

Cisco ACE Family

Cisco ACE GSS 4492R Global Site Selector

The Cisco® GSS 4492R Global Site Selector is part of the Cisco ACE Application Control Engine family and a crucial component of any data center architecture that requires an appliance-based, security-focused, universal global load balancer. The Cisco GSS 4492R is deployed with Cisco ACE Application Control Engine Modules and market-leading Cisco content switches (such as the Cisco CSS 11500 Series Content Services Switches and the Cisco Content Switching Module [CSM] for Cisco Catalyst® 6500 Series Switches), devices with Cisco IOS® Software Server Load Balancing (SLB), or older switches (such as Cisco CSS 11000 Series and Cisco LocalDirector devices).

With optional software, the Cisco GSS 4492R can be deployed as a Domain Name System (DNS) appliance supporting Cisco Network Registrar® Release 6.3 which is a full-featured DNS and Dynamic Host Configuration Protocol (DHCP) system that provides scalable naming and addressing services for enterprise and service provider networks requiring dependable, global quad-play services (voice, data, and video with mobility services).

The Cisco GSS 4492R makes unique use of other Cisco technologies to mitigate the effects of a DNS-based distributed-denial-of-service (DDoS) attack. This distinctive self-protection capability can be deployed to shield any DNS infrastructure such as Berkeley Internet Name Domain (BIND) services and Microsoft-based client devices along with Microsoft Active Directory.

Through the combination of a universal Simple Network Management Protocol (SNMP) load and health monitoring, the Cisco GSS 4492R can now essentially globally load balance any device that uses common DNS requests for access, and provide load data through an SNMP MIB.

Figure 1. Cisco GSS 4492R Global Site Selector



The Cisco GSS 4492R delivers the following capabilities:

- Provides a scalable, dedicated hardware platform for industry-leading Cisco content switches to help ensure that all applications (Web-based applications, e-mail, etc.) are always available, by detecting site outages or site congestion and rerouting client requests
- Improves the global data center selection process by offering user-selectable global load-balancing algorithms along with universal SNMP load and health probes
- Offloads, augments, or replaces DNS servers by taking over the domain resolution process, and transmits these requests at thousands of requests per second

- Scales to support hundreds of data centers or SLB devices
- Complements the existing DNS infrastructure by providing centralized domain management
- Tightly integrates with Cisco SLB devices without sacrificing the ability to work in a heterogeneous environment of DNS-capable networking products

The Cisco GSS 4492R allows businesses to deploy global Internet and intranet applications with the confidence that all application users will be quickly rerouted to a standby data center if a primary data center outage or overload occurs. The Cisco GSS 4492R traffic-management process continuously monitors the load and health of any SNMP-capable device (SLB devices, mail transfer agents, etc.) within each data center. The Cisco GSS 4492R uses this information in conjunction with customer-controlled load-balancing algorithms to select a data center that is available and not overloaded, within user-definable load conditions, in real time.

By offloading or replacing the DNS server resolution process of traditional DNS servers, the Cisco GSS 4492R adds a new level of DNS self-defense, simplifies the DNS infrastructure, optimizes global site selection, boosts DNS responsiveness, helps ensure data center availability, and increases the scalability of Websites and data centers. The Cisco GSS 4492R is a crucial component for enterprises and service providers deploying globally distributed data centers, installing disaster-recovery solutions, or looking for a way to consolidate and strengthen the DNS architecture of a standalone data center.

Features and Benefits

The Cisco GSS 4492R offers the following benefits:

- Reduces operating expenses (OpEx) and optimizes capital expenditures (CapEx) by consolidating global server load balancing (GSLB), DNS, DHCP, and Trivial File Transfer Protocol (TFTP) services on one appliance
- Provides a unique self-defending resilient architecture that is crucial for disaster recovery and for multisite Web application deployments
- Augments offloading or replaces any DNS BIND infrastructure to optimize content requests and delivery for all types of static and dynamic Web content
- Offers flexible, heterogeneous support for all Cisco SLB devices and DNS-capable networking products, including third-party load balancers
- Provides centralized command and control of the DNS resolution process for direct and precise control of the global load-balancing process
- Provides dedicated processing of DNS requests for greater performance and scalability
- Offers site persistence for e-commerce applications
- Offers two unique network proximity features that use Cisco routers and Layer 4 through 7 content switches to allow the Cisco GSS 4492R to direct content consumers to the closest data center in real time
- Supports a Web-based GUI and DNS wizard to simplify GSLB command and control
- Supports role-based access control (RBAC) and operation to limit access to Cisco GSS 4492R functions and features
- Supports configuration using a flat text file, the command-line interface (CLI), and the GUI

