# Managing Device Configuration and Software Images - The Foundation of Management of Network Services and Evolution

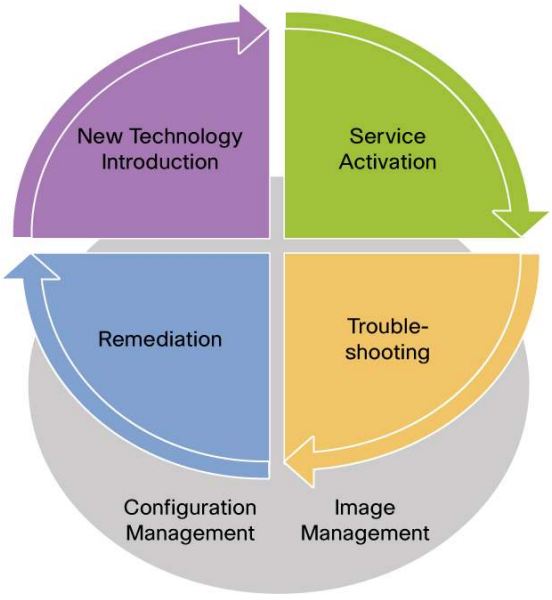
Robust configuration and software image management is fundamental to effective management of today's network services. It is the key to timely network problem remediation, augmenting the powerful troubleshooting tools offered in Cisco® Active Network Abstraction (ANA). It also renders timely technology and new service rollouts, crucial in today's rapidly evolving networks. This white paper discusses the tools provided in Cisco ANA for effective configuration management and software image management, allowing timely introduction of new technologies in the network, helping ensure detailed tracking of the configuration evolutions of network devices, and facilitating the establishment of a network baseline.

## Introduction

Telecommunications networks are becoming increasingly flexible and powerful. The converged IP next-generation networks (IP NGN) support a multitude of network services that are evolving quickly. Cisco ANA equips the network operators with tools for the service operation lifecycle from new service introduction, service activation, and troubleshooting to remediation (Figure 1), in which configuration management and software image management play a foundation role.

Configuration management facilitates control and tracking of changes that are made to a device configuration. Software image management helps enable rapid, reliable software upgrades and automates the steps associated with upgrade planning and monitoring. This white paper discusses the robust configuration management and software image management in Cisco ANA in support of the rich set of management features it provides for the IP NGN network services.

