Cisco NAC Network Module for Integrated Services Routers

The Cisco® NAC Network Module for Integrated Services Routers (NME-NAC-K9) brings the feature-rich Cisco NAC Appliance Server capabilities to Cisco 2800, 2900, 3800 and 3900 Series Integrated Services Routers. Cisco NAC Appliance (also known as Cisco Clean Access) is a rapidly deployable Network Admission Control (NAC) product that allows network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing them onto the network.

Product Overview

The Cisco NAC Network Module for Integrated Services Routers (NME-NAC-K9) extends the Cisco NAC Appliance portfolio of products to smaller locations, helping enable network admission control (NAC) capabilities from the headquarters to the branch office (Figure 1). 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. The Cisco NAC Network Module for Integrated Services Routers deployed at the branch office remediates potential threats locally before they traverse the WAN and potentially infect the network.

Figure 1. Cisco NAC Network Module for Integrated Services Routers (NME-NAC-K9)

The Cisco NAC Network Module for Integrated Services Routers is an advanced network security product that:

- Recognizes users, their devices, and their roles in the network: This first step occurs at the point of authentication, before malicious code can cause damage.
- Evaluates machines to determine their compliance with security policies: Security policies can vary by user type, device type, or operating system.
- Enforces security policies by blocking, isolating, and repairing noncompliant machines: The machines are redirected into a quarantine area, where remediation occurs at the discretion of the administrator.

Features and Benefits

The Cisco NAC Network Module is supported on modular Integrated Services Routers with a network module slot—namely the Cisco 2811, 2821, 2851, 2911, 2921, 2951, 3825, 3845, 3925, and 3945 platforms. 2900 and 3900 G2 integrated services router platforms support the NAC network module with an adapter card (SM-NM-ADPTR) starting with IOS 15.0 (M) Release. The NAC module can apply posture assessment and remediation services to all end devices, regardless of:

- **Device type**: The Cisco NAC network module can enforce security policies on all networked devices, including Windows, Mac, or Linux machines; laptops; desktops; personal digital assistants (PDAs); and corporate assets, such as printers and IP phones.
- **Device ownership**: The NAC network module can apply security policies to systems owned by the corporation, employees, contractors, and guests.
- **Device access method**: The NAC network module applies network admission control to devices connecting through the LAN, wireless LAN (WLAN), WAN, or VPN.

With the Cisco NAC Network Module, the Integrated Services Routers are unique in its ability to enforce policies for branch-office deployments without requiring separate appliances.

Networks with the Cisco NAC Network Module and Cisco Integrated Services Routers 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

Product Architecture

The Cisco NAC Appliance solution has three components:

- **Clean Access Server (CAS)**: This device—either a standalone appliance or a network module for integrated services routers—initiates assessment and enforces access privileges based on endpoint compliance. Users are blocked at the port layer and restricted from accessing the trusted network until they successfully pass inspection.

  As a network module for integrated services routers, the CAS is available in two sizes based on the number of online, concurrent users: 50 and 100 users. As an appliance, it is available in six sizes based on the number of online, concurrent users: 100, 250, 500, 1500, 2500, and 3500 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 NAC Network Module within a Cisco Integrated Services Router.
- **Clean Access Manager (CAM)**: This centralized, Web-based console establishes roles, checks, rules, and policies. It 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.
- **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.

Deployment Modes

The Cisco NAC network module can be deployed in several ways to best accommodate your branch network security requirements. Figure 2 shows the NAC network module within a Cisco 2800 or 3800 Series Integrated Services Router or 2900 or 3900 G2 Series Integrated Services Router for a branch office. The 100 or fewer employees in the branch office utilize the Clean Access Server functions on the NAC network module before being allowed access to the network. Similarly, campus employees use the Clean Access Server functions on the local NAC Appliance. A centralized Clean Access Manager across the WAN is required to configure and manage several NAC network modules or NAC appliances deployed in multiple office locations of this enterprise customer.

