

# Cisco Access Services Solution: Architecture Overview

*Service provider's profitability in the New World will be defined by their ability to rapidly introduce new services tailored to the specific needs of their customers. A flexible, multi-service Operations Support System (OSS) designed and optimized for a New World infrastructure is critical to their ability to deliver on this. Internet OSS is a broad range initiative from Cisco delivering on the New World Operations vision through an open, standards-based reference architecture. New World Operations give Service Providers the opportunity to gain competitive advantages in market share as the world transitions into this new network information structure.*

## Introduction

The first dial-in access to the Internet was available almost three decades ago to researchers and graduate students. At that time, the Internet was a network of primarily university, military, and research computers. There were no personal computers. These users had simple terminal access to various systems through their dial-in connections. From that simple environment, the first access-management systems were developed. These systems evolved and today the same technologies that manage remote access to universities and research organizations provide users with access to the Internet and employees with remote access to corporate networks.

Remote Authentication Dial-In User Service (RADIUS) was developed to address the need for authentication, authorization, and accounting (AAA) of remote-access users. RADIUS supports access to a central database of remote users and their authorized services and provides a means to collect usage and accounting information from the network access servers. Initially used to support analog and digital dial-in, RADIUS is now being used by service providers to provide AAA support for xDigital Subscriber Line (DSL), cable, wireless, and voice over IP (VoIP) services.

Service providers have often used public domain RADIUS server source code as the basis for their AAA services. As business challenges have increased, service providers have been looking for commercial off-the-shelf products that can address their requirements, but also offer the extensibility required to support their custom

requirements. In an environment where technology and services are changing so rapidly, it is no longer viable to maintain proprietary AAA systems.

To meet these needs, Cisco offers Access Registrar, a RADIUS server designed specifically for service providers. An infrastructure component of the Cisco Service Management architecture, Access Registrar offers the extensibility to rapidly support new services and provides the performance and scalability that service providers require.

## RADIUS User Authentication, Authorization and Accounting

RADIUS is addressed by Internet Engineering Task Force (IETF) RFC 2138 (authentication and authorization) and RFC 2139 (accounting). These documents define a protocol between a NAS and a central AAA server (RADIUS server). RADIUS is the AAA protocol preferred and supported by all vendors of network access servers. The network access server (NAS) and the RADIUS server share an authentication secret in order to ensure the integrity of the transactions between them.

When the NAS, which operates as a client of the RADIUS server, receives an incoming connection request, it obtains identification information from the user (name, password) and then issues a standardized authentication request to the RADIUS server. The RADIUS server, upon receiving the identification information and other NAS information, authenticates the user. The RADIUS server can also provide connection setup parameters to the NAS, such as the IP address to be used, filters to limit network access, and session

and idle time-out values. In addition to defining an authentication and authorization protocol, RADIUS defines a protocol for the transmission of usage and accounting information from the Network Access Server (NAS) to the AAA server. This information feeds back-end systems that provide billing, monitoring, and reporting functions.

To support new features which vendors add to their network access servers and other network access equipment, RADIUS allows for the definition of vendor-specific attributes (VSA) in addition to the base set of "dictionary" attributes defined by the Internet Engineering Task Force (IETF). All major vendors have used VSA to support value-added features in their devices and differentiate their products. RADIUS servers are thus required to have extensible dictionaries and be able to provide multivendor support.

Yet, vendor-specific attributes and extensible dictionaries are not sufficient to meet the requirements of today's operational environments. Service providers have pushed AAA requirements to new levels. Not only must RADIUS systems provide multivendor support, but they must also provide the performance and scalability required in these environments, integrate with other elements of a service-management system, and quickly support new service offerings. Service providers that previously developed "home-grown" RADIUS systems now find that they can no longer afford to maintain and scale such systems.

### **Cisco Access Registrar**

Cisco Access Registrar is a RADIUS server designed to meet demanding service provider AAA requirements. Not merely an enhancement or port of public domain RADIUS "freeware" Access Registrar was designed from the ground up to provide scalable performance and an extensible platform that can adapt and scale with ever-changing requirements. Based on a multithreaded architecture, Access Registrar provides numerous extension points allowing additional logic to be added as required and Lightweight Directory Access Protocol (LDAP) capabilities to allow integration with back-end directory systems. Running on a Solaris for SPARC server, Cisco Access Registrar executes hundreds of AAA transactions per second, reducing the number of servers needed to support a service infrastructure.