**Figure 1.** Cisco ANA Tools Functional Coverage



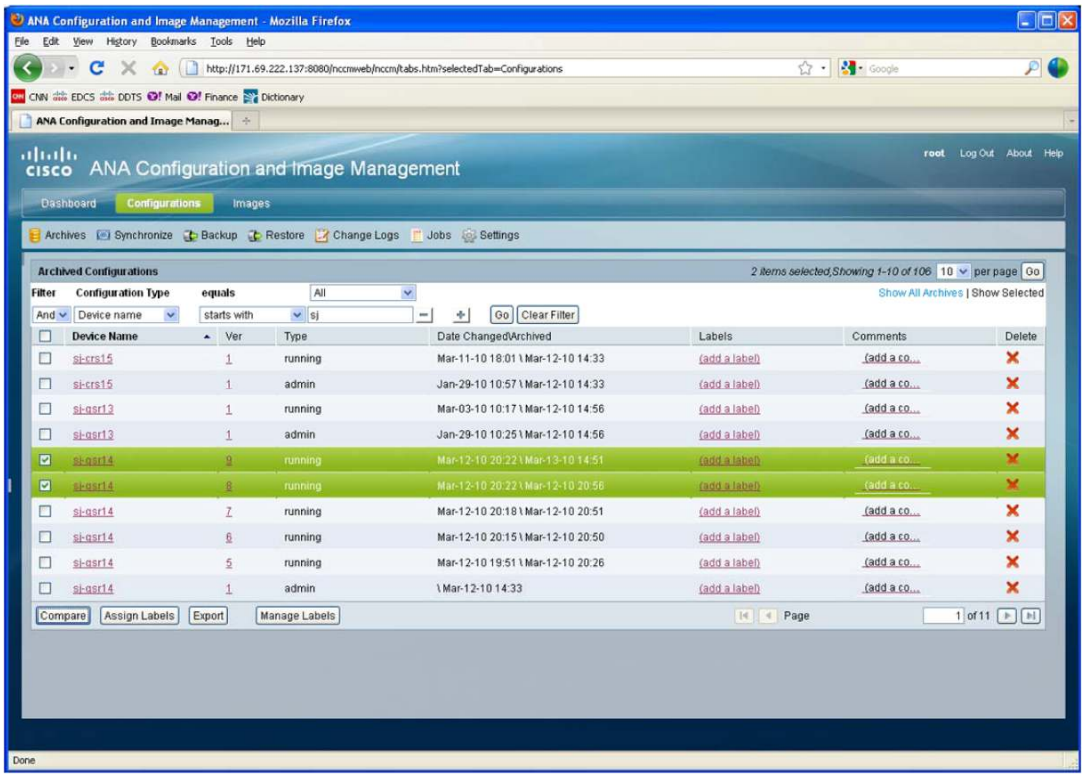
## Cisco ANA Configuration Management

The goal of configuration management is to monitor network and system configuration information so that the effects on network operation of various versions of hardware and software elements can be tracked and managed.

Cisco ANA maintains a configuration archive, which is a repository of backup copies of the device configuration files. Each backup copy of a device configuration file is indexed by the device identifier and a version number. The version number increments when Cisco ANA creates a new backup copy of the configuration file of a device. For Cisco IOS® devices, Cisco ANA maintains the backup copies of both the configuration file and the startup configuration file, with the version number incrementing independently.

The configuration archive in Cisco ANA provides a complete device configuration change history and is the foundation configuration restoration in the case of network problems. Cisco ANA provides tools for operators to view, compare, remove, and search on archives. Users can also export the configuration archives to an external file system. Figure 2 shows the configuration archive management in Cisco ANA.

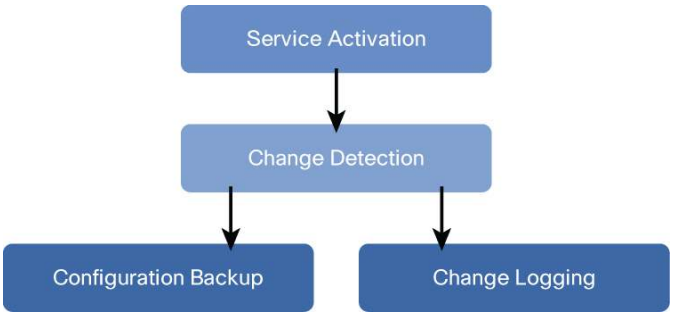
**Figure 2.** Managing the Archived Configurations in Cisco ANA




### Configuration Backup Options

Cisco ANA provides three different configuration backup options: automatic, periodic, and manual. Automatic backup is triggered by configuration changes in network devices. When a change is detected, Cisco ANA creates a backup copy of the device configuration. At the same time, the change event is logged and can be reviewed in the Change Logs. Figure 3 gives an illustration of automatic configuration backup in Cisco ANA.

**Figure 3.** Automatic Configuration Backup in Cisco ANA




Cisco ANA backs up device configuration files of all the managed network devices periodically. In addition, Cisco ANA supports manual configuration backup in which users select devices to back up the configuration files on demand or at a scheduled time. In both periodic and manual configuration backup, Cisco ANA examines each of the selected devices to determine whether its configuration file has changed since the last backup. If it is changed, a new backup copy is created.

These configuration backup options provide users with the flexibility to adapt to their specific environment and the state of the network. In a new and evolving network where there are frequent changes, users may turn off automatic configuration backup. In automatic configuration backup, Cisco ANA responds to every single change it detects. A network with frequent changes will cause a large number of configuration backups. Not only that, it will induce a lot of CPU cycles in the ANA server and the device itself; many of these intermediate changes may not be of interest, and creating backup copies of these configurations is unnecessary. In such a case, Cisco ANA allows users to turn off automatic backup and relies on periodic backup.

On the other hand, in a stable mature network where the device configurations are not expected to change frequently, automatic configuration backup should be used to detect all changes. This allows Cisco ANA to respond to configuration changes quickly. Cisco ANA also gives users the flexibility to configure a time delay of the backup after detection of changes. This is especially useful in service activation where a series of configurations is applied to the various devices. For example, to create a Layer 3 VPN service, Virtual Route Forwarding (VRF) needs to be created on the provider edge devices first. The route targets are then added to the VRF. Each of these steps will result in a device configuration change. However, we would not be interested in archiving the configuration until the whole service activation is completed. In this case, a time delay between configuration change detection and backup can be utilized.