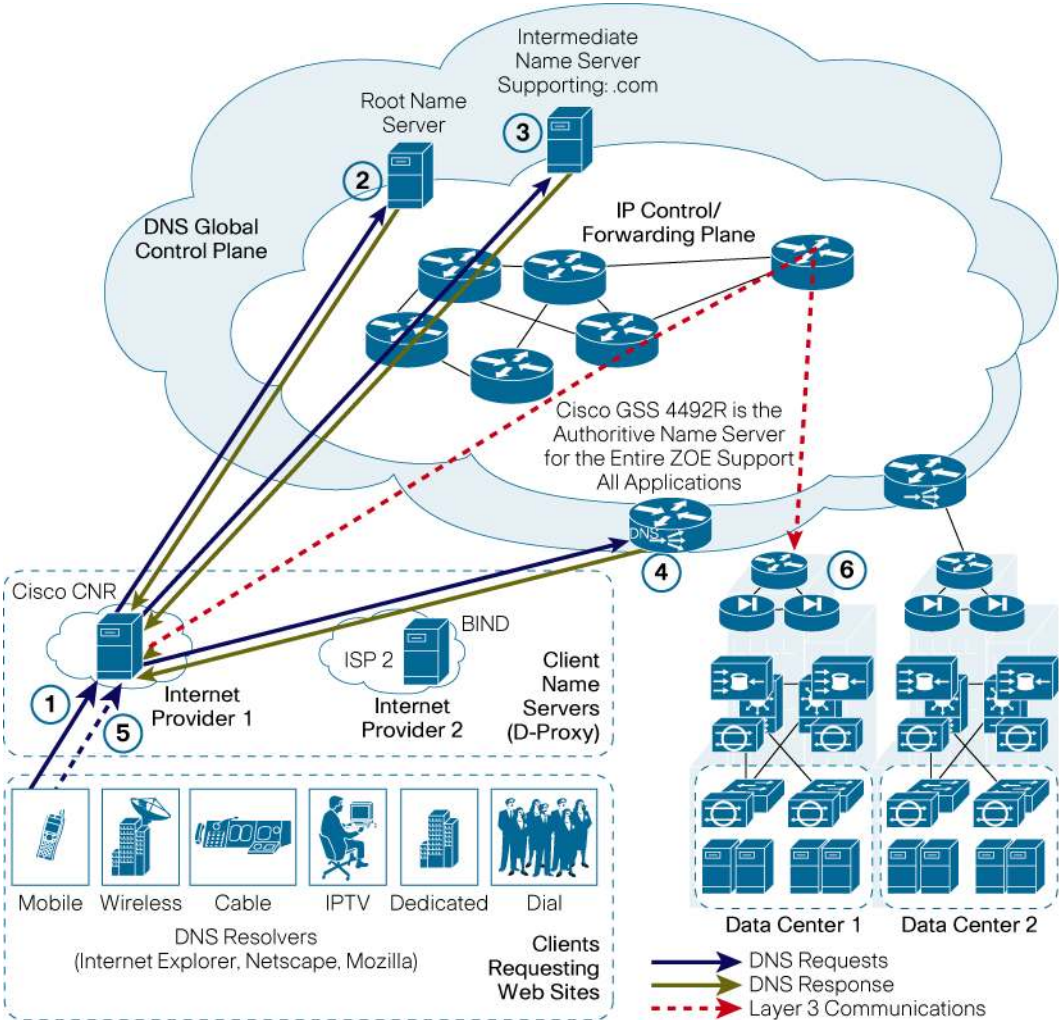
Cisco GSS 4492R and Cisco Application Switches Combine for Business Resiliency

The Cisco GSS 4492R, in combination with a local Cisco application switch, provides an outstanding solution for large enterprises and service providers planning to deploy highly reliable distributed data centers. The Cisco GSS 4492R selects the best site based on the load and availability information supplied by the Cisco application switch; the Cisco application switch selects the best local server within the data center based on availability and local load. The Cisco GSS 4492R simplifies the network deployment architecture with its centralized command and control features. For example, the Cisco GSS 4492R can gracefully take a Cisco application switch out of rotation without affecting ongoing operations.

