ASR9K Craft Tool (ACT) 1.5

- A device level management tool for ASR9K routers
- Supports IOS-XR 4.0 to 4.3.0
What is ACT?

- A Java client software runs on Windows/MAC/UNIX.
- Light weight tool for simple device level management, discovery, and configuration.
- Provides a fast, easy, and simple way to monitor and troubleshoot ASR9K family of routers.
- Real-time dynamic graphical view of the managed router.
- Real-time inventory, alarm monitoring, and any interface lookup and monitoring.
- Can be used to manage multiple routers and switch to individual router of interest.
- Provides configuration, fault, monitoring, and performance at the device level.
- Supports Telnet/SSHv1/SSHv2 connection to the router and provides terminal emulation interface for each protocol.
Table of Contents

- Overview
- Installing and Launching
- Uninstalling
- Access Permissions
- Router Requirements
- Login
- Network Element Dashboard
- Dynamic Shelf Display
- Satellite Management
- System Widget Panel
- Lookup Widget Panel
  - Interface Explorer
  - Bundle-Ether Explorer
  - XConnect Explorer
  - Bridge-Domain Explorer
  - Subscriber Explorer
- Monitor Widget Panel
- Configure Widget Panel
  - Template Manager
  - Lookup Configurations
  - License Manager
  - Configuration Editor
- Element UI Tabs
  - Inventory Tab
  - Alarms Tab
  - Interfaces Tab
  - Packages Tab
  - SMU Manager
  - FP Device Tab
  - CLI Tab
- Telnet/SSHv1/SSHv2
- Managed NEs View
Overview
Supported Chassis

- ASR9006
- ASR9010
- ASR9001
- ASR9922
- Cluster Configurations

Supported Satellites

- ASR9000v, ASR901, ASR903
ASR 9006 Chassis View
ASR 9010 Chassis View
ASR 9010 Cluster Chassis View
Installing and Launching
Java Runtime Environment (JRE)

- Requires JRE version 1.6 or higher.
- The Installation script (`SetupACT.cmd` or `SetupACT.sh`) requires JRE to be in the search path.
**Existing ACT Users**

- If you installed ACT previously, you must uninstall it before installing the new ACT. Refer to the next section Uninstalling.

- You may also want to backup LoginInformation.xml. This file contains all the device profiles you have created. It resides in act\versions\1.0.

- On Windows, it may be under
  
  ```
  C:\Documents and Settings\<username>\act\versions\1.0
  C:\Users\<username>\act\versions\1.0
  ```

- Install the new ACT (see next page).

- Copy LoginInformation.xml back to the same folder.
Windows User Installation

- Create a new folder and unzip ACT.zip to the newly created folder.
- Double-click SetupACT.cmd.
- You should see the installation starts.
- Once the installation is successful, a desktop icon for ACT is created.
- Double-click the desktop icon to launch the ACT software.

If you don’t see the installation starts, it’s possible that JRE is not in the search path. If you have already installed JRE, it should be under one of these folders.

- C:\Program Files\java
- C:\Program Files (x86)\java (Windows 7)

Follow the next section to include JRE in the search path or open a DOS window, change directory to the newly created folder, and type “<JREDir>\bin\java -jar installer.jar”

<jREDir> may be “C:\Program Files (x86)\java\jre6”
Include JRE in the Search Path

On Windows 7
- Click the Environment Variables button
- On the System variables box, select “Path” and click the Edit button. Append C:\Program Files\java\jre6\bin into the search path and click the OK button.

On Windows XP
- Open Windows Control Panel – System – Advanced Tab
- Click the Environment Variables button
- On the System variables box, select “Path” and click the Edit button. Append C:\Program Files\java\jre6\bin into the search path and click the OK button.

Double-click SetupACT.cmd to install ACT again.
MAC User Installation

- Assume ACT.zip is on your MAC desktop.
- Double-click it to unzip the contents. It should create a folder called ACT.
- Open a Terminal Window, change directory to where you extracted the zip file. In this case, `cd /Users/<username>/Desktop/ACT`.
- Type `chmod 777 SetupACT.sh`.
- Run `./SetupACT.sh`.
- The SetupACT.sh script assumes java is in the search path. If that is not the case, you can invoke java (JVM) directly using the full path `/usr/bin/java -jar installer.jar`.
- You should see the installation starts.
- Once the installation is successful, a desktop icon for ACT is created.
- Double-click the desktop icon to launch the ACT software.
UNIX User Installation

- Open a Terminal Window and unzip ACT.zip to a newly created folder (e.g., `unzip ACT.zip`)
- change directory to where you extracted the zip file.
- Type `chmod 777 SetupACT.sh`
- Run `./SetupACT.sh`
- The SetupACT.sh script assumes java is in the search path. If that is not the case, you can invoke java (JVM) directly using the full path
  
  `/usr/bin/java -jar installer.jar`
- You should see the installation starts
- To run ACT, go to the bin directory where you installed ACT. For example, if you installed ACT to `/users/<username>`, type
  
  `/users/<username>/act/bin/ACT1.4.cmd`

  to launch the ACT software.
Uninstalling
Uninstalling ACT

On Windows

- Go to the “act\uninstall” folder, click ACT<version>_uninstall.cmd
- On Windows XP, the act folder is under “C:\Documents and Settings\<username>”
- On Windows 7, the act folder is under “C:\Users\<username>”

On MAC

- Type /Users/<username>/act/uninstall/ACT<version>_uninstall.sh

On UNIX

- Simple remove the ACT application folder by typing “rm -R act”
Access Permissions

- The username and password used for ACT must be defined on the router.
- The router access permission assigned to a user is used to grant access to different areas of ACT.
- Router access permission is defined by group, usergroup, taskgroup, and task.
Access Permission Mappings

- The table below shows the mappings between default ASR9K user groups and ACT access privileges.