### **Extension Points**

Cisco Access Registrar extension points support additions to its RADIUS server logic to customize or enhance its out-of-the-box functionality. Extensions can be in the form of C/C++ shared libraries or Tcl scripts. This allows extensions to be quickly prototyped in Tcl and then coded with C or C++ for optimal performance. Extensions can be used to modify server behavior at more than 10 predefined points during packet processing. Specifically, extensions are allowed to modify the incoming or outgoing RADIUS packet or modify Access Registrar environment variables that control packet processing. An extension could be written, for example, to use a custom authentication service for a particular user or user community.

### **Directory Integration**

Directory systems are fast becoming an integration point for service management systems and the overall Operations Support System (OSS). Directories serve as a central repository for user information, service profiles, billing profiles, and other service information. Multimaster, replicated directories provide a means to rapidly distribute and allow access to this information from any location. Whether the directory is X.500, Microsoft's Active Directory, or Novell's NDS, Cisco Access Registrar can access this information using its LDAP capabilities (Figure 1).

Cisco Access Registrar authenticates users against an LDAP directory and provides the flexibility to work with a variety of directory configurations. Access Registrar can be configured to consult a single directory for all user authentication or different directories (or directory branches) for particular communities of users. Access Registrar performs an LDAP lookup to find the user record and verifies the user password as stored in the directory. Access Registrar can also map LDAP user record attributes to RADIUS attributes. Thus, a user's RADIUS profile can be configured in the corresponding LDAP user record, allowing provisioning systems to use LDAP to directly configure users that will be authenticated and authorized by Access Registrar.

### AAA Proxy

The growth of the Internet and the proliferation of service providers have naturally led to consolidation, partnerships, and other arrangements that require integration of AAA systems. For service providers offering corporate remote-access outsourcing, there is also a need to integrate with end-user customer AAA systems. Cisco Access Registrar supports RADIUS proxy where, instead of directly authenticating and authorizing users against a directory, the server selectively proxies the AAA request to another service provider's RADIUS server or a customer RADIUS server that authenticates and authorizes users against another directory or database.

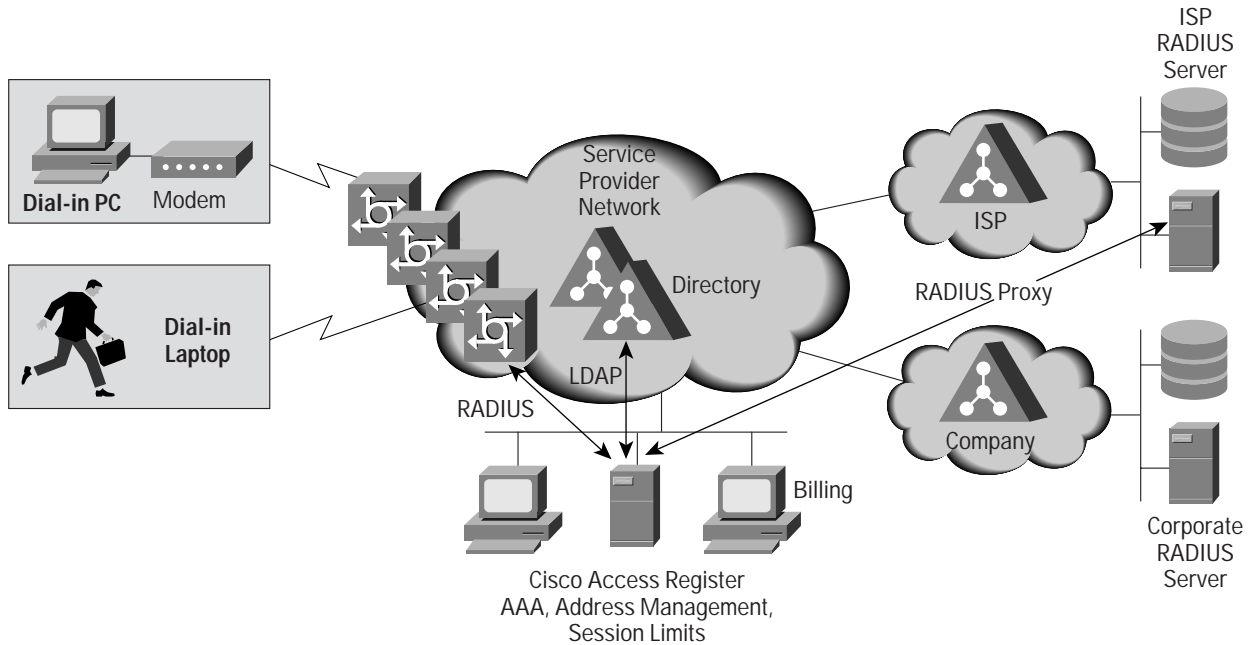
Access Registrar allows the configuration of service filters that instruct the server to proxy RADIUS requests based on the dialed number (DNIS) or realm contained in the request packet (for example, "isp\_a" in "bill@isp\_a.com"). Via extension points, Access Registrar can also proxy based on any other information in the request packet. RADIUS proxy is illustrated in the Applications section of this paper.