The Cisco GSS 4492R performs two major functions as part of the global site selection process:

- Takes an active role in the DNS infrastructure to connect the client to the SLB device that supports the requested Website
- Continuously monitors the load and availability of these SLB devices to select the SLB device most capable of supporting the new client

Figure 2. Cisco GSS 4492R Site Selection Process



In Figure 2, the Cisco GSS 4492R has optional software that allows it to act like a DNS appliance, so it can provide GSLB services for the entire DNS zone (Cisco.com). The Cisco GSS 4492R continuously monitors the load and health of up to 128 SLB devices or 4000 virtual IP addresses. These SLB devices can be located together or at disparate remote or standalone data centers.

How the Cisco GSS 4492R interacts with the client in the data center selection process is summarized in the following six steps (corresponding to the numbers in Figure 2):

- Step 1. A client wants to access an application at Cisco.com (Web, e-mail, VPN, etc.). The resolver (client) sends a query for Cisco.com to the local client DNS server (D-proxy). In this case, the Cisco Network Registrar client acting as the D-proxy could be a Cisco GSS 4492R running the Cisco Network Registrar software.
- Step 2. The local D-proxy does not have an IP address for Cisco.com, so it sends a query to a root name server. The root name server can respond to the request in two ways. The most common way is to send the D-proxy directly to the authoritative name server for Cisco.com. In the other method, iterated querying (shown in Figure 1), the root name server sends the D-proxy to an intermediate name server that knows the address of the authoritative name server for Cisco.com.
- Step 3. The local D-proxy sends a query to the intermediate name server, which responds, referring the D-proxy to the authoritative name server for Cisco.com.
- Step 4. When the local D-proxy sends a query to the authoritative name server for Cisco.com, the name server responds with the IP addresses of the two Cisco GSS 4492R devices, and tells the D-proxy to ask the Cisco GSS 4492R for the IP address for Cisco.com or www.cisco.com.
- Step 5. The local D-proxy sends its final request directly to one of the two Cisco GSS 4492R devices. The Cisco GSS 4492R is authoritative for the Cisco.com subdomain, so it sends the IP address to the D-proxy. Before this IP address is sent to the D-proxy, the Cisco GSS 4492R applies intelligence to its response. Following are examples of this intelligence, which is not supported by generic DNS servers. The Cisco GSS 4492R does the following:
 - Will not send an IP address to the D-proxy if the device (Website, e-mail, VPN, etc.) is unavailable
 - Will not send an IP address to the D-proxy if the device is overloaded
 - Sends users to the closet data center
 - Intelligently manages client traffic flow to each data center
 - Issues a virtual IP address, not a real IP address of a back-end server
 - Automatically reroutes users to an alternative data center if the primary data center becomes unavailable
 - The Cisco GSS 4492R sends the intelligent IP address of the best server load balancer at a specific data center—in this case, the SLB device at Data Center 1.
- Step 6. The DNS global load balancing process is complete; the client is directed to the SLB device at Data Center 1 by the IP control and forwarding plane.

Universal, Security-Focused Advanced DNS Services

The Cisco GSS 4492R provides a number of advanced services.

Universal Intelligent Business Continuance

If a network outage occurs, the Cisco GSS 4492R can automatically or under administrative control redirect clients to a disaster-recovery site within seconds and at a rate of 10,000 clients per second.

Customers can benefit from the new levels of centralized command and control provided by the Cisco GSS 4492R—whether they are deploying a new Cisco ACE module for Cisco Catalyst 6500 Series Switches or content switches such as the Cisco CSS 11500 Series, devices with Cisco IOS Software SLB, or any device that uses DNS for client access and has performance information available through SNMP.

Global Traffic Management

The Cisco GSS 4492R can be deployed as a standalone global traffic manager that globally load balances client requests across distributed data centers using network performance metrics such as content use, round-trip time (RTT) between client and the closest data center, routing topology, and any device performance values that are available through SNMP.