<table>
<thead>
<tr>
<th>Default ASR9K Groups</th>
<th>ACT Access Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>serviceadmin</td>
<td>None</td>
</tr>
<tr>
<td>operator</td>
<td>Can only access alarms</td>
</tr>
<tr>
<td>root-Ir</td>
<td>All areas except power/fan/license/package management</td>
</tr>
<tr>
<td>netadmin/sysadmin</td>
<td>All areas except the Configuration Widget Panel</td>
</tr>
<tr>
<td>root-system</td>
<td>All areas</td>
</tr>
</tbody>
</table>
Creating a Custom usergroup for ACT

By creating a custom ACT usergroup, “serviceadmin” and “operator” users can have additional privileges. The configurations below are recommended for all non-admin ACT users.

```plaintext
taskgroup act_user_group
    task read aaa
    task read l2vpn
    task read bundle
    task read sysmgr
    task read system
    task read drivers
    task read logging
    task read interface
    task read inventory
    task read basic-service
!
usergroup act_user_group
    taskgroup act_user_group
!
username operator
    group operator
    group act_user_group
    password 7 105D0C0B131E110E0D0027222A
!
```
Router Requirements
Router Requirements

The following packages are required on the ASR9K

- `asr9k-mgbl-p.pie` must be loaded
- `asr9k-k9sec-p.pie` must be loaded for SSHv1 & v2
  (for router with RSP3 card, the pie has “-px” instead of “-p” notation)

Required Router Configurations

- `xml agent tty` must be enabled
- `vty-pool default 0 20` to increase the default vty pool size to 20 (the default is 5 connections)
ACT supports three connection types

Depending on the Connection Type chosen, the RED configurations are required on the router.

1) XML over Telnet
   - telnet vrf default ipv4 server max-servers 20
2) XML over SSHv1
   - ssh server
   - hostname <hostname>
   - domain name <domain>
3) XML over SSHv2
   - ssh server v2
Both sshv1/v2 require crypto key on the router.
Login
Login Dialog

- The Login Dialog is displayed when ACT is launched.
- Enter the login information on the right-hand panel or create a login profile using “Add New Device”.
- You may also create Device Group and add devices to the group.
Login Dialog

- ACT uses the ASR9K authentication. The User Name and Password should have been defined.

- If there is direct connectivity between the computer which hosts ACT and the ASR9K, choose “IP” as the Connection Category. Otherwise select “Scripted”.

- There are three Connection types namely Telnet/SSHv1/SSHv2.

- For “IP” Connection Category, the Node IP address is the ASR9K Management IP address.
Scripted Login

- If ACT does not have direct connectivity to the ASR9K, select “Scripted” as the Connection Category (e.g. the ASR9K may be behind a intermediate server).
- Once “Scripted” is selected, different login parameters are shown.

  - Scripted User Name/Password. The intermediate server username and password.
  - Node Name/Port. The intermediate server name or IP.
  - Click “…” to add additional script information.
Login Script Steps

- The “Wait For” data fields contain prompted string returned by the intermediate server.

- When ACT sees the “Wait For” string, it responses by sending the data defined in the “Send” data field.

- Scripted Username/Password are intermediate server authentication which should be supplied on the previous slide.

- When ACT sees the intermediate server’s prompt “sj20lab-as1:”, it initiates a telnet to the ASR9K with management IP address 1.76.22.19.
Concurrent Login

- You can use ACT to log into multiple devices simultaneously if they share the same username and password.
- To do so, select multiple devices by using the <Ctrl> / <Shift> key or select the entire device group.
Network Element (NE)
Dashboard
Network Element (NE) Selector

- The NE Selector displays all the currently logged in devices. Select another NE from the list will switch to that NE’s Shelf Display.
- To log into another device, click the Login toolbar icon. On successful login, the device IP/name will appear under the NE Selector.
**Bi-State Active Alarm Counters**

- Bi-state alarms are syslog messages which have two states (Active and Clear). Only alarms that have an active state are counted on the Bi-State Active Alarm Counters Window.

- The running count for each alarm severity is displayed from Emergency, Alert, Critical, Error, Warning, Notification and Informational (combined counter).

- To see the Bi-State Active Alarm details, click the Bi-State Active Alarms widget on the System widget panel.
System Information

- **Alarm Log.** The event buffer size can be configured using “logging events buffer-size” on the router. The default size is 96000 bytes.

- The Current Status shows the usage percentage of the event buffer on the router. If it is above 90%, incoming alarms/syslogs may be lost if they have lower severity than existing alarms/syslogs in the buffer.

- The Notification Channel “up” status indicates ACT is receiving notification from the router.

- **Auto-Refresh.** When enabled, ACT will perform necessary polling to update the Shelf Display and Bi-State Active Alarm Counters. This is to ensure ACT is in sync with the router in case incoming alarms/syslogs are missed when the event buffer is full. ACT uses the alarms/syslogs to determine card and physical interface status.
Dynamic Shelf Display
Dynamic Shelf Display

- Displays real-time inventory data in a graphical form with RSP and line card types.
- Displays RSP active/standby status.
- Displays physical interface status on ports (green = up, amber = down, red = admin-down). The port LED is not supported on channelized SPA cards.
- Overlays the highest severity bi-state alarm color on cards.
- Displays card Product Identification Number (PID) and bi-state alarm counters via the card tooltip.
- Displays real-time card states via the card LED tooltip.
- Reacts to real-time card insertion and removal notifications.
- Right-mouse context sensitive menu.
Satellite Management
Satellite Management

- IOS-XR 4.2.1 supports management of connected satellite switches to a single ASR9K or a Cluster (i.e. two ASR9K connected together).
- Supported satellite switches are
  - ASR9000v
  - ASR901
  - ASR903
- ACT provides the Satellite Explorer to help customers to visualize, monitor, lookup interfaces, and transfer packages to connected satellites.
Satellite Explorer

- Click on the main toolbar to launch the Satellite Explorer.
- The Satellite Explorer displays all the configured and discovered satellites of the current viewing ASR9K and the Inter-Chassis Links between them.
Satellite Explorer (Coloring)

- Inter-Chassis Links (ICL) that are in the Ready state are colored green. Otherwise they are colored red.
- For Bundle-Ether ICL, if all bundle members are in the Ready state, it is colored green. If at least one member (but not all) are in the Ready state, it is colored orange. Otherwise, it is colored red.
- Satellite nodes that are configured but none of its ICL is in the Ready state, they are colored red.
- Satellite nodes which do not have the latest package version are colored yellow on the table pane.
Inter-Chassis Links (ICL)

- When a mouse cursor is over an ICL, its state is displayed as a tooltip text. For Bundle-Ether ICL, the tooltip text displays the union of all bundle member states.