### Cisco IOS Startup and Running Configuration Synchronization

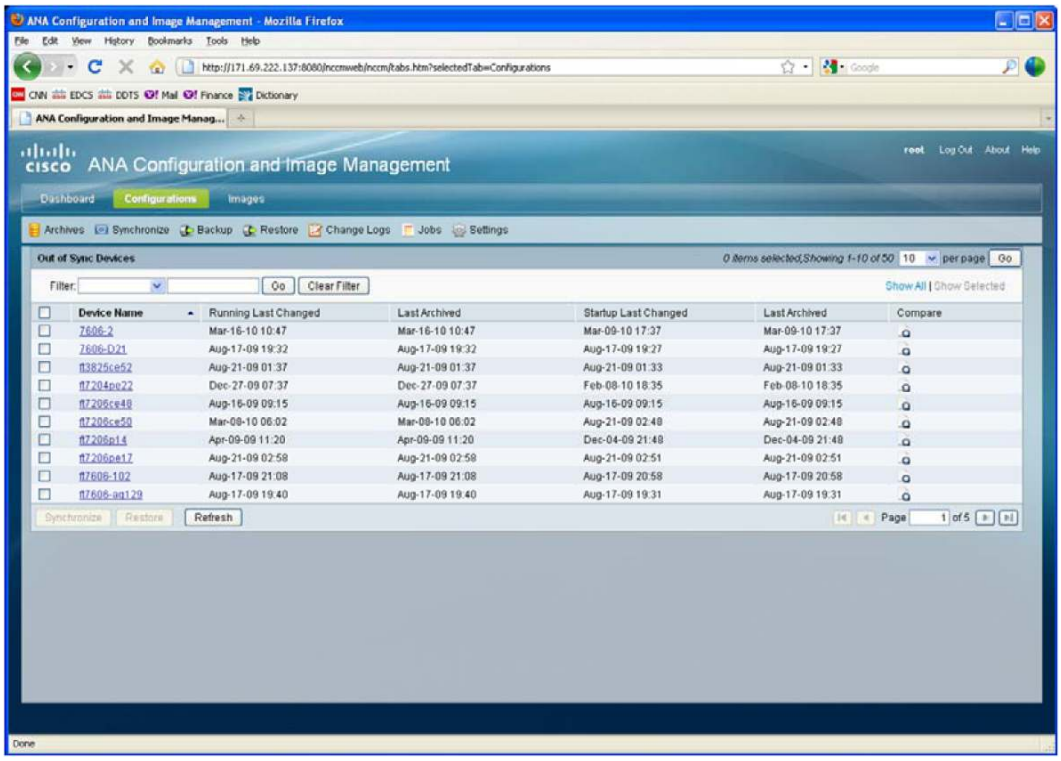
Cisco IOS Software contains two types of configurations: startup configuration and running configuration. Startup configuration is used during system startup to configure the device software, while running configuration contains the current configuration of the device software. The two configuration files can be different. For more information about Cisco IOS Software configuration files, please refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* for any given Cisco IOS Software release.

Configuration changes applied on the device are against the running configuration and will not persist across device reload. Different organizations have different configuration practices. For example, a service provider may require the running configuration to be saved to the startup configuration for each configuration change, while another service provider may prohibit altering the startup configuration until the running configuration is carefully reviewed. Synchronization of startup and running configurations is then scheduled.

Cisco ANA provides users with the tool to synchronize the startup and running configurations of the selected devices, as shown in Figure 4. It examines and determines whether the device startup configurations and running configurations are different. If they are, it will save the running configuration to the startup configuration and will also

create a new backup version of the startup configuration. Device startup and running configuration synchronization can be carried out on demand or at a scheduled time.