Complete Security-Focused IP Management

Network administrators can achieve significant server consolidation by using the Cisco GSS 4492R appliance as a complete IP management system. In the latest version of the Cisco GSS 4492R, a network administrator can load Cisco Network Registrar software directly onto the Cisco GSS 4492R appliance. The Cisco GSS 4492R supports the following security-focused DNS features:

- DDoS mitigation software
- Encrypted communication between the Cisco GSS 4492R and the network manager and between Cisco GSS 4492R appliances
- Private DNS code set

Self-Defending DNS Protection

Using acquired technology, Cisco has integrated DNS-focused DDoS protection software into the Cisco GSS 4492R. This software uses a subset of the unique Multi-Verification Process (MVP) architecture found on the Cisco Guard DDoS Mitigation Appliances. This optional software handles only DNS-related attacks and does not have the performance or full feature set of the Cisco Guard DDoS Mitigation Appliances. This software delivers the following DDoS mitigation capabilities:

- Filters
- Rate limitation per D-proxy with learning during normal operation
- Spoofing prevention through cookie insertion

The filter detects the following:

- Rapid DNS queries for the same domain (replay attack and DoS) from a specific source IP
- Broadcast IP addressing as source IP
- Multicast IP addressing as source IP
- Empty IP addressing as source IP
- Cisco GSS 4492R IP addressing as source IP
- Invalid IP range (209.165.202.128 and 209.165.202.159)

- Malformed DNS packets
- Rapid DNS queries for domains not configured on the Cisco GSS 4492R

The unique rate-limiting software establishes the DNS process rate baseline for each DNS server sending requests to the Cisco GSS 4492R during normal operations and profiles these rates. If any DNS server exceeds these normal rates, the Cisco GSS 4492R, according to the rate-limit policy set by the network administrator, will start to rate limit these DNS requests. Therefore, a compromised DNS server will not be allowed to consume all the DNS processing capabilities of the Cisco GSS 4492R.

The Cisco GSS 4492R also can insert a cookie into TCP-based DNS requests, using TCP port 53. This action allows the Cisco GSS 4492R to mark the various DNS servers communicating with the Cisco GSS 4492R. The challenge-response algorithms are based on pseudo-random information. The Cisco GSS 4492R sends a challenge, also known as cookie, to a client that tries to connect with the Cisco GSS 4492R. If the source IP address in the packet header is the IP address that is assigned to the client, the client will receive the challenge and send back a response. However, if the source IP address in the packet is spoofed, the client that generated the original traffic to the zone will not receive the Cisco GSS 4492R response and therefore will not answer with the correct challenge. The Cisco GSS 4492R considers clients as authenticated only when they return the correct challenge.

Global Load-Balancing Algorithms for Complete Site-Selection Control

The Cisco GSS 4492R supports 10 global load-balancing algorithms and gives administrators complete flexibility in selecting the global load-balancing algorithm that meets their needs.

Administrators can choose among the following algorithms:

- **Ordered list:** This user-definable list specifies one or a group of IP addresses (corresponding to a virtual IP address or the IP address of a back-end server) that the Cisco GSS 4492R uses to respond to a DNS request for a specific domain. The Cisco GSS 4492R uses the first address in the list until it becomes unavailable or overloaded; it then moves to the next address in the list. This process is repeated for every subsequent entry in the list.
- **Static algorithm based on client's DNS address:** This algorithm is a variation on the ordered list that allows the administrator to map the IP address of the client's DNS server to an available virtual IP address on a specific content switch. This feature is used when the administrator wants to allocate a specific community of users to a specific set of SLB devices or back-end servers.
- **Round robin:** This algorithm cycles through available virtual IP addresses in order. The round-robin balancing method is useful when balancing requests among multiple, active data centers that are hosting identical content—for example, SLB devices at primary and active-standby sites that serve requests.
- **Weighted Round Robin (WRR):** The Cisco GSS 4492R cycles through the list of available virtual IP addresses as requests are received, but sends requests to a favored virtual IP address based on a user-assigned weighting value.
- **Least loaded:** The Cisco GSS 4492R can receive load values from the Cisco ACE, CSS, or CSM device. The Cisco GSS 4492R monitors these load values to see if they exceed a threshold that is assigned by the administrator. If the load exceeds the specified threshold, the virtual IP on the Cisco ACE, CSS, or CSM device is considered offline and unavailable

to serve requests. If the load falls below the threshold, the Cisco GSS 4492R automatically starts sending requests to the virtual IP address. This capability has been enhanced to support SNMP MIB variables.

- **Geo database:** External geo databases can be loaded onto the Cisco GSS 4492R to allow the Cisco GSS 4492R to send a client request to the closest data center based on the source IP address of the DNS request. This database can scale up to 500,000 entries.

Performance and Scalability

Highly scalable, the Cisco GSS 4492R meets the needs of the most demanding environments. Table 1 lists performance and scalability metrics information for the Cisco GSS 4492R.