- The right mouse menu on the ICL provides access to the Inter-Chassis link port (interface) on the ASR9K and all the Satellite Ethernet access interfaces that are transported over this ICL via the Interface Explorer. In the case of a Bundle-Ether ICL, it also provides access to all of its bundle members.
Discover Satellites

- The Table displays the discovered satellites’ ID, Type, Serial Number, and Package Information.
- Single clicking the table row displays the selected satellite domain view on the right. If the satellite is inside a domain, ACT displays the domain view.
- Double clicking the table row displays the Satellite Desktop window.
- When a mouse cursor is over the Package Information cell, ACT displays the package detail information.
- To transfer package to the satellites, click the Package Transfer button.
Package Transfer

- From the Package Transfer Dialog, select the satellites which you want to perform the package transfer operation.
- Select the Package Transfer only or Transfer and Activate option.
- Click the OK button to initiate the operation.
- The transfer progress status will be displayed on the Package Info table column of the selected satellites. The Transfer and Activate option may reload the satellite.
Right mouse context sensitive menu

- The right mouse menu is available on the Main and the Domain views.
- Zoom In/Out/Reset. Control the zooming aspect of the display view.
- Center View. Zoom into the center of the display view.
- Fit Content to View. Ensure all the map elements are visible.
- Set Background Color/Image. Assign a color or an image as the background.
- Auto Layout. Perform automatic layout on map elements.
Satellite Topology Map with a Background Image
Creating a Domain

- A domain can be used to group satellites together for better viewing and management.
- To create a domain, select “Create New Domain” from the right mouse menu. A graphical icon representing a domain will appear.
- To include a satellite into a domain, drag the graphical icon representing the satellite over the domain icon.
- To enter the domain, double-clicking the domain icon or single click the satellite table row on the left.
- To return back to the Main View, click the up arrow toolbar icon.
- Or, when inside a domain, click “Go To Main View” on the right mouse menu.
- Right mouse menu is also available on a domain icon.
Positioning Map Nodes in the Center

- The canvas which map components are displayed on is much larger than the viewable area. The horizontal and vertical scrollbars can be used to position the viewable area.

- The background image, when selected, is always positioned in the center of the canvas. It can be used as a reference to position all the map nodes.

- Follow the steps below to organize map components to display in the center of the canvas.

  - Adjust both horizontal and vertical scrollbars to the center as shown below.

  - Invoke the Auto Layout feature.

  - Additionally, use the background image as a guide as it is always displayed in the Center.
Satellite Desktop Window

- Double-click the satellite graphical icon to launch the Satellite Desktop window.
- Or, double-click the satellite table row.
- Or, right-click on the satellite graphical icon and select “Open Node”.

![Satellite Desktop Window](image)
Sensors & Inter-Chassis Links
System Widget Panel

- **File Systems** – Displays the utilization information of various file systems.
- **Fan Status** – Displays the RPM of each fan on a fan tray.
- **Power Status** – Displays the wattage readings of each power module.
- **Synchronize ACT** – Re-synchronizes the Bi-state Active Alarm Counters and the Dynamic Shelf Display with the router.
File Systems/Fan Status/Power Status
Synchronize ACT

- When the Synchronize ACT widget is clicked, ACT retrieves inventory data, bi-state alarms, and physical interface information from the router and re-synchronizes its UI displays (i.e. the Bi-State Alarm Counters and the Shelf Display).

- ACT also provides an automatic 3 minute refresh cycle. When the timer counts down to 0 second, it performs the synchronization. Uncheck the checkbox to disable the automatic refresh. Once unchecked, ACT will only listen to notification without performing polling. This makes ACT more responsive.

Why is there a need to synchronize ACT?

- ACT listens to syslog notifications sent by the Alarm Logger component on the router to update its Shelf Display. When the Alarm Logger buffer is full, it is possible that less important syslog messages are purged and this may cause missing notifications. The auto/manual synchronization remedies the issue. The alarm buffer size can be configured on the router using “logging events buffer-size <1024-1024000>”.

Lookup Widget Panel
Interface Explorer – supports lookup of any interface/sub-interface and provides monitoring function.

Bundle-Ether Explorer – supports lookup of any bundle-ethernet and provides monitoring function.

XConnect Explorer – supports lookup of any xconnect and provides monitoring function.

Bridge Domain Explorer – supports lookup of any bridge domain and provides monitoring function.

Subscriber Explorer – supports lookup of any subscriber and provides monitoring function.
Interface Explorer

- Provides any interface/sub-interface lookup and monitoring functions.
- Can be launched from a card right-mouse menu via an interface type or SPA port (Shelf Display) or the Lookup Panel.
- Allows filtering interfaces based on 1) a port, 2) from the CLI command "sh int brief | inc", or 3) a VRF.
- Filtered interfaces will be displayed along with their line states (green = up, amber = admin-down and others, red = down).
- The NE Summary hyperlink displays all interface types and their statuses on the NE.
- When an interface is selected, its attributes are displayed on the Interface Attributes pane.
Interface Attributes Pane

- The Interface Attributes pane displays the interface general information, data rates, packet counters, and configuration.
- The Toolbar provides monitoring and baselining functions.
- Monitoring function includes Manual Refresh and Automatic Refresh (by setting a polling interval).
- Baselining function sets/unsets pre-defined baseline counters.
- When set, the baseline counters are zeroed out and start incrementing if Manual/Automatic Refresh is turned on. When unset, they return back to the last up-to-date values.
Interface Attributes Pane - QOS

- The Interface QOS Statistics dialog can be launched from the QOS toolbar icon on the Interface Attributes pane. The icon is enabled when there is an “input” or “output” policy map assigned to an interface.

