Tech Mahindra Access Registrar 9.3 Reference Guide

Tech Mahindra connected in 70+ countries worldwide.
Addresses, phone numbers, and fax numbers are listed on the Tech Mahindra website at
www.techmahindra.com/contact-us/

Table of Contents

Chapter 1 11

Overview 11

Tech Mahindra Access Registrar Directory Structure 12

Program Flow 12

Scripting Points 13

Client Scripting 13

Client or NAS Scripting Points 14

Authentication and/or Authorization Scripting Points 14

Script Processing Hierarchy 15

Service and Ports Used in Tech Mahindra Access Registrar 16

Secure Shell Service 16

Ports 16

Related Documentation 21

Chapter 2 22

RADIUS Accounting Log 22

Accounting Log Examples 22

Accounting-Start Packet 22

Accounting Stop Packet 22

Trace of Successful Accounting 23

Sample Error Messages 23

Chapter 3 25

Using WiMAX in Tech Mahindra Access Registrar 25

WiMAX - An Overview 25

WiMAX in Tech Mahindra Access Registrar 26

Direct Interaction Between the ASN GW and Tech Mahindra Access Registrar 27

Interaction Between ASN GW and Tech Mahindra Access Registrar Through HA 30

Prepaid and Hot-Lining 31

Configuring WiMAX in Tech Mahindra Access Registrar 31

Configuring the Resource Manager for WiMAX 32

Configuring the Session Manager for WiMAX 33

Configuring the Query Service for WiMAX 33

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Configuring WiMAX 34
WiMAX - OMA-DM Provisioning Support with BEK Key 35
Chapter 4 38
Replication Log 38
Frequently Asked Questions 38
Replication Log Messages 39
Information Log Messages 40
Warning Log Messages 41
Error Log Messages 42
Log Messages You Should Never See 43
Chapter 5 45
Using On-Demand Address Pools 45
Techm-Incoming Script 47
How the Script Works 47
TechmWithODAPIncomingScript 47
Vendor Type TechmWithODAP 48
Configuring Tech Mahindra Access Registrar to Work with ODAP 49
Configuring Tech Mahindra Access Registrar to work with ODAP 49
Configuring the ODAP Detailed Instructions 49
Setting Up an ODAP UserList 49
Adding ODAP Users 50
Setting Up an ODAP-Users Service 51
Setting Up an ODAP Accounting Service 52
Adding Session Managers 52
Setting Up Resource Managers 53
Configuring Session Managers 58
Configure Clients 59
Save Your Configuration 60
Chapter 6 61
Wireless Support 61
Mobile Node-Home Agent Shared Key 61
Use Case Example 62
Configuring User Attributes 62
3GPP2 Home Agent Support 63
Home-Agent Resource Manager 63

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Load Balancing 63
Querying and Releasing Sessions 64
Access Request Requirements 65
New 3GPP2 VSAs in the Tech Mahindra Access Registrar Dictionary 65
Session Correlation Based on User-Defined Attributes 65
Managing Multiple Accounting Start/Stop Messages 66
NULL Password Support 66
3GPP Compliance 67
SWa Access Authentication and Authorization 68
STa Access Authentication and Authorization 68
SWm Access Authentication and Authorization 69
SWd Access Authentication and Authorization 69
SWx Authentication Procedure 70
HSS Initiated Update of User Profile 70
S6b Authentication and Authorization Procedure 70
3GPP Call Flows 71
CLI for 3GPP Authorization 72
CLI for 3GPP Reverse Authorization 73
Voice over Wi-Fi (VoWiFi) Location Based Authentication 73
Mobile Equipment Identity Check Support in Tech Mahindra Access Registrar 75
5G Data Network-AAA (DN-AAA) Compliance 76
Chapter 7 78
Enforcement of Licensing Models 78
TPS Licensing Features 78
Enforcement Rules 78
Notification Logs 79
Notification - SNMP Traps 79
TPS Logging Feature 80
Concurrent Session License Features 80
Sessions Enforcement Rules 81
Notification Logs 81
Notification - SNMP Traps 82
Session Logging Feature 82
Chapter 8 83
Logging Syslog Messages 83

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Syslog Messages 83
Example 1 84
Example 2 85
Configuring Message Logging 85
Configuring Syslog Daemon (syslogd) 86
Changing Log Directory 86
Managing the Syslog File 87
Using a cron Program to Manage the Syslog Files 87
Server Up/Down Status Change Logging 88
Header Formats 88
Example Log Messages 88
Logging Subscriber Data 89
Logging User IP Information 89
Support for Logging Timeout Packets 89
Logging System Statistics 90
Logging Worker Queue Size 91
Chapter 9 92
Troubleshooting Tech Mahindra Access Registrar 92
Gathering Basic Information 92
Troubleshooting Quick Checks 93
Disk Space 93
Resource Conflicts 93
No Co-Existence With Cisco Prime Network Registrar 93
Port Conflicts 94
Tech Mahindra Access Registrar Log Files 94
Modifying File Sizes for Agent Server and MCD Server Logs 95
Using xtail to Monitor Log File Activity 95
Modifying the Trace Level 95
Installation and Server Process Start-up 96
aregcmd and Tech Mahindra Access Registrar Configuration 97
Running and Stopped States 97
RADIUS Request Processing 99
Other Troubleshooting Techniques and Resources 99
aregcmd Stats Command 99
Core Files 100
radclient 100

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Tech Mahindra Access Registrar Replication 100
Checking Tech Mahindra Access Registrar Server Health Status 100
Appendix A 102
Tech Mahindra Access Registrar Tcl, REX, and Java Dictionaries 102
Tcl Attribute Dictionaries 102
Attribute Dictionary Methods 102
Tcl Environment Dictionary 105
REX Attribute Dictionary 106
Attribute Dictionary Methods 106
REX Environment Dictionary 112
REX Environment Dictionary Methods 112
Java Attribute Dictionary 114
Java Attribute Dictionary Methods 114
Java Environment Dictionary 117
Java Environment Dictionary Methods 117
Interface Extension 118
Interface Extension Methods 119
Interface ExtensionforSession 119
Interface Extensionforsession Methods 120
Interface Extensionwithinitialization 120
Interface Extensionwithinitialization Methods 121
Interface ExtensionforSessionwithinitialization 121
Interface Extensionforsessionwithinitialization Methods 121
Interface MarkerExtension 121
Variables in the Marker Extension Interface 122
Class Sessionrecord 125
Session Record Methods 125
Appendix B 127
Environment Dictionary 127
Tech Mahindra Access Registrar Environment Dictionary Variables 127
Accepted-Profiles 128
Accounting-Service 128
Acquire-Dynamic-DNS 128
Acquire-Group-Session-Limit 128
Acquire-Home-Agent 128

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Acquire-IP-Dynamic 128
Acquire-IPX-Dynamic 128
Acquire-IP-Per-NAS-Port 129
Acquire-Subnet-Dynamic 129
Acquire-User-Session-Limit 129
Acquire-USR-VPN 129
Allow-Null-Password 129
Authentication-Service 129
Authorization-Service 129
AuthorizationInfo 130
BackingStore-Env-Vars 130
Blacklisted-IMSI 130
Broadcast-Accounting-Packet 130
Cache-Attributes-In-Session 130
Current-Group-Count 130
Cache-Outer-Identity 130
Destination-IP-Address 130
Destination-Port 131
Dest-Translation-Type 131
Dest-Numbering-Plan 131
Dest-Encoding-Scheme 131
Dest-Nature-Of-Address 132
Dest-GT-Format 132
Diameter-Application-Id 132
Diameter-Command-Code 133
Disable-Accounting-On-Off-Broadcast 133
DSA-Response-Cache 133
Dynamic-DNS-HostName 133
Dynamic-Search-Filter 133
Dynamic-Search-Path 133
Dynamic-Search-Scope 133
Dynamic-Service-Loop-Limit 134
Dynamic-User-Password-Attribute 134
EAP-Actual-Identity 134
EAP-Authentication-Mode 134

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

EnableMatchingServiceSelection5GFlag 134
Enforce-Traffic-Throttling 134
E-UTRANCellGlobalId 134
FetchAuthorizationInfo 134
Generate-BEK 135
Group-Session-Limit 135
HLR-GlobalTitle-Address 135
HLR-GlobalTitle-Cached 135
HLR-Translated-IMSI 135
Ignore-Accounting-Signature 136
IMSI 136
Incoming-Translation-Groups 136
Location-Capability 136
Master-URL-Fragment 136
Misc-Log-Message-Info 136
MSISDN 136
Notification-Code 137
Notification-Service 137
Outgoing-Translation-Groups 137
Pager 137
PoD/CoA 137
Query-Service 138
Re-Accounting-Service 138
Re-Authentication-Service 138
Re-Authorization-Service 138
Reject-Reason 138
Remote-Server 139
Remove-Session-On-Acct-Stop 139
Remote-Servers-Tried 139
Request-Authenticator 139
Request-Type 139
Require-User-To-Be-In-Authorization-List 140
Response-Type 140
Retrace-Packet 140
Send-PEAP-URI-TLV 141

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Session-Key 141
Session-Manager 141
Session-Notes 141
Session-Service 141
Set-Session-Mgr-And-Key-Upon-Lookup 141
Skip-Session-Management 141
Skip-Overriding-Username-With-LDAP-UID 142
Skip-Overriding-UserName-With-PEAPIdentity 142
Source-IP-Address 142
Source-Port 142
SQL-Sequence 142
Subnet-Size-If-No-Match 142
Trace-Level 143
Unavailable-Resource 143
Unavailable-Resource-Type 143
UserDefined1 143
User-Authorization-Script 143
User-Group 143
User-Group-Session-Limit 143
User-Name 143
User-Profile 144
User-Session-Limit 144
Virtual-Server-Outgoing-Script 144
X509- Subject-Name 144
Internal Variables 144
Appendix C 146
RADIUS Attributes 146
RADIUS Attributes 146
Tech Mahindra Access Registrar Attributes 146
RADIUS Attributes Numeric List 149
Vendor-Specific Attributes 158
3GPP VSAs 158
3GPP2 VSAs 160
ACC VSAs 167
Altiga VSAs 172

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Ascend VSAs 175
Bay Networks VSAs 190
Cabletron VSAs 191
Tech Mahindra Access Registrar Internal VSAs 191
Tech Mahindra VSAs 193
Compatible VSAs 196
Microsoft VSAs 196
Nomadix VSAs 198
RedBack VSAs 198
RedCreek VSAs 201
TACACS+ VSAs 201
Telebit VSAs 204
Unisphere VSAs 204
USR VSAs 205
WiMax 230
WISPr 230
XML 231
Configuring Unique TAG number for Vendor-Specific Sub Attributes 231
Appendix D 232
Support for REST API in Tech Mahindra Access Registrar 232
REST API Framework 232
REST API Services 233
CoA and PoD REST APIs 236
REST API Support for Query and Release Sessions 238
Support for RADIUS to JSON and JSON to RADIUS Translation 239
CSRF Token Implementation using REST 240
Appendix E 241
Supported Counters and Error Statistics 241
Interface-Level KPI Counters 241
Error Statistics (error-stats) 249
Appendix F 256
Health Monitoring in Tech Mahindra Access Registrar 256

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Chapter 1

Overview

The chapter provides an overview of the RADIUS server, including connection steps, RADIUS message types, and using Tech Mahindra Access Registrar as a proxy server.

Tech Mahindra Access Registrar is a 3GPP-compliant, 64-bit carrier-class RADIUS (Remote Authentication Dial-In User Service)/Diameter server that enables multiple dial-in Network Access Server (NAS) devices to share a common authentication, authorization, and accounting database.

Tech Mahindra Access Registrar handles the following tasks:

- Authentication—determines the identity of users and whether they can be allowed to access the network
- Authorization—determines the level of network services available to authenticated users after they are connected
- Accounting—keeps track of each user's network activity
- Session and resource management—tracks user sessions and allocates dynamic resources

Using a RADIUS server allows you to better manage the access to your network, as it allows you to store all security information in a single, centralized database instead of distributing the information around the network in many different devices. You can make changes to that single database instead of making changes to every network access server in your network.

