



## Q & A

# Cisco Configuration Assurance Solution Version 1.1

## Overview

**Q.** What is Cisco® Configuration Assurance Solution (CAS)?

**A.** Cisco CAS is a vital software tool for improving network availability as well as application and service continuity. Cisco CAS automatically performs regular, systematic audits of the production IP network configuration to diagnose device misconfigurations, policy violations, inefficiencies, and security gaps. It uses a high-fidelity software model of the IT infrastructure, accurately simulating the behavior of routers, switches, and protocols, to enable a broad scope of analyses.

An optional Cisco CAS-Service Provider Module (SPM) extends support to encompass service provider-centric protocols and technologies, including Multiprotocol Label Switching (MPLS) and Intermediate System-to-Intermediate System (IS-IS).

**Q.** What types of users will benefit from Cisco CAS?

**A.** Cisco CAS is suitable for any medium-sized or large enterprise that operates an IP-based network to support critical business applications. It provides operational decision support to network operations and engineering staff responsible for ensuring the integrity and security of the production IP network. Cisco CAS is unique in its ability to quickly and systematically analyze the configuration of the entire IP network from the level of the individual devices to the level of networkwide operations, and to predict the ability of the network to maintain integrity and security under failure conditions.

**Q.** Is Cisco CAS a combination of integrated software applications?

**A.** Yes. Cisco CAS comprises three components: the Audit and Analysis engine that actually builds the high-fidelity network model, performs analysis, and provides visualization and reporting; a Virtual Network Data Server that automatically maintains a detailed data model of the production network to enable the creation of this network model; and an integrated Web-based Report Server. The Report Server is a central repository for documents, charts, tables, and images.

**Q.** Does Cisco CAS perform policy checks against the source configuration file?

**A.** Yes. Cisco CAS performs template checking against the source configuration file. Cisco CAS is unique because it also performs checks of the detailed configuration instantiated in the high-fidelity software model. This enables analysis of connectivity and protocols-related issues to detect problems related to routing and addressing. Cisco CAS also performs simulation-based configuration audits. For example, you can determine if application flows would be affected by node, link, or resource group failures.

**Q.** What technologies and protocols does Cisco CAS support?

**A.** The high-fidelity network model in Cisco CAS supports hundreds of technologies and protocols. The following is a partial list, featuring primary examples:

- Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Routing Information Protocol (RIP), RIP Next Generation (RIPng)
- Ethernet, Gigabit Ethernet, Spanning Tree Protocol, Token Ring, SONET, Fiber Distributed Data Interface (FDDI), VLAN, and more
- IPv4, IP Multicast, Internetwork Packet Exchange (IPX), Hot Standby Router Protocol (HSRP)

- QoS – committed access rate (CAR)/Policing; Custom Queuing; Distributed Weighted Fair Queuing (DWFQ); Class-Based Weighted Fair Queuing (CBWFQ); Deficit Weighted Round Robin (DWRR); Modified Deficit Round Robin (MDRR); Modified Weighted Round Robin (MWRR); First-In, First-Out (FIFO); Low Latency Queuing (LLQ) with Rate Limit; Marking; Priority Queuing; Random Early Detection (RED); and Weighted RED (WRED)
- Voice over IP (VoIP), HTTP, FTP, Telnet, e-mail, video, others
- In addition to the above, the optional Cisco CAS-SPM provides support for MPLS and IS-IS

**Q.** What kinds of configuration rules are provided with Cisco CAS?

**A.** Cisco CAS includes more than 400 configurable rules that address the following:

- Authentication, authorization, and accounting (AAA)
- Device administration (for example, blocking specified incoming services), Simple Network Management Protocol (SNMP), system logging
- IGRP, EIGRP, OSPF, BGP, RIP; MPLS and IS-IS with the optional Cisco CAS-SPM
- IP Multicast, HSRP, remote source-route bridging (RSRB), IP Security (IPSec), IPX, Data-Link Switching (DLSw), tunnel interfaces
- IP addressing and routing, Route Maps, access control lists (ACLs)
- Cisco PIX<sup>®</sup> Security Appliance, Network Address Translation (NAT), TACACS+, RADIUS, Kerberos Protocol, other security rules
- Quality of service (QoS)
- VLANs, VoIP
- Spanning Tree Protocol, link aggregation
- Others

**Q.** What is the typical workflow when using Cisco CAS?

**A.** Users configure Cisco CAS to support their local configuration management practices. The following represents a high-level description of a possible scenario for a daily configuration audit. There may also be a weekly or monthly process that differs in terms of the scope of the target network(s), the analyses to be performed, etc., depending on the user's operational characteristics and practices.