- The Dialog displays QOS statistics which include Classification, Queueing, and Policing using a hierarchical display. The child policy statistics are indented under the parent policy.
Bundle-Ether Explorer

- Provides any bundle-ether lookup and monitoring functions.
- Can be launched from the Lookup Panel.
- The Explorer first retrieves all bundle-ethers from the NE.
- When a bundle-ether is selected, its bundle members and all of its sub-interfaces are available for selection.
- The Overview pane displays bundle summary on the NE and the last selected bundle member.
- When a bundle member or sub-interface is selected, its attributes are displayed on the Interface Attributes pane.
XConnect Explorer

- Provides any xconnect lookup and monitoring functions.
- Can be launched from the Lookup Panel.
- The Explorer first retrieves all xconnect groups from the NE.
- When a xconnect group is selected, its xconnects are retrieved from the NE. When a xconnect is selected, its segments are displayed.
- The Overview pane displays the xconnect summary on the NE and the selected xconnect configuration.
- When a segment is selected, if it’s an interface, its attributes are displayed on the Interface Attributes pane.
- For a pseudowire segment, its attributes are displayed on the Pseudowire Attributes pane.
Bridge Domain Explorer

- Provides any bridge domain lookup and monitoring functions.
- Can be launched from the Lookup Panel.
- The Explorer first retrieves all bridge groups from the NE.
- When a bridge group is selected, its bridge domains are retrieved from the NE. When a bridge domain is selected, its segments are displayed.
- The Overview pane displays the bridge group summary on the NE, the selected bridge domain, and its configuration.
- When a segment is selected, if it's an interface, its attributes are displayed on the Interface Attributes pane.
- For a pseudowire segment, its attributes are displayed on the Pseudowire Attributes pane.
Subscriber Explorer

- Provides any subscriber lookup and monitoring functions via the Subscriber and PPoE Access Interfaces tabs.
- Can be launched from the Lookup Panel.
- Subscriber interfaces can be retrieved using CLI like filter. The filter text entered will be used for “sh subscriber session all | inc <Filter Text>”. If nothing was entered, it would retrieve all subscribers.

- Depending on the subscriber type selected (PPP/PPPoE or IP), the related information is displayed on the tabbed view on the right-hand side.
- The “DHCP Summary/Bindings” link, when clicked, provides a snapshot of the DHCP binding information.
Subscriber Explorer

- The “Interface QOS statistics” icon on the Subscriber Details tab shows the subscriber interface QOS statistics with applied class maps.
- The “View Parent Interface” icon on the Subscriber Details tab launches the Interface Explorer with the subscriber’s access interface.
- The PPPoE Access Interfaces tab displays all access interfaces on a selected location of interest.
- Select an access interface and click the Show Subscribers button will switch to the Subscribers tab with all the subscribers under this access interface.
Monitor Widget Panel
Monitor Widget Panel

- Process CPU and Memory usage monitoring.
- Network Processor (NP) counter monitoring.
- Environmental Sensors – displays the card and port sensor readings.
Process Memory/CPU Monitoring

- Provides per-card per-process CPU and memory utilization information and monitoring functions.

### CPU Utilization

### Memory Utilization
NP Counter Display and Monitoring

- This feature is only available on NP-based line cards, not SPA cards.
- When a NP-based line card is selected, its physical ports are displayed.
- When a physical port is selected, the counters of the NP port which maps to the physical port are displayed.

NP counters with baseline enabled
Environmental Sensors

- Displays card and port sensors and provides monitoring functions.
- Can be launched from a card right-mouse menu or the System Panel.
- The Left-hand panel displays all available cards.
- When a card is selected, its sensors and their readings are displayed.
- The sensor types include temperature, voltage, current, and port DOM sensors.
- Monitoring function includes Manual Refresh and Automatic Refresh (by setting a polling interval).
- SPA card sensors are displayed with their parent card.
Configure Widget Panel
Template Manager
Configure Widget Panel

- Template Manager - creates CLI configurations based on a template.
- Configuration Editor – provides editing features for the Running Configuration file.
- Lookup Configurations – Displays the Running Configuration File in a sectionalized format for quick lookup.
- License Manager – provides functions for managing licensed features.
Configure Widget Panel
Template Manager
Template Manager

- A template contains a mix of CLI configuration commands or/and Apache Velocity Template Language (VTL).
- VTL is a simple, easy-to-use, and yet powerful language.
- Customers can define their own set of custom templates.
- The Template Manager processes the template and generates plain CLI configurations. Any uninitialized variables within the template will be prompted for user inputs.
- The plain CLI configurations can then be applied to the router.
- The Template Manager provides the capability to rollback previously committed configurations. It also provides a configuration lookup feature which allows copying of configurations into the system clipboard and pasting into the template.
Template Manager

- Right-mouse context sensitive menus are available when right-clicking on a folder or a template file. They are

On a Folder
- New Folder
- Rename Folder
- Delete Folder
- New Template

On a Template
- Delete Template
- Rename Template
Velocity Template Language (VTL)

- Reference variable begins with “$”, e.g. $vlanID
- “#set” directive provides variable initialization
  
  ```
  #set ( $vlanID = 1)
  #set ( $intf = “GigabitEthernet 0/1/0/1” )
  ```

- “#foreach” directive provides looping construct
  
  ```
  #set ( $interface_list= [“GigabitEthernet 0/1/0/1”, “GigabitEthernet 0/1/0/2”])
  #foreach ( $interface in $interface_list )
    interface $interface l2transport
    encapsulation dot1q 10
  #end
  ```

  Result:
  ```
  interface GigabitEthernet 0/1/0/1 l2transport
  encapsulation dot1q 10
  interface GigabitEthernet 0/1/0/2 l2transport
  encapsulation dot1q 10
  ```
Velocity Template Language (VTL)

- “#if, #elseif, #else” directives provide conditional branching

  “%” is a modulus operator. The following condition returns true if the vlan ID is an even number.