Table 1. Cisco 4492R Performance and Scalability Metrics

Feature	Description		
DNS Requests per Second	Up to 30,000		
Name Server Forwarding Requests per Second	1500		
Active SLBs	256		
DNS Rules	4000		
Hosted Domains (maximum 1000 per SLB), 128 Characters Maximum per Domain	2000		
Hosted Domain List (500 per list)	2000		
Virtual IP Addresses	2000 (4000 shared)		
Source IP Addresses Configurable for DNS Rules	500		
Source Address Lists (30 members per list)	60		
Answer Groups (100 members maximum per list)	500		
Keepalive (KAL) Limits	150 fast 500 standard per KAL type		
	KAL type	Fast	Standard
	TCP	150	1500
	HTTP Head	100	500
	ICMP	150	750
	KAP-AP	40	128
Scripted (SNMP)	60	256	

Cisco GSS 4492R Features

Table 2 summarizes the features of the Cisco GSS 4492R.

Table 2. Cisco GSS 4492R Features

Feature	Description
Devices Supported	<ul style="list-style-type: none"> • Cisco ACE module: Load and availability • Cisco CSS switch: Load and availability • Cisco Content Switching Module: Load and availability • Cisco IOS Software SLB: Load and availability • Cisco LocalDirector: Availability using HTTP head or TCP KAL • DNS servers: Availability using name server request KAL • Origin servers: Availability using HTTP head, TCP, and SNMP KAL • Content engines: Availability using Internet Control Message Protocol (ICMP) ping or TCP KAL • Content routing agents (CRAs): Availability using CRA KAL • Third-party SLB devices: Load and availability using SNMP KAL

Feature	Description
Network Management	<ul style="list-style-type: none"> • Console port—CLI • Access to system through Telnet • Secure copy (SCP) or FTP • GUI: Secure HTTP (HTTPS) for Internet Explorer and Netscape Navigator • Network management MIBs • Read-only monitoring of network and device status, including RFC 1213 (MIB-II) and RFC 1514 (HOST-RESOURCES-MIB)

Ordering Information

The Cisco GSS 4492R supports only AC power. Orderable part numbers are listed in Table 3.

Table 3. Ordering Information for Cisco GSS 4492R

Part Number	Description
GSS 4492R-K9	Cisco GSS 4492R Global Site Selector
SF-GSS-V2.0-K9	Cisco Global Site Selector Software 2.0
SF-GSS-DDOSLIC	DDoS Mitigation Software (requires Cisco Global Site Selector Software 2.0)
SF-GSS-DNSLIC	Cisco GSS DNS license (requires Cisco Network Registrar 6.2 software [CNR-6.2-BASE1K] for full DNS capability) and Cisco Global Site Selector Software 2.0

Environmental Specifications

Table 4 lists the specifications of the Cisco GSS 4492R.

Table 4. Cisco GSS 4492R Specifications

Specification	Description
Rack Units	One rack unit
Network Management	Serial port
Ports	Two 10/100/1000 Fast Ethernet autosensing ports and one console port
Storage and Memory	<ul style="list-style-type: none"> • One 80-GB hard drive • Software image SF-GSS-V1.3-K9 • 2 GB RAM; Pentium CPU
Power	Integrated AC power (autosensing 110V/60 Hz)

For More Information

For more information about the Cisco GSS 4400 Series Global Site Selector Appliances, visit <http://www.cisco.com/en/US/products/hw/contnetw/ps4162/index.html> or contact your local Cisco account representative.

For a complete listing of the Cisco Network Registrar capabilities, visit <http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/index.html>.



Americas 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: 408 527-0689

Asia Pacific Headquarters
 Cisco Systems, Inc.
 165 Robinson Road
 #29-01 Capital Tower
 Singapore 068912
www.cisco.com
 Tel: +65 6317 7777
 Fax: +65 6317 7799

Europe Headquarters
 Cisco Systems International B.V.
 Heerlenbergpark
 Heerlenbergweg 13-19
 1101 CH Amsterdam
 The Netherlands
www.europe.cisco.com
 Tel: +31 0 20 620 0791
 Fax: +31 0 20 657 1100

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.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, AirNet, BPK, Catalyst, CCD, CCDA, CCDP, CCIE, CCR, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fax, Step, Follow Me, Grouping, HomeShare, iQ, iQ Drive, HomeLink, Internet Quotient, IOS, iPhone, IPTV, iQ Expertise, the iQ logo, iQ Notepad, iQ Scorecard, iQuickStudy, iSignStream, iInlays, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, SiscoWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered 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. (9705R)