Device Discovery using STOAT

Feature Overview and Configuration Guide

Introduction

Together, Vista Manager EX 3.11 and AlliedWare Plus software version 5.5.3-1 support AMF Plus Device Discovery using the STOAT (Standardized Topology Organizer and Transport) discovery protocol. STOAT learns about network devices and their links, and Vista Manager EX, using it's AMF Plus Device Discovery feature, can then access this information so they can be displayed on the network map.

STOAT is designed to gather topology information about networks. It standardizes the output of various discovery protocols into a common format and transports the resulting topology data to a central point for use by Vista Manager EX.

Using LLDP and DHCP Snooping, STOAT can discover and gather information about devices in the local network. These devices may include IP cameras, IP phones, PCs, laptops, Wi-fi access points, printers, and so on. LLDP is limited to discovering devices directly connected to the STOAT device, however DHCP Snooping can discover devices one or more hops away.

The STOAT Collector provides Vista Manager EX with a near real-time stream of topology updates, allowing a responsive and accurate view of the network.

This document describes using STOAT Device Discovery with Vista Manager EX and STOAT Device Discovery from the AlliedWare Plus CLI.

Products and software version that apply to this guide

This guide applies to all AlliedWare Plus™ products that are AMF capable, running version 5.5.3-1 or later, and Vista Manager EX version 3.11 or later.

For the latest information, see the following documents:

- The product’s Datasheet
- The AlliedWare Plus Datasheet
- The product’s Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

Related documents

See the following documents for more detailed information:

- For more information about DHCP Snooping, see the DHCP Snooping Feature Overview and Configuration Guide.
- For more information about PKI, see the Public Key Infrastructure (PKI) Feature Overview and Configuration Guide.
- For more information about LLDP, see the LLDP Feature Overview and Configuration Guide.
- For more information about port authentication, see the AAA and Port Authentication Feature Overview and Configuration Guide.

Licensing

An active AMF Plus license is required.

Content

Overview

Vista Manager EX creates an integrated map using information from AMF and other plug-ins such as AWC and SNMP. Device Discovery using STOAT enhances the topology information present in the integrated map by providing Vista Manager EX with additional information about devices, and the links between them.

STOAT devices add information about themselves to the topology in addition to information from the following discovery protocols:

- LLDP
- DHCP Snooping
- Dot1X

Device discovery

Devices with the STOAT feature enabled record information about themselves and their network interfaces. This information includes details about:

- Hostname
- Manufacturer and model name
- Software, hardware, and firmware revision
- Switch ports, including aggregator and VLAN configuration
- Eth ports
- IPv4 and IPv6 addresses

This data is imported into Vista Manager EX to give an optimal view of the network.

LLDP

When STOAT devices are enabled to use LLDP, they utilize LLDP to discover adjacent STOAT devices and store the link adjacencies in the topology. Additionally, STOAT will discover other adjacent devices capable of LLDP and LLDP-MED, recording the advertised information and link adjacencies in the topology.

The information advertised will depend on the adjacent device and its configuration, but it can contain:

- Port ID
- Port description
- Chassis ID
- System name
- System description
- System capabilities supported and enabled.
- Management addresses
- MED device type
- MED hardware, firmware, and software revisions
- MED serial number
- MED manufacturer name
- MED model name
- MED asset ID

DHCP Snooping

When STOAT devices are enabled to use DHCP Snooping, they utilize the local DHCP Snooping database as a source of information to discover devices, and they record this information in the topology.

This information can contain:

- IP address
- MAC address
- Hostname
- DHCP request options, and their values
- Ingress VLAN and port of the DHCP request

Dot1X

When STOAT devices are enabled to use Dot1X, they use the local Port Authentication database as a source of information to discover devices, and they record this information in the topology. This covers 802.1X Authentication, Mac Authentication, Web Authentication, and MACsec.

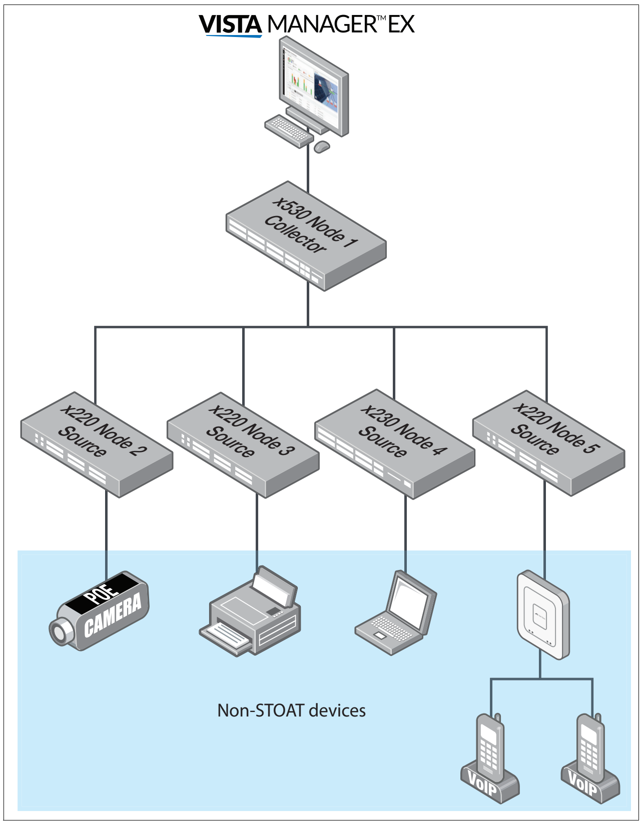
This information can contain:

- MAC address
- IP address
- NAS IP address
- Username

Devices in a STOAT network

STOAT incorporates a key feature wherein topology information is transported to a central point within the network. This enables Vista Manager EX to effectively utilize the information. To accomplish this, STOAT has 3 roles: Collector, Source, and non-STOAT device.

- **Collector** - a STOAT device that has been configured to receive topology information from other STOAT devices.
- **Source** - a STOAT device that has been configured with the destination address of a Collector, to send its topology information to.
- **non-STOAT device** - a device that you want STOAT to discover.



What are STOAT devices?

STOAT devices are AlliedWare Plus devices that have been configured with STOAT. It is possible for a STOAT device to be both a Collector and Source simultaneously.

What are non-STOAT devices?

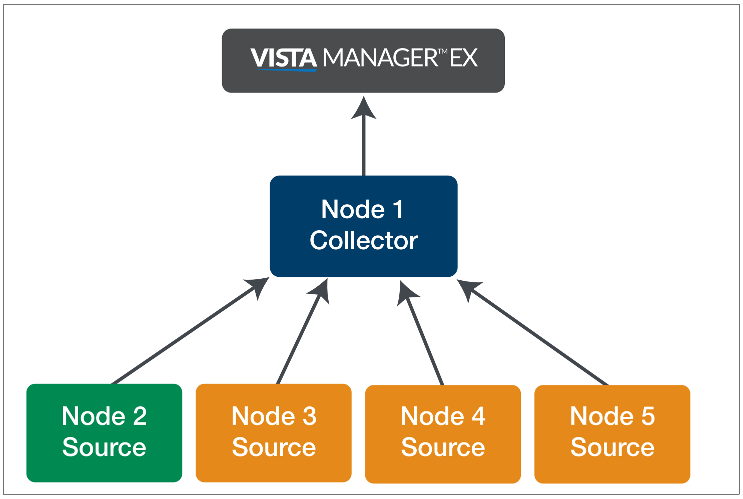
A non-STOAT device is simply any device that does not have STOAT configured. So this could include:

- Allied Telesis AlliedWare Plus device that supports STOAT, but doesn't have it configured
- Allied Telesis AlliedWare Plus device running a release that pre-dates STOAT
- Allied Telesis non-AlliedWare Plus device (WebSmart switch, unmanaged switch, Access Point, etc.)
- Third-party vendor switch
- Printer
- Laptop
- Camera
- Smart coffee machine
- And any other networked device that supports LLDP or DHCP.

How to connect your STOAT devices

Flat Collector network

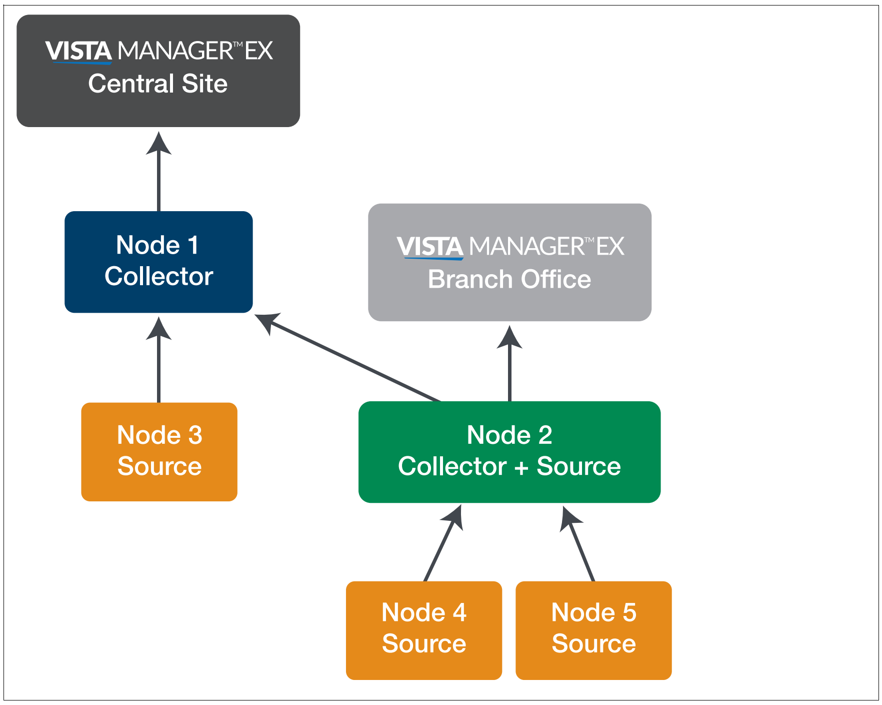
The simplest form of a STOAT network has a single Collector, that all other STOAT nodes have configured as a destination. This is the preferred layout for networks with a small number of STOAT devices (e.g., 50 or fewer) or in larger networks where the Collector is a powerful device such as a AMF Appliance Cloud.



Hierarchical Collector Network

Larger or more complex STOAT networks may require a hierarchy of Collectors. Arranging the Collectors in a hierarchy allows some of the work of the top Collector to be distributed more evenly across the network.

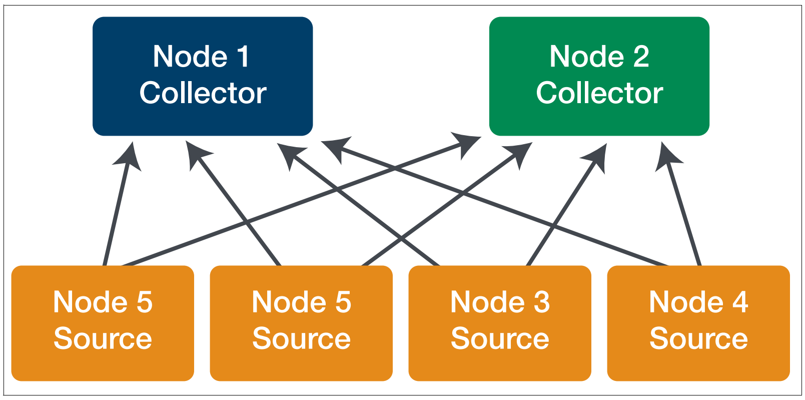
A hierarchical network also allows a hierarchy of Vista Manager EX instances. This may be useful in scenarios involving large networks with multiple branch offices, where the primary Vista Manager EX instance located at a central site can have comprehensive visibility, while additional Vista Manager EX instances co-located with the branch offices can solely observe the topology of their respective branch office.



Redundant Collector network

Each STOAT Source can be configured with multiple destinations. This allows the construction of STOAT networks with redundant Collectors.

Care should be taken when configuring multiple destinations, as each additional destination increases the workload of the STOAT Source.



Configuring STOAT

To configure a STOAT network, follow these general steps:

- "Enable the STOAT service and STOAT discovery protocols" on page 9
- "Configure a STOAT Collector" on page 10
- "Configure STOAT Sources" on page 11
- "Enable LLDP on non-STOAT devices" on page 11

Enable the STOAT service and STOAT discovery protocols

Step 1: Enable the STOAT service

```
awplus(config)# service stoat
```

Step 2: Enable discovery via LLDP

If the device supports LLDP, STOAT can use it as a discovery protocol. Note: LLDP is supported on AMF Cloud in single-tenant mode, but not on other virtual devices, or on the VST-APL or 10GbE Firewall network appliances:

Enable LLDP on all interfaces:

```
awplus(config)# lldp run
```

Enable LLDP as a STOAT discovery protocol:

```
awplus(config)# stoat discovery lldp
```

Step 3: Enable discovery via DHCP Snooping

If the device supports DHCP Snooping, STOAT can use it as a discovery protocol.