  
  ```
  #if ($vlanID % 2 == 0)
   ....
  #elseif
   ....
  #end
  ```

For more information on VTL, visit
VTL Examples

- An example to create two hundred L2 sub-interfaces

```vttl
#set ( $vlanID = 10 )
#foreach ( $subinterface in [1..200])
  interface GigabitEthernet 0/1/0/1.$subinterface l2transport
  encapsulation dot1q $vlanID
  #set ( $vlanID = $vlanID + 1 )
#end
```

- An example of a L2 Bridge Domain template. Since the variables are not defined. ACT will prompt for them at run-time.

```vttl
bridge group $bridgeName
  bridge-domain $bridgeName
    #foreach ($interface in $interfaces)
      interface $interface
    #end
```

**Result:**
- bridge group TDM-VRRP1
- bridge-domain TDM-VRRP1
- interface Bundle-Ether10.521
- interface Bundle-Ether30.521
- interface GigabitEthernet0/7/0/36.521
To process a template, select the template of interest and click the Process Template button. This will launch the Template Configuration Wizard.
On the 1\textsuperscript{st} page, the Template Configuration Wizard scans the template and prompt the user for un-initialized variables.

To lookup an interface from the router, click the binoculars icon. Currently, it only displays the physical interface. Adjustment to the name may be required after you select the physical interface.
Template Configuration Wizard – 2nd page

- Click the Check Syntax button to syntax check the generated configurations.
- Click the Commit Configurations button to commit the generated configurations.
- Depending on the size of the configurations, these two operations may take some time to complete.
Some variable names have a special meaning to ACT. When ACT sees them, it displays a binoculars icon next to the variable name. The binoculars icon, when clicked, invokes certain lookup functions.

These are the well-known variables:

- `interface`, `interface_list` - display all physical interfaces
- `bridge_group` - display all defined bridge group
- `xconnect_group` - display all defined xconnect_group
- `vrf` - display all defined VRF
Template Manager - Rollback

- Click the Rollback Configurations toolbar icon to display all the rollback points and apply the desired rollback point.
Configure Widget Panel
Lookup Configurations
Lookup Configurations

- Provides a quick and easy way to lookup the Running Configuration file contents. It sectionalizes the configurations by groups.
- When a group or an item under the group is selected, it displays the configurations on the right-hand panel.
- Using the filter, a user may enter portion of the group or item text for a quick lookup.
Configure Widget Panel
License Manager
License Manager

- Displays all the available feature licenses on the ASR9K and their assigned locations and their statuses.
- The toolbar icons allow the user to perform Add License, Configure License, Move License, Backup License, and Restore License.
License Manager – Add/Backup/Restore Licenses

- The Add/Backup/Restore License functions present a similar UI which prompt for the local disk or tftp location.
- The Restore License function will cause all existing licenses to be erased after a successful restoration.
License Manager – Configure Licenses

- The Configure License Dialog displays the current configured license features and allows a user to configure license to other locations.
- If the checkbox “all” is checked, the user must un-select it first before selecting other locations.
- Depending on the XR release version, it may be required to configure a location to a feature license before a license is available to that location.
License Manager – Move Licenses

- The Move License Dialog provides a function to move a selected feature license from one slot to another slot.
- Using the same dialog, a user can also move a selected feature license from the Allocated state back to the Available state.
- Depending on the XR release version, it may be required to configure a location to a feature license before a license can be moved to that location.
Configure Widget Panel
Configuration Editor
Configuration Editor

- Supports grouping of CLI configurations. Allows expand and collapse of those groupings.
- Supports locking of configuration file for mutual exclusive changes.
- Supports viewing of uncommitted configurations.
- Supports saving configurations to an external file.
- Supports loading of a configuration file on the router.
- Supports keyword highlightings.
- Supports hyper-linking rules.
- Supports change tracking.
- Supports syntax checking.
- Supports configuration rollback.
- Supports “?” for command-line interface help.
Configuration Editor – Change Tracking

- The change tracking feature highlights text whenever a change is made to the text.

<table>
<thead>
<tr>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>Line of configuration that you chose to delete. After you click Apply, the line is deleted.</td>
</tr>
<tr>
<td>Green</td>
<td>New line of configuration that you added since the last time you clicked Apply.</td>
</tr>
<tr>
<td>Cyan</td>
<td>Existing line of configuration that has been modified since the last time you click Apply.</td>
</tr>
</tbody>
</table>
Configuration Editor – Syntax Checking

- This feature allows a chosen block of text or the entire contents of the Configuration Editor to be checked for syntax errors.
- Select the text, if you want to check a block of text
- Choose Tools -> Syntax Check Selection. The syntax is checked.
- If there is a syntax error, an invalid command error is displayed in red in the Configuration Editor

```
00164  interface Loopback1000
00166  !
00167  interface MgmtEth0/0/CPU0/0
00168  description Management Ethernet
00169  ^
00170  % Invalid input detected at '^' marker.
00171  ipv4 address 172.19.75.41 255.255.255.128
00172  !
00173  !
```
The hyperlink rules reside in the hyperlinkrules.txt text file.

Example:  < anchor expression > : < hyperlink expression >

An anchor or hyperlink expression consists of a fixed string of text followed by an asterisk to designate the word to be hyperlinked and is used as the keyword to match the hyperlink to the corresponding section of configuration. Anchor expressions must always point to top-level (nonsubmode) configuration.

You can have only one rule definition for each line in the hyperlink rules file. In addition, you can have only one anchor expression and one hyperlink expression for each line.
Rule for linking references to access-lists to the corresponding access-list definition:

```plaintext
< ipv4 access-list * > : < ipv4 access-group * >

Ipv4 access-list test-list
   12 remark is a test
   !

Interface POS0/1/0/0
   ipv4 access-group test-list ingress
   !
```
Configuration Editor – Hyperlinking Rules Example

- **Example:** `< interface * > : < interface * >`
- When the mouse cursor is over the hyperlink, the definition of the interface is displayed.

```
00627  □ router ospf 100
00628     router-id 20.20.20.20
00629  □ area 0
00630     interface GigabitEthernet0/0/0/1
00631     !
00632     interface GigabitEthernet0/1/0/1
00633     !
00634     !
00635     !
00636  □ l2vpn
00637     bridge group bg
00638     !
```

[interface GigabitEthernet0/1/0/1
- negotiation auto
- transceiver permit pid all]
The Command-Line Interface (CLI) help feature provides a list of valid commands. Press ? to display a popup list of valid commands. Choose a command from the list to insert it into the Configuration Editor.
Element UI Tabs
UI Table Related Toolbar Icons

- The following toolbar icons apply to the UI tab applications (i.e. Tabs on the right-hand side of the Main Screen)

