avaya.com

Ethernet Routing Switch 3500 Series
Software Release 5.3.4

1. Release Summary

Release Date: 29-June-2017
Purpose: Software patch release to address customer and internally found software issues.

2. Important Notes Before Upgrading to This Release

None.

3. Platforms Supported

Ethernet Routing Switch 3500 (All models)

4. Notes for Upgrade

Please see “Ethernet Routing Switch 3500 Series, Configuration – System, Software Release 5.3” (available at http://www.avaya.com/support. Click Products, select Ethernet Routing Switch 3500 Series from the A-Z list, then select Documentation > View All Documents) for details on how to upgrade your Switch.

File Names for This Release

File Name	Module or File Type	File Size (bytes)
3500_5.3.0.8_diag.bin	Diagnostic image	2,100,273
3500_534008.img	Agent code image	9,550,260
3500_534009s.img	Agent code image (SSH)	9,813,348

5. Version of Previous Release

Software Version 5.3.3.

6. Compatibility

This software release is managed with Enterprise Device Manager (EDM) which is integrated into the agent software.

7. Changes in This Release

7.1. New Features in This Release

7.1.1 Updated 'show fa elements' command

The updated 'show fa elements' output includes a number of new components when compared to the legacy FA element display:

```
3550T-PWR+(config)#show fa elements

================================================================================
                     Fabric Attach Discovered Elements
================================================================================
UNIT/                MGMT                                              ELEM ASGN
PORT   TYPE          VLAN  STATE  SYSTEM ID                           AUTH AUTH
--------------------------------------------------------------------------------
2/16   Client         1    U / D  00:22:67:00:58:00:00:00:00:10     AP   AP

================================================================================
                   Fabric Attach Authentication Detail
================================================================================
UNIT/                                 ELEM OPER          ASGN OPER
PORT   EXPANDED TYPE                  AUTH STATUS        AUTH STATUS
--------------------------------------------------------------------------------
2/16   Switch                         successAuth        successAuth

State Legend: (Tagging/AutoConfig)
T=Tagged, U=Untagged, D=Disabled, S=Spbm, V=Vlan, I=Invalid

Auth Legend:
AP=Authentication Pass, AF=Authentication Fail, NA=Not Authenticated, N=None
```

All previously displayed data items are still present:

- Unit/Port or Trunk ID through which the FA element was discovered
  - UNIT/PORT: '**1/5**', '**2/16**', '**MLT3**'
- General FA element type and expanded type information
  - TYPE: '**Proxy**', '**Server**', '**Client**'
  - EXPANDED TYPE: '**Server (Auth)**', '**Switch**', '**Wireless AP (Type 1)**', etc.
- Management VLAN data advertised by the FA element (MGMT VLAN)
- FA element system identifier (includes MAC address) data
  - SYSTEM ID: Device MAC address occupies bytes 1 – 6 of the 10 byte identifier
- Summary FA Element TLV authentication status
  - ELEM AUTH: '**AP**', '**AF**', '**NA**'

Several **new data items** are now also presented:

- Device state information included in the received FA Element TLV (STATE)
  - Tagging requirements
    - '**T**' (all traffic tagged), '**U**' (mix of tagged and untagged traffic present)
  - FA operational mode
    - '**S**' (SPBM provisioning mode), '**V**' (VLAN provisioning mode), '**D**' (disabled)
- Summary FA I-SID/VLAN Assignment TLV authentication status

  - ASGN AUTH: '**AP**', '**AF**', '**NA**'
- Authentication status detail information for both the FA Element TLV and the FA I-SID/VLAN Assignment TLV, if present (ELEM OPER AUTH STATUS, ASGN OPER AUTH STATUS)
  - '**successAuth**' – TLV processed (successfully authenticated)
  - '**successNoAuth**' – TLV processed (no authentication required)
  - '**failRemoteNoAuth**' – TLV processing aborted (authentication failed – zeroed authentication digest received from remote FA element)
  - **failMismatchedKeys**' – TLV processing aborted (authentication failed – invalid authentication digest received from remote FA element)

Updated ACLI Command List

No new CLI commands are introduced. No existing CLI commands are updated in terms of the parameters they support. Only the output of the existing CLI command is updated to display additional details about FA elements that have been discovered.

Command: `show fa elements`

```
Mode:  privExec
      global configuration

<parameter-1> = auth-status     -- display only specified authorized status
<parameter-2> = auth-fail | auth-pass | not-auth

<parameter-1> = client-type      -- display only specified client type
<parameter-2> = <6-17>

<parameter-1> = element-type  -- display only specified element type
<parameter-2> = client | proxy | server

<parameter-1> = trunk               -- display based on trunk number
<parameter-2> = <TrunkId>

<parameter-1> = <PortList>      -- list of ports

Syntax (normal form):
      show fa elements [auth-status < auth-fail | auth-pass | not-auth >] |
   [client-type < 6-17 >] |
   [element-type < client | proxy | server >] |
   [trunk <TrunkId>] |
   [<PortList>]

Description:
      Displays discovered Fabric Attach elements.
```

Legacy Output Format:

```
Unit/ Element    Element           Element
Port   Type      Subtype            VLAN   Auth    System ID
----- ------- ------------------- ------- ---- ----------------------------
1/5   Client  Wireless AP (Type 1)  0       AP  00:22:67:00:58:00:00:00:01:0a
MLT3  Server  Server (Auth)         1234    AP  fc:a8:41:fa:f8:00:20:00:00:03
2/16  Client  Switch                20      NA  64:a7:dd:03:38:29:00:00:00:01
3/36  Client  Wireless AP (Type 1)  0       AF  64:07:34:03:12:ac:00:00:00:08
```

