CDMA2000 Wireless Data Services

The ASR 5500 provides wireless carriers with a flexible solution that functions as a Packet Data Support Node (PDSN) in CDMA 2000 wireless data networks.

This overview provides general information about the PDSN including:

Product Description

The system provides wireless carriers with a flexible solution that can support both Simple IP and Mobile IP applications (independently or simultaneously) within a single scalable platform.

When supporting Simple IP data applications, the system is configured to perform the role of a Packet Data Serving Node (PDSN) within the carrier's 3G CDMA2000 data network. The PDSN terminates the mobile subscriber's Point-to-Point Protocol (PPP) session and then routes data to and from the Packet Data Network (PDN) on behalf of the subscriber. The PDN could consist of Wireless Application Protocol (WAP) servers or it could be the Internet.

When supporting Mobile IP and/or Proxy Mobile IP data applications, the system can be configured to perform the role of the PDSN/Foreign Agent (FA) and/or the Home Agent (HA) within the carrier's 3G CDMA2000 data network. When functioning as an HA, the system can either be located within the carrier's 3G network or in an external enterprise or ISP network. Regardless, the PDSN/FA terminates the mobile subscriber's PPP session, and then routes data to and from the appropriate HA on behalf of the subscriber.

Qualified Platforms

PDSN is a StarOS application that runs on Cisco ASR 5500 and virtualized platforms. For additional platform information, refer to the appropriate System Administration Guide and/or contact your Cisco account representative.

Features and Functionality—Base Software

This section describes the features and functions supported by default in base software on PDSN service and do not require any additional licenses.

Important To configure the basic service and functionality on the system for PDSN service, refer to the configuration examples provided in the PDSN Administration Guide.

This section describes following features:

Gx and Gy Support

The PDSN supports 3GPP Release 8 standards based policy interface with the Policy and Charging Rules Function (PCRF). The policy interface is based on a subset 3GPP 29.212. based Gx interface specification. The PDSN policy interface fully supports installation/modification of dynamic and predefined rules from the PCRF.

The enforcement of dynamic and predefined PCC rules installed from the PCRF is done using Enhanced Charging Services (ECS).The full ECS functionality including the DPI and P2P detection can be enabled via predefined rules using the Gx interface.

The PDSN supports a subset of event triggers as defined in 29.212. Currently the event trigger support is limited to the following:

- RAT Change
- User location change (BSID)

- AN GW change (during inter PCF handoff)

The PDSN also supports triggering of online charging via the policy interface. 3GPP Release 8 Gy interface as defined in 32.299 is used for online charging.

The PDSN supports connectivity to multiple PCRF's. The PCRF's may be referred to by an FQDN. Load balancing of sessions across multiple servers are achieved by using a round robin algorithm. Redundancy between servers can be achieved by configuring multiple weighted sets of servers.

The configuration allows Policy support to be enabled on a per subscriber/APN basis.

The policy features supported on PDSN and GGSN will be quite similar. On PDSN the Gx will only be supported for Simple IP calls.

On PDSN additional event triggers rat type change and location change will be supported.On PDSN Gy , standard DCCA based credit control is supported 3GPP related trigger functionality is not supported on PDSN Gy.

RADIUS Support

Provides a mechanism for performing authorization, authentication, and accounting (AAA) for subscriber PDP contexts based on the following standards:

- RFC-2618, RADIUS Authentication Client MIB, June 1999
- RFC-2620, RADIUS Accounting Client MIB, June 1999
- RFC-2865, Remote Authentication Dial In User Service (RADIUS), June 2000
- RFC-2866, RADIUS Accounting, June 2000
- RFC-2867, RADIUS Accounting Modifications for Tunnel Protocol Support, June 2000
- RFC-2868, RADIUS Attributes for Tunnel Protocol Support, June 2000
- RFC-2869, RADIUS Extensions, June 2000

Description

The Remote Authentication Dial-In User Service (RADIUS) protocol is used to provide AAA functionality for subscriber PDP contexts.

Within context contexts configured on the system, there are AAA and RADIUS protocol-specific parameters that can be configured. The RADIUS protocol-specific parameters are further differentiated between RADIUS Authentication server RADIUS Accounting server interaction.

Among the RADIUS parameters that can be configured are:

- **Priority**: Dictates the order in which the servers are used allowing for multiple servers to be configured in a single context.
- **Routing Algorithm**: Dictate the method for selecting among configured servers. The specified algorithm dictates how the system distributes AAA messages across the configured AAA servers for new sessions. Once a session is established and an AAA server has been selected, all subsequent AAA messages for the session will be delivered to the same server.

In the event that a single server becomes unreachable, the system attempts to communicate with the other servers that are configured. The system also provides configurable parameters that specify how it should behave should all of the RADIUS AAA servers become unreachable.

The system provides an additional level of flexibility by supporting the configuration RADIUS server groups. This functionality allows operators to differentiate AAA services based on the subscriber template used to facilitate their PDP context.

In general, 128 AAA Server IP address/port per context can be configured on the system and it selects servers from this list depending on the server selection algorithm (round robin, first server). Instead of having a single list of servers per context, this feature provides the ability to configure multiple server groups. Each server group, in turn, consists of a list of servers.

This feature works in following way:

- All RADIUS authentication/accounting servers configured at the context-level are treated as part of a server group named "default". This default server group is available to all subscribers in that context through the realm (domain) without any configuration.
- It provides a facility to create "user defined" RADIUS server groups, as many as 399 (excluding "default" server group), within a context. Any of the user defined RADIUS server groups are available for assignment to a subscriber through the subscriber configuration within that context.

Since the configuration of the subscriber can specify the RADIUS server group to use as well as IP address pools from which to assign addresses, the system implements a mechanism to support some in-band RADIUS server implementations (i.e. RADIUS servers which are located in the corporate network, and not in the operator's network) where the NAS-IP address is part of the subscriber pool. In these scenarios, the PDSN supports the configuration of the first IP address of the subscriber pool for use as the RADIUS NAS-IP address.

Important In 12.3 and earlier releases, refer to the *AAA and GTPP Interface Administration and Reference* for more information on RADIUS AAA configuration. In 14.0 and later releases, refer to the *AAA Interface Administration and Reference*.

Access Control List Support

Access Control Lists provide a mechanism for controlling (i.e permitting, denying, redirecting, etc.) packets in and out of the system.

IP access lists, or Access Control Lists (ACLs) as they are commonly referred to, are used to control the flow of packets into and out of the system. They are configured on a per-context basis and consist of "rules" (ACL rules) or filters that control the action taken on packets that match the filter criteria. Once configured, an ACL can be applied to any of the following:

- An individual interface
- All traffic facilitated by a context (known as a policy ACL)
- An individual subscriber
- All subscriber sessions facilitated by a specific context

There are two primary components of an ACL:

- Rule: A single ACL consists of one or more ACL rules. As discussed earlier, the rule is a filter configured to take a specific action on packets matching specific criteria. Up to 128 rules can be configured per ACL.

  Each rule specifies the action to take when a packet matches the specifies criteria. This section discusses the rule actions and criteria supported by the system.

- Rule Order: A single ACL can consist of multiple rules. Each packet is compared against each of the ACL rules, in the order in which they were entered, until a match is found. Once a match is identified, all subsequent rules are ignored.

Important For more information on Access Control List configuration, refer to the IP Access Control List chapter in System Administration Guide.

IP Policy Forwarding

IP Policy Forwarding enables the routing of subscriber data traffic to specific destinations based on configuration. This functionality can be implemented in support of enterprise-specific applications (i.e. routing traffic to specific enterprise domains) or for routing traffic to back-end servers for additional processing.

Description

The system can be configured to automatically forward data packets to a predetermined network destination. This can be done in one of three ways:

- **IP Pool-based Next Hop Forwarding** - Forwards data packets based on the IP pool from which a subscriber obtains an IP address.
- **ACL-based Policy Forwarding** - Forwards data packets based on policies defined in Access Control Lists (ACLs) and applied to contexts or interfaces.
- **Subscriber specific Next Hop Forwarding** - Forwards all packets for a specific subscriber.

The simplest way to forward subscriber data is to use IP Pool-based Next Hop Forwarding. An IP pool is configured with the address of a next hop gateway and data packets from all subscribers using the IP pool are forward to that gateway.

Subscriber Next Hop forwarding is also very simple. In the subscriber configuration a nexthop forwarding address is specified and all data packets for that subscriber are forwarded to the specified nexthop destination.

ACL-based Policy Forwarding gives you more control on redirecting data packets. By configuring an Access Control List (ACL) you can forward data packets from a context or an interface by different criteria, such as source or destination IP address, ICMP type, or TCP/UDP port numbers.

ACLs are applied first. If ACL-based Policy Forwarding and Pool-based Next Hop Forwarding or Subscriber are configured, data packets are first redirected as defined in the ACL, then all remaining data packets are redirected to the next hop gateway defined by the IP pool or subscriber profile.

Important For more information on IP Policy Forwarding configuration, refer to the Policy Forwarding chapter.

AAA Server Groups

Value-added feature to enable VPN service provisioning for enterprise or MVNO customers. Enables each corporate customer to maintain its own AAA servers with its own unique configurable parameters and custom dictionaries.

Description

This feature provides support for up to 800 AAA (RADIUS and Diameter) server groups and 800 NAS IP addresses that can be provisioned within a single context or across the entire chassis. A total of 128 servers can be assigned to an individual server group. Up to 1,600 accounting, authentication and/or mediation servers are supported per chassis and may be distributed across a maximum of 1,000 subscribers. This feature also enables the AAA servers to be distributed across multiple subscribers within the same context.

Important Due to additional memory requirements, this service can only be used with 8GB Packet Accelerator Cards (PACs) or Packet Service Cards (PSCs)

Important For more information on AAA Server Group configuration, refer to the *AAA Interface Administration and Reference*.

Overlapping IP Address Pool Support

Overlapping IP Address Pools provides a mechanism for allowing operators to more flexibly support multiple corporate VPN customers with the same private IP address space without the expensive investments in physically separate routers, or expensive configurations using virtual routers.

Important For more information on IP pool overlapping configuration, refer to the VLANs chapter in the *System Administration Guide*.

Routing Protocol Support

The system's support for various routing protocols and routing mechanism provides an efficient mechanism for ensuring the delivery of subscriber data packets.

Description

The following routing mechanisms and protocols are supported by the system:

- **Static Routes:** The system supports the configuration of static network routes on a per context basis. Network routes are defined by specifying an IP address and mask for the route, the name of the interface in the currant context that the route must use, and a next hop IP address.
- **Open Shortest Path First (OSPF) Protocol version 2:** A link-state routing protocol, OSPF is an Interior Gateway Protocol (IGP) that routes IP packets based solely on the destination IP address found in the IP

packet header using the shortest path first. IP packets are routed "as is", meaning they are not encapsulated in any further protocol headers as they transit the network.

Variable length subnetting, areas, and redistribution into and out of OSPF are supported.

OSPF routing is supported in accordance with the following standards:

- RFC-1850, OSPF Version 2 Management Information Base, November 1995
- RFC-2328, OSPF Version 2, April 1998
- RFC-3101 OSPF-NSSA Option, January 2003

- **Border Gateway Protocol version 4 (BGP-4):** The system supports a subset of BGP (RFC-1771, A Border Gateway Protocol 4 (BGP-4)), suitable for eBGP support of multi-homing typically used to support geographically redundant mobile gateways, is supported.

  EBGP is supported with multi-hop, route filtering, redistribution, and route maps. The network command is support for manual route advertisement or redistribution.

  BGP route policy and path selection is supported by the following means:

  - Prefix match based on route access list
  - AS path access-list
  - Modification of AS path through path prepend
  - Origin type
  - MED
  - Weight

- **Route Policy:** Routing policies modify and redirect routes to and from the system to satisfy specific routing needs. The following methods are used with or without active routing protocols (i.e. static or dynamic routing) to prescribe routing policy:

  - **Route Access Lists:** The basic building block of a routing policy, route access lists filter routes based upon a specified range of IP addresses.
  - **IP Prefix Lists:** A more advanced element of a routing policy. An IP Prefix list filters routes based upon IP prefixes.
  - **AS Path Access Lists:** A basic building block used for Border Gateway Protocol (BGP) routing, these lists filter Autonomous System (AS) paths.