- ![Icon](image)
  Supports table printing

- ![Icon](image)
  Supports table export

- ![Icon](image)
  Supports table Find and Find Next

- ![Icon](image)
  Supports table refresh

- ![Icon](image)
  Supports table column preferences
Inventory Tab
Inventory Tab

- Displays inventory data in a tabular form.
- Display information includes Type, Description, Vendor Type, Name, Hardware Revision, Software Revision, Firmware Revision, Serial Number, Manufacturer Name, Alias, Asset ID, and FRU.
- Supports filtering based on column criteria.
- Supports printing and exporting of tabular data.
- Supports column re-arrangement through the Preference dialog.
- Supports Find and Find Next operation.
Alarms Tab
Alarms Tab

- Displays alarm entries include bi-state and non bi-state alarms.
- Display information includes TimeStamp, Severity, State, Alarm ID, Source, Category, Correlated ID, Event Code, Group, and Additional Text.
- Supports filtering based on severity, time range, alarm state, and alarm ID range criteria.
- Supports printing and exporting of tabular data.
- Supports column re-arrangement through the Preference dialog.
- Supports Alarm Clear and Purge operations. Both operations alter the alarm entries on the router.
- Supports Find and Find Next operation.
## Alarm Severity Descriptions and Associated Color

<table>
<thead>
<tr>
<th>Alarm Severity</th>
<th>Color</th>
<th>Description (Logged System Messages)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency</td>
<td>Red</td>
<td>System unusable.</td>
</tr>
<tr>
<td>Alert</td>
<td>Purple</td>
<td>Critical system condition exists and requires immediate action.</td>
</tr>
<tr>
<td>Critical</td>
<td>Orange</td>
<td>Critical system condition exists.</td>
</tr>
<tr>
<td>Error</td>
<td>Yellow</td>
<td>Noncritical errors exist.</td>
</tr>
<tr>
<td>Warning</td>
<td>Blue</td>
<td>Warning conditions exist.</td>
</tr>
<tr>
<td>Notification</td>
<td>Green</td>
<td>Notifications of changes exist to system configuration.</td>
</tr>
<tr>
<td>Informational</td>
<td>Green</td>
<td>Information about changes to system state exists.</td>
</tr>
</tbody>
</table>
Alarm Viewer

- Bi-state alarms are syslog messages which have two states (Active and Clear). Select the Bi-State Active Alarms Only checkbox to display only the Bi-state alarms.

- Invoke the Alarm Filter dialog for further filtering.

- Clear Alarms with State = Active. The alarms must be selected first.

- Purge Alarms with State = Cleared. The alarms must be selected first.
Alarm Viewer – Alarm Filter Bar

- Only applicable to alarms that have been retrieved and displayed on the Alarm Viewer table.
- Can be used to filter on a particular Alarm Category, Group, and Event Code.
- Click on the down arrow to open the cascaded menu.
- Click on the heading (e.g. PKT_INFRA) to display all alarms under this heading.
- To see all the alarms again, click the Alarm Category/Group/Event Code heading.
ACT constantly listens to alarm notification from the network element. When new alarms are available, ACT displays a yellow bell icon.

To refresh the Alarm Viewer table, click the Refresh icon on the main tool bar.
Interfaces Tab
InterfacesTab

- Displays all the interfaces on the router.
- Display information includes Name, Parent Interface, MTU, Encapsulation, Interface State, Line State, and Bundle Parent.
- Supports filtering based on column criteria.
- Supports printing and exporting of tabular data.
- Supports column re-arrangement through the Preference dialog.
- Supports Find and Find Next operation.
Packages Tab
Packages Tab

- Displays all active (including un-committed) and in-active packages on the router. Un-committed packages are highlighted in yellow or orange.
- Supports “Install Add” via a TFTP host accessible by a router.
- Supports “Install Activate”, “Remove”, “Install Commit”, and “Deactivate”.
- Displays package details on each RSP and line card.
- Displays installation log of the router.
- Supports software image upgrade and downgrade.
- Supports SMU management.
Packages Tab (Install Add Operation)

- Click the Add button and on the Add Package Dialog, enter the file path of the image and click the Add to Install List button.
- Select the package from the list and click the Install Add button.
Packages Tab (Install Activate Operation)

- To activate packages, select them on the Inactive Packages panel and click the Activate button to start the Install Activate operation.
After the Install Activate operation is completed, the packages are displayed on the Active/Committed Packages area. The orange highlight indicates the package has not been committed to the router yet.
Packages Tab (Install Commit Operation)

- To commit packages to the router, click the Commit button.
- Once the packages are committed, they will be shown with a white background color.
Packages Tab (Install Deactivate Operation)

- To deactivate packages, click the Deactivate button and select the packages of interest.
- If the packages have not been committed to the router, they will be moved to the Inactive Packages area after the deactivate operation.
- If the packages have already been committed to the router, they will be shown with a yellow highlight after the deactivate operation.
- To remove the yellow highlighted packages, click the Install Commit button.
Packages Tab (More on Install)

- All Install operations are done asynchronously. The progress status of the operation is displayed in blue text.
- Once the operation is completed, click the Install Log button to inspect the installation status.
- Once the Install Activate, Commit, or Deactivate operation starts, the “Install Abort” button will be enabled after the router accepted the request.
- If the operation is not abortable anymore, the Install Abort button will be disabled.
Packages Tab (Package Details)

- Click the Package Details button to see the individual components within each package on each line card.
Packages Tab (Upgrade to new XR SW)

- Refer to The ASR9K Upgrade/Downgrade document and HW/SW Compatibility Matrix for detailed instructions, and any pre-requisites:
- ACT can also be used to upgrade to new XR SW Packages
- Note 1: It is recommended that you perform the ‘activate test’ operation before upgrading to new SW Packages. This can be accomplished by checking the “Run this operation in Test Mode” checkbox during the Activate operation. Then examine the Install Log for compatibility issues.
- Note 2: New SW packages activate triggers a reload of Router; ACT will disconnect for some time till new packages are active and configs are applied
Manage Packages Tab (Upgrade to new XR SW) – ‘Install Add’

- To upgrade to a newer XR software, add the software packages to the list box. In the example below, the upgrade is from 3.9.1 to 3.9.2.