Tech Mahindra Access Registrar also allows you to manage the complex interconnections of the new network elements in order to:

- adequately manage the traffic
- perform appropriate load balancing for desired load distribution
- allow binding of different protocol interfaces corresponding to a subscriber/network element

Service providers transform their 3G and 4G wireless networks with complex services, tiered charging, converged billing, and more by introducing increasing numbers and types of Diameter-based network elements. LTE and IMS networks are the most likely to implement these new network elements—including Policy and Charging Rules Functions (PCRF), Home Subscriber Servers (HSS), Mobility Management Entities (MME), Online Charging Systems (OCS), and others. As a result, as the traffic levels grow, these wireless networks are becoming more difficult to manage and scale without the Tech Mahindra Access Registrar infrastructure.

Tech Mahindra Access Registrar allows GUI-based, CLI-based, and REST API-based configurations. For more details, see the "Using the Graphical User Interface" chapter of the *Tech Mahindra Access Registrar 9.3 User Guide*, the "Using the aregcmd Commands" chapter of the *Tech Mahindra Access Registrar 9.3 Administrator Guide*, and Chapter D, "REST API Framework."

This chapter contains the following sections:

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

- Tech Mahindra Access Registrar Directory Structure
- Program Flow
- Service and Ports Used in Tech Mahindra Access Registrar

Tech Mahindra Access Registrar Directory Structure

The installation process populates the **/opt/TMar** directory with the subdirectories listed in Table 1-1.

Table 1-1 /opt/TMar Subdirectories

Subdirectory	Description
.system	Contains ELFs, or binary SPARC executables that should not be run directly.
bin	Contains shell scripts and programs frequently used by a network administrator; programs that can be run directly.
conf	Contains configuration files.
data	Contains the **radius** directory, which contains session backing files; and the **db** directory, which contains configuration database files.
examples	Contains documentation, sample configuration scripts, and shared library scripts.
lib	Contains Tech Mahindra Access Registrar software library files.
logs	Contains system logs and is the default directory for RADIUS accounting.
odbc	Contains Tech Mahindra Access Registrar ODBC files.
scripts	Contains sample scripts that you can modify to automate configuration, and to customize your RADIUS server.
temp	Used for temporary storage.
ucd-snmp	Contains the UCD-SNMP software Tech Mahindra Access Registrar uses.
usrbin	Contains a symbolic link that points to **bin.**

Program Flow

When a NAS sends a request packet to Tech Mahindra Access Registrar with a name and password, Tech Mahindra Access Registrar performs the following actions. Table 1-2 describes the flow without regard to scripting points.

Table 1-2 From Access-Request to Access-Accept

Tech Mahindra Access Registrar Server Action	Explanation
Receives an Access-Request	The Tech Mahindra Access Registrar server receives an Access-Request packet from a NAS.
Determines whether to accept the request	The Tech Mahindra Access Registrar server checks to see if the client's IP address is listed in **/Radius/Clients/**<*Name*>/<*IPAddress*>.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table 1-2 From Access-Request to Access-Accept (continued)

Tech Mahindra Access Registrar Server Action	Explanation
Invokes the policy SelectPolicy if it exists	The Tech Mahindra Policy Engine provides an interface to define and configure a policy and to apply the policy to the corresponding access-request packets.
Performs authentication and/or authorization	Directs the request to the appropriate service, which then performs authentication and/or authorization according to the type specified in **/Radius/Services/***<Name>*/*<Type>*.
Performs session management	Directs the request to the appropriate Session Manager.
Performs resource management for each Resource Manager in the SessionManager	Directs the request to the appropriate resource manager listed in **/Radius/SessionManagers/***<Name>*/*<ResourceManagers>*/*<Name>*, which then allocates or checks the resource according to the type listed in **/Radius/***<ResourceManagers>*/*<Name>*/*<Type>*.
Sends an Access-Accept	Creates and formats the response, and sends it back to the client (NAS).

Tech Mahindra Access Registrar supports Diameter with Extensible Authentication Protocol (EAP) functionality to enable authentication between NAS and a backend NAS Diameter authentication server. For more information, see the "Diameter" chapter of the *Tech Mahindra Access Registrar 9.3 User Guide*.

Tech Mahindra Access Registrar also support 3GPP compliance by implementing a set of protocols. To understand more about the 3GPP AAA server support and the call flow, see the "Wireless Support" chapter of the *Tech Mahindra Access Registrar 9.3 Reference Guide*.

Scripting Points

Tech Mahindra Access Registrar lets you invoke scripts you can use to affect the Request, Response, or Environment dictionaries. This section contains the following topics:

- Client Scripting
- Client or NAS Scripting Points
- Authentication and/or Authorization Scripting Points

Client Scripting

Though Tech Mahindra Access Registrar allows external code (Tcl/C/C++/Java) to be used by means of a script, custom service, policy engine, and so forth, while processing request, response, or while working with the environment dictionaries, it shall not be responsible for the scripts used and will not be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of the script.

Tech Mahindra Access Registrar also allows you to define internal scripts, by which you can add, modify, or delete attributes in the request, response, and environment dictionaries for RADIUS, Diameter, and TACACS+.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Client or NAS Scripting Points

Table 1-3 shows the location of the scripting points within the section that determines whether to accept the request from the client or NAS. Note, the scripting points are indicated with the asterisk (*****) symbol.

Table 1-3 Client or NAS Scripting Points

Action	Explanation
Receives an Access-Request.	The Tech Mahindra Access Registrar RADIUS server receives an Access-Request packet from a NAS.
Determines whether to accept the request.	The client's IP address listed in **/Radius/Clients/**<*Name*>**/IPAddress.**
***Executes the server's incoming script.	A script referred to in **/Radius/IncomingScript.**
***Executes the vendor's incoming script.	The vendor listed in /Radius/Clients/*Name*/Vendor, and is a script referred to in **/Radius/Vendors/**<*Name*>**/IncomingScript.**
***Executes the client's incoming script.	A script referred to in **/Radius/Clients/**<*Name*>**/IncomingScript.**
Determines whether to accept requests from this specific NAS.	
	/Radius/Advanced/RequireNASsBehindProxyBeInClientList set to TRUE.
	The NAS's Identifier listed in **/Radius/Clients/**<*Name*>, or its NAS-IP-Address listed in **/Radius/Clients/**<*Name*>**/IPAddress.**
If the client's IP address listed in /Radius/Clients/<*Name*>**/IPAddress is different:**	
***Executes the vendor's incoming script.	The vendor listed in **/Radius/Clients/***Name*/Vendor, and is a script referred to in **/Radius/Vendors/**<*Name*>**/IncomingScript.**
***Executes the client's incoming script.	The client listed in the previous /Radius/Clients/*Name*, and is a script referred to in /Radius/Clients/*Name*/IncomingScript.

Authentication and/or Authorization Scripting Points

Table 1-4 shows the location of the scripting points within the section that determines whether to perform authentication and/or authorization.

Table 1-4 Authentication and Authorization Scripting Points

Action	Explanation
Determines Service to use for authentication and/or authorization.	The Service name defined in the Environment dictionary variable **Authentication-Service**, and is the same as the Service defined in the Environment dictionary variable **Authorization-Service**.
	The Service name referred to by **/Radius/DefaultAuthenticationService**, and is the same as the Service defined in **/Radius/DefaultAuthorizationService**.
Performs authentication and/or authorization.	If the Services are the same, perform authentication and authorization.
	If the Services are different, just perform authentication.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table 1-4 Authentication and Authorization Scripting Points (continued)

Action	Explanation
***Executes the Service's incoming script.	A script referred to in **/Radius/Services/**<*Name*>**/IncomingScript**.
Performs authentication and/or authorization.	Based on the Service type defined in **/Radius/Services/**<*Name*>/<*Type*>.
***Executes the Service's outgoing script.	A script referred to in **/Radius/Services/**<*Name*>**/OutgoingScript**.
Determines whether to perform authorization.	The Service name defined in **/Radius/DefaultAuthorizationService**, if different than the Authentication Service.
***Executes the Service's incoming script.	A script referred to in **/Radius/Services/**<*Name*>**/IncomingScript**.
Performs authorization.	Checks that the Service type is defined in **/Radius/Services/**<*Name*>/<*Type*>.
***Executes the Service's outgoing script.	A script referred to in **/Radius/Services/**<*Name*>**/OutgoingScript**.

Script Processing Hierarchy

For request packets, the script processing order is from the most general to the most specific. For response packets, the processing order is from the most specific to the most general.

Table 1-5, Table 1-6, and Table 1-7 show the overall processing order and flow: (1-6) Incoming Scripts, (7-11) Authentication/Authorization Scripts, and (12-17) Outgoing Scripts.

Note The client and the NAS can be the same entity, except when the immediate client is acting as a proxy for the actual NAS.

Table 1-5 Tech Mahindra Access Registrar Processing Hierarchy for Incoming Scripts

Overall Flow Sequence	Incoming Scripts
1)	Radius.
2)	Vendor of the immediate client.
3)	Immediate client.
4)	Vendor of the specific NAS.
5)	Specific NAS.
6)	Service.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table 1-6 Tech Mahindra Access Registrar Processing Hierarchy for Authentication/Authorization Scripts

Overall Flow Sequence	Authentication/Authorization Scripts
7)	Group Authentication.
8)	User Authentication.
9)	Group Authorization.
10)	User Authorization.
11)	Session Management.

Table 1-7 Tech Mahindra Access Registrar Processing Hierarchy for Outgoing Script

Overall Flow Sequence	Outgoing Scripts
12)	Service.
13)	Specific NAS.
14)	Vendor of the specific NAS.
15)	Immediate client.
16)	Vendor of the immediate client.
17)	Radius.

Service and Ports Used in Tech Mahindra Access Registrar

Secure Shell Service

SSH Daemon(SSHD) is the daemon program which is used for ssh(1). It provides secure shell encrypted communications between two hosts over network.

In case of Tech Mahindra Access Registrar, SSH is used to connect to Tech Mahindra Access Registrar server and configure Tech Mahindra Access Registrar using CLI.

Ports

The following table lists the port numbers that are used for various services in Tech Mahindra Access Registrar for AAA.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table 1-8 Ports Used in Tech Mahindra Access Registrar

Names	Description	Port Numbers	Service of the Ports	Access from Network Node	Configuration Setting	Protocol Name and Reference
AR AAA Service	The RADIUS packet listener uses these ports by default.	1812-udp	RADIUS AA	Network Access Server	You can change the default or define new RADIUS port numbers under */Radius/Advanced/Ports* in the CLI and *Configuration > Advanced > Ports* in the GUI.	RADIUS AA (Authentication, and Authorization) service.
		1813-udp radacct	RADIUS Accounting	Network Access Server	You can change the default or define new RADIUS port numbers under */Radius/Advanced/Ports* in the CLI and *Configuration > Advanced > Ports* in the GUI.	RADIUS Accounting service. Refer to RFC 6733 for more information.
		3799/udp	RADIUS Dynamic Authorization (CoA/PoD)	Network Access Server	N/A	RADIUS Dynamic authorization which is used with (CoA/PoD) packet types.
AR AAA Service	The RADIUS packet TLS listener uses this port by default.	2083-rtls	RADIUS TLS	Network Access Server	You can change the default or define new RADIUS port numbers under */Radius/Advanced/Ports* in the CLI and *Configuration > Advanced > Ports* in the GUI.	RADIUS AAA over TLS communication

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table 1-8 Ports Used in Tech Mahindra Access Registrar (continued)

Names	Description	Port Numbers	Service of the Ports	Access from Network Node	Configuration Setting	Protocol Name and Reference
AR AAA Service	The TACACS+ packet listener uses this port by default.	49/tcp	TACACS+	Network Access Server	You can change the default or define new RADIUS port numbers under */Radius/Advanced/Ports* in the CLI and *Configuration > Advanced > Ports* in the GUI.	TACACS+ based on AAA service (Authentication, Authorization, and Accounting). Refer to RFC 1491 for more information.
AR AAA Service	The DIAMETER packet listener uses these ports by default.	3868/tcp	DIAMETER	Network Access Server	You can enable or disable this service in */Radius/Advanced/Diameter/IsDiameterEnabled*.	DIAMETER AA Service (Authentication, and Authorization) by tcp protocol. Refer to RFC 4005 for more information.
		3868/sctp	DIAMETER	Network Access Server	You can enable or disable this service in */Radius/Advanced/Diameter/IsDiameterEnabled*[1].	DIAMETER AA Service (Authentication, and Authorization) by SCTP protocol.
AR MCD Server	MCD is used to store Tech Mahindra Access Registrar configuration.	2786/tcp	MCD database Server	This service can be accessed from local host by Tech Mahindra Access Registrar radius and server agent process.	N/A	Proprietary IPC mechanism.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table 1-8 Ports Used in Tech Mahindra Access Registrar (continued)