Enable the DHCP Snooping service:

```
awplus(config)# service dhcp-snooping
```

Enable DHCP Snooping on all required VLANs:

```
awplus(config)# interface <vid-list>
awplus(config-if)# ip dhcp snooping
```

If you are using an external DHCP server, mark the ports towards that server as trusted:

```
awplus(config)# interface <port-list>
awplus(config-if)# ip dhcp snooping trust
```

Enable DHCP Snooping as a STOAT discovery protocol:

```
awplus(config)# stoat discovery dhcp-snooping
```

Step 4: Enable discovery via Dot1X

If the device supports Port Authentication, STOAT can use it as a discovery protocol.

Enable Dot1X as a STOAT discovery protocol:

```
awplus(config)# stoat discovery dot1x
```

Configure a STOAT Collector

Select a device to be the STOAT Collector. This should be a powerful device that is centrally located in the network.

Step 1: Enable the STOAT service on the STOAT Collector

```
awplus(config)# stoat collector enable
```

Step 2: Enable a device to be a STOAT Collector

```
awplus(config)# service stoat
```

Step 3: Generate a number of STOAT keys

These keys match the number of Sources that will connect to this Collector.

```
awplus(config)# stoat collector key generate
F2jBktZRXBuiD1qG-zNPeDAuHv5k38zYw1FnVLCc21k=
awplus(config)# stoat collector key generate
CkXxcwcJCc8tD4LVHNWPwZgGUsWbQtYJXPHhkl3V4cg=
awplus(config)# stoat collector key generate
LdvU31CB2OHubE8S0291DAWbh2KltwEwkk8h35FBBjI=
```

Note: Store the generated output in a safe place, you will need it later, see "Configure STOAT Sources" on page 11.

- We recommended all Sources use unique keys, however it is possible for multiple Sources to share the same key.
- Adjust the Collector expiry-period to better handle network changes in Vista Manager EX. While 60 seconds is the recommended default for most networks, consider increasing it if large network segments frequently disappear and reappear:

```
awplus(config)# stoat collector expiry-period <10-300>
```

Step 4: Configure trustpoint (Optional)

- STOAT supports the use of trustpoints to establish full bi-directional trust between Sources and Collectors. STOAT can operate without trustpoints in a less secure mode of operation, however the use of trustpoints is highly recommended to ensure the security of the STOAT topology data.

  Create a new self-signed trustpoint for the STOAT Collector:

```
awplus(config)# crypto pki trustpoint stoat-collector
awplus(ca-trustpoint)# enrollment selfsigned
awplus(ca-trustpoint)# end
awplus# crypto pki trustpoint stoat-collector authenticate
awplus# crypto pki trustpoint stoat-collector enroll
```

- Alternatively you may create a CSR and use an external CA.

  Configure the STOAT Collector to use the new trustpoint:

```
awplus(config)# stoat-collector trustpoint stoat-collector.
```

Export the trustpoint CA certificate (store the output safely, you will need it in a later step):

```
awplus# crypto pki export stoat-collector pem
```

Configure STOAT Sources

All STOAT devices, other than the Collector, will need to configure a destination to the Collector.

Step 1: Create a destination to the IP address or FQDN of the Collector

```
awplus(config)# stoat destination 192.168.55.3
awplus(config-stoat-dest)#
```

Step 2: Configure the key, using one of the keys you generated earlier

```
awplus(config-stoat-dest)# key F2jBktZRXBuiD1qG-zNPeDAuHv5k=
```

Step 3: Ensure the destination is not shutdown

```
awplus(config-stoat-dest)# no shutdown
```

Step 4: Configure trustpoint (Optional)

If you have configured a trustpoint for the Collector, you should now create a matching trustpoint on the Source, and configure the destination to use it. The destination will use the trustpoint to verify the service certificate presented by the Collector was signed by the CA contained within the configured trustpoint.