Figure 2. Typical Branch Office Deployment Scenario for Cisco NAC Network Module in an Integrated Services Router

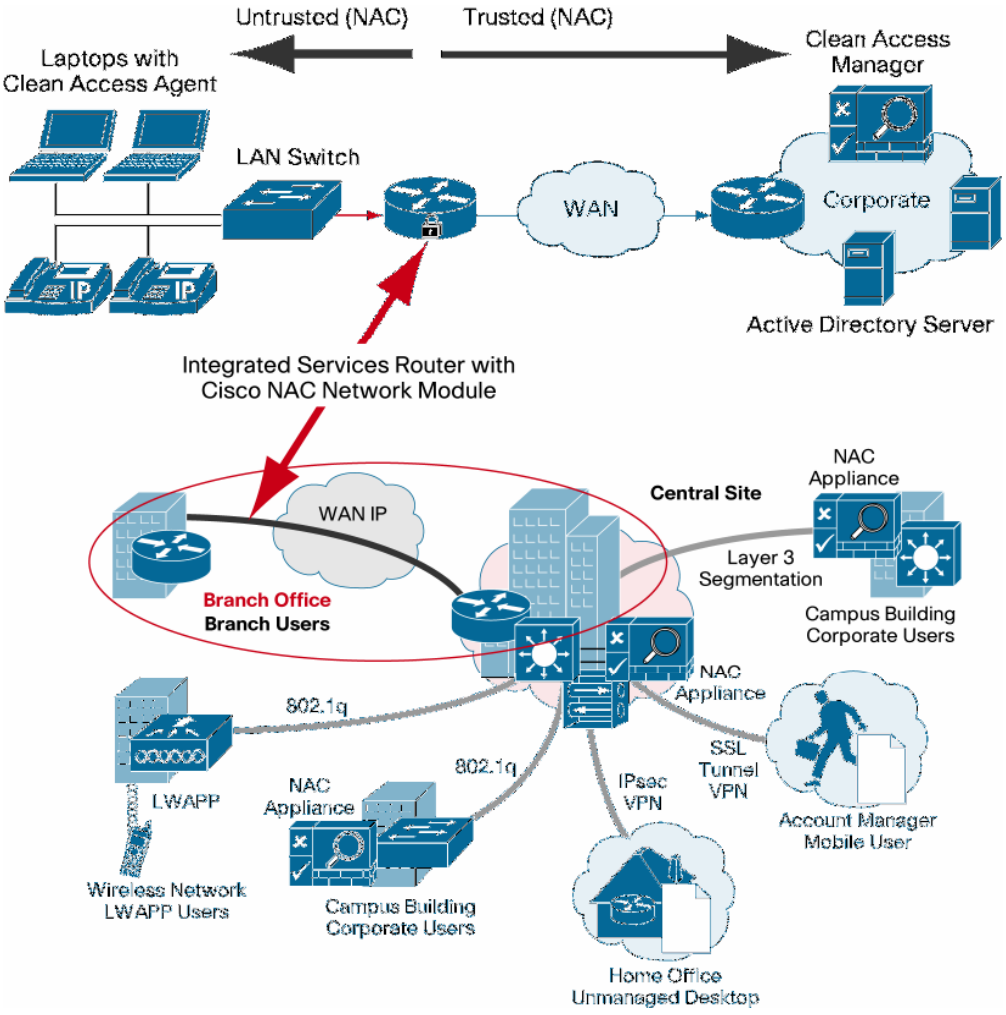

Table 1. Cisco NAC Network Module Deployment Options

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)

Although the Cisco NAC Network Module in in-band mode supports any network infrastructure, the out-of-band mode communicates with switches using the Simple Network Management Protocol (SNMP). Please visit http://www.cisco.com/en/US/products/ps6128/products_device_support_table09186a008075fff6.html for the most recent list of supported switches. This list is updated frequently.

High-Speed Intrachassis Module Interconnect on Cisco NAC Network Module

The Cisco NAC Network Module supports High-Speed Intrachassis Module Interconnect (HIMI) on Cisco 2900, 3800 and 3900 series Integrated Services Routers. On 3800 series router, the HIMI feature provides the capability to establish 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 router. On 2900 and 3900 series rouer, the HIMI feature supports SM-to-SM or SM-to-ISM communication where SM stands for an external Service Module such as NAC NME using an adapter card (SM-NM-ADPTR) and ISM stands for an Internal Service Module. The HIMI feature is a Layer 2 connection that can scale up to 1 Gbps. For more information, visit http://www.cisco.com/en/US/prod/collateral/routers/ps5855/product_data_sheet0900aecd8028d15f.html.

http://www.cisco.com/en/US/products/ps5855/prod_configuration_guide09186a008068ea83.html#wp1047623.