- *Create a daily baseline network model* – Cisco CAS Audit and Analysis is scheduled to import the updated network data from Virtual Network Data Server to create a daily baseline model of the production network. The network model may comprise the entire network, or a subset based on groups defined in the Virtual Network Data Server by the system administrator (for example, “core” and “access”). This may depend on local operating parameters and practices, such as the scope of daily changes (for example, “branch” devices may be reconfigured less frequently than “core” devices and are consequently not subject to a daily audit process).
- *Perform configuration audit* – Cisco CAS is configured to perform a series of analyses after the network model has been created. The objective of many of these is to identify configuration problems. However, some are produced for reference purposes. For example, if a failure occurs in the network, it is useful to refer to a previously executed failure study to quickly assess the potential impact.
- *Publish results and notify users* – Cisco CAS is configured to automatically publish the results of its analyses to the integrated Web-based Report Server. Users can check the daily audit results to identify issues requiring attention. Optionally, users can be notified about critical errors through e-mail or pager.
- *Repeat the workflow* – In some cases, such as environments with a high rate of unplanned changes, the audit process may be repeated one or more times prior to the beginning of that night's change window. Alternatively, the user may have configured Cisco CAS to perform a series of audits of different network views over the course of the day, for more granular management and reporting.

**Q.** Is Cisco CAS customizable?

**A.** Yes, Cisco CAS is customizable in several respects:

- The rules that comprise its extensive portfolio of standard checks are provided in source code. They can be modified or new rules developed with the integrated authoring environment.
- The scope of an audit is defined by the user in terms of target devices and analyses, as well as frequency.
- The appearance of output reports can be customized with style sheets.

**Q.** What are scalability limits or considerations for Cisco CAS?

**A.** There are no architectural limits in terms of scalability (that is, the number of supported devices). Considerations that affect scalability from an operational perspective include the scope and frequency of network audits, and the network profile. The number of network devices is less important to assessing scalability than the number of physical and logical interfaces in the target network.

**Q.** Is Cisco CAS based on solutions from OPNET Technologies?

**A.** Yes, Cisco CAS is based on OPNET applications to provide comprehensive network operations support.

## **Optional Cisco CAS-SPM**

**Q.** Is Cisco CAS suitable for service provider networks?

**A.** Cisco CAS-SPM offers support for service provider-centric technologies such as MPLS and IS-IS. Additionally, Cisco CAS-SPM supports networks that have a large number of internal Border Gateway Protocol (I-BGP) speakers, like those of network service providers, which are considered to be service provider class. Without the optional Cisco CAS-SPM, Cisco CAS supports networks that incorporate up to 30 I-BGP speakers. (There is no limit in any case to the number of external BGP [E-BGP] speakers).

**Q.** Does Cisco CAS-SPM increase scalability?

**A.** Addition of the optional Cisco CAS-SPM does not affect Cisco CAS scalability (the number of supported devices).

**Q.** Is the Virtual Network Data Server installed with Cisco CAS-SPM functionally different?

**A.** No, there are no functional differences between the Virtual Network Data Server installed with Cisco CAS and Cisco CAS-SPM.

**Q.** When upgrading to add Cisco CAS-SPM to an existing installation of Cisco CAS, does the Virtual Network Data Server also need to be upgraded?

**A.** There is no functional requirement to upgrade the Virtual Network Data Server when upgrading Cisco CAS to add Cisco CAS-SPM. However, the program structure represented in the Windows start menu (“Start→Programs→Cisco CAS 1.1...”) is slightly different between the two cases. Cisco CAS 1.1 Installation Guide provides detailed information about these installation options and implications.

**Q.** Is the Report Server installed with Cisco CAS-SPM functionally different?

**A.** No, there are no functional differences between the Report Server installed with Cisco CAS and Cisco CAS-SPM.

**Q.** When adding Cisco-SPM to an existing installation of Cisco CAS, does the Report Server also need to be upgraded?

**A.** There is no functional requirement to upgrade the Report Server when upgrading Cisco CAS to add Cisco CAS-SPM. However, the program structure represented in the Windows start menu (“Start→Programs→Cisco CAS 1.1...”) is slightly different between the two cases. Cisco CAS 1.1 Installation Guide provides detailed information about these installation options and implications.

## Product Integrations

**Q.** With what other Cisco products does Cisco CAS integrate?

**A.** Cisco CAS Virtual Network Data Server obtains network data automatically through Telnet or Secure Shell (SSH) Protocol and SNMP from Cisco routers (running Cisco IOS® Software), Cisco Catalyst® switches (with Catalyst OS, Cisco IOS Software), and the Cisco PIX Security Appliance (with Cisco PIX OS). Data can be imported from CiscoWorks LAN Management Solution (including Resource Manager Essentials and Campus Manager) for supported devices. Topology data can be imported from Cisco Connectivity Center. Traffic data can be imported from Cisco NetFlow Flow Collector.

