Cisco NAC Network Module for Integrated Services Routers

General Information

Q. What is Cisco® Network Admission Control (NAC)?

A. Cisco Network Admission Control (NAC) is a solution that uses the network infrastructure to enforce security policies on all devices seeking to access network computing resources. It helps ensure that all hosts comply with the latest corporate security policies, such as antivirus, security software, and operating system patch, prior to obtaining normal network access. Vulnerable and noncompliant hosts are isolated (quarantined) or given limited access until they reach compliance. In addition, Cisco NAC can perform user authentication at the network level so that only devices with proper user credentials are permitted network access.

Q. What is the Cisco NAC Network Module for Integrated Services Routers?

A. The Cisco NAC Network Module for Integrated Services Routers (NME-NAC-K9) brings the feature-rich Cisco NAC Appliance Server (also known as Clean Access Server) capabilities to Cisco 2800, 2900, 3800 and 3900 Series Integrated Services Routers. It extends the Cisco NAC Appliance portfolio of products to smaller locations, helping enable NAC capabilities from the headquarters to the branch office. As a network module for integrated services routers, it is available as one hardware configuration with two software license options based on the number of online, concurrent users: 50 and 100 users.

Q. What benefits does the Cisco NAC Network Module for Integrated Services Routers offer?

A. The integration of NAC Appliance Server capabilities into a network module for Integrated Services Routers allows network administrators to manage a single device in the branch office for data, voice, and security requirements, reducing network complexity, IT staff training needs, equipment sparing requirements, and maintenance costs. Also, deployment of the Cisco NAC Network Module for Integrated Services Routers at the branch office remediates potential threats locally before they can traverse the WAN and potentially infect the network. Networks with the Cisco NAC Network Module in an Integrated Services Router benefit from:

- Security protection because compliance is a condition of access
- Proactive prevention of viruses, worms, spyware, and other malicious applications
- Minimized vulnerabilities on user machines through periodic evaluation and remediation
- Significant cost savings because the process of repairing and updating user machines is automated
- Deployment flexibility and lower total cost of ownership

Q. How does the Cisco NAC Network Module differ from the existing Cisco IOS® Software-based Layer 3 NAC capabilities in Integrated Services Routers?

A. Flexible to meet a broad array of customer requirements, Cisco NAC is offered either through an appliance-based approach or an architectural framework solution. The Layer 3 NAC features available in integrated services routers from Cisco IOS Software Release 12.3(8)T are part of the Cisco NAC Framework solution, whereas the Cisco NAC Network Module is part of the Cisco NAC Appliance solution. Most customers require rapid deployment and a reduced degree of complexity. For these customers, the Cisco NAC Appliance and Cisco NAC Network Module fits best, offering a self-contained solution that does not require an immediate network infrastructure upgrade. Some customers require a solution that integrates their existing network infrastructure with vendor antivirus, security, and patch management solutions—the Cisco NAC Framework. Cisco customers can choose the NAC deployment that best meets their current needs and future plans.

Q. How does the Cisco NAC Network Module fit into the overall Cisco NAC Appliance portfolio?

A. The Cisco NAC Appliance solution has three components:

- **Cisco Clean Access Server (CAS)**: The device that initiates assessment and enforces access privileges based on endpoint compliance, the Cisco Clean Access Server is available as an appliance in six sizes based on the number of online, concurrent users: 100, 250, 500, 1500, 2500, and 3500 users. With the introduction of the Cisco NAC Network Module, CAS is now also available in two sizes based on the number of online, concurrent users: 50 and 100 users.

  A single company can have several servers of differing sizes; for example, a headquarters building would require a 1500-user Clean Access Server using the Cisco NAC 3350 Appliance, whereas a branch office for the same company might require only a 100-user server using the Cisco NAC Network Module within a Cisco 2800, 2900, 3800 or 3900 Integrated Services Router.
- **Cisco Clean Access Manager (CAM)**: A centralized, Web-based console for establishing roles, checks, rules, and policies, the Clean Access Manager is available in three sizes (appliance only): the Lite Manager manages up to 3 Clean Access Servers; the Standard Manager manages up to 20 Clean Access Servers; and the Super Manager manages up to 40 Clean Access Servers. The CAM can be used to configure and manage both types of clean access servers: network module and appliance.
- **Cisco Clean Access Agent (CAA)**: This thin, read-only agent enhances posture assessment functions and streamlines remediation. Clean Access Agents are optional and are distributed free of charge.