HIMI 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.

Product Specifications

Table 2 lists the hardware specifications for the Cisco NAC Network Module for Integrated Services Routers.

Table 2. Hardware Specifications for Cisco NAC Network Module (NME-NAC-K9)

Feature	Cisco NAC Network Module for Integrated Services Routers
Product	NME-NAC-K9
Processor	1-GHz Intel Celeron-M
Memory	512-MB double data rate 2 (DDR2)
Flash Memory	64-MB Compact Flash
Hard disk	80-GB Serial ATA (SATA) drive
Ethernet Network Interface Cards (NICs)	• One internal 1000-Mbps Ethernet interface-to-router backplane • One External 10-/100-/1000-Mbps Ethernet interface
Physical Dimensions (H x W x D)	1.55 x 7.10 x 7.2 in.(3.9 x 18.0 x 18.3 cm)
Weight	1.25 lb (0.57 kg)
Operating Humidity	5 to 95%, noncondensing
Operating Temperature	32 to 104℉ (0 to 40℃)
Nonoperating Temperature	-13 to 158℉ (–25 to 70℃)
Maximum Operating Temperatures	• 104℉ (40℃) at sea level • 104℉ (40℃) at 6,000 ft (1800m) • 86℉ (30℃) at 13,000 ft (4000m) • 80℉ (27.2℃) at 15,000 ft (4600m) • Note: De-rate 2.5℉ (1.4℃) per 1000 ft above 6000 f t
Power	21W
Safety Compliance	UL, CSA, EN, and IEC 60950-1

Feature	Cisco NAC Network Module for Integrated Services Routers
EMC Compliance	• 47 CFR Part 15 Class A • CISPR22 Class A • EN300386 Class A • EN55022 Class A • EN61000-3-2 • EN61000-3-3 • VCCI Class I • AS/NZS CISPR 22 Class A
Immunity Compliance	• CISPR24 • EN300386 • EN50082-1 • EN55024 • EN61000-6-1

The Cisco NAC Network Module for Integrated Services Routers supports the same software features as the Clean Access Server on a NAC Appliance, with the exception of high availability. NME-NAC-K9 does not support failover from one module to another.

Table 3 highlights the software features supported on the NAC Network Module.

Table 3. Software Features for Cisco NAC Network Module (NME-NAC-K9)

Software Features	Cisco NAC Network Module for Integrated Services Routers
Authentication Integration with Single Sign-On (SSO)	The Cisco NAC Network Module for Integrated Services Routers serves as an authentication proxy for most forms of authentication, natively integrating with Kerberos, Lightweight Directory Access Protocol (LDAP), RADIUS, Active Directory, and others. To minimize the inconvenience to end users, the Cisco NAC Network Module supports SSO for IP Security (IPsec) VPN clients, wireless clients, and Windows Active Directory domains. Administrators can maintain multiple user profiles with different permission levels by using role-based access control.
Vulnerability Assessment	The Cisco NAC Network Module supports scanning of all Windows, Mac OS, and Linux-based operating systems and machines, as well as non-PC networked devices such as game consoles, PDAs, printers, and IP phones. It conducts network-based scans or can use custom-built scans as required. The NAC network module can check for any application as identified by registry key settings, services running, or system files.
Device Quarantine	The Cisco NAC Network Module can place noncompliant machines into quarantine to prevent the spread of infection while enabling the machines to maintain access to remediation resources. Quarantine can be accomplished by using subnets as small as /30, or by using a quarantine VLAN.
Centralized Management	The Cisco NAC Module for Integrated Services Routers is centrally managed by a Web-based management console, the Clean Access Manager (CAM), which allows administrators to define the types of scans required for each role, as well as the related remediation packages necessary for recovery. One management console can manage multiple NAC network modules or NAC appliances.
Automatic Security Policy Updates	Automatic security policy updates that are part of the Cisco standard software maintenance package provide predefined policies for the most common network access criteria, including policies that check for critical operating system updates, common antivirus software virus definition updates, and common antispyware definition updates. These updates ease the management cost for network administrators, because the Cisco Clean Access Manager (CAM) constantly maintains updated policies.
Remediation and Repair	Quarantining gives devices access to remediation servers that can provide operating system patches and updates, virus definition files, or endpoint security solutions such as Cisco Security Agent. Administrators can enable automated remediation through the optional agent, or specify a series of remediation instructions.
Flexible Deployment Modes	The Cisco NAC Network Module offers a broad array of deployment modes to fit into any customer network. Customers can deploy the product as a virtual or real IP gateway,with Layer 2 or Layer 3 client access, and in-band or out-of-band with network traffic.