The Virtual Network Data Server can be configured to integrate with Cisco Info Center to obtain real-time awareness of network events that may indicate a configuration change, and automatically update its data for the affected devices.

For topology and configuration information, the Virtual Network Data Server automatically reconciles conflicting or overlapping data based on user-configurable priorities.

**Q.** Does Cisco CAS provide multiple-vendor device support? How does support for these differ from support for Cisco devices?

**A.** Cisco CAS supports Check Point, Extreme, Foundry, Juniper, Nokia, and Nortel devices. In every case, support is more robust for Cisco devices. That is, the scope of supported configuration commands and device attributes is significantly broader for Cisco devices.

## Installation and Implementation

**Q.** Does installation require multiple platforms?

**A.** Yes. As noted previously, Cisco CAS contains an Audit and Analysis engine, Virtual Network Data Server, as well as a Report Server, each on separate installation CDs. The Audit and Analysis engine as well as a library of technology, protocol, and device models are typically implemented on a single server. The Virtual Network Data Server is generally implemented on a dual-processor platform with the prerequisite database environment.

**Q.** Can the Virtual Network Data Server and prerequisite Oracle data systems be implemented on separate platforms?

**A.** Yes, these components can be implemented on separate platforms. However, it is highly recommended that they be installed on the same dual processor server. If they are implemented on separate platforms, then these should feature a fast FSB (~800 MHz) and be connected through a high-speed link (not over a WAN) that is unimpeded by a firewall. Implementing the database at a location remote from the Virtual Network Data Server is not supported.

**Q.** Can other network-management applications be implemented on any of the platforms for Cisco CAS?

**A.** The Virtual Network Data Server and Audit and Analysis engine are each quite memory- and compute-intensive when performing scheduled operations (for example, updating the daily configuration baseline, or performing an audit). Consequently it is not advisable to implement them on the same platform with another application. The Report Server can be implemented on a server with other intranet applications.

**Q.** What Web browsers does the Web-based Report Server support?

**A.** The Web-based Report Server supports Microsoft Internet Explorer Version 6.

**Q.** How is Cisco CAS licensed?

**A.** All the components of Cisco CAS obtain a license from a License Server at the time of startup. It is recommended that a License Server be implemented for each component of Cisco CAS and on the same platform to help ensure high availability.

**Q.** Is a separate license required for Cisco CAS-SPM?

**A.** Yes. Installation requires a separate Cisco CAAS-SPM license as well as a license for the underlying Cisco CAS.

**Q.** What skill level is required to implement and use Cisco CAS?

**A.** There are two types of Cisco CAS users, including administrators who configure its operation, and users who are “consumers” of its analyses. A basic working understanding is required of the network technologies, protocols, and devices and the configuration commands and variables that are to be analyzed in Cisco CAS in order to configure its operation and to interpret and respond to its results. In addition, the administrator will need to learn how to configure the solution components.

**Q.** How much time and effort is required to implement Cisco CAS? Are professional services required for implementation?

**A.** The Virtual Network Data Server component of Cisco CAS is integrated with the production network and management environment, and requires thoughtful planning, some assessment and configuration of target data sources to enable integration, custom configuration of the Virtual Network Data Server, and subsequent validation of the end-to-end workflow. Troubleshooting is often required to resolve unanticipated issues that result from target devices or network-management platforms not being configured properly, device credentials being inaccurate, source data being unreliable, etc.

Configuring the Audit and Analysis engine requires a working understanding of the organization’s operating objectives for Cisco CAS and as well as current network-management practices. For example, the scope and frequency of various audits must be defined and reflected in the setup (for example, audit core devices daily and branch devices weekly). The configuration of the Audit and Analysis engine is menu-driven and relatively straightforward.

Cisco CAS requires professional services to accelerate solution deployment. Engagements vary depending on the scope and complexity of the target network and data sources, but are typically two to four weeks long. These services are priced, contracted, and delivered separately.

For more information about the Cisco Configuration Assurance Solution, visit <http://www.cisco.com/en/US/products/ps6364/index.html> or contact your local account representative or send an e-mail to the Product Marketing group at [netwrk-ap-mktg@cisco.com](mailto:netwrk-ap-mktg@cisco.com).

**Corporate Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

**European Headquarters**

Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

**Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

**Asia Pacific Headquarters**

Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica  
Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR  
Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico  
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia  
Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan  
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

KW/LW10004 12/05