- Create a new trustpoint to contain the Collector CA:

```
awplus(config)# crypto pki trustpoint stoat-collector
awplus(ca-trustpoint)# enrollment terminal
```

- Authenticate the trustpoint using the CA certificate you exported earlier:

```
awplus# crypto pki authenticate stoat-collector
<paste the ----BEGIN CERTIFICATE----text you recorded earlier here>
```

- Configure the STOAT destination to use the new trustpoint:

```
awplus(config)# stoat destination 172.16.0.1
awplus(config-stoat-dest)# trustpoint stoat-collector
```

- Optionally enable TLS name-check to verify the Collector’s server certificate contains the configured destination address. If you are unsure, skip this step.

```
awplus(config-stoat-dest)# name-check
```

Enable LLDP on non-STOAT devices

To get the best experience with STOAT, we recommend you enable LLDP on all non-STOAT devices you wish to discover. Additionally, for certain devices, when configuring the advertised LLDP TLVs, we recommend selecting all options in these cases.

For information on whether a specific Allied Telesis device supports LLDP and how to configure it, please consult the Document Library on our website: alliedtelesis.com.

Monitoring STOAT

You can use show commands to monitor the ongoing activities of STOAT:

- To display STOAT sessions, use the command **show stoat collector sessions**:

```
awplus#show stoat collector sessions

STOAT Collector Session Information:
------------------------------------

Sessions created                      : 1
Sessions expired                      : 0
Sessions failed                       : 0
Sessions failed sync authentication   : 0
Sessions failed update                : 0
Sessions failed update authentication : 0

Session ID                            : 133369FC
 Source IP Address                    : 192.168.1.2
 State                                : Active
 Counters
  Sync success                        : 1
  Sync failure                        : 0
  Update success                      : 0
  Update failure                      : 0
  Keepalive                           : 4
  RX bytes                            : 9076
```

- To display a list of keys, use the command **show stoat collector keys**:

```
awplus#show stoat collector keys

STOAT Collector Key Information:
                                                                  Last Used Time
Key                                           Description            (H:M:S ago)
--------------------------------------------------------------------------------
secretsecret                                  -                         00:00:14
```

- To display Source information, use the command **show stoat destinations detail**:

```
awplus# show stoat destinations detail

STOAT Destination Detailed Information:
---------------------------------------

Address                            : 10.0.0.1
 State                             : Active
 Session ID                        : 420F0F57
 Expiry-period                     : 60 seconds
 Counters:
  Sync OK                          : 1
  Sync failed - unreachable        : 0
  Sync failed - incompatible       : 0
  Sync failed - authentication     : 0
  Sync failed - bad response       : 0
  Sync failed - server error       : 0
  Update OK                        : 0
  Update failed - unreachable      : 0
  Update failed - authentication   : 0
  Update failed - unknown session  : 0
  Update failed - server error     : 0
  RX bytes                         : 30
  TX bytes                         : 26474                      -
```

Device discovery and removing a switch from a stack

If you remove a switch from a stack and use it elsewhere, you have to clean it first.

Each switch in a stack has an ID number, which can be an integer between 1 and 8. The default on each switch is a stack ID of 1. The ID number of a stack member is an important identifier. All commands that are port or switch specific need to use the stack ID to identify which stack member the commands apply to.

If you remove a switch from a VCStack and want to use it elsewhere in the network, return it to its factory default state first. This is essential if you are using Vista Manager EX or Device Discovery using STOAT, but we recommend doing it in all cases.

If you want to remove a switch from a stack, use the following steps:

1. Shut down all stacking links to the switch you wish to remove from the stack. This is optional but recommended, especially if someone other than you will do the step of physically uncabling the switch.
2. Remove all of the cabling used for stacking links.
3. Re-cable the remaining stack members together correctly.
4. Log into the disconnected device through its console port. If you use SSH to connect, you will lose connectivity to the switch after resetting it.
5. Reset the switch to its factory default state, using either of the commands:

   ```
   awplus# atmf cleanup
   ```

   or

   ```
   awplus# erase factory-default
   ```

   These commands are synonyms and will erase all NVS, all flash contents except for the boot release, a GUI resource file, and any license files.
6. Reboot the switch.
7. If you want to use the switch as a standalone switch, disable stacking using the command **no stack 1 enable** and reboot the device.

NOTES:
If the full factory-default reset is inconvenient, it is important to change or delete the ‘`stack virtual-chassis-id`’ in the startup configuration.

For devices running AlliedWare Plus software version 5.5.3-0.x or later, reset the device unique-id using the privileged exec command **unique-id** to avoid serious network conflicts.

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com