Names	Description	Port Numbers	Service of the Ports	Access from Network Node	Configuration Setting	Protocol Name and Reference
AR Server Agent	AR Server Agent is used to log all the activities of Tech Mahindra Access Registrar processes.	2785/tcp	Internal IPC mechanism	This service can be accessed from local host by Tech Mahindra Access Registrar radius and server agent process.	N/A	Proprietary IPC mechanism.
AR GUI Service	Tech Mahindra Access Registrar GUI processes use these ports by default.	8080/tcp	AR HTTP service	This service is accessible from any end user desktop browser using http protocol.	You can change the default port numbers in editing the *server.xml* file.	Standard HTTP protocol
		8443/tcp	AR HTTPS service	This service is accessible from any end user desktop browser using https protocol.	You can change the default port numbers in editing the *server.xml* file.	Standard HTTPS protocol
		8005/tcp	Internally used by Apache Tomcat container	Local host	You can change the default port numbers in editing the *server.xml* file..	To shutdown Tomcat JVM service instance.
		8009/tcp	Apache Tomcat container AJP 1.3 Connector	Local host	You can change the default port numbers in editing the *server.xml* file.	Apache JServ protocol. AJP 1.3 Connector.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table 1-8 Ports Used in Tech Mahindra Access Registrar (continued)

Names	Description	Port Numbers	Service of the Ports	Access from Network Node	Configuration Setting	Protocol Name and Reference
SNMP Master Agent	SNMP Packet listener supports these ports by default.	161/udp	Simple Net Management Protocol	This service is accessible from any network management host.	Refer to net-snmp documentation for more information.	SNMP MIBs server
		162/udp	Traps for SNMP	This service is accessible to any SNMP trap client when you want to use net-snmp snmptrap daemon as a SNMP trap server.	Refer to SNMP chapter of the *Tech Mahindra Access Registrar 9.3 User Guide* for more information.	SNMP trap server
TMAR SIGTRAN Stack (radius)	Listen on these ports for internal configuration from stack manager events	9041/TCP	Stack Manager Configuration/Event Listener	This service can be accessed from local host by Tech Mahindra Access Registrar – Radius Process.	N/A	TMAR Specific IPC Protocol implementation
		9041/UDP	Stack Manager Configuration/Event Listener	This service can be accessed from local host by Tech Mahindra Access Registrar – Radius Process.	N/A	TMAR Specific IPC Protocol implementation

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table 1-8 Ports Used in Tech Mahindra Access Registrar (continued)

Names	Description	Port Numbers	Service of the Ports	Access from Network Node	Configuration Setting	Protocol Name and Reference
TMAR SIGTRAN stack manager(m3ua-stackmgr)	Configure stack and receive configuration from m3ua-cliclient	9100/TCP	SIGTRAN Stack Manager	This service can be accessed from local host by Tech Mahindra Access Registrar – Radius Process and m3ua-cliclient Process.	N/A	TMAR Specific IPC Protocol implementation
		9100/UDP	SIGTRAN Stack Manager	This service can be accessed from local host by Tech Mahindra Access Registrar – Radius Process and m3ua-cliclient Process.	N/A	TMAR Specific IPC Protocol implementation

1. If an error occurs while starting the Diameter SCTP interface, add **install sctp /bin/true** to /etc/modprobe.conf. Then, configure port 3868 with Type Diameter-TCP using aregcmd in /Radius/Advanced/Ports.

Related Documentation

For a complete list of Tech Mahindra Access Registrar documentation, see the *Tech Mahindra Access Registrar 9.3 Documentation Overview*.

Note We sometimes update the documentation after original publication. Therefore, you should also review the documentation on tmar.techmahindra.com for any updates.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Chapter 2

RADIUS Accounting Log

This chapter describes RADIUS accounting log information in Tech Mahindra Access Registrar . For more information about RADIUS accounting in Tech Mahindra Access Registrar, see the “RADIUS Accounting” chapter of the *Tech Mahindra Access Registrar 9.3 User Guide*.

This chapter contains the following sections:

- Accounting Log Examples
- Sample Error Messages

Accounting Log Examples

This section provides examples of accounting log information recorded in an accounting log file.This section contains the following topics:

- Accounting-Start Packet
- Accounting Stop Packet
- Trace of Successful Accounting

Accounting-Start Packet

The Accounting-Start packet describes the type of service and the user attempting to login.

```
Tue, 06 Dec 2013 12:32:17.036
        User-Name = bob
        NAS-Port = 1
        Framed-IP-Address = 1.1.1.1
        Class = yahoo.com
        NAS-Identifier = localhost
        Acct-Status-Type = Start
        Acct-Session-Id = 1
```

Accounting Stop Packet

When the session ends, the NAS sends an Accounting Stop packet that describe the type of service that was delivered. The Accounting Stop packet might also contain statistics such as elapsed time, input and output octets, or input and output packets.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
Tue, 06 Dec 2013 12:32:17.036
    User-Name = bob
    NAS-Port = 1
    Framed-IP-Address = 1.1.1.1
    Class = yahoo.com
    NAS-Identifier = localhost
    Acct-Status-Type = Stop
    Acct-Session-Id = S209524
```

Trace of Successful Accounting

The following is a trace example of a successful accounting sequence.

```
11/12/2013 21:27:58: P6699: Packet received from 10.1.9.204
11/12/2013 21:27:58: P6699: Trace of Accounting-Request packet
11/12/2013 21:27:58: P6699:    identifier = 127
11/12/2013 21:27:58: P6699:    length = 45
11/12/2013 21:27:58: P6699:    reqauth = ed:d6:a6:ae:57:09:b8:55:a8:d4:c4:0d:f7:be:06:2a
11/12/2013 21:27:58: P6699:    User-Name = bob
11/12/2013 21:27:58: P6699:    NAS-Identifier = localhost
11/12/2013 21:27:58: P6699:    Acct-Status-Type = Start
11/12/2013 21:27:58: P6699:    Acct-Session-Id = 1
11/12/2013 21:27:58: P6699: Using Client: cubone (10.1.9.204)
11/12/2013 21:27:58: P6699: Using NAS: localhost (127.0.0.1)
11/12/2013 21:27:58: P6699: Request is directly from a NAS: FALSE
11/12/2013 21:27:58: P6699: Running NAS localhost (127.0.0.1) IncomingScript: ParseServiceHints
11/12/2013 21:27:58: P6699:     Rex: environ->get( "Request-Type" ) -> "Accounting-Request"
11/12/2013 21:27:58: P6699:     Rex: environ->get( "User-Name" ) -> ""
11/12/2013 21:27:58: P6699:     Rex: request->get( "User-Name", 0 ) -> "bob"
11/12/2013 21:27:58: P6699: Accounting with Service accserv1
11/12/2013 21:27:58: P6699: Trace of Accounting-Response packet
11/12/2013 21:27:58: P6699:    identifier = 127
11/12/2013 21:27:58: P6699:    length = 20
11/12/2013 21:27:58: P6699:    reqauth = a6:40:45:02:4c:8b:6f:00:4f:18:4a:b8:fe:28:9d:f4
11/12/2013 21:27:58: P6699: Sending response to 10.1.9.204
```

Sample Error Messages

The following are sample accounting error messages:

Error message logged in name_radius_1_log file when the disk is full and AR is trying to record an accounting request.

