Cisco Clean Access: In-Band and Out-Of-Band Deployment Options and Considerations

Cisco Clean Access (NAC Appliance) is an easily deployed 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 users onto the network. The solution identifies whether machines are compliant with security policies and repairs vulnerabilities before permitting access to the network. Cisco Clean Access is available in two modes: as either an in-band or out-of-band solution. This white paper explores when and how each mode is appropriate, depending on individual network characteristics and customer preferences.

CISCO CLEAN ACCESS OVERVIEW

In 2003, Cisco Systems® introduced the NAC concept as a way for networks to make compliance with security policies a prerequisite for network access. Today, customers can choose to deploy NAC in two ways—either through an industry-collaborative framework that takes advantage of the solutions of other vendors, or through the Cisco Clean Access product family, which combines the features of authentication, posture assessment, quarantine, and remediation into a self-contained product.

The Cisco Clean Access solution consists of three components:

- **Cisco Clean Access Server**—This is an in-band or out-of-band device that acts as the first challenge for any end user trying to access the network. The Cisco Clean Access Server challenges the end user with a login page or requires the download of a Cisco Clean Access Agent before permitting access to the network.
- **Cisco Clean Access Manager**—This server manages Cisco Clean Access servers remotely, globally, or individually and enables administrators to establish user roles, device checks, and remediation requirements. It also acts as the authentication proxy to the authentication servers that reside on the back end.
- **Cisco Clean Access Agent**—This is an optional client-side component of the Cisco Clean Access system. It is a read-only client that delivers device-based registry scans on unmanaged environments. It is downloadable and provisioned over the Internet; in fact, customers that use the Cisco Clean Access Agent often make it a required download before network access is granted.

Cisco Clean Access was built with several principles in mind:

Flexibility. Every network is different. Cisco Clean Access can be deployed in-band or out-of-band in a variety of ways, including as a virtual gateway or as a real IP gateway. Cisco Clean Access can also operate with an agent (for incoming machines) or without an agent, a decision that often depends on the types of users that are supported on the network. And in terms of network environments, the in-band Cisco Clean Access solution can support switching and routing infrastructures from any vendor.

Ease of installation and use. Most Cisco Clean Access deployments have taken less than a day. The Web-based Cisco Clean Access Manager enables administrators to set up user roles, rules, checks, and requirements. Security updates for Microsoft hot fixes and antivirus software virus definitions files are automatically downloaded into Cisco Clean Access.

Scalability. A single Cisco Clean Access Server easily supports 1500 concurrent users with a throughput of roughly 1 Gbps. Cisco Clean Access is offered in configurations that serve as few as 100 users and as many as tens of thousands of users.

IN-BAND OR OUT-OF-BAND?

Customers often ask which deployment modes are most appropriate for their networks. In fact, an organization can deploy both, each geared toward certain types of access (in-band for supporting wireless users and out-of-band for wired users, for example). The Cisco

Clean Access Manager is designed to support both in-band and out-of-band Cisco Clean Access servers, as well as the switches associated with the out-of-band portion of the network.

Table 1 outlines the advantages and disadvantages of each deployment mode.

Table 1. Comparing In-Band and Out-of-Band Modes

	In-Band	Out-of-Band
PROS	• Agnostic to switch/router platform and versions • Appropriate for wired and wireless • Full network access control • Bandwidth management control	• Inline-only for quarantined traffic • Full access control in quarantine • Smooth switch control via Simple Network Management Protocol (SNMP) • Port- or role-based VLAN assignment
CONS	• Inline dependency • No switch-port-level control	• Switch platform and version dependencies • Most appropriate for wired scenarios

IN-BAND IN-DEPTH

With the Cisco Clean Access in-band deployment, the Clean Access Server is always inline with user traffic—before, during, and after authentication, posture assessment, and remediation. The server can be used to securely control authenticated and unauthenticated user traffic by managing traffic policies based on protocol/port or subnet, providing bandwidth policy management based on shared or per-user, or using time based sessions and heartbeat controls.