Product Details

Q. Does the Cisco NAC Network Module have the same capabilities as the Cisco NAC Appliances ?

A. Yes. All the Clean Access Server features of the Cisco NAC Appliance are supported on the Cisco NAC Network Module (NME-NAC-K9), with the exception of high availability.

Q. How many simultaneous users can the Cisco NAC Network Module support?

A. The Cisco NAC Network Module can support up to a maximum of 100 simulatenous users. The number of supported users is determined by the software license that you order along with the network module: part number NACNM-50-K9 for a Cisco NAC Network Module Server License with a maximum of 50 users or part number NACNM-100-K9 for a Cisco NAC Network Module Server License with a maximum of 100 users.

Q. Which Cisco routers support the NAC network module?

A. The Cisco NAC Network Module is supported on modular integrated services routers with a network module slot; that is, the Cisco 2811, 2821, 2851, 3825, and 3845 Integrated Services Router platforms. Note that the Cisco NAC Network Module is not supported on Cisco 3700 or 2600XM Routers.

Q. What are the Cisco IOS Software requirements for the host integrated services router to support the NAC network module?

A. The Cisco integrated services router platform needs to run Cisco IOS Software Release 12.4(11)T or later (IP Base image or higher) in order to support the NAC network module (NME-NAC-K9) on 2800 and 3800 routers. 2900 and 3900 G2 integrated services router platforms support the NAC network module with a jacket card starting with IOS 15.0 (M) Release.

Q. What software runs on the NAC network module?

A. At product launch, the NAC network module will run Clean Access Server Software Version 4.1.2. As new features are developed for the NAC appliances, they can be deployed on the Cisco NAC Network Module by installing the latest version of Cisco CAS software.

Q. How many NAC network modules can be installed in Cisco 2800, 2900, 3800 and 3900 Integrated Services Routers?

A. One. Currently, the installation of only one NAC network module is supported within a Cisco 2800, 2900, 3800 or 3900 Integrated Services Router (2900 and 3900 series routers require a jacket card). If you need to support more than 100 users in a branch office, Cisco recommends that you deploy a Cisco Clean Access Server on a NAC appliance of the right size.

Configuration and Deployment

Q. How do I configure and manage the Cisco NAC Network Module for Integrated Services Routers?

A. The Cisco NAC Network Module for Integrated Services Routers is configured and managed primarily by the Web-based GUI of Clean Access Manager (deployed as a separate appliance for the entire network). Initial setup for the NAC network module is done through the router command-line interface (CLI) and a reverse Telnet session to the module, which includes assigning an IP address to the trusted (internal) port of the NAC network module. If needed, you can retrieve the support logs for the Clean Access Server by Web browsing to the IP address of the trusted port of the NAC network module.

Q. Can the Cisco Clean Access Manager (NAC Appliance Manager) configure and manage both types of Clean Access Servers—NAC network modules and NAC appliances simultaneously?

A. Yes, the Cisco Clean Access Manager can manage both NAC network modules and NAC appliance servers simultaneously. The Cisco Clean Access Manager is available in three sizes: the Lite Manager manages up to 3 clean access servers; the Standard Manager manages up to 20 clean access servers; and the Super Manager manages up to 40 clean access servers. From a CAS count perspective, the CAM treats the NAC network module and NAC appliance server equivalently.

Q. Does the NAC network module work in both in-band and out-of-band (OOB) modes?

A. Yes, all the existing deployment scenarios for CAS as a NAC appliance are supported with a NAC network module. Note that a NAC network module installed in an integrated services router is an example of edge deployment (centralized deployment model does not apply to the NAC network module). Refer to Table 1 for NAC network module deployment options.

Table 1. Cisco NAC Network Module Deployment Options

Deployment Model	Options
Passing Traffic Mode	• Virtual gateway (bridged mode) • Real IP gateway (routed mode)
Client Access Mode	• Layer 2 (client is adjacent to the Clean Access Server) • Layer 3 (client is multiple hops from the Clean Access Server)
Traffic Flow Model	• In-band (Clean Access Server is always in line with user traffic) • Out-of-band (Clean Access Server is in line only during authentication, posture assessment, and remediation)

Q. What are the hardware specifications for the NAC network module?

A. The NAC network module runs the clean access server application on the Linux-based services engine for integrated services routers. The hardware architecture is based on a 1-GHz processor, 512-MB double-data-rate 2 (DDR2) RAM, 80-GB Serial ATA (SATA) hard disk, 64-MB Compact Flash module. It has 2 Ethernet network interface cards: one internal 1000-Mbps Ethernet interface to the router backplane and one external 10-/100-/1000-Mbps Ethernet interface. Please refer to the data sheet for more information.