- **Route Maps:** Route-maps are used for detailed control over the manipulation of routes during route selection or route advertisement by a routing protocol and in route redistribution between routing protocols. This detailed control is achieved using IP Prefix Lists, Route Access Lists and AS Path Access Lists to specify IP addresses, address ranges, and Autonomous System Paths.
- **Equal Cost Multiple Path:** ECMP allows distribution of traffic across multiple routes that have the same cost to the destination. In this manner, throughput load is distributed across multiple paths, typically to lessen the burden on any one route and provide redundancy.

Important For more information on IP Routing configuration, refer to the *Routing* chapter in the *System Administration Guide*.

Management System Overview

The system's management capabilities are designed around the Telecommunications Management Network (TMN) model for management -- focusing on providing superior quality Network Element (NE) and element management system (Web Element Manager) functions. The system provides element management applications that can easily be integrated, using standards-based protocols (CORBA and SNMPv1, v2), into higher-level management systems -- giving wireless operators the ability to integrate the system into their overall network, service, and business management systems. In addition, all management is performed out-of-band for security and to maintain system performance.

Description

Cisco's O&M module offers comprehensive management capabilities to the operators and enables them to operate the system more efficiently. There are multiple ways to manage the system either locally or remotely using its out-of-band management interfaces.

These include:

- Using the Command Line Interface (CLI)
- Remote login using Telnet, and Secure Shell (SSH) access to CLI through SPIO card's Ethernet management interfaces
- Local login through the Console port on SPIO card using an RS-232 serial connection
- Using the Web Element Manager application
- Supports communications through 10 Base-T, 100 Base-TX, 1000 Base-TX, or 1000
- Base-SX (optical gigabit Ethernet) Ethernet management interfaces on the SPIO
- Client-Server model supports any browser (i.e. Microsoft Internet Explorer v5.0 and above or Netscape v4.7 or above, and others)
- Supports Common Object Request Broker Architecture (CORBA) protocol and Simple Network Management Protocol version 1 (SNMPv1) for fault management
- Provides complete Fault, Configuration, Accounting, Performance, and Security (FCAPS) capabilities
- Can be easily integrated with higher-level network, service, and business layer applications using the Object Management Group's (OMG's) Interface Definition Language (IDL)

Important For more information on command line interface based management, refer to the *Command Line Interface Reference* and *PDSN Administration Guide*.

Bulk Statistics Support

The system's support for bulk statistics allows operators to choose to view not only statistics that are of importance to them, but also to configure the format in which it is presented. This simplifies the post-processing of statistical data since it can be formatted to be parsed by external, back-end processors.

When used in conjunction with the Web Element Manager, the data can be parsed, archived, and graphed.

Description

The system can be configured to collect bulk statistics (performance data) and send them to a collection server (called a receiver). Bulk statistics are statistics that are collected in a group. The individual statistics are grouped by schema. The following schemas are supported:

- System: Provides system-level statistics
- **Card**: Provides card-level statistics
- **Port**: Provides port-level statistics
- **BCMCS**: Provides BCMCS service statistics
- **FA**: Provides FA service statistics
- **HA**: Provides HA service statistics
- **IP Pool**: Provides IP pool statistics
- **MIPv6HA**: Provides MIPv6HA service statistics
- **PPP**: Provides Point-to-Point Protocol statistics
- **RADIUS**: Provides per-RADIUS server statistics
- **ECS**: Provides Enhanced Charging Service Statistics

The system supports the configuration of up to 4 sets (primary/secondary) of receivers. Each set can be configured with to collect specific sets of statistics from the various schemas. Statistics can be pulled manually from the IMG or sent at configured intervals. The bulk statistics are stored on the receiver(s) in files.

The format of the bulk statistic data files can be configured by the user. Users can specify the format of the file name, file headers, and/or footers to include information such as the date, IMG host name, IMG uptime, the IP address of the system generating the statistics (available for only for headers and footers), and/or the time that the file was generated.

When the Web Element Manager is used as the receiver, it is capable of further processing the statistics data through XML parsing, archiving, and graphing.

The Bulk Statistics Server component of the Web Element Manager parses collected statistics and stores the information in the PostgreSQL database. If XML file generation and transfer is required, this element generates the XML output and can send it to a Northbound NMS or an alternate bulk statistics server for further processing.

Additionally, if archiving of the collected statistics is desired, the Bulk Statistics server writes the files to an alternative directory on the server. A specific directory can be configured by the administrative user or the default directory can be used. Regardless, the directory can be on a local file system or on an NFS-mounted file system on the Web Element Manager server.

Threshold Crossing Alerts (TCA) Support

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

The system supports Threshold Crossing Alerts for certain key resources such as CPU, memory, IP pool addresses, etc. With this capability, the operator can configure threshold on these resources whereby, should the resource depletion cross the configured threshold, a SNMP Trap would be sent.

Description

The following thresholding models are supported by the system:

- **Alert:** A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.
- **Alarm:** Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values.

  Generation of specific traps can be enabled or disabled on the chassis. Ensuring that only important faults get displayed. SNMP traps are supported in both Alert and Alarm modes.

- **Logs:** The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

  Logs are supported in both the Alert and the Alarm models.

- **Alarm System:** High threshold alarms generated within the specified polling interval are considered "outstanding" until a the condition no longer exists or a condition clear alarm is generated. "Outstanding" alarms are reported to the system's alarm subsystem and are viewable through the Alarm Management menu in the Web Element Manager.

  The Alarm System is used only in conjunction with the Alarm model.

Important For more information on threshold crossing alert configuration, refer to the *Thresholding Configuration Guide*.

IP Header Compression - Van Jacobson

Implementing IP header compression provides the following benefits:

- Improves interactive response time

- Allows the use of small packets for bulk data with good line efficiency
- Allows the use of small packets for delay sensitive low data-rate traffic
- Decreases header overhead
- Reduces packet loss rate over lossy links

Description

The system supports the Van Jacobson (VJ) IP header compression algorithms by default for subscriber traffic.

The VJ header compression is supported as per RFC 1144 (CTCP) header compression standard developed by V. Jacobson in 1990. It is commonly known as VJ compression. It describes a basic method for compressing the headers of IPv4/TCP packets to improve performance over low speed serial links.

By default IP header compression using the VJ algorithm is enabled for subscribers. You can also turn off IP header compression for a subscriber.

Important For more information on IP header compression support, refer to the IP Header Compression chapter.

DSCP Marking

Provides support for more granular configuration of DSCP marking.

For different Traffic class, the PDSN supports per-service and per-subscriber configurable DSCP marking for Uplink and Downlink direction based on Allocation/Retention Priority in addition to the current priorities.

Features and Functionality - Optional Enhanced Software Features

This section describes the optional enhanced features and functions for PDSN service.

Each of the following features require the purchase of an additional license to implement the functionality with the PDSN service.

This section describes following features:

Session Recovery Support

The Session Recovery feature provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault within the system preventing a fully connected user session from being disconnected.

Description

Session recovery is performed by mirroring key software processes (e.g. session manager and AAA manager) within the system. These mirrored processes remain in an idle state (in standby-mode), wherein they perform no processing, until they may be needed in the case of a software failure (e.g. a session manager task aborts). The system spawns new instances of "standby mode" session and AAA managers for each active Control Processor (CP) being used.

Additionally, other key system-level software tasks, such as VPN manager, are performed on a physically separate Packet Services Card (PSC) to ensure that a double software fault (e.g. session manager and VPN manager fails at same time on same card) cannot occur. The PSC used to host the VPN manager process is in active mode and is reserved by the operating system for this sole use when session recovery is enabled.

The additional hardware resources required for session recovery include a standby System Processor Card (SPC) and a standby PSC.

There are two modes for Session Recovery.

- **Task recovery mode:** Wherein one or more session manager failures occur and are recovered without the need to use resources on a standby PSC. In this mode, recovery is performed by using the mirrored "standby-mode" session manager task(s) running on active PACs. The "standby-mode" task is renamed, made active, and is then populated using information from other tasks such as AAA manager.
- **Full recovery mode:** Used when a PSC hardware failure occurs, or when a PSC migration failure happens. In this mode, the standby PSC is made active and the "standby-mode" session manager and AAA manager tasks on the newly activated PSC perform session recovery.

Session/Call state information is saved in the peer AAA manager task because each AAA manager and session manager task is paired together. These pairs are started on physically different PACs to ensure task recovery.

Important For more information on session recovery support, refer to the Session Recovery chapter in the *System Administration Guide*.

IPv6 Support

This feature allows IPv6 subscribers to connect via the CDMA 2000 infrastructure in accordance with the following standards:

- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification
- RFC 2461: Neighbor Discovery for IPv6
- RFC 2462: IPv6 Stateless Address Autoconfiguration
- RFC 3314: Recommendations for IPv6 in 3GPP Standards
- RFC 3316: Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts

- RFC 3056: Connection of IPv6 domains via IPv4 clouds
- 3GPP TS 23.060: General Packet Radio Service (GPRS) Service description
- 3GPP TS 27.060: Mobile Station Supporting Packet Switched Services
- 3GPP TS 29.061: Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)

Description

The PDSN allows a subscriber to be configured for IPv6 PDP contexts. Also, a subscriber may be configured to simultaneously allow IPv4 PDP contexts.

The PDSN supports IPv6 stateless dynamic auto-configuration. The mobile station may select any value for the interface identifier portion of the address. The link-local address is assigned by the PDSN to avoid any conflict between the mobile station link-local address and the PDSN address. The mobile station uses the interface identifier assigned by the PDSN during the stateless address auto-configuration procedure. Once this has completed, the mobile can select any interface identifier for further communication as long as it does not conflict with the PDSN's interface identifier that the mobile learned through router advertisement messages from the PDSN.

Control and configuration of the above is specified as part of the subscriber configuration on the PDSN, e.g., IPv6 address prefix and parameters for the IPv6 router advertisements. RADIUS VSAs may be used to override the subscriber configuration.

Following IPv6 PDP context establishment, the PDSN can perform either manual or automatic 6to4 tunneling, according to RFC 3056, Connection of IPv6 Domains Via IPv4 Clouds.

L2TP LAC Support

The system configured as a Layer 2 Tunneling Protocol Access Concentrator (LAC) enables communication with L2TP Network Servers (LNSs) for the establishment of secure Virtual Private Network (VPN) tunnels between the operator and a subscriber's corporate or home network.

Description

The use of L2TP in VPN networks is often used as it allows the corporation to have more control over authentication and IP address assignment. An operator may do a first level of authentication, however use PPP to exchange user name and password, and use IPCP to request an address. To support PPP negotiation between the PDSN and the corporation, an L2TP tunnel must be setup in the PDSN running a LAC service.

L2TP establishes L2TP control tunnels between LAC and LNS before tunneling the subscriber PPP connections as L2TP sessions. The LAC service is based on the same architecture as the PDSN and benefits from dynamic resource allocation and distributed message and data processing. This design allows the LAC service to support over 4000 setups per second or a maximum of over 3G of throughput. There can be a maximum up to 65535 sessions in a single tunnel and as many as 500,000 L2TP sessions using 32,000 tunnels per system.

The LAC sessions can also be configured to be redundant, thereby mitigating any impact of hardware of software issues. Tunnel state is preserved by copying the information across processor cards.

Important For more information on L2TP Access Concentrator support, refer to the L2TP Access Concentrator chapter.

L2TP LNS Support

The system configured as a Layer 2 Tunneling Protocol Network Server (LNS) supports the termination secure Virtual Private Network (VPN) tunnels between from L2TP Access Concentrators (LACs).

Description

The LNS service takes advantage of the high performance PPP processing already supported in the system design and is a natural evolution from the LAC. The LNS can be used as a standalone, or running alongside a PDSN service in the same platform, terminating L2TP services in a cost effective and seamless manner.

L2TP establishes L2TP control tunnels between LAC and LNS before tunneling the subscriber PPP connections as L2TP sessions. There can be a maximum of up to 65535 sessions in a single tunnel and up to 500,000 sessions per LNS.

The LNS architecture is similar to the PDSN and utilizes the concept of a de-multiplexer to intelligently assign new L2TP sessions across the available software and hardware resources on the platform without operator intervention..

Important For more information on L2TP LNS support, refer to the L2TP Access Concentrator chapter.

Proxy Mobile IP

Mobility for subscriber sessions is provided through the Mobile IP protocol as defined in RFCs 2002-2005. However, some older Mobile Nodes (MNs) do not support the Mobile IP protocol. The Proxy Mobile IP feature provides a mobility solution for these MNs.

