size": 1500,
    "mppdu-priority": 3
},
"privacy-frame": {
    "pf": "frame-a",
    "max-mppdu-size": 1500,
    "mppdu-priority": 6
}
"ieee802-dot1x:pae": {
    "pae-system": "pae1"
}
"ietf-system:system": {
    "contact": "test",
    "ieee802-dot1x:pae-system": {
        "name": "pae1",
        "system-access-control": "enabled"
    }
}
```

**Note** this table only shows configured items – Defaults are used for other priorities

**Note** Uncontrolled port and Controlled port have no configurable options. They do not show up in a configuration view like this. (Currently stats are read write but that is an error)
How traffic can pass through the Mac Privacy Shim?

Is interface granular enough?

This is a priority table-based map
- Privacy Channel or
- Privacy Frame or
- No Privacy

This is not explicitly supported by the YANG
This is the uncontrolled port but there is no YANG control

Missing two cases?
Non-Priority based Traffic
- Mapped to MACsec only (streams)
- Bypass Plain text
Do We have this Right?

• Currently following the precedent set by 802.1X:
• Bridge-port, pae, secy and pry are all at the level of an interface.
• Shouldn’t pae, secy and pry be tied to a bridge-port – cases where there are multiple bridge ports on an interface?
• Alternatively we create multiple virtual interfaces
Maybe we should have this?

This would scope traffic to the bridge port. But still no way to indicate Controlled or uncontrolled port.
Stream/ Scheduler is under a bridge port component.

```json
{
  "ieee802-dot1q-bridge:bridges": {
    "bridge": {
      "name": "bridge1",
      "address": "10-10-10-10-10-10",
      "bridge-type": "customer-vlan-bridge",
      "component": {
        "name": "cv1",
        "id": 1,
        "type": "c-vlan-component",
        "ieee802-dot1q-stream-filters-gates:streamfilters": {
          "streamfilter-instance-table": {
            "streamfilter-instance-id": 1,
            "wildcard": [null],
            "priority-spec": "three",
            "max-sdu-size": 0,
            "stream-blocked-due-to-oversize-frame-enabled": true,
            "stream-blocked-due-to-oversize-frame": true,
            "stream-gate-ref": 1,
            "ieee802-dot1q-psfp:flow-meter-instance-id": 1,
            "ieee802-dot1q-psfp:flow-meter-enabled": true
          }
        },
        "ieee802-dot1q-stream-filters-gates:streamgates": {
          "streamgate-instance-table": {
            "streamgate-instance-id": 1,
            "gate-enabled": true,
            "admin-gate-states": "open",
            "ieee802-dot1q-psfp:operation": "null",
            "ieee802-dot1q-psfp:admin-control-list": {
              "gate-control-entry": {
                "index": 1,
                "operation-name": "set-gate-and-ipv",
                "time-interval-value": 1000,
                "gate-state-value": "open",
                "ipv-spec": "null",
                "interval-octet-max": 1000
              }
            }
          }
        }
      }
    }
  }
}
```
Stream is under a bridge port.

```json
"ietf-interfaces:interfaces": {
    "interface": [
        {
            "name": "eth0",
            "type": "iana-if-type:bridge",
            "ieee802-dot1q-bridge:bridge-port": {
                "bridge-name": "bridge1",
                "component-name": "cv1",
                "port-type": "c-vlan-bridge-port",
                "pvid": 1,
                "interface": "eth0",
                "type": "iana-if-type:bridge",
                "ieee802-dot1q-bridge:bridge-port": {
                    "bridge-name": "bridge1",
                    "component-name": "cv1",
                    "port-type": "c-vlan-bridge-port",
                    "pvid": 1,
                    "interface": "eth0",
                    "type": "iana-if-type:bridge",
                    "ieee802-dot1q-sched:gate-parameter-table": {
                        "queue-max-sdu-table": {
                            "traffic-class": 0,
                            "queue-max-sdu": 100
                        },
                        "gate-enabled": true,
                        "admin-gate-states": 255,
                        "admin-control-list": {
                            "gate-control-entry": {
                                "index": 1,
                                "operation-name": "set-gate-states",
                                "time-interval-value": 100,
                                "gate-states-value": 255
                            }
                        },
                        "admin-cycle-time": {
                            "numerator": 10,
                            "denominator": 1000
                        },
                        "admin-cycle-time-extension": 999,
                        "admin-base-time": {
                            "seconds": 1,
                            "nanoseconds": 1000
                        },
                        "config-change": true,
                        "supported-list-max": 100,
                        "supported-cycle-max": {
                            "numerator": 10,
                            "denominator": 1000
                        },
                        "supported-interval-max": 100
                    }
                }
            }
        }
    ]
}
```

```
" IEEE 802.1 November Plenary 2020
```

11/5/2020
Back up

• Yanglint Validation
MACsec and MAC Privacy
YANG Some lessons learned

• Instance Model – Where the YANG trees lives
• YANG Models – What to configure and what to display
  • Our bridge Model is a large superset that supports many permutations.
  • The model contains a lot of detail.
  • The tree provides a useful summary (a slice of the instance model)
• Validation
  • Pyang – validates a single model
  • Various other tools
• Instance Configuration – IEEE is in general only beginning to look at this
  • Yuma123
  • Confd (free version)
  • Yanglint (Used by IETF)
Validation versus Instance configuration

• Validation
  • YANG syntax is correct
  • YANG xpath is syntactically correct $x=y$ (but $x$ may be apples and $y$ may be oranges)
  • The whole set of permutations it the tree file or the xml description.

• Instance configuration
  • Config values are tested reference pointers are checked
  • YANG syntax is correct and multiple modules that are not related can exist side by side
  • $x = y$ and $x$ is the set of apple types and $y$ is a type of apple (Macintosh but not iphone!).
  • A slice of valid configuration references links are tested