Q. Which are the trusted and untrusted interfaces on the NAC network module?

A. The external visible interface on the NAC network module is the untrusted interface through which traffic from the local LAN network in the branch office enters the network module and the router. The trusted interface of the NAC network module is internal to the module and connects to the backplane of the host integrated services router through a Gigabit Ethernet port.

Q. How does the "reverse Telnet" connection from the router CLI to the NAC network module work?

A. Reverse Telnet uses an internal, virtual Telnet interface from the router to the module. You can reach the actual CLI with the service-module g x/y session command. This technique allows a console-type access to the module without an external console connection.

Q. Can I upgrade software images on the NAC network module and host router independently?

A. Yes. As long as the minimum Cisco IOS Software release requirements are met, you may change images on either the router or the NAC network module. You can upgrade the NAC network module application image independently, reboot, and reload it without affecting the router.

Q. How is the software image loaded onto the NAC network module?

A. You can load the CAS application image onto the NAC network module through a TFTP server. Please refer to product documentation for details.

Integrated Services Router Integration and Interoperability

Q. Does the Cisco NAC Network Module support the Cisco High-Speed Intrachassis Module Interconnect (HIMI) feature?

A. Yes. The network module supports the Cisco HIMI feature, which provides a dedicated, point-to-point internal connection from an enhanced network module (NME) to another NME or to the onboard Gigabit Ethernet Small Form-Factor Pluggable (SFP) port on a Cisco 3825 or 3845 Integrated Services Router. The HIMI feature, a Layer 2 connection that can scale up to 1 Gbps, supports a maximum of two NMEs per router chassis. Currently, Cisco EtherSwitch® Service Modules are NMEs that support HIMI. This feature allows an unprecedented level of integration between the Cisco NAC Network Module and other HIMI-capable enhanced network modules such as the Cisco EtherSwitch Service Modules. For more details about HIMI, visit http://www.cisco.com/en/US/products/ps5855/prod_configuration_guide09186a008068ea83.html#wp1047623.

Q. Can the Cisco NAC Network Module be deployed along with a Cisco EtherSwitch Service Module in the same integrated services router?

A. Yes. The NAC network module (NME-NAC-K9) can interoperate in the same chassis with any of the Cisco EtherSwitch Service Modules with the following part numbers: NME-16ES-1G-P, NME-X-23ES-1G-P, NME-XD-24ES-1S-P, NME-XD-48ES-2S-P, NME-16ES-1G, or NME-X-23ES-1G. The local LAN traffifc from end stations (laptops, PCs, IP phones, etc.) plugged into the Cisco EtherSwitch Module can be directed to the untrusted port of the NAC network module and the user traffic assessed by the NAC network module before being sent across the WAN through the router. On a Cisco 3825 or 3845, these two enhanced modules (Cisco NAC Network Module and Cisco EtherSwitch Service Module) can be connected directly through an internal, high-speed link (HIMI).

Q. Can the Cisco NAC Network Module be deployed along with Cisco Wireless LAN Controller Module in the same integrated services router?

A. Yes. The NAC network module can interoperate in the same chassis as any of the Cisco Wireless LAN Controller Modules with the following part numbers: NM-AIR-WLC6-K9, NME-AIR-WLC8-K9, or NME-AIR-WLC12-K9. For this deployment, wireless (and wired) LAN traffic must be policy routed through an onboard Gigabit Ethernet interface of an integrated services router to the untrusted interface on the NAC network module. The result is that some of the traffic traverses the router twice, potentially affecting performance.

If the predicted services load on the host router is heavy, you can deploy the wireless LAN controller as an appliance (Cisco 2100 or 4400 Series Wireless LAN Controllers) or as a switch (Cisco Catalyst® 3750 Series) along with the NAC network module. Alternatively, you can deploy the clean access server as an appliance (Cisco NAC 3300 Appliance) instead of a network module within the integrated services router along with a wireless LAN controller (NME-AIR-WLC).