```
05/15/2013 2:52:29 name/radius/1 Error System 0 Failed to write records to the accounting
report file '/usr/accounting.log' - accounting records lost
```

Note An Accounting-Response packet is sent only if the accounting record is written to the file in the disk. If the disk is full, an Accounting-Response packet is not sent.

Error message logged in name_radius_1_log file when the path specified in the FilenamePrefix property is not valid.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
05/15/2013  4:11:12 name/radius/1 Error Configuration 0 Error in property
/Radius/Services/TechMahindraAccounting/FilenamePrefix: Unable to write to the specified
report file prefix (/tmp/AR/accounting)
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Chapter 3

Using WiMAX in Tech Mahindra Access Registrar

Tech Mahindra Access Registrar supports Worldwide Interoperability for Microwave Access (WiMAX) technology. This feature support in Tech Mahindra Access Registrar complies with the WiMAX forum NWG_R1_V1.3.1-Stage-3 specifications.

This chapter contains the following sections:

- WiMAX - An Overview
- WiMAX in Tech Mahindra Access Registrar

WiMAX - An Overview

WiMAX is a standards-based wireless technology that offers high throughput broadband connections over long distances. WiMAX can be used for a number of applications, including “last mile” broadband connections, fixed and mobile cellular service, hotspots and cellular backhaul, and high-speed enterprise connectivity for business. WiMAX is based on the IEEE 802.16d standard for fixed wireless, and the 802.16e standard for mobile wireless. This standard is appealing to customers because it allows mass production of chipsets that reduce CPE costs, ensures multi-vendor interoperability, and reduces investment risk for operators.

The architectural framework of a WiMAX network consists of the Access Service Network (ASN), the Connectivity Service Network (CSN), and a AAA Server. An Access Service Network is a set of network functions that provide radio access to a WiMAX subscriber. The ASN typically provides functions such as network discovery and selection, connectivity service between the MSS and CSN, Radio Resource Management, Multicast and Broadcast Control, Intra-ASN mobility, Paging, and Location Management. The WiMAX architecture consists of both mobile and fixed subscribers, as well as the ASN and CSN.

A CSN is defined as a set of network functions that provide IP connectivity services to the WiMAX subscribers. CSN might comprise network elements such as Routers, Home Agent, AAA proxy/servers, user databases, Policy Servers, Content Service Gateways, Service Selection Gateways, and interworking gateway devices.

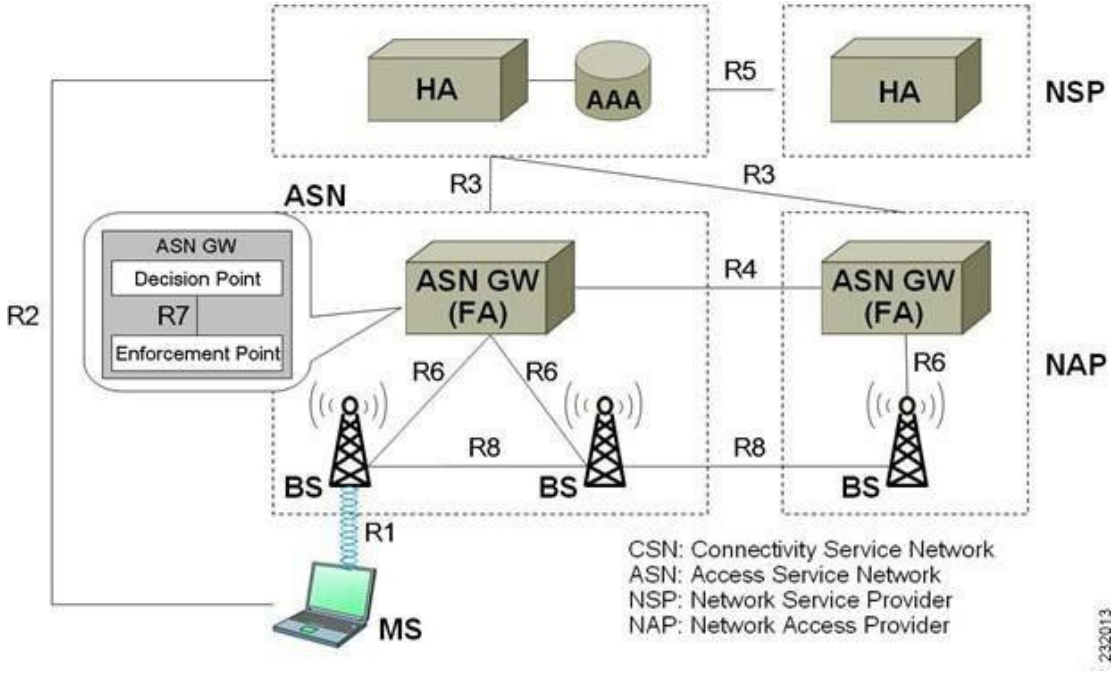
The Access Service Network is connected to a home network HCSN (Home Connectivity Service Network) via at least one visited network (Visited Connectivity Service Network VCSN) or intermediate network.

The Visited CSN plays the role of a AAA proxy. During all AAA interaction the VCSN AAA server acts as a RADIUS proxy transporting RADIUS packets between the ASN and the HCSN.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Figure 3-1 describes the network reference model of a typical WiMAX scenario.

Figure 3-1 WiMAX Network Reference Model

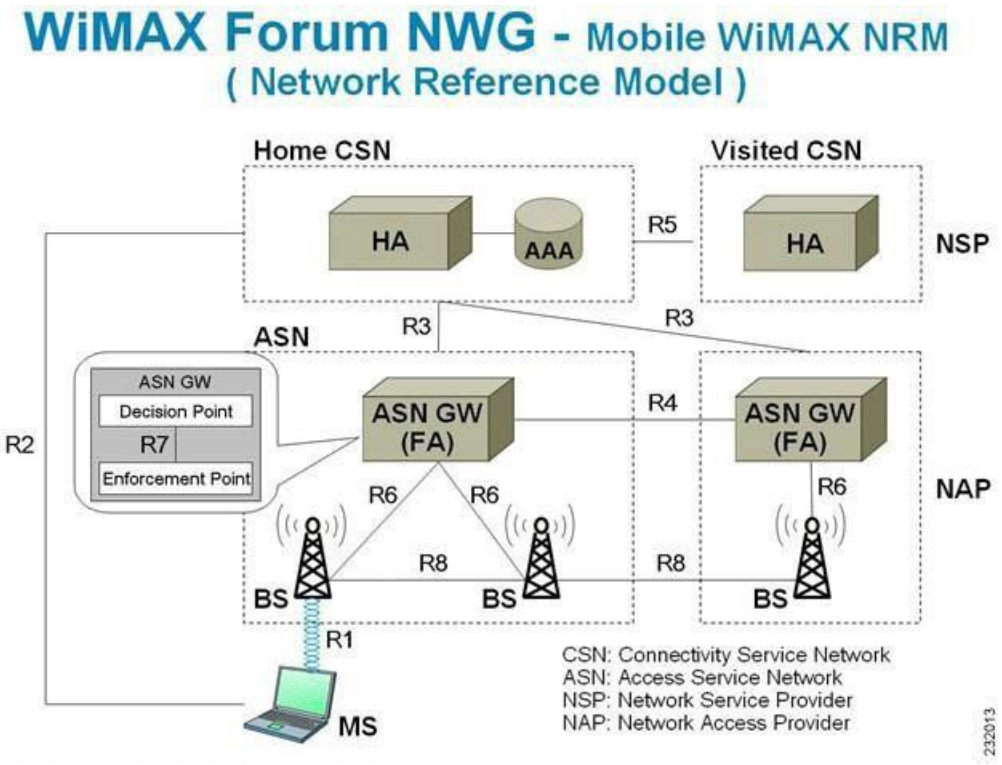


WiMAX in Tech Mahindra Access Registrar

Tech Mahindra Access Registrar uses the Extensible Authentication Protocol (EAP) to enable the WiMAX feature. It also caches the IP attributes and Mobility Keys that are generated during network access authentication. To enable caching of the WiMAX attributes, you must configure the respective resource managers. See Configuring the Resource Manager for WiMAX, for information on configuring resource manager. Figure 3-2 shows the WiMAX workflow in Tech Mahindra Access Registrar.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Figure 3-2 WiMAX Workflow



The WiMAX workflow in Tech Mahindra Access Registrar includes:

- Direct interaction between the ASN GW and Tech Mahindra Access Registrar
- Interaction between the ASN GW and Tech Mahindra Access Registrar through the HA

This section contains the following topics:

- Direct Interaction Between the ASN GW and Tech Mahindra Access Registrar
- Interaction Between ASN GW and Tech Mahindra Access Registrar Through HA
- Prepaid and Hot-Lining

Direct Interaction Between the ASN GW and Tech Mahindra Access Registrar

When the mobile node (MN) sends a RADIUS request to the ASN GW, it forwards this request to the CSN. If it is VCSN, the VAAA proxies the request with Visited HA address in the Access Request to HAAA. The HAAA initiates an authentication using the EAP service, **for example, eap-ttls**. The initial Access-Request containing the WiMAX capability and NAS-Port-Type (Type:61) attributes indicate that the specified flow is for a WiMAX request from ASN GW. Tech Mahindra Access Registrar redirects this request to the WiMAX service that you configure. The WiMAX service redirects the request to the EAP-based Wimax-Authentication-Service for authentication. Upon successful authentication, the WiMAX service redirects the request to Wimax-Session-Manager to allocate the home agent. Subsequently, Tech Mahindra Access Registrar generates the appropriate keys based on the Extended Master Session Key (EMSK) and records the generated keys in the session cache resource manager as configured, before sending Access-Accept to the ASN GW.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

If there is no VCSN, then the HAAA will send the Access-Accept to ASNGW. Otherwise, the HAAA sends the Access-Accept to VAAA. The VAAA then generates the visited HA-RK Key with SPI and Lifetime and sends the access-accept to ASNGW.

The authentication methods followed by Tech Mahindra Access Registrar are:

- User-only
- Device-only
- Single-EAP Device or User authentication

Tech Mahindra Access Registrar uses the following values to identify the service-type:

- Framed—for initial authentication
- Authenticate-Only—for reauthentication
- Authorize-Only—for prepaid request

Note Prepaid attributes can also be sent in the initial authentication.

The attributes contained in this flow are listed in Table 3-1. For detailed information on the attributes refer to the WiMAX forum NWG_R1_V1.3.1-Stage-3 specifications document.

Table 3-1 Attributes: ASN GW-Tech Mahindra Access Registrar Flow

Attribute	Description
User-Name	Must be present. This attributes gets the NAI from the EAP-Response/Identity.
Service-Type	Must be present and the value is Framed, Authenticate-Only or Authorize-Only.
WiMAX Capability	This attribute is chosen by the ASN GW. The request to the Tech Mahindra Access Registrar is provided through the WiMAX-Capability attribute. The server might respond with the chosen WiMAX Capability.
NAS-Port-Type	The request must contain this attribute with the value 27. This indicates Wireless IEEE 802.16 port when coming from a WiMAX ASN.
Calling-Station-ID	The request must contain this attribute with the value set to the MAC address of the device in binary format.
Device-Authentication-Indicator	The request might contain this attribute to indicate whether the device authentication was performed or not and the result of the action.
CUI	The NAS might intimate the support for CUI by sending the CUI attribute with the value ‘null’.
GMT-Time-Zone-Offset	The request must contain the offsets in seconds from the GMT at the NAS.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table 3-1 Attributes: ASN GW-Tech Mahindra Access Registrar Flow (continued)

Attribute	Description
Framed-IP-Address	This is the CMIPv4 Home address to be assigned to the MN. If this attribute is not present then the Home address is derived by the ASN from MIP procedures or through DHCP.
WiMax-Session-ID	This attribute shall not be present in the initial authentication. The value is a unique identifier in the home realm for this session as set by the HAAA(Tech Mahindra Access Registrar) in the Access-Accept, when the authentication is successful and it will be included in all subsequent requests from the NAS, such as online accounting.
MSK	The MSK shall be provided by the AAA Server as a result of successful EAP-authentication. MSK can be transmitted using either the MS-MPPE-Keys or the MSK attribute.
Packet-Flow-Descriptor	The pre-provisioned service flow which might be present in the Access-Accept packet.
QoS-Descriptor	The pre-provisioned service flow which might be present in the Access-Accept packet, if configured in Tech Mahindra Access Registrar.
BS-ID	Might be present in the Access-Request packet which will identify NAP-ID base station. If both NAP-ID and BS-ID are present, the NAP-ID will be ignored.
Acct-Interim-Interval	Sent in the Access-Accept packet. It indicates the accounting update intervals.

Tech Mahindra Access Registrar generates a few more attributes upon successful authentication. These attributes are described in Table 3-2.

Table 3-2 Additional Attributes: ASN-GW Tech Mahindra Access Registrar Flow

Attribute	Description
hHA-IP-MIP4	The IP address of the home HA allocated for the incoming request.
vHA-IP-MIP4	The IP address of the visited HA. To be used by the PMIP4 client.
MN-hHA-MIP4-KEY	The MN-hHA key is used for MIP4 procedures.
MN-hHA-MIP4-SPI	The SPI associated with the MN-hHA-MIP4-KEY.
MN-vHA-MIP4-KEY	The MN-vHA key is used for MIP4 procedures.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table 3-2 Additional Attributes: ASN-GW Tech Mahindra Access Registrar Flow (continued)

Attribute	Description
MN-vHA-MIP4-SPI	The SPI associated with the MN-vHA-MIP4-KEY.
FA-RK-KEY	The FA-RK key will be used at ASN GW to derive MN-FA for MIP4 procedures.

Note A policy engine can parse the NAI decoration and conclude the type of authentication method for the incoming access-request for passing on to WiMAX service.

Interaction Between ASN GW and Tech Mahindra Access Registrar Through HA

After Tech Mahindra Access Registrar returns the Access-Accept to the ASN GW, the mobile node, which initially sent the request, sends a registration request to the ASN GW. The ASN GW receives this request and sends an Access-Request to the HA. A Query-Request will be sent to the Tech Mahindra Access Registrar by HA to receive the security context for authenticating the FA.

Tech Mahindra Access Registrar identifies the request as HA query request, if:

- the WiMAX mobility attribute is present
- the NAS-Port-Type attribute is absent

Tech Mahindra Access Registrar checks for a valid session in the session cache based on NAI and sends an Access-Accept to the HA.

Table 3-3 HAAA Cached Attributes

Attribute	Description
Pseudo Identity	As received from the MS in the NAI in the EAP-Response/Identity. The HAAA is required to correlate this to the true identity of the user.
NAS-ID/NAS-IP address	One or both of these parameters are cached by the HAAA. This is required to locate the serving NAS.
Framed-IP Address	The IP address allocated to the user session. This information is useful in identifying the session during AAA dynamic procedures.
MIP-RK, hHA-RK, FA-RK, MN-hHA	Mobility keys generated during network access authentication. These keys are cached and used by the network for mobility authentication.
hHA-IP address	The IP address of the home HA assigned to the MS.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table 3-4 VAAA Cached Attributes

Attribute	Description
vHA-RK, vHA-RK-SPI, vHA-RK Lifetime, MN-vHA	Mobility keys generated during network access authentication. These keys are cached and used by the network for mobility authentication.
vHA-IP address	The IP address of the visited HA assigned to the MS.

Note Tech Mahindra Access Registrar responds with the correct keys back to the HA based on the NAI in **User-Name** attribute. Tech Mahindra Access Registrar returns an Access-Reject if it does not find a valid session for the NAI during the user authentication and authorization or if there are other errors.

Prepaid and Hot-Lining

Tech Mahindra Access Registrar supports prepaid and hot-lining flows for WiMAX. These are supported by the existing mechanisms.

Configuring WiMAX in Tech Mahindra Access Registrar

A new service type named **wimax** will be used for the WiMAX feature in Tech Mahindra Access Registrar. **aregcmd** command is used to configure WiMAX in Tech Mahindra Access Registrar. WiMAX service contains—Session Manager (with a session-cache resource manager and HA resource manager), Query Service that is connected to the session manager configured for this service, and Prepaid Service, which are required to connect all the flows appearing in Tech Mahindra Access Registrar for WiMAX. This service will be used as a container for the new key generation modules and the existing modules such as EAP services.

Configuring WiMAX in Tech Mahindra Access Registrar involves configuration of:

- Resource Manager for WiMAX
- Session Manager for WiMAX
- Query Service for WiMAX
- WiMAX properties

This section contains the following topics:

- Configuring the Resource Manager for WiMAX
- Configuring the Session Manager for WiMAX
- Configuring the Query Service for WiMAX
- Configuring WiMAX

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Configuring the Resource Manager for WiMAX

You must configure the following two Resource Managers:

- HA (home-agent or home-agent-ipv6)
- HA Cache (session-cache)

The HA Resource Manager must contain the IP ranges covering all the HA IP addresses that are to be assigned in round-robin. You must configure the HA Cache Resource Manager to cache the mobility keys (Table 3-3).

Note The HA Resource Manager allocates the IP addresses to the HA. If you do not configure the HA Resource Manager properly, Tech Mahindra Access Registrar will not generate some of the keys, which result in an Access-Reject by the NAS.

The following shows the sample configuration for HA:

```
[ /Radius/ResourceManagers/HA ]
Name = HA
Description =
Type = home-agent
Home-Agent-IPAddresses/
Entries 1 to 1 from 1 total entries
Current filter: <all>
209.165.200.225-209.165.200.254/
```

The following shows the sample configuration for HA Cache in HAAA:

```
[ /Radius/ResourceManagers/HA-Cache ]
Name = HA-Cache
Description =
Type = session-cache
OverwriteAttributes = TRUE
QueryKey = User-Name
PendingRemovalDelay = 10
AttributesToBeCached/
        1. WiMax-Session-ID
        2. hHA-RK-Key
        3. hHA-RK-SPI
        4. MN-hHA-MIP4-Key
        5. hHA-RK-Lifetime
        6. MIP-RK
```

The following shows the sample configuration for HA Cache in VAAA:

```
[ /Radius/ResourceManagers/HA-Cache ]
Name = HA-Cache
Description =
Type = session-cache
OverwriteAttributes = TRUE
QueryKey = User-Name
PendingRemovalDelay = 10
AttributesToBeCached/
        1. vHA-RK-Key
        2. vHA-RK-SPI
        3. MN-vHA-MIP4-Key
        4. vHA-RK-Lifetime
```

When the OverwriteAttributes value is set as TRUE, the newly generated mobility keys will be cached with the session record. By default, the value is FALSE.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

The HA-RK-Lifetime attribute type must be of type STRING instead of UINT32 under **/Radius//advanced/attribute\ dictionary/vendor-Specific/vendors/wimAX/subAttribute\ Dictionary.**

Note For generating RRQ-MN-HA key, we must configure MIP-RK in the AttributesToBeCached list.

Configuring the Session Manager for WiMAX

Before configuring WiMAX service, you must configure a session manager for WiMAX with a HA and session cache resource manager. The following shows an example configuration of a session manager with HA and session cache resource managers.

```
[ /Radius/SessionManagers/session-mgr-2 ]
    Name = session-mgr-2
    Description =
    IncomingScript =
    OutgoingScript =
    AllowAccountingStartToCreateSession = FALSE
    SessionTimeOut =
    PhantomSessionTimeOut =
    SessionKey =
    ResourceManagers/
        1. HA-Cache
        2. HA
```

Note If a default session manager is configured with the same key as that of the WiMAX session manager, the incoming WiMAX request will fail.

Configuring the Query Service for WiMAX

When you configure a query service for the WiMAX service in Tech Mahindra Access Registrar, you must refer it to the WiMAX Session Manager that you created. While configuring WiMAX, you must refer the **WiMAX-Query-Service** parameter to a valid Query Service.

You must configure the Query key as the **User-Name** attribute, which contains the NAI. You must also configure the query service to return all the relevant mobility keys as described in Table 3-5.

Table 3-5 Mobility Keys

Key	Generated By	Used At
MN-HA-CMIP4	MN and HAAA	HA and MN
MN-HA-PMIP4	MN and HAAA	HA and PMIP4 client
MN-HA-CMIP6	MN and HAAA	MN and HA
FA-RK	MN and HAAA	MN and Authenticator
MN-FA	MN and Authenticator	FA and MN or PMIP4 client
HA-RK	HAAA or VAAA	HA and Authenticator
FA-HA	HA and Authenticator	HA and FA

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

The following shows a sample configuration for a WiMAX Query Service:

```
[../haQueryService ]
Name = haQueryService
Description =
Type = radius-query
IncomingScript~ =
OutgoingScript~ =
SessionManagersToBeQueried/
1. session-mgr-2
AttributesToBeReturned/
1. WiMax-Session-ID
2. HA-RK-Key
```

Note If AttributesToBeReturned is not configured, all the cached attributes will be returned.

Configuring WiMAX

When you configure the WiMAX service under **/Radius/Services**, you must set its type to **wimax** and provide the following configuration options:

```
[ //localhost/Radius/Services/wimax ]
Name = WiMAX
Description =
Type = WiMAX
IncomingScript~ =
OutgoingScript~ =
OutagePolicy~ = RejectAll
OutageScript~ =
HA-RK-Key = TechMahindra112
HA-RK-LifeTime = 60
WiMAX-Authentication-Service = None
WiMAX-Session-Manager = None
WiMAX-Query-Service = None
WiMAX-Prepaid-Service = None
Allow-HAAA-To-Include-Keys = TRUE
Require-MSK = False
```

The syntax to generate the a WiMAX request from radclient is

simple_wimax_asn_test bob(username) bob(password)

Table 3-6 WiMAX Service Parameters

Parameter	Description
Name	Required; inherited from the upper directory.
Description	An optional description of the service.
Type	Must be set to **wimax** for WiMAX service.
IncomingScript	Optional.
OutgoingScript	Optional.
OutagePolicy	Required; must be set to **AcceptAll**, **DropPacket**, or **RejectAll**. Default is **DropPacket.**

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table 3-6 WiMAX Service Parameters (continued)

Parameter	Description
OutageScript	Optional. if you set this property to the name of a script, Tech Mahindra Access Registrar runs it when an outage occurs. This property allows you to create a script that notifies you when the RADIUS server detects a failure.
HA-RK-Key	Used as the base key to generate random HA-RK-Key for all the HAs that are configured in Tech Mahindra Access Registrar. By default, the value is `Cisco112`. You can change this value.
HA-RK-LifeTime	Used as time (in minutes) to regenerate the HA-RK-Keys based on its lifetime.
WiMAX-Authentication-Service	A valid eap service which can be used for WiMAX authentication. By default, this value is `none`. For VAAA, it should be configured with valid radius proxy service.
WiMAX-Session-Manager	A valid session manager which has HA and HA Cache as resource managers. By default, this value is `none`.
WiMAX-Query-Service	A valid RADIUS query service configured with WiMAX session manager. By default, this value is `none`.
WiMAX-Prepaid-Service	A valid prepaid service can be given to carry out the prepaid functionality of WiMAX. Otherwise this value is set to `none`.
Allow-HAAA-To-Include-Keys	If this is set, the HAAA will include the hHA-RK-Key, hHA-RK-SPI and hHA-RK-Lifetime in the Access-Accept. Otherwise, those attributes will not be in the Access-Accept. By default this value is True.
Require-MSK	If this is set, the MSK will be provided by the AAA server as a result of successful EAP-Authentication. By default, this value is False.

WiMAX - OMA-DM Provisioning Support with BEK Key

In addition to WiMax subscriber authentication, the Tech Mahindra Access Registrar generates and caches the Bootstrap Encryption Key (BEK) when it receives the authentication request from the unprovisioned WiMax subscriber/device. Tech Mahindra Access Registrar can identify the unprovisioned device either by looking the special pattern in Access-Request or by performing explicit database lookup.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

The BEK key derived from EMSK is calculated as follows:

BEK = the 16 most significant (leftmost) octets of HMAC-SHA256(EMSK, “bek@wimaxforum.org”).

When Tech Mahindra Access Registrar receives the accounting start packet for the unprovisioned device,

1. IP, MAC address, and BEK of the unprovisioned device notifies the OMA-DM server to initiate the provisioning.
2. Tech Mahindra Access Registrar maintains the IP address to MAC address association using web-service until it receives the provisioning complete message from the OMA-DM server.

The Backend Portal queries the Tech Mahindra Access Registrar web-service for this unprovisioned device MAC address by giving the device IP address and also the OMA-DM server request the Tech Mahindra Access Registrar web-service to validate the MAC to IP address association

The communication between Tech Mahindra Access Registrar and OMA-DM/Portal server is through web-service by using SOAP over HTTPS. It is assumed that the OMA-DM server (or a mediation function) will have a web-service using which AR can communicate.

Configuring the WiMax-Provisioning

To configure WiMax provisioning:

Step 1 Configure a script object, such as wimax-provision.

```
[ //localhost/Radius/Scripts/wimax-provision ]
    Name = wimax-provision
    Description =
    Language = rex
```

--> set FileName to 'libProvisioning.so'

```
set FileName /techm-ar/scripts/radius/rex/libProvisioning.so
```

--> set EntryPoint 'ProvisionedDeviceLookup'

```
set EntryPoint ProvisionedDeviceLookup
```

--> set InitEntryPoint 'InitializeProvisioning'

```
set InitEntryPoint InitializeProvisioning
```

--> set InitEntryPointArgs to 'ldap:wimax'

```
set InitEntryPointArgs ldap:wimax
```

ls

```
[ //localhost/Radius/Scripts/wimax-provision ]
    Name = wimax-provision
    Description =
    Language = rex
    Filename = /techm-ar/scripts/radius/rex/libProvisioning.so
    EntryPoint = ProvisionedDeviceLookup
    InitEntryPoint = InitializeProvisioning
    InitEntryPointArgs = ldap:wimax
```

The file libProvisioning.so is come up with Tech Mahindra Access Registrar kit. You have to copy it into **/techm-ar/scripts/radius/rex** path. Entrypoint ProvisionedDeviceLookup literally looks up a datastore to check if the user is provisioned. InitEntryPoint 'InitializeProvisioning' takes care of all initialization work

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

for entry point. InitEntryPointArgs 'ldap-wimax' says the user look up to be performed against ldap datastore. Oracle datastore can also be used wherein you have to give this property to 'oracle:wimax'.

Step 2 Configure the configured script object to the server's incoming scripting point.

set IncomingScript wimax-provsion

ls

```
[ //localhost/Radius ]
    Name = Radius
    Description =
    Version = 7.2.0.0
    IncomingScript~ = provision
    OutgoingScript~ =
```

Step 3 Webclient setup

Create a script object which calls the Tech Mahindra Access Registrar's wimax-provisioning webservice.

```
[ //localhost/Radius/Scripts/WebServicecall ]
    Name = WebServicecall
    Description =
    Language = rex
    Filename = libProvisioning.so
    EntryPoint = WebServiceCall
    InitEntryPoint =
    InitEntryPointArgs =
```

Entry point should be set to WebServiceCall.

Step 4 Save the configuration:

save

Step 5 Reload the configuration:

reload

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Chapter 4

Replication Log

Tech Mahindra Access Registrar's replication feature allows you to maintain identical configurations on multiple machines simultaneously. For more information on replication, see the "Using Replication" chapter of the *Tech Mahindra Access Registrar 9.3 User Guide*.

This chapter provides information about replication log messages in Tech Mahindra Access Registrar and certain frequently asked questions on replication.

This chapter contains the following sections:

- Frequently Asked Questions
- Replication Log Messages

Frequently Asked Questions

Question: When I do a **save** in **aregcmd** and the validation fails, is anything replicated?

Answer: No; replication does not occur until **aregcmd** successfully saves the changes.

Question: Can I specify multiple masters with the same members?

Answer: No; the replication feature was designed to be used with a single-master. Also, it is not possible to specify more than one master in a member's configuration.

Question: Do I have to configure the master as a client on the member servers?

Answer: No. In-fact, it would be erroneous to do so. With the exception of Administrators, Interfaces, Replication, and Advanced machine-specific settings, the configuration between master and member must be identical. The replication feature's purpose is to maintain that relationship. Altering configuration settings on the member which are managed by the master will likely result in an unstable and possibly non-operational server.

Question: What configuration elements are replicated and what are not?

Answer: With the exception of Administrators, Interfaces, Replication, and Advanced machine-specific settings, all other settings are replicated.

Question: What configuration elements are hot-configured and what are not?

Answer: Session Managers, Resource Managers and Remote servers are not hot-configured because they maintain state, such as an active session, and cannot be manipulated dynamically.

Question: What is an appropriate TransactionSyncInterval setting?

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Answer: This depends upon how long you want to allow an out-of-sync condition to persist. The shorter the interval, the more often an out-of-sync condition is checked. However, this results in added network traffic, additional processing by Tech Mahindra Access Registrar and, if the interval is too small, frequent unnecessary resynchronization requests. The default value of 60,000 milliseconds (1 minute) is usually sufficient; however, values of as little as 10,000 milliseconds (10 seconds) have been tested and have worked well.

Question: What is an appropriate TransactionArchiveLimit setting?

Answer: This depends upon two things:

1. How much hard disk space you are willing to devote to transaction archive storage
2. How often your configuration is changed (a save is issued through Aregcmd).

If you have limited hard disk space, then perhaps smaller values (less than 1000) are appropriate; however if you have sufficient hard disk space, values of 10,000 or greater are better. The primary reason for this preference is to limit the possibility of a full-resynchronization being required. A full-resynchronization is required when the member has missed so many transactions that the master no longer contains all the transaction necessary to resynchronize the member. The greater the limit, the longer the member can be down without requiring a full-resynchronization.

Question: Can I specify a member in the member configuration?

Answer: Yes, and this is recommended. In the member's replication configuration Rep Members list, specify another server, perhaps one which can be used in-case of critical failure of the master. If the master suffers a catastrophic failure (a hard disk crash, for example) the member can be reconfigured to be the master simply by setting the RepIsMaster to TRUE and changing the MasterIPAddress to its own IP Address and the member specified in its Rep Members list will perform as the member. Because the member has an archive of transactions, the new member can be automatically resynchronized. If the archive limit on the new master has been exceeded (the transaction file txn0000000001 is no longer present in the new master's archive directory), then the new member will require a full-resynchronization. Setting the member up in this manner prevents down-time if the master fails and allows configuration changes to be made on the new master.

Question: How can I prevent a full-resynchronization from ever being necessary?

Answer: You can't, but you can limit the possibility by setting the TransactionArchiveLimit to a large value (greater than 10000). Another technique is to periodically check the archive when the master and member are synchronized. If the number of transaction files is approaching 10,000, then you can stop the master and member servers, delete all files in the replication archive, and restart the master and member. The only side effect is that if the master or member suffers a catastrophic failure, a full resynchronization will be required.

Question: Can I use the member to process RADIUS requests along with the master?

Answer: Yes, and this was one of the goals of the replication feature. Keep in mind that session information is not replicated between master and member. To use session management in this environment, use Tech Mahindra Access Registrar's central session manager.

Replication Log Messages

This section contains typical replication log messages and explains what each means.

This section include the following topics:

- Information Log Messages
- Warning Log Messages

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

- Error Log Messages
- Log Messages You Should Never See

Information Log Messages

Info Message `Starting Replication Manager`

Displayed at start-up and indicates the Replication Manager is configured and enabled. (RepType=SMDBR)

Info Message `Replication Disabled`

Displayed at start-up and indicates that Replication is not enabled. (RepType=NONE)

Info Message `Radius Server is On-Line`

Displayed by the member at start-up to indicate the member is synchronized with the master and processing RADIUS requests. It is also displayed after a successfully completed resynchronization. This message is never displayed on the master.

Info Message `Radius Server is Off-Line`

Displayed by the member at start-up to indicate the radius server is not processing RADIUS requests until it can ensure synchronization with the master. When this is displayed after startup, it indicates the member is no longer synchronized with the master and is directly associated with a resynchronization request to the master. This message is never displayed on the master.

Info Message `Resynchronizing <member name>`

Displayed by the master to indicate that it is resynchronizing the specified member (member).

Info Message `Resynchronization from Master in progress.`

Displayed by the member to indicate the master is in the process of resynchronizing it.

Info Message `Resynchronization complete.`

Displayed by the member to indicate the resynchronization has completed successfully.

Info Message `Resynchronization did not complete before timeout. Retrying.`

Indicates the master did not complete the resynchronization before the member expected it to complete and that the member is re-requesting resynchronization from the master for the remaining missed transactions.

Info Message `Master Selected As Partner (DEFAULT)`

Displayed by the member to indicate that it has selected the master as a partner after successfully getting connected with the master. Partner selection is performed after analyzing the replication workloads on other replication members.

Info Message `Initiating Replication of Transaction <transaction #> with <# of elements> Elements.`

Displayed by the master to indicate that it is beginning replication of a transaction to the member.

Info Message `Replication Transaction #<transaction #> With <# of elements> Elements Initiated`

Displayed by the master to indicate that it has completed sending the transaction to the member.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Info Message Committing Replication of Transaction <transaction #> with <# of elements> Elements.

Displayed by the member to indicate that it has received a transaction and is processing it.

Info Message Replication Transaction #<transaction#> With <# of element> Elements Committed

Displayed by the member to indicate that the transaction has been successfully processed.

Info Message Stopping Replication Manager

Displayed at shutdown by both the master and member to indicate the replication manager is being shut down.

Info Message Stopping Replication Manager - waiting for replication to complete...

Displayed by the member when a shutdown is attempted while received replications are being processed. After the replications are complete, the shutdown will complete.

Info Message Replication in progress. Please wait...

Periodically displayed while a shutdown is pending and replications are being completed.

Info Message Replication Manager Stopped

Displayed by both the master and member to indicate the replication manager has been successfully shutdown.

Warning Log Messages

Warning Message Transaction Sync not received within configured TransactionSyncInterval. Communication with the Master may not be possible.

The member displays this log messages to indicate that it has not received a TransactionSync message from the master within its configured TransactionSync interval.

Warning Message TXN_SYNC Received by Master from unknown member <ip address>. Validation Failed

Displayed by the master when a TransactionSync message is received by the master. Since there can be only one configured master in a replication network, and the master is the only server who can send a TransactionSync message, this indicates there is another configured master in the replication network.

Warning Message TXN_SYNC Received from unknown Master <ip address>. Validation Failed

Displayed by the member to indicate that a TransactionSync message was received from a server not configured as its master.

Warning Message Requesting resynchronization from Master: Last Txn#<transaction#>

Displayed by the member to indicate that it is requesting resynchronization from the master. The LastTxn# is the last transaction number the member received and processed successfully.

Warning Message Resynchronization Request received from unknown member.

Displayed by the master when a resynchronization request is received by a member who is not listed in its **/radius/replication/rep** members configuration.

Warning Message Resynchronization of <member name> requires Full Resynchronization.

Displayed by the master to indicate that the member cannot be automatically resynchronized because its last transaction number is not within the configured history length of the archive (TransactionArchiveLimit). A manual resynchronization of the member is required to put the member back in-sync.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Warning Message `MEMBER_SYNC Received from unknown Master at <ip address>. Validation Failed`

Displayed by a member indicating that a master, other than its configured master, is requesting partnership.

Warning Message `MEMBER_SYNC Received by Master from unknown member <ip address>. Validation Failed`

Displayed by the master to indicate a member not listed in its **/radius/replication/rep** members configuration has requested partnership.

Warning Message `TXN_EXPECT Received by Master from unknown <ip address>.`

Displayed by the master to indicate it has received a transaction which originated from another illegal master.

Warning Message `TXN_EXPECT Received from unknown Master <ip address>.`

Displayed by the member to indicate it has received a transaction which originated from a master other than its configured master.

Warning Message `TXN_EXPECT Broadcast failed.`

Indicates that the master could not initiate a replication.

Warning Message `DATA_SYNC Received by Master from unknown <ip address>`

Displayed by the master to indicate that it received a replication transaction from another illegal master.

Warning Message `DATA_SYNC Received from unknown <ip address>`

Displayed by the member to indicate that a transaction was received from a server external to the replication network.

Error Log Messages

Error Message `DATA_SYNC Validation failed - CRC Mismatch`

Displayed by the member to indicate a received transaction element is invalid.

Error Message `TXN_SYNC: Failed To Get Member Socket Handle.`
`TXN_SYNC: Failed to get master's socket handle.`
`MEMBER_SYNC could not get socket handle`
`TXN_EXPECT: Failed to get socket handle.`
`DATA_SYNC could not get socket handle.`
`These messages indicate an invalid interface configuration in Tech Mahindra Access Registrar.`
`They could also be the result of specifying an invalid RepPort setting.`
`Failed To Create TXN_SYNC packet. (out of packets?)`
`Failed To Create TXN_SYNC packet.`
`MEMBER_SYNC Failed to create packet.(out of packets?)`
`MEMBER_SYNC Failed to create packet.`
`TXN_EXPECT Failed to create packet.(out of packets?)`
`TXN_EXPECT Failed to create packet.`
`DATA_SYNC Create packet failed.(out of packets?)`
`DATA_SYNC Create packet failed.`

These message indicate that a packet could not be created. This could be the result of a low memory condition or the result of the /Radius/Advanced/ MaximumNumberOfRadiusPackets setting being set too low

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Error Message `TXN_SYNC validation failed - Internal error (pTxnSync=NULL).`
`MEMBER_SYNC validate failed - Internal Error (pMemberSync=NULL)`
`DATA_SYNC Validation Failed - Internal (pDataSync = NULL).`
`TXN_EXPECT Could not add new datablock to pending transaction queue.`
`Replication Member could not be added to member list.`
`Replication Member could not be added to member list.`

These messages are the result of a failed memory allocation possibly due to an out of memory condition.

Error Message `DATA_SYNC Packet creation failed - Invalid ordinal.`
`Attempt To Replicate Transaction With Zero Elements.`
`Internal Error - Selected member not valid`
`Internal Replication Error ChangeType <change type> For <element path>`
`Internal error - Replication manager is invalid`

These messages indicate an internal application failure.

Error Message `Cannot archive transaction datablock`
`Could not archive transaction`

These messages are the result of a failed archive attempt. This could be the result of a low disk space condition.

Error Message `Could not commit transaction to MCD`
`Cannot Get Value For Unsupported DataType <data type id>`
`MCD Replication Cannot Delete Value <element path>`
`MCD Replication Cannot Delete Directory <element path>`
`MCD Replication Cannot Delete Value For <element path> With Unsupported DataType <data type id>`
`MCD Replication Cannot Create Dir For <element path>`
`MCD Replication Cannot Set Value For <element path>`
`MCD Replication Cannot Set Value For <element path>`
`MCD Replication Cannot Set Value For <element path>`
`MCD Replication Cannot Set Value For <element path>`
`MCD Replication Cannot Set Value For <element path> With Unsupported DataType <data type id>`
`MCD Replication Cannot Set Value For <element path> With UNKNOWN DataType <data type id>`

These messages are the result of a failed replication commit attempt.

Log Messages You Should Never See

The following list contains log messages which you should never see displayed in a log. If any of these messages are displayed in the log, contact Tech Mahindra Access Registrar technical support for assistance.

Error Message
`DATA_SYNC Received from non-partner <ip address>`
`DATA_RE_SYNC CRC mismatch. Replying with NAK`
`DATA_RE_SYNC Commit Failed. Replying with NAK`

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

EVAL_SYNC Validation failed. <ip address> is not a Master or Member of the Replication network
EVAL_SYNC Received from unknown member.
PARTNER_SYNC Received from unknown member <ip address>.
PARTNER_SYNC Received from unknown member <ip address>.
EVAL_SYNC Cannot get socket handle.
EVAL_SYNC Failed to create packet.(out of packets?)
EVAL_SYNC Failed to create packet.
EVAL_SYNC Validation failed - Internal Error (pEvalSync=NULL). PARTNER_SYNC Failed to get socket handle.
PARTNER_SYNC Failed to create packet. (out of packets?)
PARTNER_SYNC Failed to create packet.
DATA_RE_SYNC Can't get socket handle
DATA_RE_SYNC Failed to create packet (out of packets?)
DATA_RE_SYNC Failed to create packet
DATA_RE_SYNC Failed validation - Internal Error (pReSync = NULL)
DATA_RE_SYNC Cannot Set Value For <element path>
DATA_RE_SYNC Cannot Set Value For <element path>
DATA_RE_SYNC Cannot Set Value For <element path>
DATA_RE_SYNC Cannot Set Value For <element path>
DATA_RE_SYNC Cannot Set Value For <element path> With Unsupported DataType <data type id>
DATA_RE_SYNC Cannot Set Value For <element path> With UNKNOWN DataType <data type id>;
DATA_RE_SYNC Received by Master from unknown member <ip address>
DATA_RE_SYNC Received from unknown Master <ip address>DATA_RE_SYNC Reply received by Master from unknown Member <ip address>
Could not replicate data element to partners. Could not replicate to partners - Invalid Ordinal.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Chapter 5

Using On-Demand Address Pools

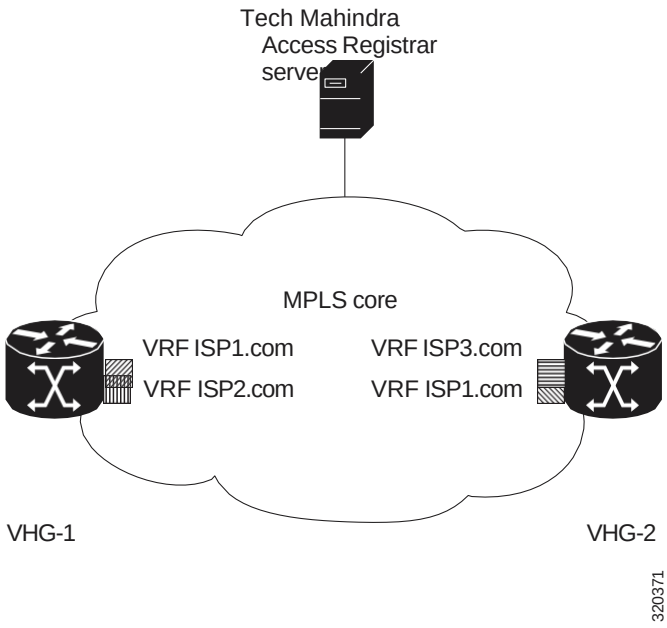
Tech Mahindra Access Registrar provides support for On-Demand Address Pools (ODAP). Using ODAP, the Tech Mahindra Access Registrar server manages pools of addresses. Each pool is divided into subnets of various sizes, and the Tech Mahindra Access Registrar server assigns the subnets to virtual home gateways (VHG) and Provider Edge (PE) routers. The VHG/PE router has one On-Demand Address Pool configured for each VPN supported by that VHG/PE.

Tech Mahindra Access Registrar has been enhanced to make ODAP functionality more accessible and to enable ODAP requests and normal user authentication to occur on the same Tech Mahindra Access Registrar server. To achieve this functionality, a new Tech Mahindra vendor script **TechmWithODAPIncomingScript** was written to direct ODAP requests to particular services and session managers. **TechmWithODAPIncomingScript** also provides the same functionality as the previous **TechmIncomingScript**.

Additionally, Tech Mahindra Access Registrar has a new vendor type, **TechmWithODAP** which references **TechmWithODAPIncomingScript** as its IncomingScript and references the existing script, **Tech Mahindra,** as its Outgoing Script.

Figure 5-1 shows a simple MPLS VPN network with two VHG/PE routers, VHG-1 and VHG-2. The Tech Mahindra Access Registrar server allocates IP subnets to the VHGs by way of VRFs which contain the subnets and addresses (address space) available.

Figure 5-1 MPLS Core



Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

In Tech Mahindra Access Registrar, the VRFs are configured as users in an ODAP-users list under **/Radius/UserLists**. The VRF name is set in IOS for the ODAP pool. When a VRF requests a pool of addresses, Tech Mahindra Access Registrar directs the request to a Session-Manager configured with the name **odap-<*VRF name*>**. Tech Mahindra Access Registrar also directs ODAP accounting requests to the service odap-accounting.

In the example network shown in Figure 5-1, the VRFs are configured with the following address spaces:

- **VRF-ISP1.com**—consists of the address range 10.255.0.0 - 10.255.255.255 divided among the following subnets:
  - 10.255.0.0/24
  - 10.255.1.0/24
  - ...
  - 10.255.255.0/24
- **VRF-ISP2.com**—consists of the address ranges 10.0.0.0 - 10.10.255.255 and 10.255.0.0 - 10.255.10.255 divided among the following subnets:
  - 10.0.0.0/16
  - 10.1.0.0/16
  - ...
  - 10.10.0.0/16

  and:
  - 10.255.0.0/24
  - 10.255.1.0/24
  - ...
  - 10.255.10.0/24

Note VRF-ISPe.com requires two ResourceManagers because it has subnets of two different sizes.

- **VRF-ISP3.com**—consists of the address range 1172.21.0.0 - 172.21.255.255 divided among the following subnets:
  - 172.21.0.0/18
  - 172.21.64.0/18
  - 172.21.128.0/18

  and
  - 172.21.192.0/24
  - 172.21.193.0/24
  - ...
  - 172.21.255.0/24

Note VRF-ISP3.com requires two ResourceManagers because it also has subnets of two different sizes.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

This chapter contains the following sections:

- Techm-Incoming Script
- Vendor Type TechmWithODAP
- Configuring Tech Mahindra Access Registrar to Work with ODAP

Techm-Incoming Script

The **TechmWithODAPIncomingScript** makes ODAP functionality more accessible. This script eases the configuration required to enable ODAP requests and normal user authentication to occur on the same Tech Mahindra Access Registrar server. **TechmWithODAPIncomingScript** also provides the functionality of the original TechmIncomingScript.

If the Tech Mahindra Access Registrar server receives an ODAP request, the server sets the Session-Key from the AcctSessionID and sets the services and session managers.

If the Tech Mahindra Access Registrar server receives a non-ODAP request, other scripts, rules or policies that you might already have in place on the Tech Mahindra Access Registrar server handle these requests.

This section contains the following topics:

- How the Script Works
- TechmWithODAPIncomingScript

How the Script Works

The following describes how the script **TechmWithODAPIncomingScript** works:

1. The script examines the incoming NAS-Identifier sent by the client (VHG). If the NAS-Identifier does not equal ***odap-dhcp*** then this request is not an ODAP request. Since this is not an ODAP request, the script does not do any more ODAP-specific processing and just calls **TechmIncomingScript** to allow that script to process the request. If this is an ODAP request, this script removes the NAS-Identifier attribute because it is no longer needed.
2. The script sets the Authentication-Service and the Authorization-Service to ***odap-users***, and it sets the Accounting-Service to ***odap-accounting***.
3. The Tech Mahindra Access Registrar server sends the request to the appropriate Session Manager based on the username. Session Managers with ***odap-<username>*** must be created and configured in Tech Mahindra Access Registrar.
4. The script then uses Session IDs to identify each ODAP request. The script uses the Acct-Session-Id attribute as the Session-Key.

TechmWithODAPIncomingScript

The following is a Tcl script example of the script **TechmWithODAPIncomingScript**.

Note **TechmWithODAPIncomingScript** is written in C language. This example script is more easily understood in Tcl.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
proc TechmWithODAPIncomingScript {request response environ} {

  set RequestType [ $environ get Request-Type ]

  if { [ string compare $RequestType "Access-Request" ] == 0 ||
       [ string compare $RequestType "Accounting-Request" ] == 0 } {

       set NasID [ $request get NAS-Identifier ]

       if { [ string compare $NasID "odap-dhcp" ] == 0 } {
              # Remove the NAS-Identifier - it has done it's job
              $request remove NAS-Identifier

              set UserName [ $environ get User-Name ]
              if { [ string length $UserName ] == 0 } { set UserName [ $request get
User-Name ] }

              # ODAP SUBNET ASSIGNMENT
              $environ put Authentication-Service "odap-users"
              $environ put Authorization-Service "odap-users"
              $environ put Accounting-Service "odap-accounting"
              $environ put Session-Manager "odap-$UserName"

              set AcctSessionId [ $request get Acct-Session-Id ]
              if { [ string length $AcctSessionId ] != 0 } { $environ put Session-Key
$AcctSessionId
              } else {
              $environ log LOG_ERROR "Missing Acct-Session-Id attribute in request-unable
to set Session-Key"
             }
     }
  }
TechmIncomingScript $request $response $environ
}
```

Note The final line in the example above is not how the script really works because a Tcl script cannot call a C script. This is one reason why **TechmWithODAPIncomingScript** was written in C.

Vendor Type TechmWithODAP

You must configure any Clients that might forward ODAP requests to the Tech Mahindra Access Registrar server as being of Vendor **TechmWithODAP.**

This vendor type references the new script, **TechmWithODAPIncomingScript**, as its IncomingScript and references the existing script, Tech Mahindra, as its .

After setting Vendor to **TechmWithODAP,** ODAP requests are directed to the AA service, set to ***odap-users***, the accounting service is set to ***odap-accounting***, and the Session Manager is set to ***odap-username***, where username is filled from the request. The username received in the request is a VRF name, the request is directed to the appropriate Session Manager.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Configuring Tech Mahindra Access Registrar to Work with ODAP

This section provides information about how to configure Tech Mahindra Access Registrar to work with ODAP.

Configuring Tech Mahindra Access Registrar to work with ODAP

You must configure any Clients that might forward ODAP requests to the Tech Mahindra Access Registrar server as being of Vendor **TechmWithODAP.**

Configuring Tech Mahindra Access Registrar to work with ODAP

To configure Tech Mahindra Access Registrar to work with ODAP:

Step 1 Create and configure an ODAP-users UserList. All ODAP users are configured under this UserList.

Step 2 Add all ODAP users to the ODAP-users UserList. Usernames must be of the form `<vrf name>` with the AllowNullPassword property set to TRUE.

Step 3 Create and configure a service for ODAP-users.

Step 4 Create and configure an ODAP accounting service. Set the accounting service Type to ***file*** and FilenamePrefix ***odap-accounting***.

Step 5 Create a Session Manager for each of the VRFs. There must be a separate Session Manager for each VRF pool.

Step 6 Create and configure Resource Managers to be referenced by the Session Managers.

Note Subnet pools of different sizes (different subnet masks) require separate Resource Managers

Step 7 Configure the Session Managers with the Resource Managers.

Step 8 Configure any Clients that might send ODAP requests to Vendor type TechmWithODAP.

Step 9 Save your configuration.

Configuring the ODAP Detailed Instructions

You must configure any Clients that might forward ODAP requests to the Tech Mahindra Access Registrar server as being of Vendor **TechmWithODAP.**

Configuring the ODAP Detailed Instructions

To configure Tech Mahindra Access Registrar to work with ODAP:

Setting Up an ODAP UserList

Step 1 Create a UserList for ODAP users.

```
--> cd /radius/userlists
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
[ //localhost/Radius/UserLists ]
    Entries 1 to 1 from 1 total entries
    Current filter: <all>

    Default/

--> add odap-users

Added odap-users
```

Adding ODAP Users

Step 2 Add the ODAP users to the ODAP UserList and set the AllowNullPassword property to TRUE. Each user is a VRF name set for each ODAP client.

```
[ //localhost/Radius/UserLists/odap-users ]

    Entries 0 to 0 from 0 total entries
    Current filter: <all>

    Name = odap-users
    Description =

--> add vrf-ISP1.com

Added vrf-ISP1.com


--> add vrf-ISP2.com

Added vrf-ISP2.com


--> add vrf-ISP3.com

Added vrf-ISP3.com

--> ls

[ //localhost/Radius/UserLists/odap-users ]
    Entries 1 to 3 from 3 total entries
    Current filter: <all>

    Name = odap-users
    Description =
    vrf-ISP1.com/
    vrf-ISP2.com/
    vrf-ISP3.com/
```

Step 3 Set the AllowNullPassword property to TRUE for each ODAP user.

```
--> cd vrf-ISP2.com


[ //localhost/Radius/UserLists/odap-users/vrf-ISP2.com ]
    Name = vrf-ISP2.com
    Description =
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
    Password =
    Enabled = TRUE
    Group~ =
    BaseProfile~ =
    AuthenticationScript~ =
    AuthorizationScript~ =
    UserDefined1 =
    AllowNullPassword = FALSE

--> set AllowNullPassword TRUE
```

Setting Up an ODAP-Users Service

Step 4 Add and configure a service for ODAP Users.

```
--> cd /radius/services

[ //localhost/Radius/Services ]
    Entries 1 to 2 from 2 total entries
    Current filter: <all>

    local-file/
    local-users/

--> add odap-users

Added odap-users

--> cd odap-users
[ //localhost/Radius/Services/odap-users ]
    Name = odap-users
    Description =
    Type =
    IncomingScript~ =
    OutgoingScript~ =

--> set type local

Set Type local

--> set userlist odap-users

Set UserList odap-users

--> ls

[ //localhost/Radius/Services/odap-users ]
    Name = odap-users
    Description =
    Type = local
    IncomingScript~ =
    OutgoingScript~ =
    OutagePolicy~ = RejectAll
    OutageScript~ =
    UserList = odap-users
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Setting Up an ODAP Accounting Service

Step 5 Add and configure an ODAP accounting service.