Description

For IP PDP contexts using Proxy Mobile IP, the MN establishes a session with the PDSN as it normally would. However, the PDSN/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the IP PDP context with the PDSN, no Agent Advertisement messages are communicated with the MN).

The MN is assigned an IP address by either the HA, an AAA server, or on a static-basis. The address is stored in a Mobile Binding Record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Proxy Mobile IP can be performed on a per-subscriber basis based on information contained in their user profile, or for all subscribers facilitated by a specific subscriber. In the case of non-transparent IP PDP contexts, attributes returned from the subscriber's profile take precedence over the configuration of the subscriber.

Important For more information on Proxy Mobile IP configuration, refer to the *Proxy Mobile IP* chapter.

IP Security (IPSec)

IP Security provides a mechanism for establishing secure tunnels from mobile subscribers to pre-defined endpoints (i.e. enterprise or home networks) in accordance with the following standards:

- RFC 2401, Security Architecture for the Internet Protocol
- RFC 2402, IP Authentication Header (AH)
- RFC 2406, IP Encapsulating Security Payload (ESP)
- RFC 2409, The Internet Key Exchange (IKE)
- RFC-3193, Securing L2TP using IPSEC, November 2001

Description

IP Security (IPSec) is a suite of protocols that interact with one another to provide secure private communications across IP networks. These protocols allow the system to establish and maintain secure tunnels with peer security gateways. IPSec can be implemented on the system for the following applications:

- PDN Access: Subscriber IP traffic is routed over an IPSec tunnel from the system to a secure gateway on the Packet Data Network (PDN) as determined by Access Control List (ACL) criteria.
- Mobile IP: Mobile IP control signals and subscriber data is encapsulated in IPSec tunnels that are established between Foreign Agents (FAs) and Home Agents (HAs) over the Pi interfaces.

  Once an IPSec tunnel is established between an FA and HA for a particular subscriber, all new Mobile IP sessions using the same FA and HA are passed over the tunnel regardless of whether or not IPSec is supported for the new subscriber sessions. Data for existing Mobile IP sessions is unaffected.
- L2TP: L2TP-encapsulated packets are routed from the system to an LNS/secure gateway over an IPSec tunnel.

Important For more information on IPSec support, refer to the *IPSec Reference* Guide.

Traffic Policing and Rate Limiting

Allows the operator to proportion the network and support Service-level Agreements (SLAs) for customers

Description

The Traffic-Policing/Shaping feature enables configuring and enforcing bandwidth limitations on individual PDP contexts of a particular 3GPP traffic class. Values for traffic classes are defined in 3GPP TS 23.107 and are negotiated with the SGSN during PDP context activation using the values configured for the subscriber on the PDSN. Configuration and enforcement is done independently on the downlink and the uplink directions for each of the 3GPP traffic classes. Configuration is on a per-subscriber basis, but may be overridden for individual subscribers or subscriber tiers during RADIUS authentication/authorization.

A Token Bucket Algorithm (a modified trTCM, as specified in RFC2698) is used to implement the Traffic-Policing feature. The algorithm measures the following criteria when determining how to mark a packet.

- **Committed Data Rate (CDR):** The guaranteed rate (in bits per second) at which packets may be transmitted/received for the subscriber during the sampling interval.
- **Peak Data Rate (PDR):** The maximum rate (in bits per second) that packets may be transmitted/received for the subscriber during the sampling interval.
- **Burst-size:** The maximum number of bytes that may be transmitted/received for the subscriber during the sampling interval for both committed (CBS) and peak (PBS) rate conditions. This represents the maximum number of tokens that can be placed in the subscriber's "bucket". Note that the committed burst size (CBS) equals the peak burst size (PBS) for each subscriber.

Tokens are removed from the subscriber's bucket based on the size of the packets being transmitted/received. Every time a packet arrives, the system determines how many tokens need to be added (returned) to a subscriber's CBS (and PBS) bucket. This value is derived by computing the product of the time difference between incoming packets and the CDR (or PDR). The computed value is then added to the tokens remaining in the subscriber's CBS (or PBS) bucket. The total number of tokens can not be greater than the configured burst-size. If the total number of tokens is greater than the burst-size, the number is set to equal the burst-size. After passing through the Token Bucket Algorithm, the packet is internally classified with a color, as follows:

- There are not enough tokens in the PBS bucket to allow a packet to pass, then the packet is considered to be in violation and is marked "red" and the violation counter is incremented by one.
- There are enough tokens in the PBS bucket to allow a packet to pass, but not in the CBS "bucket", then the packet is considered to be in excess and is marked "yellow", the PBS bucket is decremented by the packet size, and the exceed counter is incremented by one.
- There are more tokens present in the CBS bucket than the size of the packet, then the packet is considered as conforming and is marked "green" and the CBS and PBS buckets are decremented by the packet size.

The subscriber on the PDSN can be configured with actions to take for red and yellow packets. Any of the following actions may be specified:

- **Drop**: The offending packet is discarded.
- **Transmit**: The offending packet is passed.
- **Lower the IP Precedence**: The packet's ToS octet is set to "0", thus downgrading it to Best Effort, prior to passing the packet.
- **Buffer the Packet**: The packet stored in buffer memory and transmitted to subscriber once traffic flow comes in allowed bandwidth.

Different actions may be specified for red and yellow, as well as for uplink and downlink directions and different 3GPP traffic classes.

Refer to the Intelligent Traffic Control section for additional policing and shaping capabilities of the PDSN.

Important For more information on per subscriber traffic policing and shaping, refer to the Traffic Policing and Shaping section.

Intelligent Traffic Control

Enables operators to provide differentiated tiered service provisioning for native and non-native subscribers.

Description

Mobile carriers are looking for creative methods for maximizing network resources while, at the same time, enhancing their end users overall experience. These same mobile operators are beginning to examine solutions for providing preferential treatment for their native subscribers and services as compared to, for example, roaming subscribers, Mobile Virtual Network Operators (MVNOs) and/or Peer-to-Peer (P2P) applications. The overall end goal is to provide superior levels of performance for their customers/services, while ensuring that non-native users/applications do not overwhelm network resources.

ITC provides the ability to examine each subscriber session and respective flow(s) such that selective, configurable limits on a per-subscriber/per-flow basis can be applied. Initially, QoS in this context is defined as traffic policing on a per-subscriber/per-flow basis with the potential to manipulate Differentiated Services Code Points (DSCPs), queue redirection (i.e. move traffic to a Best Effort (BE) classification) and/or simply dropping out of profile traffic. ITC enables 5 tuple packet filters for individual application flows to be either manually configured via CLI or dynamically established via RSVP TFT information elements in 1xEV-DO Rev A or as a consequence of PDP context establishments in CDMA networks. Policy rules may be locally assigned or obtained from an external PCRF via push/pull policy signaling interactions. Policies may be applied on a per-subscriber, per-context and/or chassis-wide basis.

Important For more information on intelligent traffic control support, refer to the *Intelligent Traffic Control* chapter.

Dynamic RADIUS Extensions (Change of Authorization)

Dynamic RADIUS extension support provide operators with greater control over subscriber PDP contexts by providing the ability to dynamically redirect data traffic, and or disconnect the PDP context.

This functionality is based on the RFC 3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), July 2003 standard.

Description

The system supports the configuration and use of the following dynamic RADIUS extensions:

- **Change of Authorization**: The system supports CoA messages from the AAA server to change data filters associated with a subscriber session. The CoA request message from the AAA server must contain attributes to identify NAS and the subscriber session and a data filter ID for the data filter to apply to the subscriber session.
- **Disconnect Message:** The DM message is used to disconnect subscriber sessions in the system from a RADIUS server. The DM request message should contain necessary attributes to identify the subscriber session.

The above extensions can be used to dynamically re-direct subscriber PDP contexts to an alternate address for performing functions such as provisioning and/or account set up. This functionality is referred to as Session Redirection, or Hotlining.

Session redirection provides a means to redirect subscriber traffic to an external server by applying ACL rules to the traffic of an existing or a new subscriber session. The destination address and optionally the destination port of TCP/IP or UDP/IP packets from the subscriber are rewritten so the packet is forwarded to the designated redirected address.

Return traffic to the subscriber has the source address and port rewritten to the original values. The redirect ACL may be applied dynamically by means of the Radius Change of Authorization (CoA) extension.

Important For more information on dynamic RADIUS extensions support, refer to the *CoA, RADIUS, And Session Redirection (Hotlining)* chapter.

Features and Functionality - Inline Service Support

This section describes the features and functions of inline services supported on the PDSN. These services require additional licenses to implement the functionality.

Content Filtering

The Cisco PDSN offers two variants of network-controlled content filtering / parental control services. Each approach leverages the native DPI capabilities of the platform to detect and filter events of interest from mobile subscribers based on HTTP URL or WAP/MMS URI requests:

- Integrated Content Filtering: A turnkey solution featuring a policy enforcement point and category based rating database on the Cisco PDSN. An offboard AAA or PCRF provides the per-subscriber content filtering information as subscriber sessions are established. The content filtering service uses DPI to extract URL's or URI's in HTTP request messages and compares them against a static rating database to determine the category match. The provisioned policy determines whether individual subscribers are entitled to view the content.
- Content Filtering ICAP Interface: This solution is appropriate for mobile operators with existing installations of Active Content Filtering external servers. The service continues to harness the DPI functions of the ASR 5500 platform to extract events of interest. However in this case, the extracted requests are transferred via the Integrated Content Adaptation Protocol (ICAP) with subscriber identification information to the external ACF server which provides the category rating database and content decision functions.

Integrated Adult Content Filter

Provides a value-added service to prevent unintended viewing of objectionable content that exploits underage children. Content Filtering offers mobile operators a way to increase data ARPU and subscriber retention through a network-based solution for parental controls and content filtering. The integrated solution enables a single policy decision and enforcement point thereby streamlining the number of signaling interactions with external AAA/Policy Manager servers. When used in parallel with other services such as Enhanced Content Charging (ECS) it increases billing accuracy of charging records by insuring that mobile subscribers are only charged for visited sites they are allowed to access.

The Integrated Adult Content Filter is a subscriber-aware inline service provisioned on an ASR 5500 running PDSN services. Integrated Content Filtering utilizes the local DPI engine and harnesses a distributed software architecture that scales with the number of active PDSN sessions on the system.

Content Filtering policy enforcement is the process of deciding if a subscriber should be able to receive some content. Typical options are to allow, block, or replace/redirect the content based on the rating of the content and the policy defined for that content and subscriber. The policy definition is transferred in an authentication response from a AAA server or Diameter policy message via the Gx reference interface from an adjunct

PCRF. The policy is applied to subscribers through rulebase or APN/Subscriber configuration. The policy determines the action to be taken on the content request on the basis of its category. A maximum of one policy can be associated with a rulebase.

ICAP Interface

Provides a value-added service to prevent unintended viewing of objectionable content that exploits underage children. Content Filtering offers mobile operators a way to increase data ARPU and subscriber retention through a network-based solution for parental controls and content filtering. The Content Filtering ICAP solution is appropriate for operators with existing installations of Active Content Filtering servers in their networks.

The Enhanced Charging Service (ECS) provides a streamlined Internet Content Adaptation Protocol (ICAP) interface to leverage the Deep Packet Inspection (DPI) to enable external Application Servers to provide their services without performing the DPI functionality and without being inserted in the data flow. The ICAP interface may be attractive to mobile operators that prefer to use an external Active Content Filtering (ACF) Platform. If a subscriber initiates a WAP (WAP1.x or WAP2.0) or Web session, the subsequent GET/POST request is detected by the deep packet inspection function. The URL of the GET/POST request is extracted by the local DPI engine on the ASR 5500 platform and passed, along with subscriber identification information and the subscriber request, in an ICAP message to the Application Server (AS). The AS checks the URL on the basis of its category and other classifications like, type, access level, content category and decides if the request should be authorized, blocked or redirected by answering the GET/POST message. Depending upon the response received from the ACF server, the PDSN either passes the request unmodified or discards the message and responds to the subscriber with the appropriate redirection or block message.

Network Address Translation (NAT)

NAT translates non-routable private IP address(es) to routable public IP address(es) from a pool of public IP addresses that have been designated for NAT. This enables to conserve on the number of public IP addresses required to communicate with external networks, and ensures security as the IP address scheme for the internal network is masked from external hosts, and each outgoing and incoming packet goes through the translation process.