Q. Does the Cisco NAC Network Module support Single Sign-On (SSO) for wireless users?

A. Yes. The router would need to be configured to use the NAC network module as a RADIUS accounting server. When users log in to the wireless network, their login credentials are provided through RADIUS accounting messages to the NAC network module. If login credentials are valid, the NAC network module does not require users to log in to the network a second time.

Q. Can the Cisco NAC Network Module be deployed with Cisco IOS Firewall and site-to-site VPN configured on the host router?

A. Yes, it can be deployed with Cisco IOS Firewall and site-to-site VPN configured on the router.

Q. Can the Cisco NAC Network Module be deployed in an integrated services router that is also configured to terminate remote-access VPN (IPsec and SSL VPN) ?

A. Yes. The NAC network module can be configured to interoperate with an integrated services router that is terminating remote-access VPN connections. For this deployment, decrypted traffic from remote-access VPN users must be policy routed through an onboard Gigabit Ethernet interface of an integrated services router to the untrusted interface on the NAC network module, but some of the traffic traverses the router twice, potentially affecting performance.

Q. Does the Cisco NAC Network Module support SSO for remote-access VPN users—both IPsec and SSL VPN?

A. Yes. For IPsec, the router is confgured to use the NAC network module as a RADIUS accounting server. When users log in to the VPN network, their login credentials are provided through RADIUS accounting messages to the NAC network module. If login credentials are valid, the NAC network module does not require users to log in to the network a second time. SSO support for SSL VPN will be available beginning with the Cisco NAC Appliance Release 4.1.3.

Ordering, Licensing, and Miscellanous

Q. How do I order the Cisco NAC Network Module for Integrated Services Routers?

A. When you configure a Cisco 2800, 2900, 3800 or 3900 Integrated Services Router chassis or bundle, select the NAC network module as an option within Network Modules. After confirming the software version for the NAC network module, please select between the two Cisco NAC Network Module Server Licenses: part number NACNM-50-K9 or NACNM-100-K9. If you initially purchase the 50-user license (NACNM-50-K9) for the NAC network module, you can upgrade to the 100-user license later by ordering part number NACNM-50UL=. You can select all the licenses in the same way and apply them to the module spare (NME-NAC-K9=). Refer to Table 2 for details.

Table 2. Ordering Information for Cisco NAC Network Module for Integrated Services Routers

Hardware and Software Part Number	Needed for Supporting Cisco NAC Network Module
NME-NAC-K9	Cisco NAC Network Module for 2800, 2900, 3800 and 3900 ISR
NACNM-50-K9	NAC Network Module Server License -max 50 users
NACNM-100-K9	NAC Network Module Server License -max 100 users
NACNM-50UL=	NAC Network Module Server License Upgrade -50 to 100 users
NME-NAC-K9=	Cisco NAC Network Module for 2800, 2900, 3800 and 3900 ISR (spare)

Q. Are the user licenses on the NAC network module upgradable?

A. Yes. You can upgrade a NAC network module from its original 50-user license to the 100-user license by ordering part number NACNM-50UL=. For more details about licensing, please visit http://www.cisco.com/en/US/products/ps6128/prod_pre_installation_guide09186a008073136b.html.

Q. Can I purchase the Cisco NAC Network Module as a spare?

A. Yes. If you have already deployed an integrated services router in your network, you can order the Cisco NAC Network Module as a spare (order part number NME-NAC-K9=). Please note that you can use the same software and license part numbers when ordering the spare enhanced network module.

Q. Is there a license upgrade path from the Cisco NAC Network Module to the Cisco NAC Appliance?

A. No. The NAC network module and NAC appliance are fundamentally different hardware platforms and there is no license upgrade path from one to another. If you anticipate the number of users in a given location to grow beyond 100 users, Cisco recommends that you deploy the Cisco Clean Access Server as a NAC appliance.

Q. Do I need to buy a separate technical services (support) contract for the NAC network module?

A. No. If you purchase the technical services contract for the host router (Cisco 2800, 2900, 3800 or 3900 Integrated Services Router), support for the NAC network module is included. Please note that you might still have to purchase a separate services contract for the clean access manager (deployed as a NAC appliance) deployed centrally in the network.

For More Information

For more information about the Cisco NAC Appliance, visit http://www.cisco.com/go/isr and http://www.cisco.com/go/nac/appliance, contact your local Cisco account representative, or send an e-mail message with your questions to cca-questions@external.cisco.com.

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 C67-424308-01 10/09