**Figure 4.** Startup and Running Configuration Out of Sync Report in Cisco ANA




### Configuration Restoration

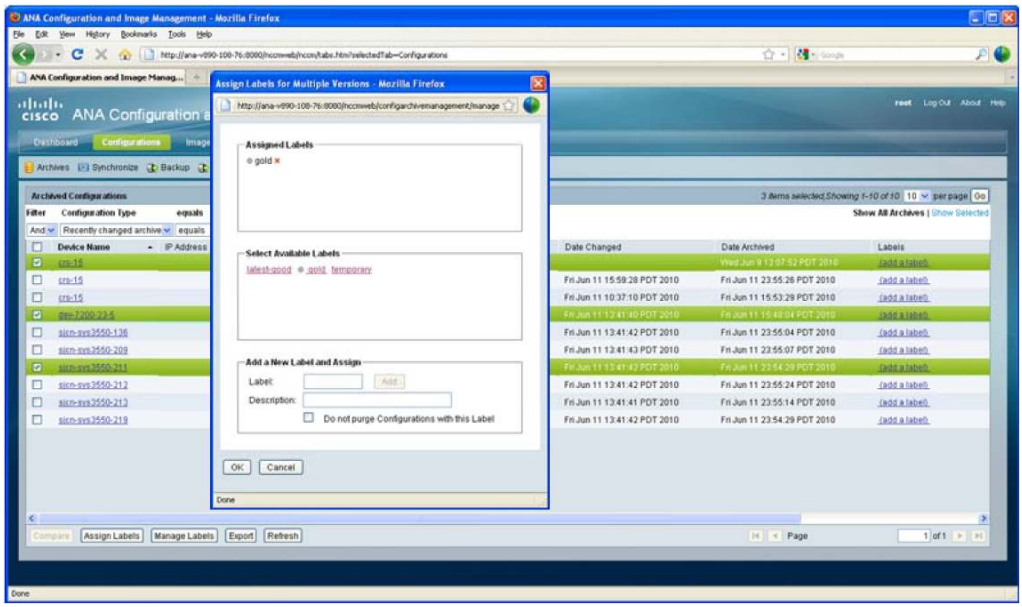
By maintaining active archives of the device configurations, Cisco ANA keeps the history of changes made to the devices of the managed network. More importantly, in the case of troubleshooting, it helps the operators to pinpoint the exact portion of the device configuration that causes the network problem and allows users to restore the device configuration to the last known good state.

Cisco ANA provides operators with a set of powerful troubleshooting tools for network problems; for example, network maps of physical, logical, and service topologies, virtual connection visualization, and Path Tracer. The *In-Depth Carrier Ethernet Device Configuration Representation - The Foundation for Troubleshooting* white paper discusses troubleshooting in a Carrier Ethernet environment in detail. These tools help the operators to pinpoint the specific location within the network that causes the network problem. Users can then compare the current device configuration with any of the archived versions, including the last known good state.

Cisco ANA allows users to bookmark a device configuration archive with any text strings as label; for example, “Golden Configuration.” Users can configure a labeled device configuration archive to be permanent, that is, it will not be affected by the system configuration archive purging process. This provides an extra level of confidence to the operators by maintaining golden snapshots of the network configuration, which can be restored to as needed.

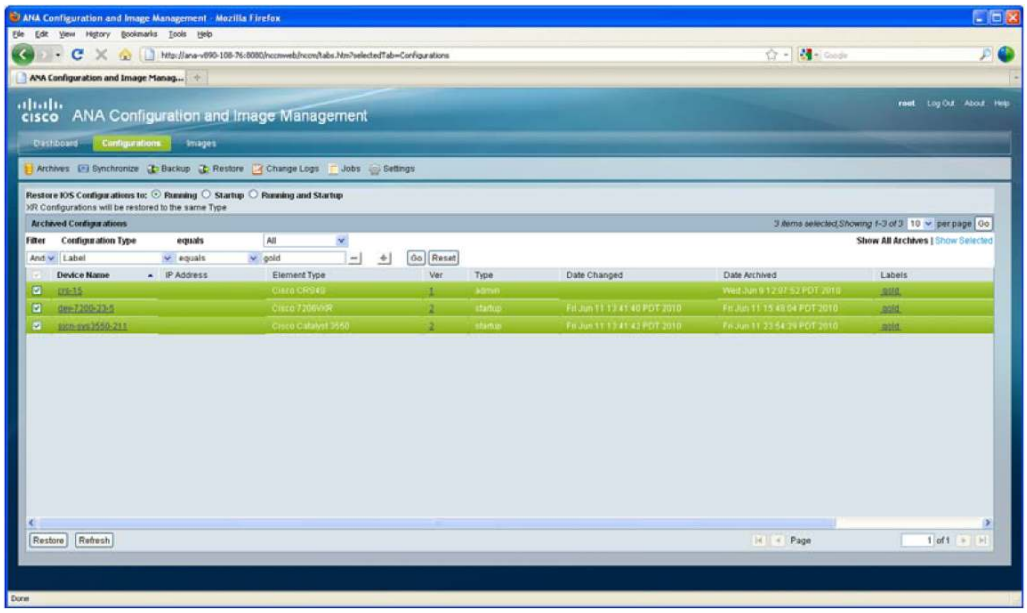
For example, users can label a set of device configuration archives with the “Gold config Q1 2010 certified” label and another set of configuration archives with “Gold config Q2 2010 certified.” Figure 5 shows how an operator can easily bookmark an archived version of the configuration from different devices in Cisco ANA with a label.