- Select the packages and click the Install Add button.
Manage Packages Tab (Upgrade to new XR SW) – ‘Install Activate’

- Select the new XR software packages and check the “Run this operation in Test mode” checkbox before activating.
- Check the Install Log for any issues.
- If there is no issue, initiate the actual activation by unchecking the “Run this operation in Test mode” checkbox.

- During the upgrade, the router will reload and ACT will disconnect.
- When ACT re-connects, click the Refresh button to see the new upgraded packages.
Packages Tab (Upgrade to new XR SW) – ‘Verify New SW’

- The new version shows up on the System Information panel.

- To commit the new software version, click the Commit button.
Packages Tab (Upgrade to new XR SW) – ‘Package Details of New SW’

- To verify the new software version on each line card, click the “Package Details” button.
The SMU Manager

- The SMU Manager helps validate SMUs that can be installed onto the NE. It verifies if the correct software version, platform (-p, -px), and package dependencies are met. It also displays SMU statuses on the NE.
- It can be launched from the Packages tab via the SMU Manager button.
The SMU Manager

- Read the instructions carefully before proceeding. Click Next to continue.

Welcome to the SMU Manager

Software Maintenance Upgrade (SMU) is a software 'patch' delivery unit which once installed and activated provides a 'point-fix' for a critical issue in a given software release.

The SMU Manager will guide you through the necessary processes. You will be prompted to specify:

- **TFTP Directory Path** - This path will be prepended to the selected SMUs to form a complete installation path.
- **SMU Repository Directory** - Absolute directory where SMUs are stored and can be located on your file system.
- **SMU Meta File** - This file describes SMUs that are available for a particular IOS-XR release and can be obtained from Cisco.

To continue, click Next.
The Directory and File Locations page

- Define the TFTP Directory Path, SMU Repository Directory, and SMU Meta File.
- To create a customized SMU meta file, click Create Custom Meta File.
- To create a SMU conformance report, click Create Conformance Report.
Create a Custom Meta File

- This feature allows the users to create a custom meta file to be used to validate a set of NEs with a user-defined SMU list from a selected SMU meta file.
- Click the Create Custom Meta File button and select the desired SMUs. When finished, click the Save button.
Create a Conformance Report

- Click the Create Conformance Report button. ACT uses the SMU meta file to validate SMU conformance on the NE.
The SMU Pre-Installation page

- After clicking Next on the Directory and File Locations page, the SMU Manager uses the SMU meta file to validate SMUs in the SMU repository and the device.

- Only SMU entries with green highlight color are available for install as they are found in the SMU repository.

- SMU entries that are highlighted in red represent SMUs that not found in the SMU repository and may require download from Cisco.

- Other highlights on the SMU entries represent different SMU status on the device.
The Install Add Operation

- To proceed, select the SMU entries with green highlight color and click the Install Add button on the SMU Pre-Installation page.
- ACT performs SMU dependency check. If the check fails, ACT displays the Pre-requisite SMUs Dialog.
- If the check succeeds, the user is presented with the Add Package dialog.
- Click the Install Add button on the Add Package dialog to start the Installation.
View the SMU Details

- Double-click on any table row of interest to display additional information about the SMU.
View the DDTS Information

- To view the DDTS information, the user must have Internet access and cisco.com username and password.
- Double-click on a hyperlink under the DDTS column to launch the browser.

To view the DDTS information, the user must have Internet access and cisco.com username and password. Double-click on a hyperlink under the DDTS column to launch the browser.

Remote ping packets are lost when multiple IPSLA sessions are configured

Symptom:
A few remote ping packets are lost by LPTS when multiple IPSLA sessions are configured.

Conditions:
- Multiple IPSLA session for reachability check are configured
- Remote ping packets are incoming with high rate

Workaround:
There is no workaround when IPSLA sessions are exist.
FP Device Tab
FPD Devices Tab

- Displays all the Field Programmable Devices with their hardware and software versions. In addition, the FPD devices which require software upgrade are highlighted.
CLI Tab

- Allows the user to send non-admin CLI operational command (i.e. show).
- Provides intelligent help tips while formulating the CLI command.
- Supports tab completion while formulating the CLI command.
- Supports Find, Find Next, Find Previous, Highlight, and Match Case operations on returned results.
- Supports copying of results to the Windows clipboard.
- Supports saving of results to an external file.
Managed NEs View
Managed Network Elements View

- The Managed NEs view displays all the connected network elements and their connectivity statuses. To access this view, click the Managed NEs tab.

- The connectivity icon with a red cross indicates that ACT previously established a connection to the NE, but it is no longer connected. In the background, ACT will attempt to re-establish the connection.

- To switch to the individual network element, double-click the network element name.
Consolidated Alarm Viewer

- The Consolidated Alarm Viewer is shown when the Managed NEs view is entered. It is similar to the Element level Alarm Viewer. The only difference is, by default, it displays alarms from all the connected network elements. To select alarms from particular network elements, use the Alarm Filter dialog.
Telnet/SSHv1/SSHv2
Telnet/SSHv1/SSHv2 (via Toolbar Icons)

- Provides direct CLI connection to the router via non-secure or secure connection protocols.
- Supports screen information capturing.
- Supports processing of batch mode commands.
- Supports loading and saving of previously used commands.
- Supports copying of last executed command.
- Supports copy of selected text and paste operation.
- Supports color and font preferences.
Telnet/SSHv1/SSHv2 – Launch Screen Capture

- Highlight the texts on the window and click the Camera icon to capture the selection. If you do not choose any text, the entire contents are captured.