Updated Output Format:

```
================================================================================
                     Fabric Attach Discovered Elements
================================================================================
UNIT/                MGMT                                              ELEM ASGN
PORT    TYPE         VLAN  STATE  SYSTEM ID                           AUTH AUTH
--------------------------------------------------------------------------------
1/5     Client       0     U / S  00:22:67:00:58:00:00:00:01:0a     AP   AP
MLT3    Server       1234  T / S  fc:a8:41:fa:f8:00:20:00:00:03     AP   AP
2/16    Client       20    U / D  64:a7:dd:03:38:29:00:00:00:01     NA   N
3/36    Client       0     U / D  64:07:34:03:12:ac:00:00:00:08     AF   AF

================================================================================
                    Fabric Attach Authentication Detail
================================================================================
UNIT/                          ELEM OPER              ASGN OPER
PORT   EXPANDED TYPE           AUTH STATUS            AUTH STATUS
--------------------------------------------------------------------------------
1/5    Wireless AP (Type 1)    successAuth            successAuth
MLT3   Server (Auth)           successAuth            successAuth
2/16   Switch                  successNoAuth          none
3/36   Wireless AP (Type 1)    failMismatchedKeys     failRemoteNoAuth

State Legend: (Tagging/AutoConfig)
T=Tagged, U=Untagged, D=Disabled, S=Spbm, V=Vlan, I=Invalid

Auth Legend:
AP=Authentication Pass, AF=Authentication Fail, NA=Not Authenticated, N=None

--------------------------------------------------------------------------------
2 out of 2 total number of Fabric Attach discovered elements displayed
--------------------------------------------------------------------------------
```

Where:

- State = FA Element TLV state field data
- Elem Auth = FA Element TLV authentication status
- Asgn Auth = FA I-SID/VLAN Assignment TLV authentication status
- Elem Oper Auth Status = FA Element TLV authentication status detail data
- Asgn Oper Auth Status = FA I-SID/VLAN Assignment TLV authentication status detail data

SNMP Support

New FA MIB attributes have previously been introduced to support the export of discovered FA element details to external management elements. These attributes are available on all platforms that support the enhanced FA element display:

```
avFabricAttachDiscElemsElementOperAuthStatus OBJECT-TYPE
    SYNTAX     INTEGER {
                  none(1), -- no packets received yet
                  successNoAuth(2), -- success with no-auth on either
```

```
                                        local or remote
                successAuth(3), -- success with auth on both local
                                      and remote
                failMismatchedKeys(4), -- failure due to key mismatch
                failLocalAuthRemoteNoAuth(5), -- failure due to local
                                                  auth and remote no-auth
                failLocalNoAuthRemoteAuth(6) -- failure due to local
                                                  no-auth and remote auth
            }
    MAX-ACCESS     read-only
    STATUS         current
    DESCRIPTION
        "The current operational Fabric Attach elements
       authentication status for the associated interface."

    ::= { avFabricAttachDiscElemsEntry 8 }

avFabricAttachDiscElemsElementAsgnsOperAuthStatus OBJECT-TYPE
    SYNTAX     INTEGER {
                none(1), -- no packets received yet
                successNoAuth(2), -- success with no-auth on either
                                        local or remote
                successAuth(3), -- success with auth on both local
                                      and remote
                failMismatchedKeys(4), -- failure due to key mismatch
                failLocalAuthRemoteNoAuth(5), -- failure due to local
                                                  auth and remote no-auth
                failLocalNoAuthRemoteAuth(6) -- failure due to local
                                                  no-auth and remote auth
            }
    MAX-ACCESS     read-only
    STATUS        current
    DESCRIPTION
        "The current operational Fabric Attach assignment
       authentication status for the associated interface."

    ::= { avFabricAttachDiscElemsEntry 9 }

avFabricAttachDiscElemsAsgnsAuth OBJECT-TYPE
    SYNTAX     INTEGER {
                authenticationPass(1),
                authenticationFail(2),
                notAuthenticated(3),
                none(4)
            }
    MAX-ACCESS     read-only
    STATUS        current
    DESCRIPTION
        "The assignment authentication status"

    ::= { avFabricAttachDiscElemsEntry 10 }
```

7.2 Old Features Removed From This Release

None.

7.3 Problems Resolved in This Release

ERS3500-516 - EDM does not show the option to configure I-sid

ERS3500-530 - Random ports show negative value for last change field

ERS3500-531 - CVE-2016-2183,CVE-2016-6329 vulnerabilities reported while scanning for threats

ERS3500-532 - "terminal length 0" command has no effect after logout and is not appearing in show run

ERS3500-540 - End-user / client intermittently loses network connection through the switch with dynamic ARP-inspection or IP Guard configuration when corresponding entry in DHCP binding table expires prematurely due to a negative uptime difference.

8. Outstanding Issues

None.

9. Known Limitations

ERS3500-539 - EDM: Users can't connect on switch via secure EDM using Chrome version 59.
Problem description: Starting with version 59, Chrome reports the self-signed certificate issued by ERS family as having bad format and will fail to connect via secure EDM.
Work around: Use Firefox (v54 or older), IE (v11 or older), Edge (v20 or older) or Chrome (v58 or older).

10. Documentation Corrections

None.

For other known issues, please refer to the product release notes and technical documentation available from the Avaya Technical Support web site at: http://www.avaya.com/support .

11. Troubleshooting

As good practices of help for troubleshooting various issues, AVAYA recommends:

- configuring the device to use the Simple Network Time Protocol to synchronize the device clock;
- setting a remote logging server to capture all level logs, including informational ones. (#logging remote level informational).

To access more technical documentation, search our knowledge base, or open a service request online, please visit Avaya Technical Support on the web at: http://www.avaya.com/support.