**Figure 5.** Bookmarking an Archived Version of Configuration from Different Devices in Cisco ANA




After the specific root cause of a network problem is pinpointed, a typical remediation step is to restore the configuration of selected devices to the last known good operating state. Cisco ANA allows operators to restore the network configuration quickly to any known good state. Figure 6 shows how an operator can easily restore the snapshot of the network configurations labeled as “gold” to the network.

**Figure 6.** Configuration Restoration in Cisco ANA




## Cisco ANA Software Image Management

Device software images are introduced continuously for routine bug fixes and release of new features and network technologies. In the rapid pace of technology advancement, efficient software image upgrade is more critical than ever for service providers, in order to capture the new technology opportunities in a timely manner.

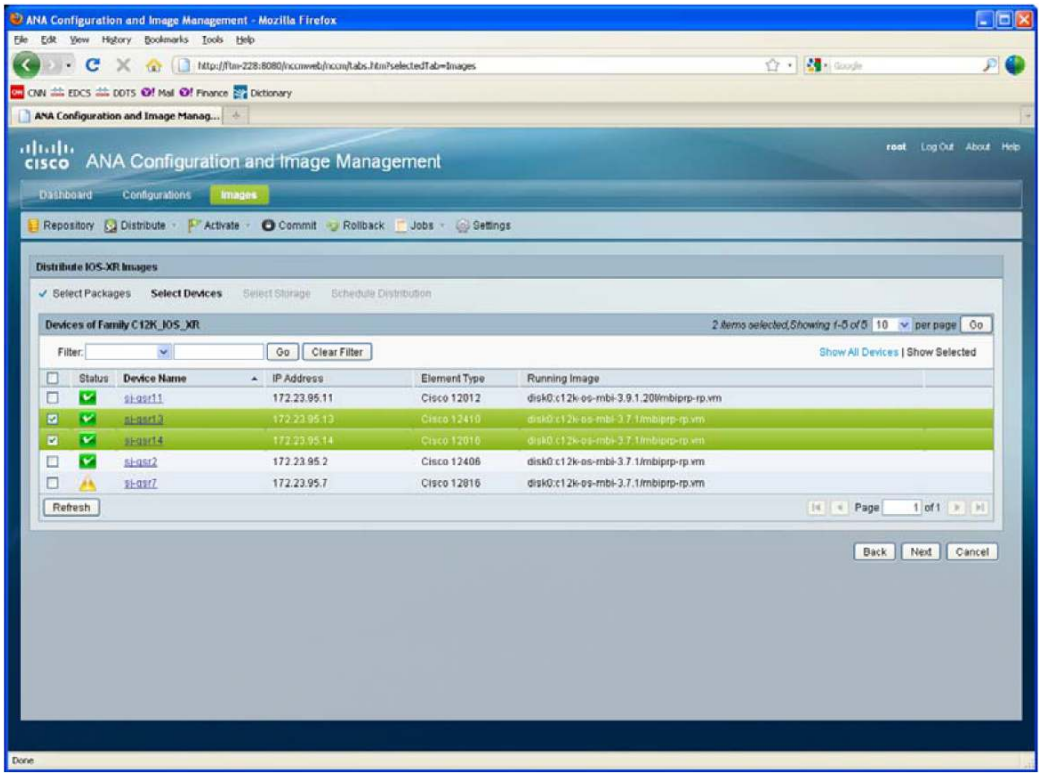
There are typically strict guidelines and certification processes for service providers before a software image can be rolled out into the network. Once certified, thousands of devices will need to be upgraded to new certified images quickly. This is an important first step to new service introduction. Cisco ANA provides tools for efficient software image rollout, the first step to new technology introduction. Users can then use the service activation feature set in Cisco ANA to launch the new services.

Cisco ANA provides a software image repository where the software images for the managed network are being maintained. It is fully integrated with Cisco.com, allowing operators to import images directly. In an environment where the operators do not have direct access to Cisco.com, operators can import images from a local file system.

Cisco ANA equips the operators with tools to upgrade or downgrade software images to network devices. Before an image is activated, Cisco ANA performs an analysis to help ensure that the network element is compatible with the image. Cisco ANA provides automation of the software image management procedures for both Cisco IOS devices and Cisco IOS XR devices. For more information about Cisco IOS device software image management background, please refer to the *Cisco IOS Configuration Fundamentals Configuration Guide* for any given Cisco IOS software release. For more information about the Cisco IOS XR device software package management background, please refer to the *System Management Configuration Guide* for the Cisco IOS XR device of interest.