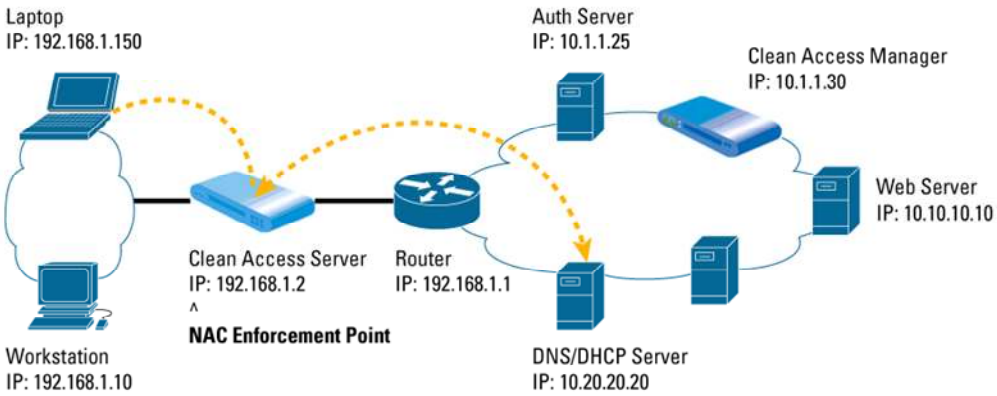
In-band deployment supports any edge access device as long as the MAC address and IP address of the client machine are visible to the Clean Access Server. Because the server is in-band with traffic, the in-band deployment mode is ideal for environments with the following characteristics:

- Shared media ports
- Bandwidth throttling by role required
- Wireless access points
- Voice over IP (VoIP) phones
- Network infrastructure built with products other than Cisco products

Cisco Clean Access In-Band Process Flow: How It Works

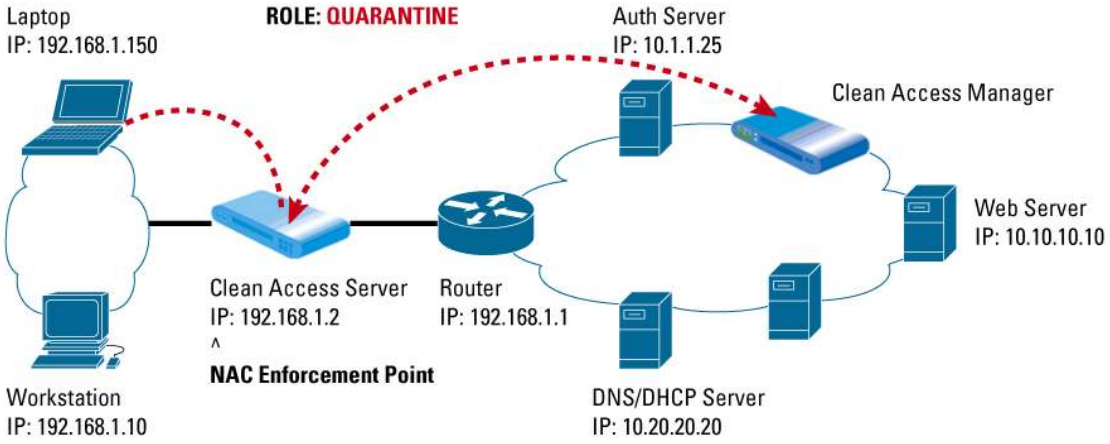
Figures 1–4 follow the process flow of an in-band deployment.