NAT works by inspecting both incoming and outgoing IP datagrams and, as needed, modifying the source IP address and port number in the IP header to reflect the configured NAT address mapping for outgoing datagrams. The reverse NAT translation is applied to incoming datagrams.

NAT can be used to perform address translation for simple IP and mobile IP. NAT can be selectively applied/denied to different flows (5-tuple connections) originating from subscribers based on the flows' L3/L4 characteristics—Source-IP, Source-Port, Destination-IP, Destination-Port, and Protocol.

NAT supports the following mappings:

- One-to-One
- Many-to-One

Important For more information on NAT, refer to the *Network Address Translation Administration Guide.*

Peer-to-Peer Detection

Allows operators to identify P2P traffic in the network and applying appropriate controlling functions to ensure fair distribution of bandwidth to all subscribers.

Peer-to-Peer (P2P) is a term used in two slightly different contexts. At a functional level, it means protocols that interact in a peering manner, in contrast to client-server manner. There is no clear differentiation between the function of one node or another. Any node can function as a client, a server, or both—a protocol may not clearly differentiate between the two. For example, peering exchanges may simultaneously include client and server functionality, sending and receiving information.

Detecting peer-to-peer protocols requires recognizing, in real time, some uniquely identifying characteristic of the protocols. Typical packet classification only requires information uniquely typed in the packet header of packets of the stream(s) running the particular protocol to be identified. In fact, many peer-to-peer protocols can be detected by simple packet header inspection. However, some P2P protocols are different, preventing detection in the traditional manner. This is designed into some P2P protocols to purposely avoid detection. The creators of these protocols purposely do not publish specifications. A small class of P2P protocols is stealthier and more challenging to detect. For some protocols no set of fixed markers can be identified with confidence as unique to the protocol.

Operators care about P2P traffic because of the behavior of some P2P applications (for example, Bittorrent, Skype, and eDonkey). Most P2P applications can hog the network bandwidth such that 20 P2P users can generate as much as traffic generated by the rest 80% non-P2P users. This can result into a situation where non-P2P users may not get enough network bandwidth for their legitimate use because of excess usage of bandwidth by the P2P users. Network operators need to have dynamic network bandwidth / traffic management functions in place to ensure fair distributions of the network bandwidth among all the users. And this would include identifying P2P traffic in the network and applying appropriate controlling functions to the same (for example, content-based premium billing, QoS modifications, and other similar treatments).

Cisco's P2P detection technology makes use of innovative and highly accurate protocol behavioral detection techniques.

Important For more information on peer-to-peer detection, refer to the *Application Detection and Control Administration Guide*.

Personal Stateful Firewall

The Personal Stateful Firewall is an in-line service feature that inspects subscriber traffic and performs IP session-based access control of individual subscriber sessions to protect the subscribers from malicious security attacks.

The Personal Stateful Firewall supports stateless and stateful inspection and filtering based on the configuration.

In stateless inspection, the firewall inspects a packet to determine the 5-tuple—source and destination IP addresses and ports, and protocol—information contained in the packet. This static information is then compared against configurable rules to determine whether to allow or drop the packet. In stateless inspection the firewall examines each packet individually, it is unaware of the packets that have passed through before it, and has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is a rogue packet.

In stateful inspection, the firewall not only inspects packets up through the application layer / layer 7 determining a packet's header information and data content, but also monitors and keeps track of the connection's state.

For all active connections traversing the firewall, the state information, which may include IP addresses and ports involved, the sequence numbers and acknowledgement numbers of the packets traversing the connection, TCP packet flags, etc. is maintained in a state table. Filtering decisions are based not only on rules but also on the connection state established by prior packets on that connection. This enables to prevent a variety of DoS, DDoS, and other security violations. Once a connection is torn down, or is timed out, its entry in the state table is discarded.

The Enhanced Charging Service (ECS) / Active Charging Service (ACS) in-line service is the primary vehicle that performs packet inspection and charging. For more information on ECS, see the *Enhanced Charging Service Administration Guide*.

Important For more information on Personal Stateful Firewall, refer to the *Personal Stateful Firewall Administration Guide*.

Features and Functionality - External Application Support

This section describes the features and functions of external applications supported on the PDSN. These services require additional licenses to implement the functionality.

Mobility Unified Reporting

The Cisco Mobility Unified Reporting (MUR)/Mobility Unified Reporting and Analytics (MURAL) system is a Web-based application providing a unified reporting interface for diverse data from Cisco Systems In-line service and storage applications.

The MUR/MURAL application provides comprehensive and consistent set of statistics and customized reports, report scheduling and distribution from ASR chassis / in-line service product. For example, a subscriber's Quality of Experience, top 10 sites visited, top 10 users, and so on.

The MUR/MURAL application provides reporting capability for Content Filtering (CF) data, bulk statistics, Key Performance Indicators (KPIs), EDRs data from in-line service and storage applications. The MUR/MURAL application facilitates and enhances the operators' ability to simply and easily determine the health and usage of the network.

Important For more information on MUR support, refer to the *MUR Installation and Administration Guide*.

For more information on MURAL support, refer to the *MURAL Installation and Administration Guide* and *MURAL User Guide*.

CDMA2000 Data Network Deployment Configurations

This section provides examples of how the system can be deployed within a wireless carrier's network. As noted previously in this chapter, the system can be deployed in standalone configurations, serving as a Packet Data Serving Node/Foreign Agent (PDSN/FA), a Home Agent (HA), or in a combined PDSN/FA/HA configuration providing all services from a single chassis. Although XT-2 systems are highly flexible, but

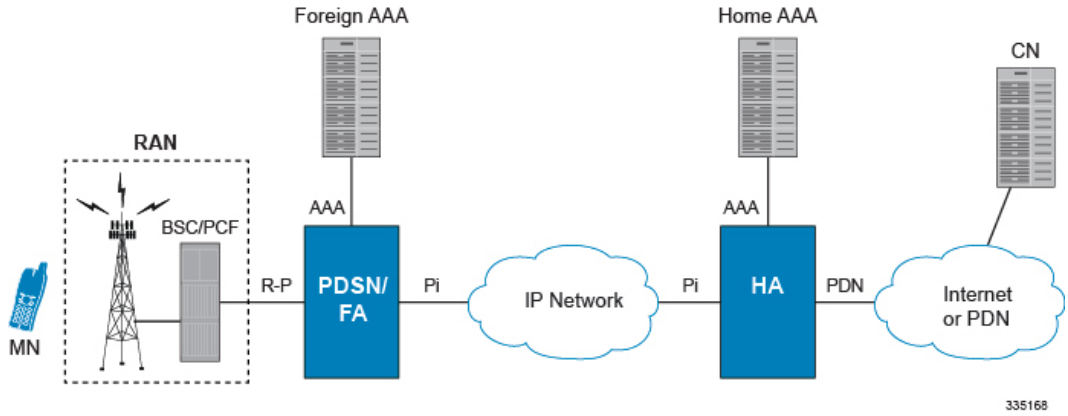
XT-2 systems are pre-loaded with purchased services and operator can not add additional services through license. Operator needs to predefine the services required on a system.

Standalone PDSN/FA and HA Deployments

The PDSN/FA serves as an integral part of a CDMA2000 network by providing the packet processing and re-direction to the mobile user's home network through communications with the HA. In cases where the mobile user connects to a PDSN that serves their home network, no re-direction is required.

The following figure depicts a sample network configuration wherein the PDSN/FA and HA are separate systems.

Figure 1: PDSN/FA and HA Network Deployment Configuration Example



The HA allows mobile nodes to be reached, or served, by their home network through its home address even when the mobile node is not attached to its home network. The HA performs this function through interaction with an FA that the mobile node is communicating with using the Mobile IP protocol. Such transactions are performed through the use of virtual private networks that create Mobile IP tunnels between the HA and FA.

Interface Descriptions

This section describes the primary interfaces used in a CDMA2000 wireless data network deployment.

R-P Interface

This interface exists between the Packet Control Function (PCF) and the PDSN/FA and implements the A10 and A11 (data and bearer signaling respectively) protocols defined in 3GPP2 specifications.

This interface exists between the Packet Control Function (PCF) and the PDSN/FA and implements either the A10 and A11 (data and bearer signaling respectively) protocols defined in 3GPP2 specifications or the proprietary Closed R-P protocol from Nortel Networks®. The Closed R-P protocol encapsulates PPP packets using an enhanced version of the Layer 2 Tunneling Protocol (L2TP) between the PCF and the Packet Data Serving Node (PDSN).

Important A valid feature use key is required to be installed before the Closed R-P protocol may be used. For more information on obtaining this feature key, please contact your sales representative.

The PCF can be co-located with the Base Station Controller (BSC) as part of the Radio Access Node (RAN). The PDSN/FA is connected to the RAN via Ethernet ports. These ports also support outbound IP traffic that carries user data to the HA for Mobile IP services, or to the Internet or Wireless Access Protocol (WAP) gateway for Simple IP services.

Pi Interfaces

The Pi interface provides connectivity between the HA and its corresponding FA. The Pi interface is used to establish a Mobile IP tunnels between the PDSN/FA and HA.

PDN Interfaces

PDN interface provide connectivity between the PDSN and/or HA to packet data networks such as the Internet or a corporate intranet.

AAA Interfaces

Using the LAN ports located on the Switch Processor I/O (SPIO) and Ethernet line cards, these interfaces carry AAA messages to and from RADIUS accounting and authentication servers. The SPIO supports RADIUS-capable management interfaces using either copper or fiber Ethernet connectivity through two auto-sensing 10/100/1000 Mbps Ethernet interfaces or two SFP optical gigabit Ethernet interfaces. User-based RADIUS messaging is transported using the Ethernet line cards.

While most carriers will configure separate AAA interfaces to allow for out-of-band RADIUS messaging for system administrative users and other operations personnel, it is possible to use a single AAA interface hosted on the Ethernet line cards to support a single RADIUS server that supports both management users and network users.

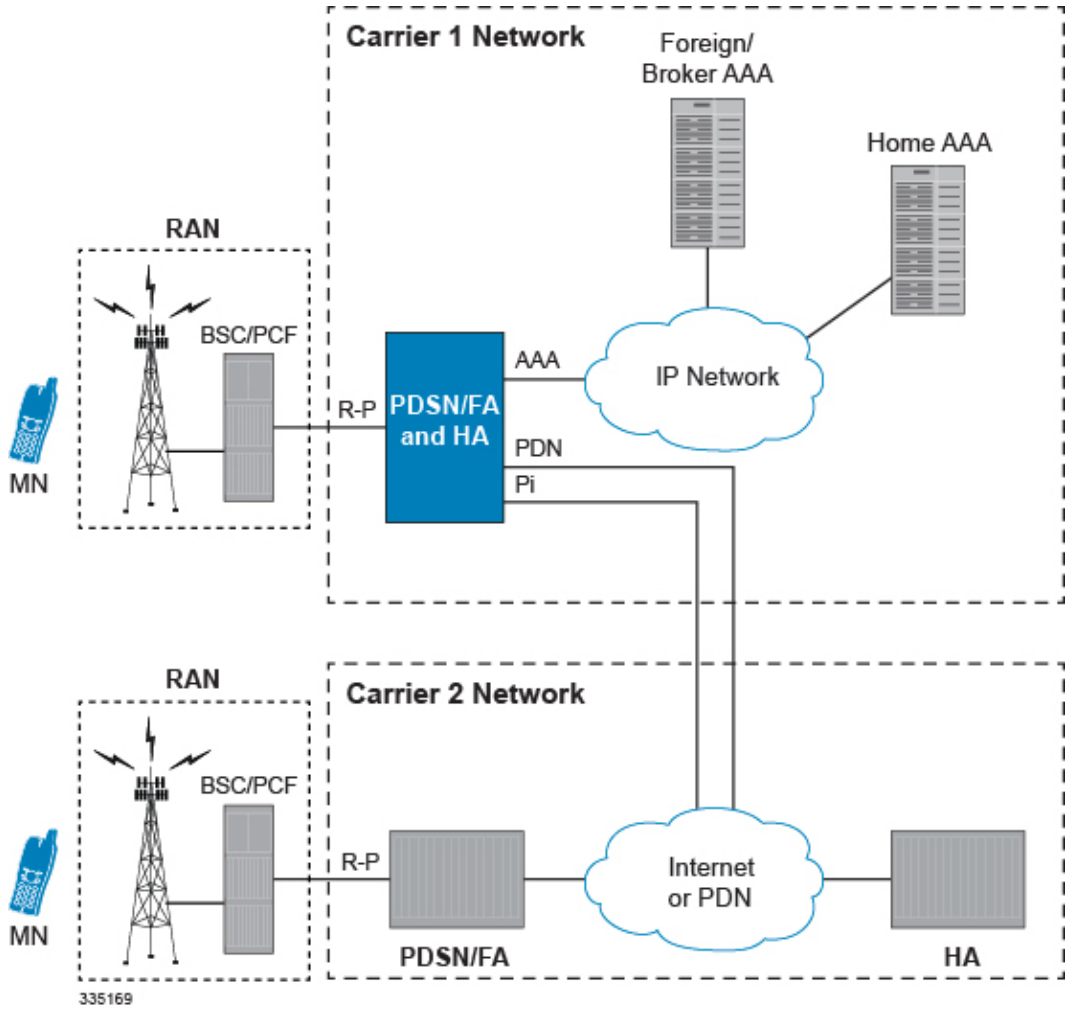
Important Subscriber AAA interfaces should always be configured using Ethernet line card interfaces for the highest performance. The out-of-band local context should not be used for service subscriber AAA functions.