Figure 7 illustrates how an operator can select a software package containing a new technology to be applied on selected applicable devices.

**Figure 7.** Software Image Upgrade in Cisco ANA

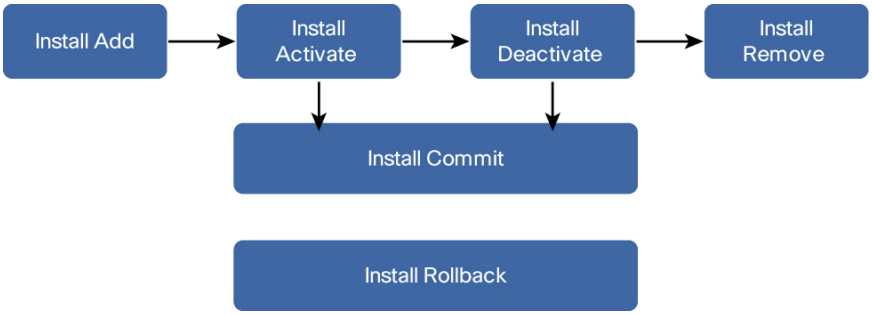



For Cisco IOS devices, software image upgrade or downgrade involves distributing the target software image to the device and activating it. This procedure is fully automated in Cisco ANA. In addition, Cisco ANA provides the flexibility to perform only software image distribution, distribution followed by immediate activation, distribution followed by activation at a scheduled later time, or activation only. These options help ensure easy adoption of Cisco ANA in different user environments and various software image upgrade or downgrade scenarios.

Cisco IOS XR Software is divided into software packages so that you can select which features to run on your router. Each package contains the components to perform a specific set of router functions, such as routing or security support. Bundles are groups of packages that can be downloaded as a set. Package Installation Envelopes (PIEs) contain a single package or a set of packages (called a composite package or bundle). PIE files have a pie extension. When a PIE file contains software for a specific bug fix, it is called a software maintenance upgrade (SMU). Cisco ANA supports both Cisco IOS XR PIE and SMU files.

Cisco ANA supports the full software package management lifecycle of Cisco IOS XR devices, as shown in Figure 8. It supports all the following Cisco IOS XR software package management operations: distribute, install add, install activate, install deactivate, install commit, install remove, and install rollback, with full automation. Cisco ANA also provides the flexibility to perform only software package distribution, distribution and activation with or without commit, activation with or without commit, deactivation with or without commit, or commit only. This helps ensure that Cisco ANA can be readily used in various user environments. Cisco ANA's support of the Cisco IOS XR Software package management lifecycle is unique in the industry and its flexibility is second to none.

**Figure 8.** Cisco IOS XR Software Package Management Lifecycle




As part of software package activation, Cisco ANA performs upgrade analysis to make sure that the target software packages are compatible with the selected network devices, helping ensure that incompatible packages will not be loaded in the devices.

Service providers typically specify certain maintenance windows, only within which software image can upgrades take place. Cisco ANA provides the operators with the flexibility to perform any software image operations on demand or at a scheduled time.

### Cisco ANA - The Foundation for Managing Converged, Multiservice IP Networks

Cisco Active Network Abstraction (ANA) is a network management foundation for Cisco-based service provider networks. It addresses the challenge of managing converged, multiservice IP networks through its unique model-based virtual network abstraction and robust configuration management and software image management.

Cisco ANA equips the network operators with tools for the service operation lifecycle from new service introduction, service activation, and troubleshooting to remediation. Cisco ANA provides tools for efficient software image rollout, as well as tools for new service activation. Cisco ANA's virtual network abstraction represents, in detail, the configuration of network elements. This deep network knowledge powers Cisco ANA with the set of monitoring and troubleshooting features. They are augmented by configuration management and software image management features that provide a complete history of the network configuration evolution and a repository of software images - a foundation of remediation.

Cisco ANA is the network management application of choice for today's converged, multiservice IP NGN networks.

## For More Information

For more information about ANA, visit http://www.cisco.com/go/ana, contact your local Cisco account representative, or send an email to mailto:ask_ana_pm@cisco.com.

Integration information can be found at http://developer.cisco.com/web/ana/home.

The latest ANA user and reference guides are available at http://www.cisco.com/en/US/products/ps6776/tsd_products_support_series_home.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**



Printed in USA C11-612773-00 08/10