### Address and Session Management

RADIUS servers are stateless servers that independently handle incoming requests as they are received. While this is sufficient for rudimentary AAA, the efficient operation and utilization of access networks today require "stateful" tasks such as IP pool management and address allocation and the enforcement of session limits. Previously handled by each NAS, these tasks need to be centralized and managed in a vendor-independent manner. Cisco Access Registrar provides resource managers that handle the dynamic allocation of IP or IPX, addresses and enforces both user and group session limits across multiple network access servers. Here again, Cisco Access Registrar extensions can be used to select or override default IP address pools or session managers.

Cisco Network Services (CNS) Concurrency Control Services provides additional session management scalability where required. CNS Concurrency Control Services is a distributed Solaris application that can manage session limits across multiple Access Registrar servers and remove single points of failure.

Figure 1 Cisco Access Registrar



## Cisco Access Registrar Applications

### Wholesale Dial

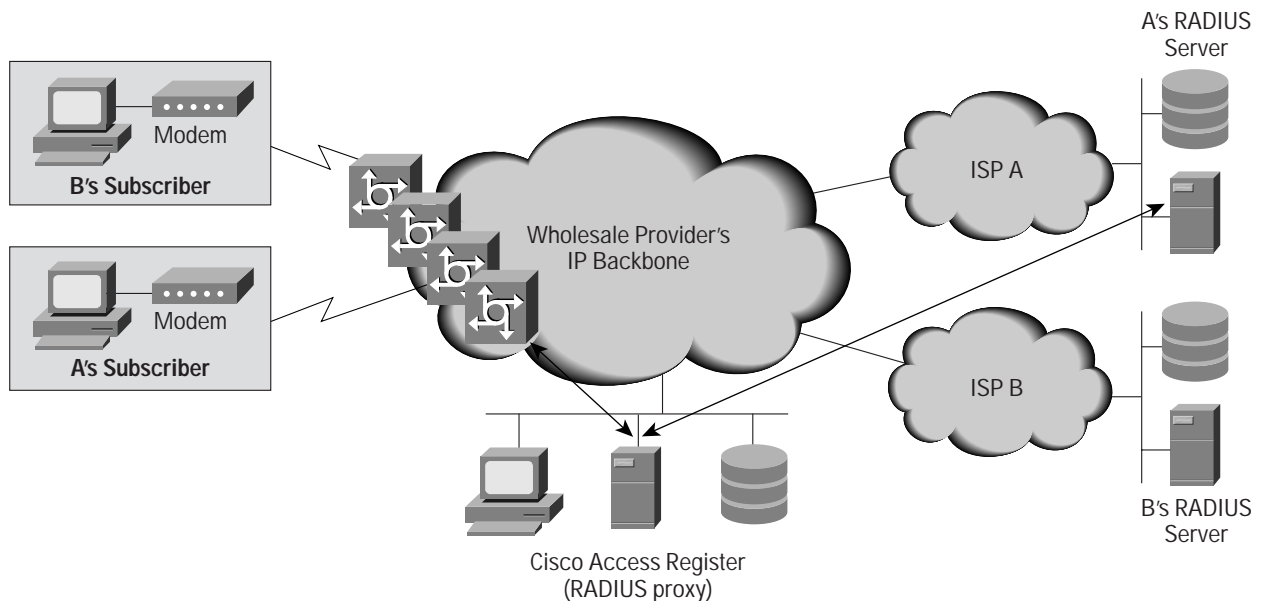
Many Internet service providers (ISPs), application service providers (ASP), and content providers (or “portals”) must provide dial-up Internet access as part of their service package. However, many of these providers do not want to invest the time in building out dial-up access infrastructure, or cannot build out infrastructure fast enough—particularly when expanding into new regions. Other retail companies want to offer “private-label” Internet access as part of their brand, but do not want to build out their own service.

