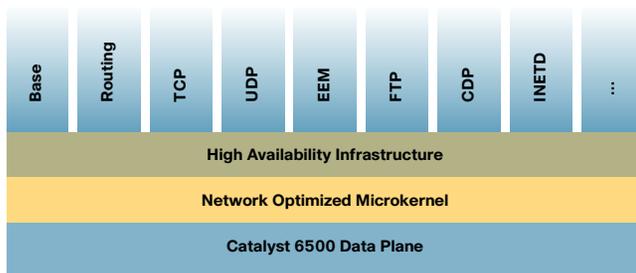## Cisco IOS Software Modularity

Cisco IOS Software Modularity on the Catalyst 6500 sets new standards for network availability by providing fault containment and faster fault recovery in places where it is needed the most—single points of failure in the network ranging from data centers to enterprise wiring closets.

This innovation on the Catalyst 6500 reduces the complexity of the software certification and upgrade process by allowing network administrators to apply incremental patches to address time-sensitive requirements such as critical security fixes without impacting their network availability.
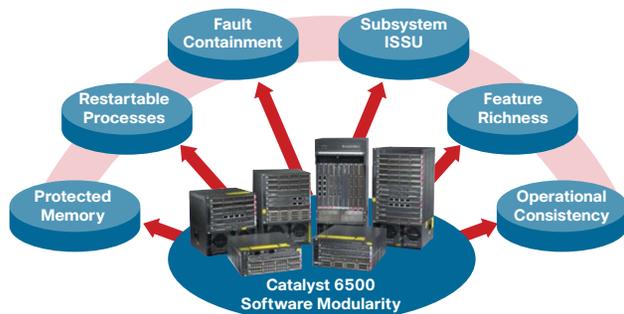
Furthermore, a combination of these capabilities with the monitoring and automated response features of Embedded Event Manager (EEM) on the Catalyst 6500 simplifies network operations.

Figure 1. Cisco IOS Software Modularity Architecture

Benefits

Figure 2. Software Modularity Benefits

First on Cisco's Premier Enterprise Platform!

Cisco IOS Software Modularity enhances Cisco IOS by dynamically grouping modular subsystems into **modular run-time processes**

The **High Availability infrastructure** determines what action to take if a fault occurs: restart a process or switchover to a standby Supervisor

Minimize Unplanned Downtime

- **Protected Memory:** Each process and its associated subsystems "live" in an individual memory space.
- **Fault Containment:** Problems occurring in one process will not affect other parts of the system.
- **Restartable Processes:** In the case a process or subsystem gets into an undesirable state (for example, stuck waiting for a signal from another process) the affected process can easily be restarted automatically or manually based on operations considerations.

Minimize Planned Downtime

- **Subsystem In-Service Software Upgrades (ISSU):** Code certification and deployment time is significantly reduced since a patch is the single desired fix and can be applied with no impact to packet forwarding.

Software Modularity Availability

- **Feature Richness:** Software Modularity offers high availability and manageability enhancements on top of existing Cisco IOS Software functionality in 12.2SX for the Catalyst 6500 Series.
- **Operational Consistency:** Software Modularity adds new commands to enable the new functionality. Other CLI, SNMP MIBs, and Syslog messages stay the same.
- **Modular Processes:** Several control plane functions have been modularized to cover the most commonly used features. Examples of modular processes include but are not limited to:
  - Routing Process
  - Internet Daemon
  - Raw IP Processing
  - TCP Process
  - UDP Process
  - Cisco Discover Protocol Process
  - Syslog Daemon
  - All Embedded Event Manager components
  - File Systems
  - Media Drivers
  - Install Manager
- **Patching Support:** Patching will be supported for fixes related to publicly announced security vulnerabilities. Patches will be delivered in maintenance packs which are cumulative sets of patches.

Embedded Event Manager

The Embedded Event Manager (EEM) represents a powerful enhancement to the Cisco IOS infrastructure. Based on defined events, custom actions can be executed on the local system. Triggers for actions as well as the individual steps themselves can be defined with the help of Tool Command Language (TCL)

scripts. This gives the user the freedom of customizing the trigger as well as the action taken according to the individual needs.

Since EEM is part of the Cisco IOS Infrastructure it can act autonomously even if connectivity to a central management station is temporarily unavailable. To describe the architecture of EEM it can be broken down into three components:

- Event Detectors
- Policy Engine
- Embedded Event Manager Server

Event Detectors can be viewed as sensors in various parts the operating system. These Event Detectors can then trigger the execution of scripts which contains custom actions. Event Detectors can publish events based upon CLI input, counters, resource thresholds, timer based services, SNMP and SYSLOG messages, routing protocol events and more. For a complete list of Event Detectors please consult the EEM documentation.

The **Policy Engine** binds the user-defined policies to the system. The policy engine offers two interfaces to do so:

- TCL scripts
- CLI applets

The policy engine for Tool Command Language (TCL) scripts offers a TCL interface. While some predefined scripts are part of the system, network operators can make use of the TCL scripting interface to add their own scripts to have the system perform actions based on the individual need. Actions that can be performed reach from gathering output from specifiable commands up to full patch management for switches.

Embedded Event Manager Server finally ties all this together. The event detectors deliver their output to the EEM server where the server makes use of the policy engine.

Having both Software Modularity and EEM provides an even more powerful combination. EEM, which itself is a modularized process, can take action based on process behavior. For example, in the event of a process crash, relevant information such as crash dump and memory allocation information can be stored locally or on a centralized server to ease troubleshooting. Once this is done, the switch can send a notification to the network administrator, who in return can then do further root cause analysis or contact the Cisco Technical Assistance Center (TAC).