Co-Located Deployments

An advantage of the system is its ability to support both high-density PDSN/FA and HA configurations within the same chassis. The economies of scale presented in this configuration example provide for both improved session handling and reduced cost in deploying a CDMA2000 data network.

The following figure depicts a sample co-located deployment.

Figure 2: Co-located PDSN/FA and HA Configuration Example



It should be noted that all interfaces defined within the 3GPP2 standards for 1x deployments exist in this configuration as they are described in the two previous sections. This configuration can support communications to external, or standalone, PDSNs/FAs and/or HAs using all prescribed standards.

Understanding Simple IP and Mobile IP

From a mobile subscriber's perspective, packet data services are delivered from the service provider network using two access methods:

- Local and public network access
- Private network access

Within the packet data network, access is similar to accessing the public Internet through any other access device. In a private network access scenario, the user must be tunneled into the private network after initial authentication has been performed.

These two methods are provided using one of the following access applications:

- **Simple IP:** The mobile user is dynamically assigned an IP address from the service provider. The user can maintain this address within a defined geographical area, but when the user moves outside of this area, their IP address will be lost. This means that whenever a mobile user moves to a new location, they will need to re-register with the service provider to obtain a new IP address.
- **Mobile IP:** The mobile subscriber uses either a static or dynamically assigned IP address that belongs to their home network. As the subscriber roams through the network, the IP address is maintained providing the subscriber with the opportunity to use IP applications that require seamless mobility such as performing file transfers.
- **Proxy Mobile IP:** Provides a mobility solution for subscribers whose Mobile Nodes (MNs) do not support the Mobile IP protocol. The PDSN/FA proxy the Mobile IP tunnel with the HA on behalf of the MS. The subscriber receives an IP address from either the service provider or from their home network. As the subscriber roams through the network, the IP address is maintained providing the subscriber with the opportunity to use IP applications that require seamless mobility such as transferring files.

The following sections outline both Simple IP, Mobile IP, and Proxy Mobile IP and how they work in a 3G network.

Simple IP

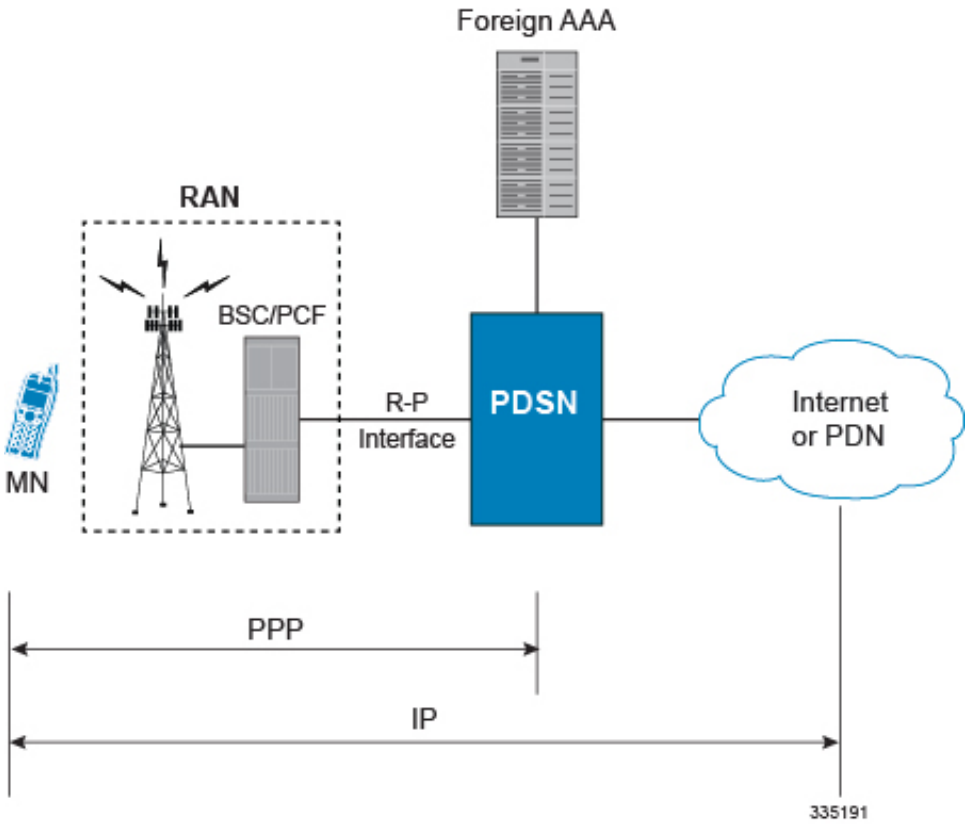
From a packet data perspective, Simple IP is similar to how a dial-up user would connect to the Internet using the Point-to-Point Protocol (PPP) and the Internet Protocol (IP) through an Internet Service Provider (ISP). With Simple IP, the mobile user is assigned a dynamic IP address from a PDSN or AAA server that is serving them locally (a specific geographic area). Once the mobile user is connected to the particular radio network that the assigning PDSN belongs to, an IP address is assigned to the mobile node. The PDSN provides IP routing services to the registered mobile user through the wireless service provider's network.

There is no mobility beyond the PDSN that assigns the dynamic IP address to the mobile user, which means that should the mobile user leave the geographic area where service was established (moves to a new radio network service area), they will need to obtain a new IP address with a new PDSN that is serving the new area. This new connection may or may not be provided by the same service provider.

How Simple IP Works

As described earlier, Simple IP uses two basic communications protocols, PPP and IP. The following figure depicts where each of these protocols are used in a Simple IP call.

Figure 3: Simple IP Protocol Usage



As depicted in the figure above, PPP is used to establish a communications session between the MN and the PDSN. Once a PPP session is established, the Mobile Node (MN) and end host communicate using IP packets.

The following figure and table provides a high-level view of the steps required to make a Simple IP call that is initiated by the MN to an end host. Users should keep in mind that steps 2, 3, 11, and 12 in the call flow are related to the Radio Access Node (RAN) functions and are intended to show a high-level overview of radio communications iterations, and as such are outside the scope of packet-based communications presented here.

Figure 4: Simple IP Call Flow

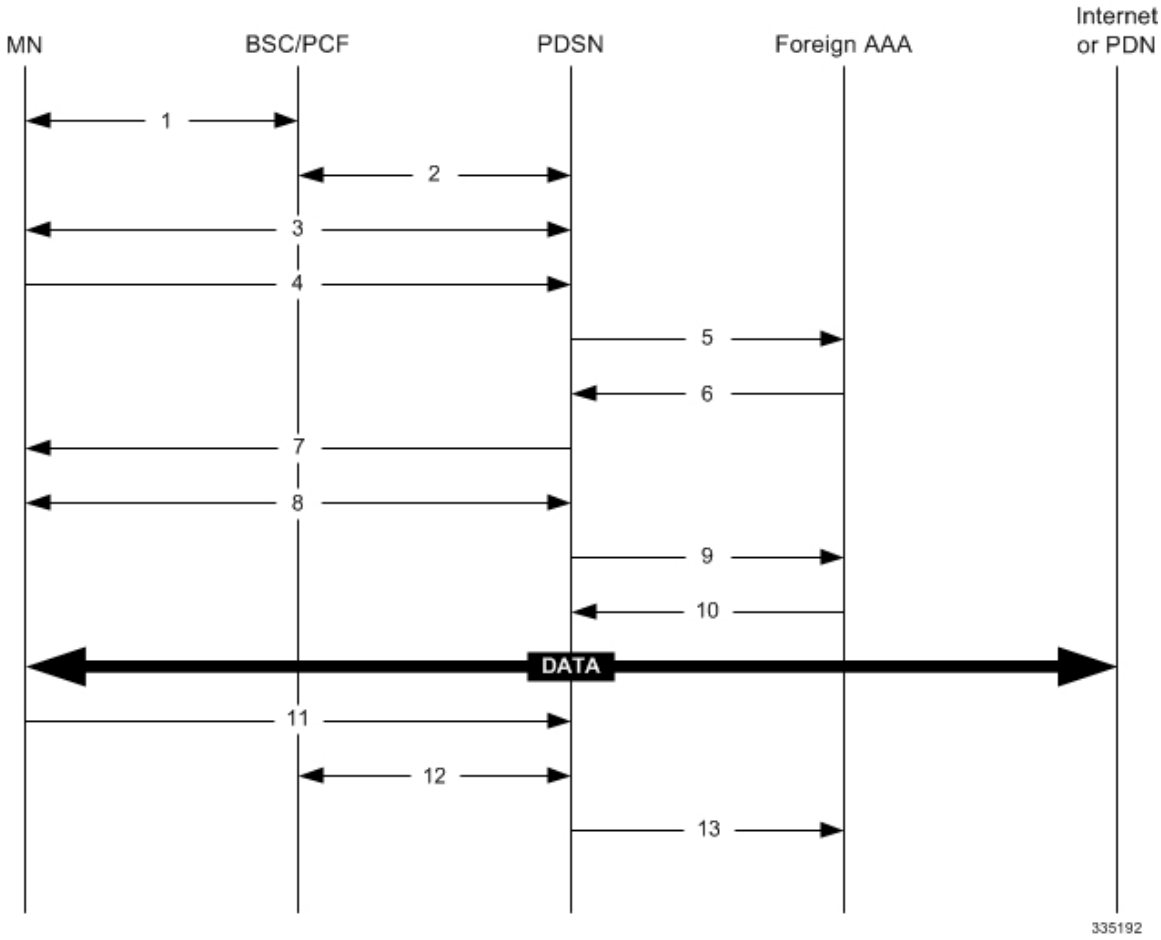


Table 1: Simple IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the RAN through the BSC/PCF.
2	The PCF and PDSN establish the R-P interface for the session.
3	The PDSN and MN negotiate Link Control Protocol (LCP).
4	Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the PDSN.
5	The PDSN sends an Access Request message to the RADIUS AAA server.

Step	Description
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the PDSN. The Accept message may contain various attributes to be assigned to the MN.
7	The PDSN sends a PPP Authentication Response message to the MN.
8	The MN and the PDSN negotiate the Internet Protocol Control Protocol (IPCP) that results in the MN receiving an IP address.
9	The PDSN forwards a RADIUS Accounting Start message to the AAA server fully establishing the session allowing the MN to send/receive data to/from the PDN.
10	Upon completion of the session, the MN sends an LCP Terminate Request message to the PDSN to end the PPP session.
11	The BSC closes the radio link while the PCF closes the R-P session between it and the PDSN. All PDSN resources used to facilitate the session are reclaimed (IP address, memory, etc.).
12	The PDSN sends accounting stop record to the AAA server, ending the session.

Mobile IP

Mobile IP provides a network-layer solution that allows mobile nodes (MNs, i.e. mobile phones, wireless PDAs, and other mobile devices) to receive routed IP packets from their home network while they are connected to any visitor network using their permanent or home IP address. Mobile IP allows mobility in a dynamic method that allows nodes to maintain ongoing communications while changing links as the user traverses the global Internet from various locations outside their home network.

In Mobile IP, the Mobile Node (MN) receives an IP address, either static or dynamic, called the "home address" assigned by its Home Agent (HA). A distinct advantage with Mobile IP is that MNs can hand off between different radio networks that are served by different PDSNs.

In this scenario, the PDSN in the visitor network performs as a Foreign Agent (FA), establishing a virtual session with the MN's HA. Each time the MN registers with a different PDSN/FA, the FA assigns the MN a care-of-address. Packets are then encapsulated into IP tunnels and transported between FA, HA, and the MN.

Mobile IP Tunneling Methods

Tunneling by itself is a technology that enables one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within a packet, carried by the second network. Tunneling is also called encapsulation. Service providers typically use tunneling for two purposes first, to transport otherwise un-routable packets across the IP network and second, to provide data separation for Virtual Private Networking (VPN) services. In Mobile IP, tunnels are used to transport data packets between the FA and HA.

The system supports the following tunneling protocols, as defined in the IS-835-A specification and the relevant Request For Comments (RFCs) for Mobile IP:

IP in IP tunnels

IP in IP tunnels basically encapsulate one IP packet within another using a simple encapsulation technique. To encapsulate an IP datagram using IP in IP encapsulation, an outer IP header is inserted before the datagram's existing IP header. Between them are other headers for the path, such as security headers specific to the tunnel configuration. Each header chains to the next using IP Protocol values. The outer IP header Source and Destination identify the "endpoints" of the tunnel. The inner IP header Source and Destination identify the original sender and recipient of the datagram, while the inner IP header is not changed by the encapsulator, except to decrement the TTL, and remains unchanged during its delivery to the tunnel exit point. No change to IP options in the inner header occurs during delivery of the encapsulated datagram through the tunnel. If needed, other protocol headers such as the IP Authentication header may be inserted between the outer IP header and the inner IP header.

The Mobile IP working group has specified the use of encapsulation as a way to deliver datagrams from an MN's HA to an FA, and conversely from an FA to an HA, that can deliver the data locally to the MN at its current location.

GRE tunnels

The Generic Routing Encapsulation (GRE) protocol performs encapsulation of IP packets for transport across disparate networks. One advantage of GRE over earlier tunneling protocols is that any transport protocol can be encapsulated in GRE. GRE is a simple, low overhead approach—the GRE protocol itself can be expressed in as few as eight octets as there is no authentication or tunnel configuration parameter negotiation. GRE is also known as IP Protocol 47.

Important The chassis simultaneously supports GRE protocols with key in accordance with RFC-1701/RFC-2784 and "Legacy" GRE protocols without key in accordance to RFC-2002.

Another advantage of GRE tunneling over IP-in-IP tunneling is that GRE tunneling can be used even when conflicting addresses are in use across multiple contexts (for the tunneled data).

Communications between the FA and HA can be done in either the forward or reverse direction using the above protocols. Additionally, another method of routing information between the FA and various content servers used by the HA exists. This method is called Triangular Routing. Each of these methods is explained below.

Forward Tunneling

In the wireless IP world, forward tunneling is a tunnel that transports packets from the packet data network towards the MN. It starts at the HA and ends at the MN's care-of address. Tunnels can be as simple as IP-in-IP tunnels, GRE tunnels, or even IP Security (IPSec) tunnels with encryption. These tunnels can be started automatically, and are selected based on the subscriber's user profile.

Reverse Tunneling

A reverse tunnel starts at the MN's care-of address, which is the FA, and terminates at the HA.

When an MN arrives at a foreign network, it listens for agent advertisements and selects an FA that supports reverse tunnels. The MN requests this service when it registers through the selected FA. At this time, the MN may also specify a delivery technique such as Direct or the Encapsulating Delivery Style.

Using the Direct Delivery Style, which is the default mode for the system, the MN designates the FA as its default router and sends packets directly to the FA without encapsulation. The FA intercepts them, and tunnels them to the HA.

Using the Encapsulating Delivery Style, the MN encapsulates all its outgoing packets to the FA. The FA then de-encapsulates and re-tunnels them to the HA, using the FA's care-of address as the entry-point for this new tunnel.

Following are some of the advantages of reverse tunneling:

- All datagrams from the mobile node seem to originate from its home network
- The FA can keep track of the HA that the mobile node is registered to and tunnel all datagrams from the mobile node to its HA

Triangular Routing

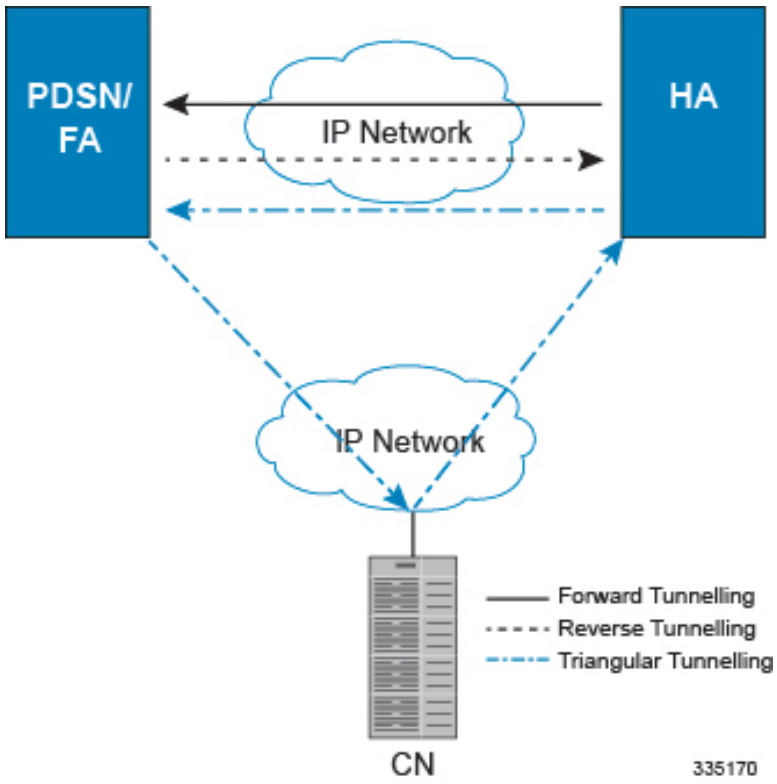
Triangular routing is the path followed by a packet from the MN to the Correspondent Node (CN) via the FA. In this routing scenario, the HA receives all the packets destined to the MN from the CN and redirects them to the MN's care-of-address by forward tunneling. In this case, the MN sends packets to the FA, which are transported using conventional IP routing methods.

A key advantage of triangular routing is that reverse tunneling is not required, eliminating the need to encapsulate and de-capsulate packets a second time during a Mobile IP session since only a forward tunnel exists between the HA and PDSN/FA.

A disadvantage of using triangular routing is that the HA is unaware of all user traffic for billing purposes. Also, both the HA and FA are required to be connected to a private network. This can be especially troublesome in large networks, serving numerous enterprise customers, as each FA would have to be connected to each private network.

The following figure shows an example of how triangular routing is performed.

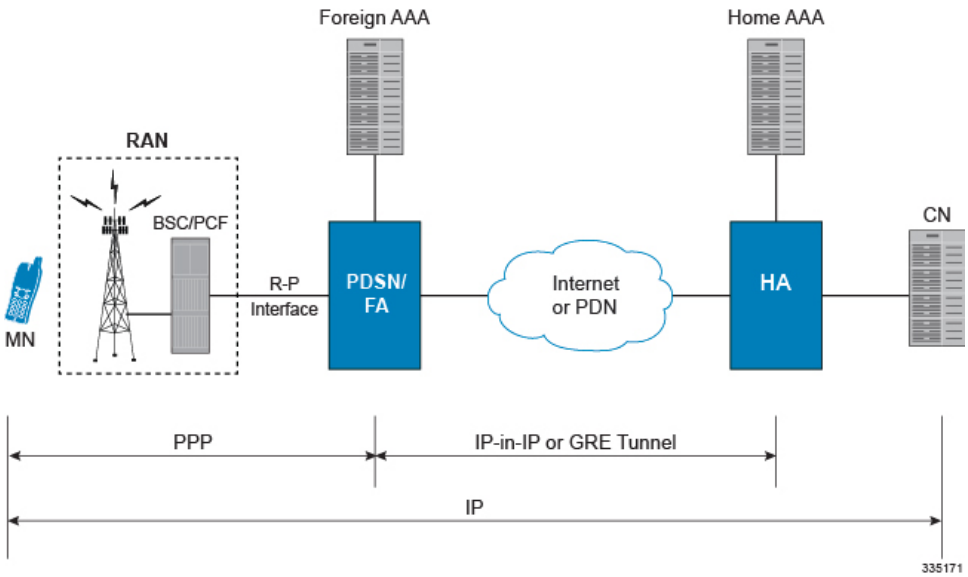
Figure 5: Mobile IP, FA and HA Tunneling/Transport Methods



How Mobile IP Works

As described earlier, Mobile IP uses three basic communications protocols PPP, IP, and Tunneled IP in the form of IP-in-IP or GRE tunnels. The following figure depicts where each of these protocols are used in a basic Mobile IP call.

Figure 6: Mobile IP Protocol Usage



As depicted in the figure above, PPP is used to establish a communications session between the MN and the FA. Once a PPP session is established, the MN can communicate with the HA, using the FA as a mediator or broker. Data transport between the FA and HA use tunneled IP, either IP-in-IP or GRE tunneling. Communication between the HA and End Host can be achieved using the Internet or a private IP network and can use any IP protocol.

The following figure provides a high-level view of the steps required to make a Mobile IP call that is initiated by the MN to a HA and table that follows, explains each step in detail. Users should keep in mind that steps in the call flow related to the Radio Access Node (RAN) functions are intended to show a high-level overview of radio communications iterations, and as such are outside the scope of packet-based communications presented here.

Figure 7: Mobile IP Call Flow

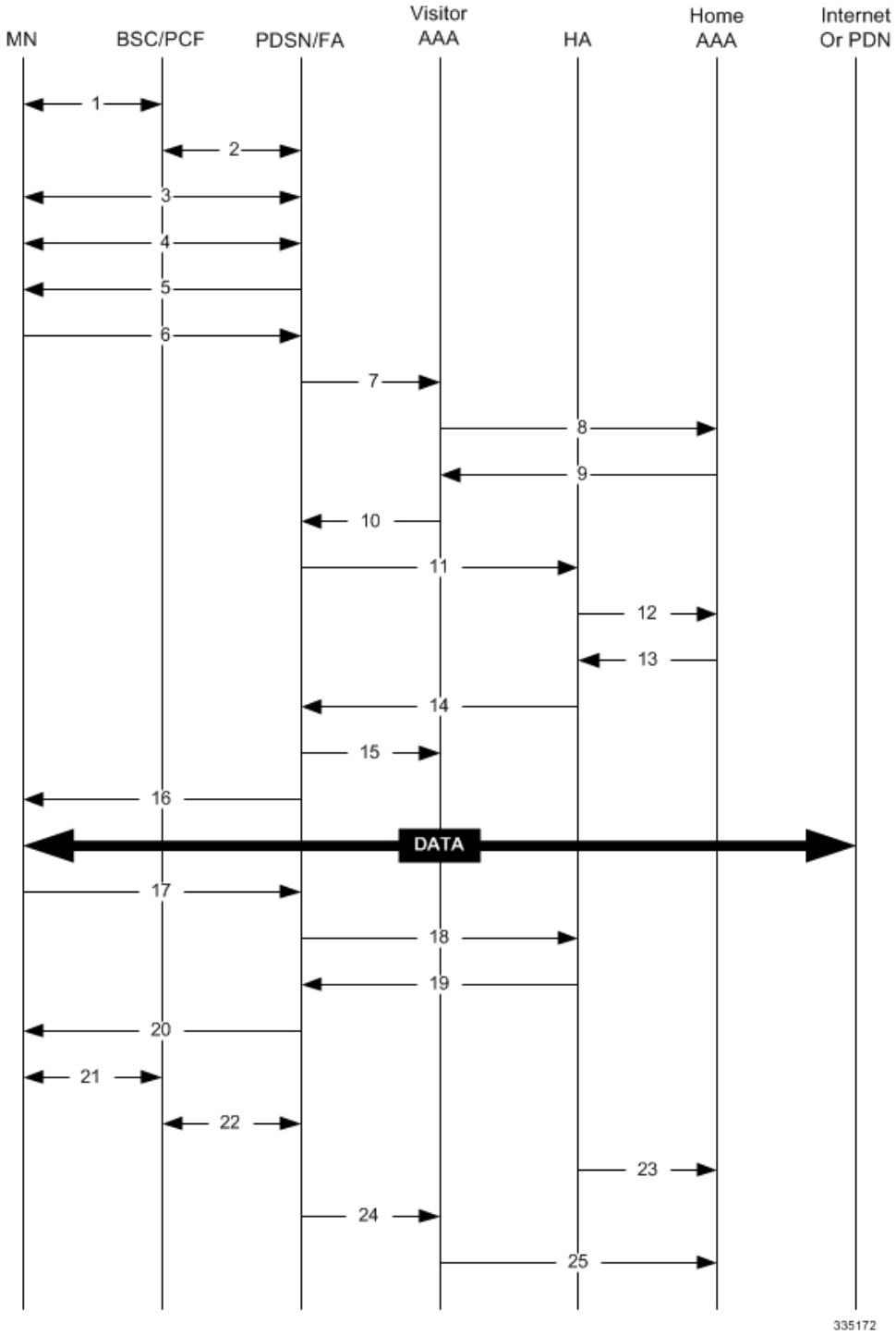


Table 2: Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the RAN through the BSC/PCF.
2	The PCF and PDSN establish the R-P interface for the session.
3	The PDSN and MN negotiate Link Control Protocol (LCP).
4	The PDSN and MN negotiate the Internet Protocol Control Protocol (IPCP).
5	The PDSN/FA sends an Agent Advertisement to the MN.
6	The MN sends a Mobile IP Registration Request to the PDSN/FA.
7	The PDSN/FA sends an Access Request message to the visitor AAA server.
8	The visitor AAA server proxies the request to the appropriate home AAA server.
9	The home AAA server sends an Access Accept message to the visitor AAA server.
10	The visitor AAA server forwards the response to the PDSN/FA.
11	Upon receipt of the response, the PDSN/FA forwards a Mobile IP Registration Request to the appropriate HA.
12	The HA sends an Access Request message to the home AAA server to authenticate the MN/subscriber.
13	The home AAA server returns an Access Accept message to the HA.
14	Upon receiving response from home AAA, the HA sends a reply to the PDSN/FA establishing a forward tunnel. Note that the reply includes a Home Address (an IP address) for the MN.
15	The PDSN/FA sends an Accounting Start message to the visitor AAA server. The visitor AAA server proxies messages to the home AAA server as needed.
16	The PDSN return a Mobile IP Registration Reply to the MN establishing the session allowing the MN to send/receive data to/from the PDN.

Step	Description
17	Upon session completion, the MN sends a Registration Request message to the PDSN/FA with a requested lifetime of 0.
18	The PDSN/FA forwards the request to the HA.
19	The HA sends a Registration Reply to the PDSN/FA accepting the request.
20	The PDSN/FA forwards the response to the MN.
21	The MN and PDSN/FA negotiate the termination of LCP effectively ending the PPP session.
22	The PCF and PDSN/FA close terminate the R-P session.
23	The HA sends an Accounting Stop message to the home AAA server.
24	The PDSN/FA sends an Accounting Stop message to the visitor AAA server.
25	The visitor AAA server proxies the accounting data to the home AAA server.

Proxy Mobile IP

Proxy Mobile IP provides mobility for subscribers with MNs that do not support the Mobile IP protocol stack.

For subscriber sessions using Proxy Mobile IP, R-P and PPP sessions get established as they would for a Simple IP session. However, the PDSN/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN while the MN performs only Simple IP processes. The protocol details are similar to those displayed in figure earlier for Mobile IP.

The MN is assigned an IP address by either the PDSN/FA or the HA. Regardless of its source, the address is stored in a Mobile Binding Record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will receive the same IP address stored in the MBR on the HA.

Note that unlike Mobile IP-capable MNs that can perform multiple sessions over a single PPP link, Proxy Mobile IP allows only a single session over the PPP link. In addition, simultaneous Mobile and Simple IP sessions will not be supported for an MN by an FA currently facilitating a Proxy Mobile IP session for the MN.

How Proxy Mobile IP Works

This section contains call flows displaying successful Proxy Mobile IP session setup scenarios. Two scenarios are described based on how the MN receives an IP address:

- **Scenario 1:** The AAA server specifies an IP address that the PDSN allocates to the MN from one of its locally configured static pools.
- **Scenario 2:** The HA assigns an IP address to the MN from one of its locally configured dynamic pools.

Scenario 1: AAA server and PDSN/FA Allocate IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the AAA server and PDSN/FA.

Figure 8: AAA/PDSN Assigned IP Address Proxy Mobile IP Call Flow

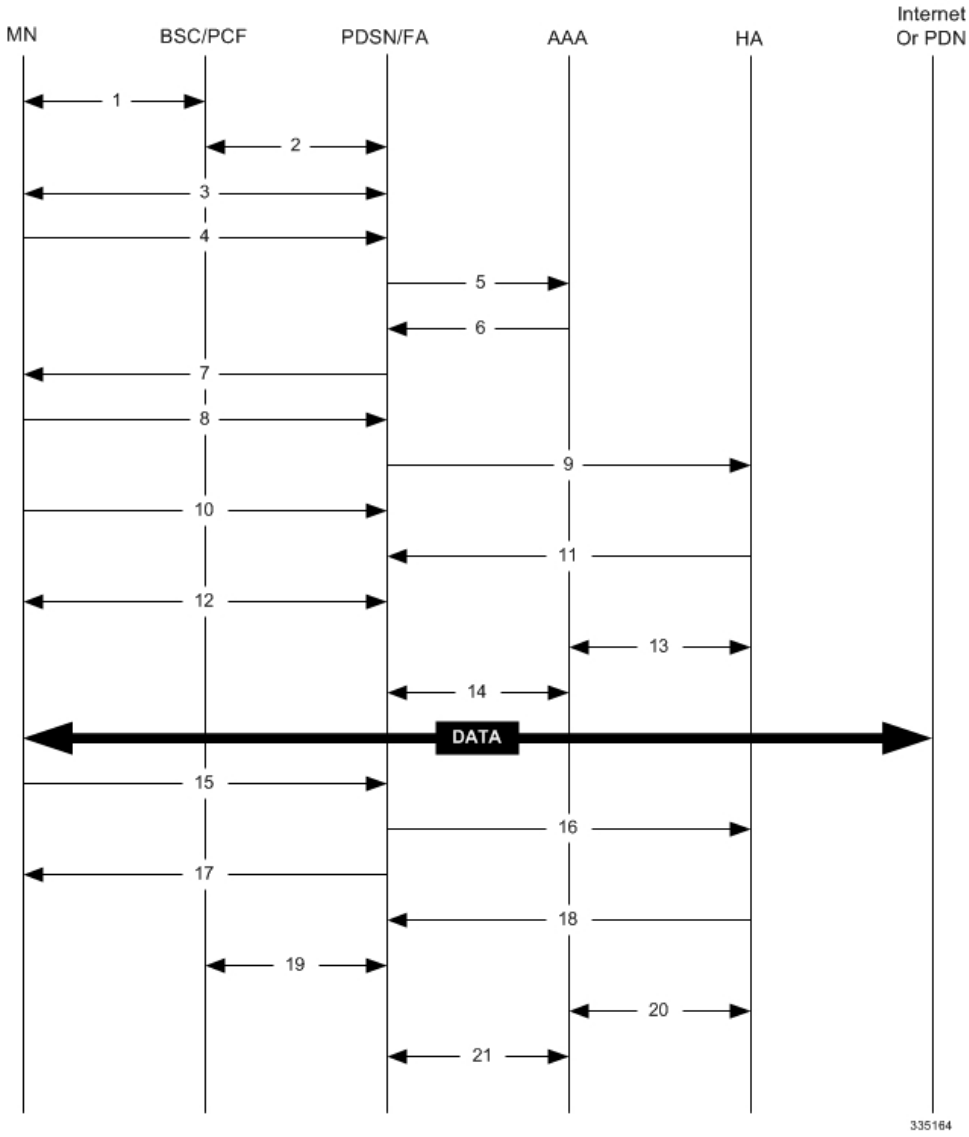


Table 3: AAA/PDSN Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the RAN through the BSC/PCF.
2	The PCF and PDSN/FA establish the R-P interface for the session.

Step	Description
3	The PDSN/FA and MN negotiate Link Control Protocol (LCP).
4	Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the PDSN/FA.
5	The PDSN/FA sends an Access Request message to the RADIUS AAA server.
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the PDSN/FA. The Accept message may contain various attributes to be assigned to the MN including the MN's Home Address (IP address) and the IP address of the HA to use.
7	The PDSN/FA sends a PPP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the PDSN/FA with an MN address of 0.0.0.0.
9	The PDSN/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes such things as the MN's home address, the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.
11	The HA responds with a Proxy Mobile IP Registration Response after validating the home address against it's pool(s). The HA also creates a Mobile Binding Record (MBR) for the subscriber session.
12	The MN and the PDSN/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.
13	While the MN and PDSN/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the PDSN/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the PDSN to end the PPP session.

Step	Description
16	The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The PDSN/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the Pi interface
19	The PDSN/FA and the PCF terminate the R-P session.
20	The HA and the AAA server stop accounting for the session.
21	The PDSN and the AAA server stop accounting for the session.

Scenario 2: HA Assigns IP Address to MN from Locally Configured Dynamic Pools

The following figure and table display and describe a call flow in which the MN receives its IP address from the AAA server and PDSN/FA.

Figure 9: HA Assigned IP Address Proxy Mobile IP Call Flow

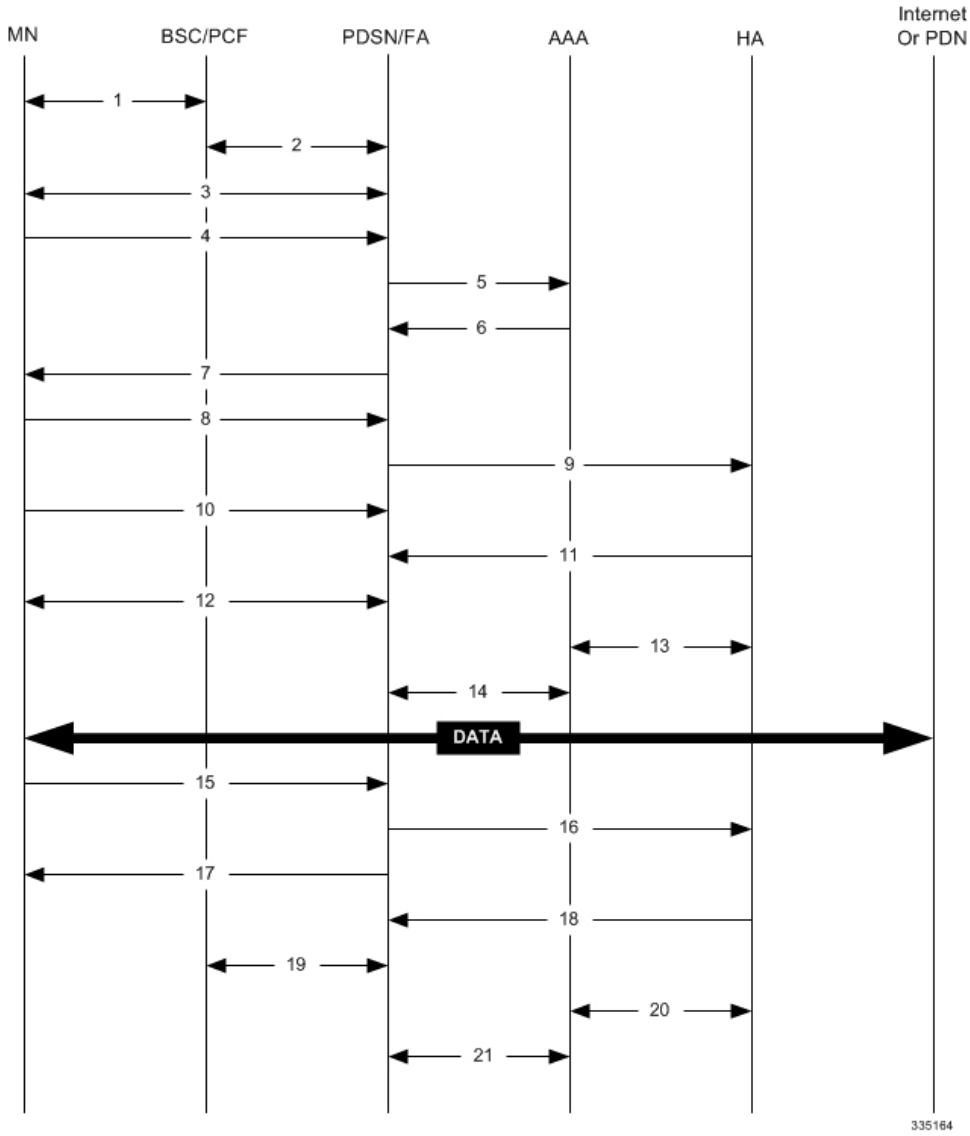


Table 4: HA Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the RAN through the BSC/PCF.
2	The PCF and PDSN/FA establish the R-P interface for the session.
3	The PDSN/FA and MN negotiate Link Control Protocol (LCP).