Wholesale dial is a service that offers these providers cost and efficiency savings and improved time to market by having a wholesale service provider manage their dial-up needs. This model allows all organizations involved to focus on their core competencies. The wholesaler focuses on infrastructure and sells port access to service providers. The service providers focus on content and the sales and marketing of their services.

In a wholesaler’s dial infrastructure (Figure 2) Cisco Access Registrar provides the following functions:

1. Receives the RADIUS authentication and authorization request from the NAS
2. Determines the wholesale customer identity (such as ISP A) by the dialed number (DNIS), realm in the user name (such as “bill@isp\_a.com”), or other criteria
3. Proxies the AAA transaction to the RADIUS server specified by the wholesale customer modifying the user name if required (“bill@isp\_a.com” becomes “bill”)
4. Receives the validated authentication and service authorization parameters for the user (or the rejected authentication)
5. Issues IP addresses and checks configured session limits
6. Modifies the response, if necessary, for interoperability with the wholesaler’s access equipment or to enforce service agreements made with the customer
7. Returns the response to the NAS
8. Receives RADIUS accounting records from the NAS and both proxy the records to the customer RADIUS server and maintain a local copy for billing purposes

Figure 2 Wholesale Dial with Cisco Access Registrar



### Outsourced Corporate Dial-In with Virtual Private Networking

Another major business opportunity for service providers is the outsourcing of enterprise dial-in networks. Enterprise network managers are looking to service providers to handle the worldwide operation of dial-in modem and Integrated Services Digital Network (ISDN) banks, and they expect that all of this dial-in traffic will arrive over high-speed links at their major enterprise sites. They want the service provider to provide a highly available, secure virtual private networking (VPN) service, but they want to retain ownership and control of the authentication and authorization database used to identify their employees and other authorized personnel.

Rather than dedicating specific sets of network access servers and modems to a particular enterprise, service providers need to share resources and achieve economies of scale. Similar to the wholesale dial scenario, Cisco Access Registrar examines each incoming access request in real time to determine its community—the enterprise to which it belongs. Via proxy RADIUS, the appropriate AAA server is consulted, and if authentication is successful and session limits are not exceeded, a secure tunnel can be established from the NAS to the destination home gateway.

### Telco Return and Roaming with Cisco Subscriber Registration Center

Data-over-cable services represent new opportunities for the cable industry. To effectively offer services such as data, voice, and video on demand, cable multiple system operators (MSOs) and cable service providers need systems that reduce

administrative costs and accommodate rapid subscriber growth. To address these requirements, Cisco offers Cisco Subscriber Registration Center (CSRC), a suite of products for configuring and managing broadband modems and enabling and administering subscriber self-registration.

Cisco Access Registrar is a component of CSRC, providing RADIUS services to DOCSIS-compliant modems. This enables the deployment of high-speed data services in one-way cable plants requiring telco-return for upstream data. For MSOs and cable service providers wishing to offer access to users roaming outside of their cable service areas, Access Registrar is used to provide AAA support for dial services.

### Conclusion

Service providers require scalable infrastructure components that provide multivendor support and integrate with existing and evolving systems. AAA systems are a key infrastructure component that must enforce access policies across a wide range of access services beyond dial. Cisco is committed to delivering leading-edge management solutions that meet the specialized needs of service providers. Cisco Access Registrar provides a carrier-class AAA platform that enables the rapid deployment and the efficient operation of new service offerings.



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

European Headquarters  
Cisco Systems Europe s.a.r.l.  
Parc Evolic, Batiment L1/L2  
16 Avenue du Quebec  
Villebon, BP 706  
91961 Courtaboeuf Cedex  
France  
<http://www-europe.cisco.com>  
Tel: 33 1 69 18 61 00  
Fax: 33 1 69 28 83 26

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

Asia Headquarters  
Nihon Cisco Systems K.K.  
Fuji Building, 9th Floor  
3-2-3 Marunouchi  
Chiyoda-ku, Tokyo 100  
Japan  
<http://www.cisco.com>  
Tel: 81 3 5219 6250  
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

**Cisco Connection Online Web site at <http://www.cisco.com/offices>.**

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE  
Finland • France • Germany • Greece • Hong Kong • 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 • Singapore  
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela