



Cisco CDMA2000 Packet Data Solution

The Internet has changed the way individuals access information, make decisions, and transact business. The mobile wireless industry is changing how people access the Internet. Mobility brings new opportunities such as location-based services, allowing applications to interact and provide services based on location. Internet services such as messaging, email, and Web access, enable mobile operators to grow their installed customer base and revenue. As mobile wireless networks and the Internet connect in new and exciting ways, the opportunities for mobile operators to increase revenue, service offerings, and customer satisfaction grow as well.

As the mobile market evolves, the technology must also change to enable the data-transfer rates that will make mobile Internet access both attractive and useful. To make high-speed data access possible, international standards bodies are developing several new standards that provide the reliability, speed, and security required to offer mobile data services.

This paper describes the Cisco® CDMA2000 Packet Data Services solution, which enables mobile operators to deliver packet data services in a code-division multiple access (CDMA) environment. The Cisco CDMA2000 Packet Data Services solution includes the Cisco Packet Data Serving Node (PDSN); Cisco Packet Data Serving Node (PDSN) with foreign agent functionality; the Cisco mobile wireless home agent; an authentication, authorization, and accounting (AAA) server (the Cisco CNS Access Registrar®); and several security products and features.

A Cisco PDSN provides access to the Internet, intranets, and Wireless Application Protocol (WAP) servers for mobile stations that use a CDMA2000 radio access network (RAN). CDMA is one of three key mobile communication technologies, the other two being time-division multiple access (TDMA) IS-136 and the Global System for Mobile Communications (GSM). CDMA2000 is the name for the third-generation (3G) CDMA technology that offers packet data. The largest CDMA technology networks are found in Korea, Taiwan, Japan, Malaysia, and North America.

The Cisco PDSN acts as an access gateway and provides simple IP and mobile IP access, foreign agent functionality, and packet transport for virtual private networks (VPNs). It acts as a client for the AAA servers, and also allows operators to enable prepaid billing services. Additionally, standalone Cisco PDSNs can be logically tied together under a clustering architecture to provide further benefits in terms of scalability, redundancy, load sharing, and more.

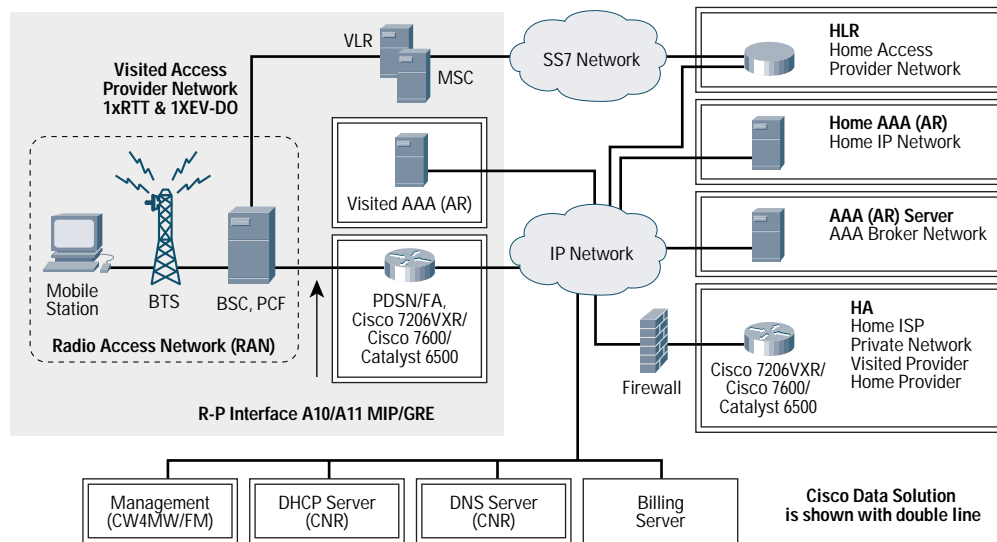
The home agent acts as an anchor point for mobile devices with mobile IP or proxy Mobile IP services. Working with Cisco PDSN's foreign agent functionality (PDSN/FA), the home agent allows mobile clients with Mobile IP services to reach the Internet or corporate intranets by extending the coverage area of the existing PDSN/FA. Traffic is routed through the home agent, and the home agent also provides proxy Address Resolution Protocol (ARP) services. When reverse tunneling is used, traffic from the terminal is also routed from the mobile and back through to the home agent.

A Cisco PDSN network is similar to a traditional routed network. Mobile stations, which can be personal computers with wireless adapters, personal digital assistants (PDAs), or mobile handsets, are IP hosts. Like a default router in a traditional routing environment, the Cisco PDSN provides the gateway to the IP network for the mobile stations. What makes this different from a traditional routed network is mobility. Because the host in this case can move around, there must be a means to find the host so packets can be forwarded to it. The Cisco CDMA2000 Packet Data Services solution offers a secure means to provide packet data services to mobile stations.

Architectural Overview

Figure 1 illustrates the components of a CDMA2000 network. The mobile station, which must support either simple IP or mobile IP, connects to a radio tower and base transceiver station (BTS) that connects to a base station controller (BSC). The BSC communicates to the Cisco PDSN through a component called a packet control function (PCF), over a Generic Routing Encapsulation (GRE) tunnel. The PCF and Cisco PDSN communicate with each other using a standard interface known as the RAN-to-PDSN interface, which has two components: the A11 interface, used for control messages, and the A10 interface, used for user data.

Figure 1
CDMA2000 Network Topology



How It Works

When a mobile station first makes a data service call, it establishes a Point-to-Point Protocol (PPP) session with the Cisco PDSN. The Cisco PDSN may authenticate the mobile station by communicating with the AAA server in the visited IP network, which in turn may communicate to the AAA server in the home IP network (possibly through a AAA server in a broker network). The AAA server verifies that the user is a valid subscriber, determines what services are available for the user, and tracks usage for billing. In the absence of Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) authentication, the Cisco PDSN solution also supports mobile station identifier (MSID) based no-authentication access. When the mobile station is authenticated, it may use the IP Control Protocol (ICP) to request an IP address. For simple IP routing, the mobile station is assigned an IP address by the local Cisco PDSN. For simple IP virtual private dialup networks, the mobile station may get its address from its home AAA server. And, for mobile IP, the home agent assigns the IP address for the mobile node during the mobile IP

registration process. [Mobile node is the term used in the mobile IP standards to refer to an IP host that supports mobile IP. Mobile station is the terminology used in the PDSN standards. It is more generic and may include an IP host that supports only simple IP or multiple IP hosts sharing a common mobile access point. This document uses the term mobile node only when referring to a device that supports mobile IP.]

A mobile node registers with a home agent when it determines that it is no longer in its home network. This is necessary to receive datagrams because they would not otherwise be directed to the host at its current location. The mobile node communicates to the home agent through the Cisco PDSN, acting as a foreign agent. This communication uses either IP-in-IP encapsulation (RFC 2003) or GRE (RFC 1701).

When not in its home network, the mobile node will be associated with a care-of address (CoA) (typically the address of the foreign agent). This address identifies the mobile node while the user visits other locations. As part of the registration process, the home agent puts a mobility binding into its binding table. This mobility binding associates the home address of a mobile node with its CoA.

When the mobile node is authenticated, it can then communicate to any authorized IP device and through any authorized IP network.

If the operator is offering VPN services, the mobile station can securely access private resources through a public Internet or dedicated links. The VPN tunnel extends from the Cisco PDSN to the home IP network (the IP network associated with the network address identifier; for example, the home IP network of xxx@ispxyz.com would be "ispxyz").

So far, this is fairly straightforward IP networking applied to the mobile node. When the mobile station becomes mobile and starts to change its physical location, the scenario becomes more complicated. The mobile station can move to a different BTS or BSC. Because the PPP session exists between the Cisco PDSN and the mobile station, as shown in Figures 2 and 3, the Cisco PDSN maintains the PPP session while the mobile station is handed off between BTSs or BSCs. If, however, the mobile station moves beyond the area of the Cisco PDSN, then the session is handed off to a new PDSN and the PPP session is renegotiated. If the mobile station supports mobile IP, the home agent maintains the IP address of the mobile station and its communication with any IP devices. If the mobile station supports only simple IP, it may be assigned a new IP address, and any application-level connections it has may be broken. This disruption can be avoided by using the Cisco proxy mobile IP. The Cisco intelligent PDSN selection may also prevent a disruption. Both of these features are described later in this white paper.

Figure 2
Protocol Reference Model for Simple IP

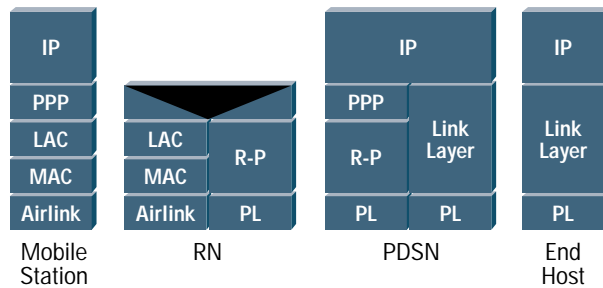
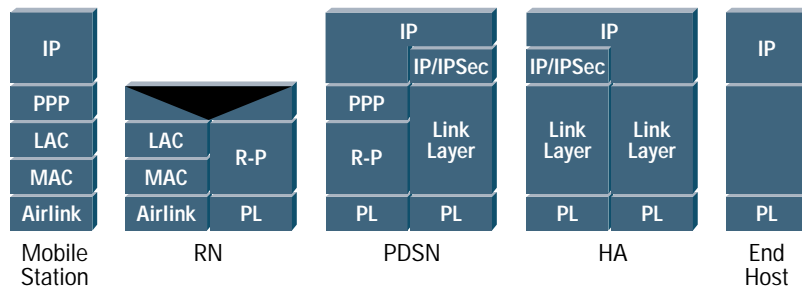


Figure 3
Protocol Reference Model for Mobile IP User Data



Cisco PDSN/Home Agent Solution Feature Highlights

Providing mobile access to the Internet does not ensure success for mobile operators. The profitable companies will be those operators that offer the best services, the best customer experience, and the highest availability at the lowest cost. The Cisco PDSN solution is a cost-effective solution that is standards-compliant and offers many features to improve availability and scalability, tighten security, and enhances the customer experience.

PDSN/Home Agent Features and Standards Compliance

The Cisco PDSN solution supports all required standards, including the 3GPP2 TSG-P standard and Wireless IP Network Standard (also known as TIA/EIA/IS-835), which defines the overall structure of a CDMA2000 network. It includes features such as enhanced mobile IP, carrier-class accounting, compression, security, and authentication. Cisco also supports 3GPP2 TSG-A, Interoperability Specification (IOS[®]) for CDMA2000 Access Network Interfaces, also known as TIA/EIA/IS-2001. The 3GPP2 TSG-A standard focuses on the radio side and the interfaces between radio components and the Cisco PDSN. Cisco supports IOS Version 4.2 in Release 1.2 of the Cisco PDSN.

Cisco Home Agent

The Cisco Home Agent maintains mobile user registrations and tunnels packets destined for the mobile client to the Cisco PDSN with the home agent function (PDSN/HA). It supports reverse tunneling, and can securely tunnel packets to the Cisco PDSN using IP Security (IPSec). Broadcast packets are not tunneled. The home agent can also perform dynamic home address assignment for the mobile from address pools configured locally, through Dynamic Host Configuration Protocol (DHCP), or from the AAA server. The Cisco Home Agent supports Wireless IP Network Standard (TIA/EIA/IS-835-B) and the wireless IP network architecture based on Internet Engineering Task Force (IETF) Protocols (TIA/EIA/TSB-115).

Dynamic Home Agent Assignment

The Cisco Home Agent can be dynamically assigned by the Cisco CNS Access Registrar server for load-balancing purposes by distributing mobile clients among a pool of home agents. At the same time, the Cisco CNS Access Registrar server ensures that the same home agent is always assigned to the same Mobile IP client for the same session. The selection procedure is performed by the Cisco CNS Access Registrar server and can use either a round robin or a hashing algorithm over user network access identifier (NAI) selection criteria.

Home Agent Redundancy

Home agent redundancy takes advantage of the Cisco Hot Standby Router Protocol (HSRP) and allows for two or more home agents to back up each other in the event of a failure. The active home agent sends binding updates to the backup home agent every time a new registration is entered into the binding table, a scenario that keeps the binding tables synchronized. If a new home agent boots up on the LAN, it can have the entire binding table loaded into its memory so that it can be ready in case of any network failure.

Proxy Mobile IP

The latest chipsets used in mobile devices are starting to provide a mobile IP client stack. This is a requirement for mobile IP, but is currently still not supported in a lot of end systems today. To enhance the customer experience, the Cisco PDSN Packet Data Services solution supports proxy mobile IP, which enables non-mobile IP clients to maintain IP connectivity while changing Cisco PDSNs. The IP address of the end system does not change, so any application sessions it has that are dependent on that IP address remain active.

When a simple IP mobile station makes a data services call, the Cisco PDSN prompts it for a NAI and password. If the user is authenticated and authorized (through AAA) for proxy mobile node service, the Cisco PDSN/FA will initiate a proxy mobile registration to a home agent on behalf of the mobile station. The home agent authenticates the registration and assigns the mobile station an IP address, which it returns to the PDSN/FA. The mobile station receives the IP address during the IPCP phase of PPP session establishment. When the mobile station moves to another Cisco PDSN, the PPP session is renegotiated. Using this capability, end systems that do not support mobile IP will have the same benefits as end systems with mobile IP. The mobile stations maintain the same IP address regardless of where they attach to the network, and they do not lose application connectivity if they move. Thus, they can take advantage of Layer 3 VPN services with corporate networks. The only restrictions are that the mobile station must use CHAP, and the mobile station can have only one single IP flow per PPP session.

Mobile IP Flows

The Cisco PDSN Packet Data Services solution enables multiple IP access points from the same mobile station, as long as each IP flow registers individually (each IP flow requires a unique NAI). Each IP flow is assigned a unique IP address. This can be used, for example, when multiple IP hosts share the same device to communicate through the mobile network.

PDSN Clustering

The Cisco PDSN clustering feature brings added value in domains such as availability, performance, scalability, load balancing, intelligent selection, and hand-off. It also enables additional Cisco PDSNs to be added non-disruptively to an existing network, and spreads the load intelligently across all the Cisco PDSNs. Cisco PDSN clustering includes configuring of numbers of Cisco PDSNs into groups that exchange session information about existing PPP sessions and workload. PDSN R1.2 uses a controller-member clustering architecture to provide reliability and capacity. The functions and benefits of controller-member clustering architecture include the following:

- Controller maintains load and session information for each member within the cluster and performs member selection and load balancing. A controller keeps track of the operational state of each member and detects member failure.
- Two controllers are grouped together within one HSRP group in order to provide redundancy and availability.
- Member is responsible for notifying the active controller about its load and session information and to provide Cisco PDSN control and bearer plane functionality.
- The initial A11 registration request for a given session is sent from the PCF to the active cluster controller (in fact the IP address of the HSRP group to which belongs the controllers). Based on its members' load table and existing call registered by the same user, the active controller chooses a member in its list.

- The cluster controller then sends back to the PCF a registration reject with reject code cause set to 0x88 (136decimal) and the IP address of the selected member in the cluster. The PCF will then send a new registration request for that session to the indicated cluster member. This approach assures optimal performance, and provides a scalable approach to growing the network. As demand increases, additional Cisco PDSNs can be added to a cluster without disrupting service, and ensuring that the load is distributed evenly across all Cisco PDSNs.

The Cisco PDSN/Home Agent Hardware Platform

The Cisco PDSN solution is supported on three platforms. The first is the Cisco 7206VXR Router with an NPE-400 Network Processing Engine. It requires a special software feature set (based on Cisco IOS Software Release 12.2.8BY) for Cisco PDSN Release 1.2 (http://www.cisco.com/warp/public/cc/general/bulletin/software/ios122/1862_pp.pdf). Hardware assistance for IPsec requires the use of the Integrated Service Adapter (ISA) card for scalable encryption acceleration. Fast Ethernet and Gigabit Ethernet on the Cisco 7206VXR are supported for the Cisco PDSN. For more information about the Cisco 7200VXR product, refer to the specifications at: <http://www.cisco.com/warp/public/cc/pd/rt/7200/index.shtml>.

The Cisco PDSN/HA is also supported on the Multiprocessor WAN Application Module (MWAM) for both the Cisco Catalyst® 6500 Series and the Cisco 7600 Series platforms. Each module runs five separate instances of either the Cisco PDSN or Home Agent as virtual routers and benefits from the embedded virtual LAN (VLAN) architecture inherent to both the Cisco Catalyst 6500 Series and Cisco 7600 Series platforms. Hardware assistance for IPsec operations requires the use of the IPsec VPN Services Module and requires one available slot on the chassis.

The Cisco PDSN and the Cisco Mobile Wireless Home Agent supports the full set of Cisco IOS Software features. It also has additional software that supports CDMA2000 packet data services and mobility. CDMA-specific software features are listed in the next section. For more information about the Cisco IOS Software feature set, go to: <http://www.cisco.com/warp/public/cc/pd/iosw/index.shtml>.

Mobile IP

Mobile IP enables a host to be identified by a single IP address, even while the device physically moves its point of attachment from one network to another, and allows data packets to be transparently forwarded to that single address. This IETF-proposed standard maintains sessions, regardless of movement between locations on different networks, because there are no address changes. Movement from one point of attachment to another is seamlessly achieved without the intervention or the knowledge of the user. Therefore, mobile IP provides ubiquitous connectivity for users whether they are within their enterprise networks or away from home.

The Cisco IOS Software implementation of Mobile IP has enhancements to ensure scalability, resiliency, and security. Cisco IOS platforms can function as home agents or foreign agents. Because it is possible for large numbers of devices to be mobile, the number of keys needed to perform the authentication function could become very large. For this reason, Cisco IOS Software allows for the mobility keys to be stored on an AAA server that can be accessed through either Terminal Access Controller Access Control System (TACACS+), or Remote Authentication Dial-In User Service (RADIUS). This allows for scalability to large numbers of potential mobile users, and provides a single place for maintenance.

For security, Cisco IOS Software can use registration filters to restrict who is allowed to register. This mechanism can be used on both the foreign agents and the home agent to prevent certain mobile nodes from registering, and to prevent registration through some mobility agents. This also provides the ability to restrict usage only to areas where administrators have trust relationships in place. The Cisco Home Agent feature offers additional built-in redundancy. Because the home agent specification has no “keep-alive” mechanism between the home agent and registered mobile nodes, the failure of a home agent could interrupt data flow to the mobile node. If a home agent fails, the mobile node has no way of knowing if there is simply no traffic destined for it, if the home agent has failed, or if the binding table is lost. This situation is avoided with the implementation of home agent redundancy.

Virtual Private Networks

VPNs deliver enterprise-scale connectivity deployed on a shared infrastructure with the same policies enjoyed in a private network. They are attractive to corporate customers and may be one of the most used applications for mobile data. The Cisco PDSN solution enables companies to offer VPNs to their corporate customers, while taking advantage of the Cisco IOS VPN features to enable world-class security, scalability, quality of service (QoS), and manageability.

VPN Security

Many robust security measures, such as encrypted data, restricted access to authorized users, user tracking after users are connected to the network, and real-time intrusion auditing are available from Cisco Systems® to keep information confidential.

VPN Scalability

The Cisco IOS Software feature and technology, Multiprotocol Label Switching (MPLS) fuses the intelligence of routing with the performance of switching to scale existing networks to meet future growth demands. With this technology, networks can handle more traffic, users, media-rich data, and bandwidth-intensive applications. In intranet and extranet VPNs based on MPLS, packets are forwarded using a unique route distinguisher. Route distinguishers are unknown to end users and uniquely assigned automatically when the VPN is provisioned. MPLS packets are forwarded using labels attached in front of the IP header. Because the MPLS network does not read IP addresses in the packet header, it allows the same IP address space to be shared among different customers, simplifying IP address management. Service providers can deliver fully managed MPLS-based VPNs with the same level of security that users are accustomed to in Frame Relay and ATM services, without the complex provisioning associated with manually establishing permanent virtual circuits (PVCs) and performing per-VPN customer premises equipment (CPE) router design.

VPN Quality of Service

Cisco offers a range of solutions that provide greater granularity to individual applications for priority and bandwidth management so that providers can easily deliver incremental services. QoS affords an enormous opportunity to service providers to provision varying service levels (such as first class, business class, and economy class) and subsequently create differentiated pricing models. It is an essential ingredient of a VPN because it determines the ability of the network to assign resources to mission-critical or delay-sensitive applications. QoS mechanisms ensure that mission-critical applications receive priority over other traffic.

QoS is an essential ingredient in intranet and extranet VPN services that support exciting services such as packet telephony, e-commerce, IP-based video, and other multimedia offerings. Cisco offers a comprehensive set of QoS capabilities that enable providers to prioritize service classes, allocate bandwidth, and avoid congestion. It offers both link Layer 2 and Layer 3 QoS mechanisms. One of the best examples is committed access rate (CAR), which classifies packets by application and protocol, and specifies bandwidth allocation. Weighted fair queuing (WFQ), and class-based queuing techniques implement efficient bandwidth usage by always delivering mission-critical application traffic and deferring noncritical application traffic when necessary. Weighted random early detection (WRED) provides congestion avoidance to slow transmission rates before congestion occurs and ensures predictable service for mission-critical applications that require specific delivery guarantees. Cisco also provides a robust set of Layer 3 traffic engineering tools that let service providers map traffic through specific routes. This lets them simply engineer backbone networks to deliver the total subscribed capacity to all intranet and extranet VPN customers more efficiently.

VPN Manageability

As service providers build VPNs that include WAN switches, routers, firewalls, and Cisco IOS Software, they need to seamlessly manage these devices across the network infrastructure and provide service-level agreements to their customers. They also need to enable business customers to personalize their access to network services and applications. The Cisco Internet OSS framework addresses these needs with a suite of service management solutions to enable service providers to effectively plan, provision, operate, and bill VPN service and provides an integrated set of products for service planning, provisioning, operations, and accounting and billing.

Cisco Access Registrar

Cisco CNS 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,” Cisco CNS Access Registrar was designed to provide scalable performance and an extensible platform that can adapt and scale with ever-changing requirements. Based on a multithreaded architecture, Cisco CNS Access Registrar provides numerous extension points that allow 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, the Cisco CNS Access Registrar executes hundreds of AAA transactions per second, reducing the number of servers needed to support a service infrastructure.

Extension Points

Cisco CNS 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 or C++ shared libraries or tool command language (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 Cisco CNS Access Registrar environment variables that control packet processing. An extension can 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. Multi-master, 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 CNS Access Registrar can access this information using its LDAP capabilities.

Cisco CNS Access Registrar authenticates users against an LDAP directory and provides the flexibility to work with a variety of directory configurations. Cisco CNS 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. Cisco CNS Access Registrar performs an LDAP lookup to find the user record, and verifies the user password as stored in the directory. Cisco CNS 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 Cisco CNS 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 CNS 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 to a customer RADIUS server that authenticates and authorizes users against another directory or database.

Cisco CNS Access Registrar allows the configuration of service filters that instruct the server to proxy RADIUS requests based on the dialed number identification string (DNIS) or realm contained in the request packet (for example, “isp_a” in “bill@isp_a.com”). Through extension points, Cisco CNS Access Registrar can also proxy based on any other information in the request packet.

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 network access server (NAS),

these tasks need to be centralized and managed in a vendor-independent manner. Cisco CNS Access Registrar provides resource managers that handle the dynamic allocation of IP or international packet exchange (IPX), addresses and enforces both user and group session limits across multiple network access servers. Here again, Cisco CNS Access Registrar extensions can be used to select or override default IP address pools or session managers. Cisco CNS Concurrency Control Services provides additional session management scalability where required. Cisco CNS Concurrency Control Services is a distributed Solaris application that can manage session limits across multiple Cisco CNS Access Registrar servers and remove single points of failure.

Prepaid

The Cisco PDSN allows mobile operators to provide prepaid data services by taking full advantage of their existing architecture and AAA server as a mediation device for the billing server. After the user is identified as a prepaid user, quota information is retrieved from the billing server, and allows the Cisco PDSN to do real-time metering on different criteria.

Conclusion

The Cisco CDMA Packet Data Services solution meets the needs of the mobile wireless industry as it drives toward new third-generation cellular (3G) data services and solutions. It is standards compliant, yet offers additional features to address the most critical needs of the mobile wireless operators. Cisco Systems brings a wealth of data experience into the mobile wireless arena—along with some of the first mobile IP solutions and leading security solutions. And Cisco brings openness into an industry previously governed by vendor-proprietary solutions. Cisco also offers a cost-effective means to increase revenue today while building an infrastructure and migration road map to provide the best 3G services in the future.

References

Cisco Access Registrar: <http://www.cisco.com/en/US/products/sw/netmgts/ps411/index.html>

VPNs: <http://www.cisco.com/warp/public/779/servpro/services/vpn>

Mobile IP: http://www.cisco.com/warp/public/cc/pd/iosw/iore/iomjre12/prodlit/817_pb.htm

Cisco 7200VXR Series: <http://www.cisco.com/warp/public/cc/pd/rt/7200/index.shtml>

Cisco Catalyst 6500 Series: <http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/>

Cisco 7600 Series: <http://www.cisco.com/en/US/products/hw/routers/ps368/index.html>

Cisco IOS Software Features: <http://www.cisco.com/warp/public/cc/pd/iosw/index.shtml>

For More Information

For more information about Cisco mobile wireless products and solutions, go to <http://www.cisco.com/go/mobile>.

CISCO SYSTEMS



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 Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 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 Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
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