Figure 1. Laptop Attempts to Access the Internal Network



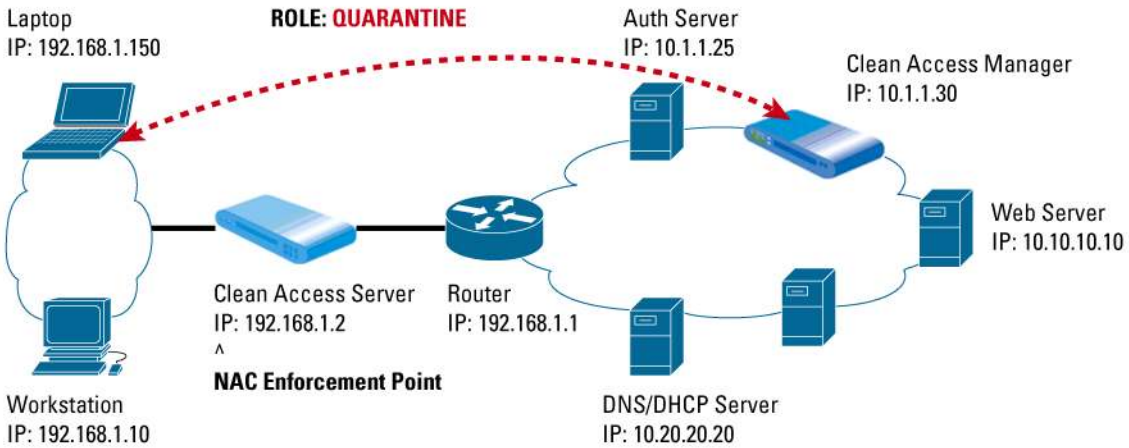
1. When the laptop first accesses the network, the Cisco Clean Access Server determines that the computer's MAC address is not in the list of certified devices, and that laptop is placed into an unauthenticated role. While in this role, only User Datagram Protocol (UDP) Port 53 (Domain Name System [DNS]) and Dynamic Host Control Protocol (DHCP) traffic (via DHCP and VLAN passthrough) is allowed.
2. The laptop gets an IP address from the DHCP server, but cannot get past the Clean Access Server acting as an IP filter.
3. The laptop user opens a browser and is redirected to an SSL-based Web login page where she enters her credentials, which in turn map her into the "employee" role.
4. As an "employee," she is asked to download the Clean Access Agent.
5. The Clean Access Agent performs the posture assessment and forwards the results to the Clean Access Server to make the network admissions decision.

Figure 2. Laptop Goes Through Posture Assessment



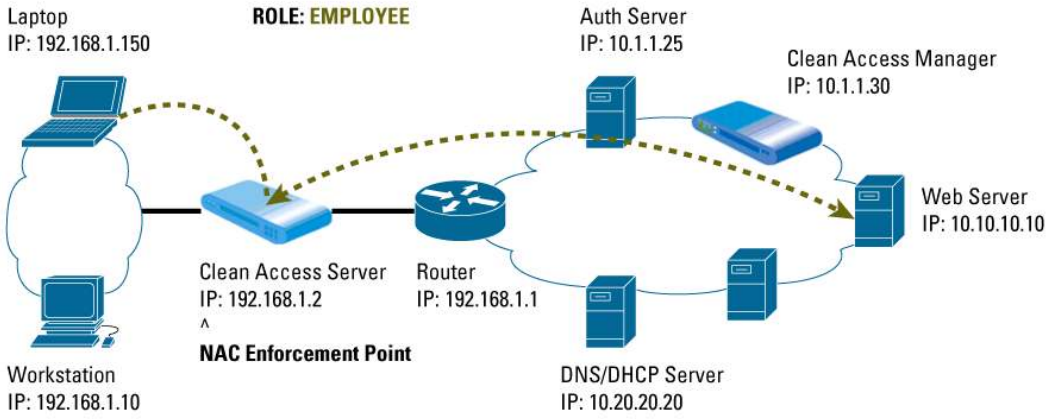
6. The Clean Access Server forwards the report to the Clean Access Manager, which determines that the laptop is not in compliance. The manager instructs the server to put the laptop into the "quarantine" role, which can be as small as a /30 subnet.
7. The Clean Access Manager then sends the remediation steps to the Clean Access Agent.

Figure 3. Clean Access Manager Sends Remediation Instructions to the Clean Access Agent on the Laptop



8. A clock displays the time remaining in the quarantine role for the laptop user while the Clean Access Agent guides the user step-by-step through remediation. Patches can be downloaded either from an internal or external update sites (such as http://windowsupdate.microsoft.com) or from the Clean Access Manager itself.
9. After the remediation process, the Clean Access Agent informs the Clean Access Server that the laptop is now compliant.