![Telnet Plus - 172.27.149.141](image)

<table>
<thead>
<tr>
<th>Intf</th>
<th>Name</th>
<th>State</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>FE10</td>
<td>down</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>FE100</td>
<td>down</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Lo0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>Nu0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>Mg0/RSP0/CPU0/0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>Mg0/RSP0/CPU0/1</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>Mg0/RSP1/CPU0/0</td>
<td>admin-down</td>
<td>admin-down</td>
<td></td>
</tr>
<tr>
<td>Mg0/RSP1/CPU0/1</td>
<td>admin-down</td>
<td>admin-down</td>
<td></td>
</tr>
<tr>
<td>Gi0/0/0/0</td>
<td>down</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Gi0/0/0/1</td>
<td>down</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Gi0/0/0/2</td>
<td>down</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Gi0/0/0/3</td>
<td>admin-down</td>
<td>admin-down</td>
<td></td>
</tr>
<tr>
<td>Gi0/0/0/4</td>
<td>down</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Gi0/0/0/5</td>
<td>down</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Gi0/0/0/6</td>
<td>down</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Gi0/0/0/7</td>
<td>down</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Gi0/0/0/8</td>
<td>down</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Gi0/0/0/9</td>
<td>down</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Gi0/0/0/10</td>
<td>down</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Gi0/0/0/11</td>
<td>down</td>
<td>down</td>
<td></td>
</tr>
</tbody>
</table>

![Telnet Capture - 172.27.149.141](image)

<table>
<thead>
<tr>
<th>Intf</th>
<th>State</th>
<th>State</th>
<th>Interface</th>
<th>MTU</th>
<th>BW</th>
</tr>
</thead>
<tbody>
<tr>
<td>FE10</td>
<td>down</td>
<td>down</td>
<td>ARPA</td>
<td>1514</td>
<td>0</td>
</tr>
<tr>
<td>FE100</td>
<td>down</td>
<td>down</td>
<td>ARPA</td>
<td>1514</td>
<td>0</td>
</tr>
<tr>
<td>Lo0</td>
<td>up</td>
<td>up</td>
<td>Loopback</td>
<td>1500</td>
<td>0</td>
</tr>
<tr>
<td>Nu0</td>
<td>up</td>
<td>up</td>
<td>Null</td>
<td>1500</td>
<td>0</td>
</tr>
<tr>
<td>Mg0/RSP0/CPU0/0</td>
<td>up</td>
<td>up</td>
<td>ARPA</td>
<td>1514</td>
<td>1000000</td>
</tr>
<tr>
<td>Mg0/RSP0/CPU0/1</td>
<td>up</td>
<td>up</td>
<td>ARPA</td>
<td>1514</td>
<td>1000000</td>
</tr>
<tr>
<td>Mg0/RSP1/CPU0/0</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA</td>
<td>1514</td>
<td>1000000</td>
</tr>
<tr>
<td>Mg0/RSP1/CPU0/1</td>
<td>admin-down</td>
<td>admin-down</td>
<td>ARPA</td>
<td>1514</td>
<td>1000000</td>
</tr>
<tr>
<td>Gi0/0/0/0</td>
<td>down</td>
<td>down</td>
<td>802.1Q</td>
<td>1514</td>
<td>1000000</td>
</tr>
<tr>
<td>Gi0/0/0/1</td>
<td>down</td>
<td>down</td>
<td>802.1Q</td>
<td>1514</td>
<td>1000000</td>
</tr>
<tr>
<td>Gi0/0/0/2</td>
<td>down</td>
<td>down</td>
<td>802.1Q</td>
<td>1514</td>
<td>1000000</td>
</tr>
<tr>
<td>Gi0/0/0/3</td>
<td>admin-down</td>
<td>admin-down</td>
<td>802.1Q</td>
<td>1514</td>
<td>1000000</td>
</tr>
<tr>
<td>Gi0/0/0/4</td>
<td>down</td>
<td>down</td>
<td>802.1Q</td>
<td>1514</td>
<td>1000000</td>
</tr>
<tr>
<td>Gi0/0/0/5</td>
<td>down</td>
<td>down</td>
<td>802.1Q</td>
<td>1514</td>
<td>1000000</td>
</tr>
<tr>
<td>Gi0/0/0/6</td>
<td>down</td>
<td>down</td>
<td>802.1Q</td>
<td>1514</td>
<td>1000000</td>
</tr>
<tr>
<td>Gi0/0/0/7</td>
<td>down</td>
<td>down</td>
<td>802.1Q</td>
<td>1514</td>
<td>1000000</td>
</tr>
<tr>
<td>Gi0/0/0/8</td>
<td>down</td>
<td>down</td>
<td>802.1Q</td>
<td>1514</td>
<td>1000000</td>
</tr>
<tr>
<td>Gi0/0/0/9</td>
<td>down</td>
<td>down</td>
<td>802.1Q</td>
<td>1514</td>
<td>1000000</td>
</tr>
<tr>
<td>Gi0/0/0/10</td>
<td>down</td>
<td>down</td>
<td>802.1Q</td>
<td>1514</td>
<td>1000000</td>
</tr>
<tr>
<td>Gi0/0/0/11</td>
<td>down</td>
<td>down</td>
<td>802.1Q</td>
<td>1514</td>
<td>1000000</td>
</tr>
</tbody>
</table>
Telnet/SSHv1/SSHv2 – Process Batch Mode Commands

- Batch Mode allows the user to execute multiple CLI commands from an external file and optionally capture the outputs to an external log file.
- As an example, the command file input.txt may include:
  ```
  terminal length 0
  sh platform
  sh inventory
  ```

There are two modes of operations:

- Run - All commands in the batch file are executed at once, one after another.
- Step – Commands can be executed one at a time.
Telnet/SSHv1/SSHv2 – Executing a Batch Mode File

- If Run is chosen, the Telnet Batch Mode dialog box is closed and the commands are run sequentially.
- If Step is chosen, the Telnet Batch Mode dialog box is closed and a Step Mode dialog box appears.

Click Step to execute a command.
Click Continue to run through all the commands sequentially without stopping.
Click Stop to stop the execution of a command.
Click Cancel to close the Step Mode dialog box.
To view the logged contents, click the Process Batch Mode Commands icon and the View button.
The Telnet and SSH applications have an internal clipboard that allows you to copy, save, and load commands in a command list.

You can copy the last command executed to the Clipboard by clicking the Copy Last Command icon (circled in red).

The saved commands can be saved to an external file.
Telnet/SSHv1/SSHv2 – Preferences

- You can customize the following Telnet and SSH preferences:
  - Background color
  - Foreground color
  - Font type, size, and style
  - Buffer size (number of lines displayed)
The End