The Cisco NAC Network Module supports SSO for wireless and remote-access users using certain IPsec VPN and WebVPN clients. Table 4 outlines these components.

Table 4. VPN and Wireless Components Supported with SSO

Product	Clients
Cisco Integrated Services Routers	-
Cisco Wireless LAN Controllers	• Cisco SSL VPN (Tunnel) • Cisco IPsec VPN Client
Cisco ASA 5500 Series Adaptive Security Appliances	
Cisco VPN 3000 Series Concentrators	
Cisco PIX® Security Appliances	

System Requirements

Table 5 gives the system requirements for the Cisco NAC Network Module.

Table 5. System Requirements (Hardware and Software)

Router Platforms (Supported Hardware)	IOS Software Releases/Images Supported
• Cisco 2811, 2821 or 2851 Integrated Series Routers • Cisco 3825 or 3845 Integrated Series Routers	• Cisco IOS® Software Release 12.4(11)T or later • Cisco IOS IP Base image or above
• Cisco 2911, 2921, and 2951 Integrated Services Router G2 • Cisco 3925 and 3945 Integrated Services Router G2	• Cisco IOS® Software Release 15.0(1)M • IP Base (No license required)

The optional Clean Access Agent works on systems with the characteristics listed in Table 6.

Table 6. Cisco Clean Access Agent System Requirements

Feature	Minimum Requirement
Supported OS	Windows Vista Home, Windows Vista Business, Windows Vista Ultimate, Windows Vista Enterprise, Windows XP Professional, Windows XP Home, Windows XP Media Center Edition, Windows XP Tablet PC, Windows 2000, Windows 98, Windows SE, Windows ME, and Mac OS X (authentication only)
Hard Drive Space	Minimum of 10 MB of free hard drive space
Hardware	No minimum hardware requirements (works on various client machines)

For the latest information about Cisco Clean Access Agent support, please visit http://www.cisco.com/en/US/products/ps6128/products_device_support_table09186a00807600e1.html#wp42008.

Cisco NAC Appliance Manager is preconfigured to offer policy checks for more than 300 applications from 50 vendors. This list is constantly being expanded; please visit http://www.cisco.com/en/US/products/ps6128/prod_release_notes_list.html for the latest supported applications (listed under “Cisco NAC Appliance Supported AV/AS Product List”). Note: Not all check types are supported for all products, and some vendors do not support Windows 95, 98. In addition to the preconfigured checks, you have full access to the Cisco NAC Appliance rules engine and can create any custom check or rule for any other third-party application.

Ordering Information

You can order the Cisco NAC Network Module through Cisco sales and distribution channels worldwide by using the Cisco Ordering Tool at http://www.cisco.com/en/US/ordering/index.shtml. Refer to Table 7 for ordering information.

Table 7. 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 & 3800 ISR, 2900 & 3900 ISR G2
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 & 3800 ISR, 2900 & 3900 G2(spare)

When you configure either a Cisco 2800 or 3800 Integrated Services Router chassis or bundle or a Cisco 2900 or 3900 Integrated Services Router G2 chassis, select part number NME-NAC-K9 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 the license part numbers and apply them to the module spare (NME-NAC-K9=) in a similar manner. Licensing information is available at http://www.cisco.com/en/US/products/ps6128/prod_pre_installation_guide09186a008073136b.html

Cisco and Partner Services for the Branch

Services from Cisco and our certified partners can help you transform the branch experience and accelerate business innovation and growth in the Borderless Network. We have the depth and breadth of expertise to create a clear, replicable, optimized branch footprint across technologies. Planning and design services align technology with business goals and can increase the accuracy, speed, and efficiency of deployment. Technical services help improve operational efficiency, save money, and mitigate risk. Optimization services are designed to continuously improve performance and help your team succeed with new technologies. For more information, visit http://www.cisco.com/go/services.

For More Information

For more information about the Cisco NAC Module for Integrated Services Routers, visit http://www.cisco.com/go/isr and http://www.cisco.com/go/nac/appliance or contact your local Cisco account representative.

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 C78-422309-01 10/09