Figure 4. Once Compliant, Laptop's MAC Address is Added to List of Certified Devices and Access is Granted



10. The Clean Access Server then adds the MAC address of the laptop onto the certified devices list and assigns it to the employee role, which enables the laptop to complete its access to the internal Web server.

OUT-OF-BAND IN-DEPTH

In an out-of-band deployment of Cisco Clean Access, the Clean Access Server is in-band only during the process of authentication, posture assessment, and remediation. Once the user's device has successfully logged on, its traffic then bypasses the Clean Access Server and traverses the switch port directly. In the meantime, the Clean Access Manager provides port- or role-level control by assigning ports to specific VLANs, assigning users to specific roles that map to specific VLANs, and providing a time-based session timeout per role.

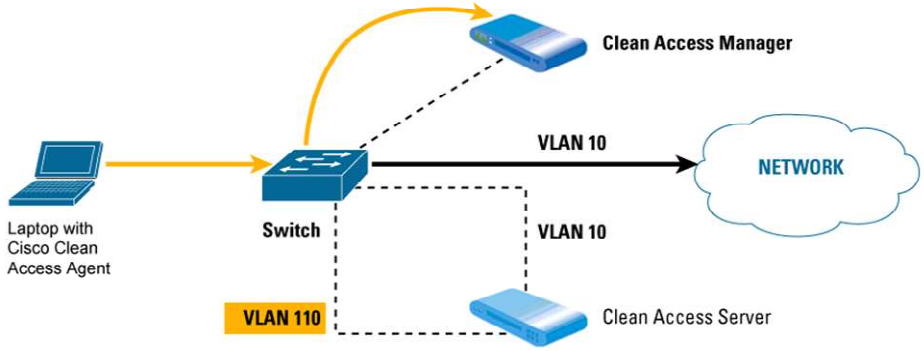
Cisco Clean Access out-of-band is most appropriate for high-throughput, highly routed environments such as campuses, branch offices, and extranets. It is not suitable for use with shared media devices, such as hubs and wireless access points.

Cisco Clean Access Out-of-Band Process Flow: How It Works

Figures 5–8 follow the process flow of an out-of-band deployment.

1. When a device first accesses the network, the switch sends the MAC address of the device via SNMP-based notification to the Cisco Clean Access Manager.

Figure 5. Laptop Attempts Access to Network, Switch Sends MAC Address to the Clean Access Manager



2. The Clean Access Manager verifies whether the device is on the out-of-band online list or certified devices list.
3. If the device does not appear on either list, the Clean Access Manager instructs the switch to assign the port the device is on to the authentication or quarantine VLAN. A DHCP address is assigned as DHCP/DNS traffic traverses the Clean Access Server using VLAN mapping.

Figure 6. If Laptop is Not on the Out-Of-Band Online List or Certified Devices List, the Switch Assigns the Device to a Quarantine VLAN

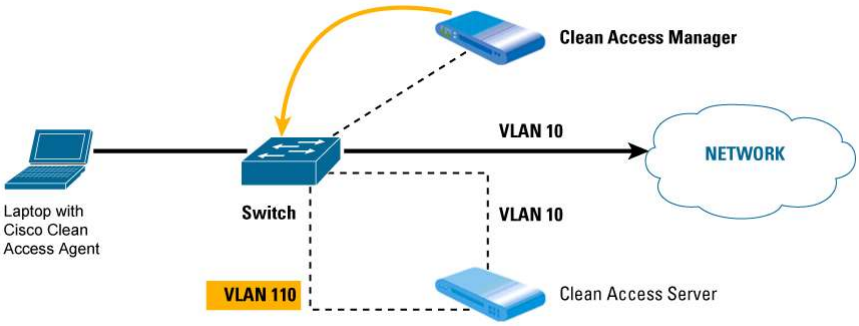
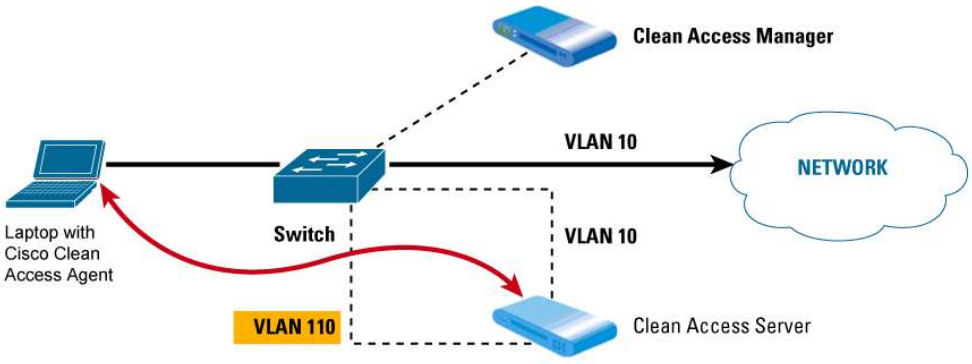


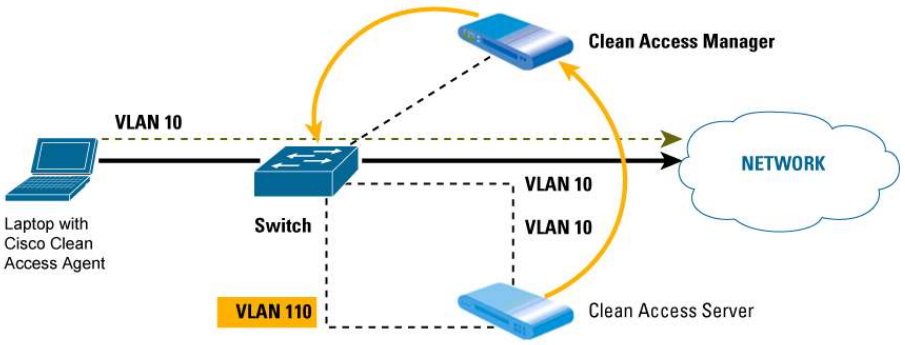
Figure 7. While on the Quarantine VLAN, Laptop Undergoes Posture Assessment



4. The Clean Access Server is on the same authentication VLAN (110) as the device. While in this VLAN, the device is challenged for its credentials to determine the role of its user. If the Clean Access Agent is enforced, it receives compliance checks from the Clean Access Server based on the requirements of that role.

5. The Clean Access Agent guides the user through a step-by-step remediation process; the user is allowed access to remediation sites enforced by the Clean Access Server.
6. Once remediation is completed, the Clean Access Server informs the Clean Access Manager that the device is now certified.
7. The Clean Access Manager then instructs the switch to put the device's port onto the access VLAN (10) based on port mapping or the role assignment. The device is now allowed access to the network.

Figure 8. After Successful Remediation, the Clean Access Manager Instructs the Switch to Move the Laptop to the "Trusted" VLAN



Summary of Differences

While both the in-band and out-of-band deployments of Cisco Clean Access accomplish the basic tasks of authentication, posture assessment, quarantine, and remediation, deciding which one to deploy depends largely on how the system will be used. Table 2 summarizes the salient differences.

Table 2. In-Band and Out-of-Band Deployment Environments

	In-Band	Out-of-Band
Environments	Wireless, shared media	Fast core switching infrastructures; high throughput requirements
NAC Enforcement Point	Cisco Clean Access Server in-band	Cisco Clean Access Server with authentication/quarantine VLAN
Quarantine	Based on access control list (ACL)	Based on VLAN
Switches Supported	Vendor-agnostic	Cisco Catalyst 2950, 3550, 3560, 3750, 4500, and 6500 switches*

*Please check with your Cisco sales representative for the latest list of support switches or visit http://www.cisco.com/en/US/partner/products/ps6128/prod_release_notes_list.html.

FOR MORE INFORMATION

For more information about the Cisco Clean Access solution, visit http://www.cisco.com/go/cca, send questions to cca-questions@external.cisco.com, or contact your local account representative.

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.com Website at 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

C11-337382-00 02/06