Step	Description
4	Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the PDSN/FA.
5	The PDSN/FA sends an Access Request message to the RADIUS AAA server.
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the PDSN/FA. The Accept message may contain various attributes to be assigned to the MN including the IP address of the HA to use.
7	The PDSN/FA sends a PPP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the PDSN/FA with an MN address of 0.0.0.0.
9	The PDSN/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes such things as a Home Address indicator of 0.0.0.0, the IP address of the FA (the care-of-address), the IP address of the FA (the care-of-address), and the FA-HA extension (Security Parameter Index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.
11	The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MN (its Home Address). The HA also creates a Mobile Binding Record (MBR) for the subscriber session.
12	The MN and the PDSN/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.
13	While the MN and PDSN/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the PDSN/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the PDSN to end the PPP session.

Step	Description
16	The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The PDSN/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the Pi interface
19	The PDSN/FA and the PCF terminate the R-P session.
20	The HA and the AAA server stop accounting for the session.
21	The PDSN and the AAA server stop accounting for the session.

Supported Standards

The system supports the following industry standards for 1x/CDMA2000/EV-DO devices.

Requests for Comments (RFCs)

- RFC-768, User Datagram Protocol (UPD), August 1980
- RFC-791, Internet Protocol (IP), September 1982
- RFC-793, Transmission Control Protocol (TCP), September 1981
- RFC-894, A Standard for the Transmission of IP Datagrams over Ethernet Networks, April 1984
- RFC-1089, SNMP over Ethernet, February 1989
- RFC-1144, Compressing TCP/IP headers for low-speed serial links, February 1990
- RFC-1155, Structure and Identification of Management Information for TCP/IP-based Internets, May 1990
- RFC-1157, Simple Network Management Protocol (SNMP) Version 1, May 1990
- RFC-1212, Concise MIB Definitions, March 1991
- RFC-1213, Management Information Base for Network Management of TCP/IP-based Internets: MIB-II, March 1991
- RFC-1215, A Convention for Defining Traps for use with the SNMP, March 1991
- RFC-1224, Techniques for Managing Asynchronously Generated Alerts, May 1991
- RFC-1256, ICMP Router Discovery Messages, September 1991
- RFC-1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis, March 1992
- RFC-1332, The PPP Internet Protocol Control Protocol (IPCP), May 1992

- RFC-1398, Definitions of Managed Objects for the Ethernet-Like Interface Types, January 1993
- RFC-1418, SNMP over OSI, March 1993
- RFC-1570, PPP LCP Extensions, January 1994
- RFC-1643, Definitions of Managed Objects for the Ethernet-like Interface Types, July 1994
- RFC-1661, The Point to Point Protocol (PPP), July 1994
- RFC-1662, PPP in HDLC-like Framing, July 1994
- RFC-1701, Generic Routing Encapsulation (GRE), October 1994
- RFC-1771, A Border Gateway Protocol 4 (BGP-4)
- RFC-1850, OSPF Version 2 Management Information Base, November 1995
- RFC-1901, Introduction to Community-based SNMPv2, January 1996
- RFC-1902, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1903, Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1904, Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1905, Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1906, Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1907, Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1908, Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework, January 1996
- RFC-1918, Address Allocation for Private Internets, February 1996
- RFC-1919, Classical versus Transparent IP Proxies, March 1996
- RFC-1962, The PPP Compression Control Protocol (CCP), June 1996
- RFC-1974, PPP STAC LZS Compression Protocol, August 1996
- RFC-2002, IP Mobility Support, May 1995
- RFC-2003, IP Encapsulation within IP, October 1996
- RFC-2004, Minimal Encapsulation within IP, October 1996
- RFC-2005, Applicability Statement for IP Mobility Support, October 1996
- RFC-2118, Microsoft Point-to-Point Compression (MPPC) Protocol, March 1997
- RFC-2136, Dynamic Updates in the Domain Name System (DNS UPDATE)

- RFC-2211, Specification of the Controlled-Load Network Element Service
- RFC-2246, The Transport Layer Security (TLS) Protocol Version 1.0, January 1999
- RFC-2290, Mobile IPv4 Configuration Option for PPP IPCP, February 1998
- RFC-2328, OSPF Version 2, April 1998
- RFC-2344, Reverse Tunneling for Mobile IP, May 1998
- RFC-2394, IP Payload Compression Using DEFLATE, December 1998
- RFC-2401, Security Architecture for the Internet Protocol, November 1998
- RFC-2402, IP Authentication Header (AH), November 1998
- RFC-2406, IP Encapsulating Security Payload (ESP), November 1998
- RFC-2408, Internet Security Association and Key Management Protocol (ISAKMP), November 1998
- RFC-2409, The Internet Key Exchange (IKE), November 1998
- RFC-2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998
- RFC-2475, An Architecture for Differentiated Services, December 1998
- RFC-2484, PPP LCP Internationalization Configuration Option, January 1999
- RFC-2486, The Network Access Identifier (NAI), January 1999
- RFC-2571, An Architecture for Describing SNMP Management Frameworks, April 1999
- RFC-2572, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), April 1999
- RFC-2573, SNMP Applications, April 1999
- RFC-2574, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), April 1999
- RFC-2597, Assured Forwarding PHB Group, June 1999
- RFC2598 - Expedited Forwarding PHB, June 1999
- RFC-2618, RADIUS Authentication Client MIB, June 1999
- RFC-2620, RADIUS Accounting Client MIB, June 1999
- RFC-2661, Layer Two Tunneling Protocol "L2TP", August 1999
- RFC-2697, A Single Rate Three Color Marker, September 1999
- RFC-2698, A Two Rate Three Color Marker, September 1999
- RFC-2784, Generic Routing Encapsulation (GRE) - March 2000, IETF
- RFC-2794, Mobile IP Network Access Identifier Extension for IPv4, March 2000
- RFC-2809, Implementation of L2TP Compulsory Tunneling via RADIUS, April 2000
- RFC-2845, Secret Key Transaction Authentication for DNS (TSIG), May 2000

- RFC-2865, Remote Authentication Dial In User Service (RADIUS), June 2000
- RFC-2866, RADIUS Accounting, June 2000
- RFC-2867, RADIUS Accounting Modifications for Tunnel Protocol Support, June 2000
- RFC-2868, RADIUS Attributes for Tunnel Protocol Support, June 2000
- RFC-2869, RADIUS Extensions, June 2000
- RFC-3007, Secure Domain Name System (DNS) Dynamic Update, November 2000
- RFC-3012, Mobile IPv4 Challenge/Response Extensions, November 2000
- RFC-3095, Robust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP and uncompressed, July 2001
- RFC-3101, OSPF NSSA Option, January 2003.
- RFC-3141, CDMA2000 Wireless Data Requirements for AAA, June 2001
- RFC-3143, Known HTTP Proxy/Caching Problems, June 2001
- RFC-3193, Securing L2TP using IPSEC, November 2001
- RFC-3241 Robust Header Compression (ROHC) over PPP, April 2002
- RFC-3409, Lower Layer Guidelines for Robust (RTP/UDP/IP) Header Compression, December 2002
- RFC-3519, NAT Traversal for Mobile IP, April 2003
- RFC-3543, Registration Revocation in Mobile IPv4, August 2003
- RFC 3576 - Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), July 2003
- RFC-3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers, February 2004
- RFC-3759, Robust Header Compression (ROHC): Terminology and Channel Mapping Examples, April 2004
- RFC-3588, Diameter Based Protocol, September 2003
- RFC-4005, Diameter Network Access Server Application, August 2005
- RFC-4006, Diameter Credit-Control Application, August 2005
- Draft, Generalized Key Distribution Extensions for Mobile IP
- Draft, AAA Keys for Mobile IP

TIA and Other Standards

Telecommunications Industry Association (TIA) Standards

- TIA/EIA/IS-835-A, CDMA2000 Wireless IP Network Standard, April 2001
- TIA/EIA/IS-835-B, CDMA2000 Wireless IP Network Standard, October 2002

- TIA/EIA/IS-835-C, CDMA2000 Wireless IP Network Standard, August 2003
- TIA/EIA/IS-707-A-1, Data Service Options for Wideband Spread Spectrum Systems
- TIA/EIA/IS-707-A.5 Packet Data Services
- TIA/EIA/IS-707-A.9 High Speed Packet Data Services
- TIA/EIA/IS-2000.5, Upper Layer (Layer 3) Signaling for CDMA2000 Spread Spectrum Systems
- TIA/EIA/IS-2001, Interoperability Specifications (IOS) for CDMA2000 Access Network Interfaces
- TIA/EIA/TSB100, Wireless Network Reference Model
- TIA/EIA/TSB115, CDMA2000 Wireless IP Architecture Based on IETF Protocols
- TIA/EIA J-STD-025 PN4465, TR-45 Lawfully Authorized Electronic Surveillance

Object Management Group (OMG) Standards

- CORBA 2.6 Specification 01-09-35, Object Management Group

3GPP2 Standards

- 3GPP2 A.S0001-A v2: 3GPP2 Access Network Interfaces Interoperability Specification (also known as 3G-IOS v4.1.1)
- 3GPP2 P.S0001-A-3: Wireless IP Network Standard
- 3GPP2 P.S0001-B: Wireless IP Network Standard
- 3GPP2 S.R0068: Link Layer Assisted Robust Header Compression
- [9] 3GPP2 C.S0047-0: Link Layer Assisted Service Options for Voice-over-IP: Header Removal (SO60) and Robust Header Compression (SO61)
- 3GPP2 A.S0008 v3.0 Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Access Network Interfaces
- 3GPP2 A.S0015-0 v2: Interoperability Specification (IOS) for CDMA2000 11 Access Network Interfaces — Part 5 (A3 and A7 12 Interfaces) (Partial Support) (also know as 3G-IOSv4.2)
- 3GPP2 P.S0001-B V1.0.0 Wireless IP Network Standard October 25, 2002 (relating to MIP interactions with IPSEC)
- 3GPP2 P.S0001 (TIA/EIA/IS-835-1) Version 1.0, Wireless IP Network Standard - December 10, 1999
- 3GPP2 P.R0001 (TSB115) Version 1.0.0, Wireless IP: Architecture Based on IETF Protocols - July 14, 2000
- 3GPP2 3GPP2 X.S0011-005-C Version: 1.0.0, CDMA2000 Wireless IP Network Standard: Accounting Services and 3GPP2 RADIUS VSAs - August 2003
- 3GPP2 X.S0011-006-C Version: 1.0.0, CDMA2000 Wireless IP Network Standard: PrePaid Packet Data Service - Date: August 2003
- 3GPP2 TSGA A.S0013-c v0.4 Interoperability Specification (IOS) for CDMA2000 June 2004

- 3GPP2 TSG-A A.S.0017-C baseline Interoperability Specification (IOS) for CDMA2000 Access Network Interfaces - Part 7(A10 and A11 Interfaces) (IOS v5.0 baseline) June 2004
- 3GPP2 A.S0012-D Segmentation for GRE January, 2005
- Inter-operability Specification (IOS) for CDMA2000 Access Network Interfaces
- 3GPP2 X.S0011-005-D Accounting Services and 3GPP2 RADIUS VSAs, February 2006
- 3GPP2 TSG-X (PSN) X.P0013-014-0, Service Based Bearer Control – Ty Interface Stage-3

IEEE Standards

- 802.1Q VLAN Standard