```
--> cd /radius/services

[ //localhost/Radius/Services ]
    Entries 1 to 3 from 3 total entries
    Current filter: <all>

    local-file/
    local-users/
    odap-users/

--> add odap-accounting

Added odap-accounting

--> cd odap-accounting

[ //localhost/Radius/Services/odap-accounting ]
    Name = odap-accounting
    Description =
    Type =
    IncomingScript~ =
    OutgoingScript~ =

--> set type file

Set Type file

--> ls

[ //localhost/Radius/Services/odap-accounting ]
    Name = odap-accounting
    Description =
    Type = file
    IncomingScript~ =
    OutgoingScript~ =
    OutagePolicy~ = RejectAll
    OutageScript~ =
    FilenamePrefix = accounting
    MaxFileSize = "10 Megabytes"
    MaxFileAge = "1 Day"
    RolloverSchedule =

--> set FilenamePrefix odap-accounting

Set Filenameprefix odap-accounting
```

Adding Session Managers

Step 6 Create one Session Manager for each of the VRF pools.

Create one Session Manager for each of the users you specify in the odap-users UserList. The Session Managers must be called odap-*VRF_name* to meet the requirements of **TechmWithODAPIncomingScript**.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
--> cd /radius/sessionmanagers

[ //localhost/Radius/SessionManagers ]
    Entries 1 to 1 from 1 total entries
    Current filter: <all>

    session-mgr-1/

--> add odap-vrf-ISP1.com

Added odap-vrf-ISP1.com

--> add odap-vrf-ISP2.com

Added odap-vrf-ISP2.com

--> add odap-vrf-ISP3.com

Added odap-vrf-ISP3.com
```

Setting Up Resource Managers

Step 7 Set up subnet-dynamic Resource Managers that are to be referenced by the Session Managers.

Session Managers can manage multiple Resource Managers. One or more subnet pools can be set up of varying sizes to allocate the ranges of subnet addresses you have available. Subnets of different sizes require different Resource Managers.

--> cd /radius/resourcemanagers

```
[ //localhost/Radius/ResourceManagers ]
    Entries 1 to 5 from 5 total entries
    Current filter: <all>

    IPA-Pool/
    IPA-Pool-2/
    IPX-Pool/
    Per-Group/
    Per-User/
```

--> add odap-vrf-ISP1.com

Note The names of Resource Managers do not have to be related to VRFs.

```
Added odap-vrf-ISP1.com
```

--> cd odap-vrf-ISP1.com

```
[ //localhost/Radius/ResourceManagers/odap-vrf-ISP1.com ]
    Name = odap-vrf-ISP1.com
    Description =
    Type =
```

--> set type subnet-dynamic

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
Set Type subnet-dynamic
```

--> ls

```
[ //localhost/Radius/ResourceManagers/odap-vrf-ISP1.com ]
    Name = odap-vrf-ISP1.com
    Description =
    Type = subnet-dynamic
    NetMask =
    SubnetAddresses/
```

-> set netmask 255.255.255.0

```
Set NetMask 255.255.255.0
```

-> cd subnetaddresses

```
[ //localhost/Radius/ResourceManagers/odap-vrf-ISP1.com/SubnetAddresses ]
    Entries 0 to 0 from 0 total entries
    Current filter: <all>

--> add 10.255.0.0-10.255.255.255

Added 10.255.0.0-10.255.255.255
```

Note Two Resource Managers are required for VRF-ISP3.com and VRF-ISP2.com because their address spaces are made up of subnets of the different sizes.

--> cd /radius/resourcemanagers

```
[ //localhost/Radius/ResourceManagers ]
    Entries 1 to 5 from 5 total entries
    Current filter: <all>

    IPA-Pool/
    IPA-Pool-2/
    IPX-Pool/
    odap-vrf-ISP1.com/
    Per-Group/
    Per-User/

--> add odap-vrf-ISP3-a.com

Added odap-vrf-ISP3-a.com
```

--> cd odap-vrf-`ISP3-a.com`

```
[ //localhost/Radius/ResourceManagers/odap-vrf-ISP3-a.com ]
    Name = odap-vrf-ISP3-a.com
    Description =
    Type =
```

--> set type subnet-dynamic

```
Set Type subnet-dynamic
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

--> ls

```
[ //localhost/Radius/ResourceManagers/odap-vrf-ISP3-a.com ]
    Name = odap-vrf-ISP3-a.com
    Description =
    Type = subnet-dynamic
    NetMask =
    SubnetAddresses/
```

-> set netmask 255.255.192.0

```
Set NetMask 255.255.192.0
```

-> cd subnetaddresses

```
[ //localhost/Radius/ResourceManagers/odap-vrf-ISP3-a.com /SubnetAddresses ]
    Entries 0 to 0 from 0 total entries
    Current filter: <all>

--> add 171.21.0.0-172.21.191.255

Added 172.21.0.0-172.21.191.255
```

-> cd /radius/resourcemanagers

```
[ //localhost/Radius/ResourceManagers ]
    Entries 1 to 10 from 10 total entries
    Current filter: <all>

    IPA-Pool/
    IPA-Pool-2/
    IPX-Pool/
    odap-vrf-ISP1.com/
    odap-vrf-ISP3-a.com /
    Per-Group/
    Per-User/

--> add odap-vrf-ISP3-b.com

Added odap-vrf-ISP3-b.com
```

--> cd odap-vrf-`ISP3-b.com`

```
[ //localhost/Radius/ResourceManagers/odap-vrf-ISP3-b.com ]
    Name = odap-vrf-ISP3-b.com
    Description =
    Type =
```

--> set type subnet-dynamic

```
Set Type subnet-dynamic
```

--> ls

```
[ //localhost/Radius/ResourceManagers/odap-vrf-ISP3-b.com ]
    Name = odap-vrf-ISP3-b.com
    Description =
    Type = subnet-dynamic
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
    NetMask =
    SubnetAddresses/
```

-> set netmask 255.255.255.0

```
Set NetMask 255.255.255.0
```

-> cd subnetaddresses

```
[ //localhost/Radius/ResourceManagers/odap-vrf-ISP3-b.com /SubnetAddresses ]
    Entries 0 to 0 from 0 total entries
    Current filter: <all>

--> add 172.21.191.0-172.21.255.255

Added 172.21.191.0-172.21.255.255
```

-> cd /radius/resourcemanagers

```
[ //localhost/Radius/ResourceManagers ]
    Entries 1 to 10 from 10 total entries
    Current filter: <all>

    IPA-Pool/
    IPA-Pool-2/
    IPX-Pool/
    odap-vrf-ISP1.com/
    odap-vrf-ISP3-a.com /
    odap-vrf-ISP3-b.com /
    Per-Group/
    Per-User/

--> add odap-vrf-ISP2-a.com

Added odap-vrf-ISP2-a.com
```

--> cd odap-vrf-`ISP2-a.com`

```
[ //localhost/Radius/ResourceManagers/odap-vrf-ISP2-a.com ]
    Name = odap-vrf-ISP2.com
    Description =
    Type =
```

--> set type subnet-dynamic

```
Set Type subnet-dynamic
```

--> ls

```
[ //localhost/Radius/ResourceManagers/odap-vrf-ISP2-a.com ]
    Name = odap-vrf-ISP2-a.com
    Description =
    Type = subnet-dynamic
    NetMask =
    SubnetAddresses/
```

-> set netmask 255.255.0.0

```
Set NetMask 255.255.0.0
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

-> cd subnetaddresses

```
[ //localhost/Radius/ResourceManagers/odap-vrf-ISP2-a.com /SubnetAddresses ]
    Entries 0 to 0 from 0 total entries
    Current filter: <all>

--> add 10.0.0.0-10.10.255.255

Added 10.0.0.0-10.255.255.255
```

-> cd /radius/resourcemanagers

```
[ //localhost/Radius/ResourceManagers ]
    Entries 1 to 10 from 10 total entries
    Current filter: <all>

    IPA-Pool/
    IPA-Pool-2/
    IPX-Pool/
    odap-vrf-ISP1.com/
    odap-vrf-ISP3-a.com /
    odap-vrf-ISP3-b.com /
    odap-vrf-ISP2-a.com /
    Per-Group/
    Per-User/

--> add odap-vrf-ISP2-b.com

Added odap-vrf-ISP2-b.com
```

--> cd odap-vrf-`ISP2-b.com`

```
[ //localhost/Radius/ResourceManagers/odap-vrf-ISP2-b.com ]
    Name = odap-vrf-ISP2-b.com
    Description =
    Type =
```

--> set type subnet-dynamic

```
Set Type subnet-dynamic
```

--> ls

```
[ //localhost/Radius/ResourceManagers/odap-vrf-ISP2-b.com ]
    Name = odap-vrf-ISP2-b.com
    Description =
    Type = subnet-dynamic
    NetMask =
    SubnetAddresses/
```

-> set netmask 255.255.255.0

```
Set NetMask 255.255.255.0
```

-> cd subnetaddresses

```
[ //localhost/Radius/ResourceManagers/odap-vrf-ISP2-b.com /SubnetAddresses ]
    Entries 0 to 0 from 0 total entries
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
    Current filter: <all>

--> add 10.255.0.0-10.255.10.255

Added 10.255.0.0-10.255.10.255
```

Configuring Session Managers

Note It is not necessary to configure Session Managers in two instances. All SessionManager configuration can be done at one time before configuring the Resource Managers.

Step 8 Configure the Session Managers to be referenced by the Resource Managers.

--> **cd/radius/sessionmanagers**

```
[ //localhost/Radius/SessionManagers ]
    Entries 1 to 4 from 4 total entries
    Current filter: <all>

    odap-vrf-ISP1.com/
    odap-vrf-ISP2.com/
    odap-vrf-ISP3.com/
    session-mgr-1/
```

--> **cd odap-vrf-ISP2.com**

```
[ //localhost/Radius/SessionManagers/odap-vrf-ISP2.com ]
    Name = odap-vrf-ISP2.com
    Description =
    AllowAccountingStartToCreateSession = FALSE
    ResourceManagers/
```

--> **cd resourcemanagers**

--> **set 1 odap-vrf-ISP2-a.com**

```
Set 1 odap-vrf-ISP2-a.com
```

--> **set 2 odap-vrf-ISP2-b.com**

```
Set 2 odap-vrf-ISP2-b.com
```

--> **cd/radius/sessionmanagers**

```
[ //localhost/Radius/SessionManagers ]
    Entries 1 to 4 from 4 total entries
    Current filter: <all>

    odap-vrf-ISP1.com/
    odap-vrf-ISP2.com/
    odap-vrf-ISP3.com /
    session-mgr-1/
```

--> **cd odap-vrf-ISP3.com**

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
[ //localhost/Radius/SessionManagers/odap-vrf-ISP3.com ]
    Name = odap-vrf-ISP3.com
    Description =
    AllowAccountingStartToCreateSession = FALSE
    ResourceManagers/
```

--> **cd resourcemanagers**

--> **set 1 odap-vrf-ISP3-a.com**

```
Set 1 odap-vrf-ISP3-a.com
```

--> **set 2 odap-vrf-ISP3-b.com**

```
Set 2 odap-vrf-ISP3-b.com
```

--> **cd/radius/sessionmanagers**

```
[ //localhost/Radius/SessionManagers ]
    Entries 1 to 4 from 4 total entries
    Current filter: <all>

    odap-vrf-ISP1.com/
    odap-vrf-ISP2.com/
    odap-vrf-ISP3.com/
    session-mgr-1/
```

--> **cd odap-vrf-ISP1.com**

```
[ //localhost/Radius/SessionManagers/odap-vrf-ISP1.com ]
    Name = odap-vrf-ISP1.com
    Description =
    AllowAccountingStartToCreateSession = FALSE
    ResourceManagers/
```

--> **cd resourcemanagers**

--> **set 1 odap-vrf-ISP1.com**

```
Set 1 odap-vrf-ISP1.com
```

Configure Clients

Step 9 For any client that might forward ODAP requests to the Tech Mahindra Access Registrar server, set the Vendor property to TechmWithODAP.

--> **cd /radius/clients**

```
[ //localhost/Radius/Clients ]
    Entries 1 to 2 from 2 total entries
    Current filter: <all>

    localhost/
    vhg-1/
    vhg-2/

--> cd vhg-1
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
[ //localhost/Radius/Clients/vhg-1 ]
        Name = vhg-1
        Description =
        IPAddress = 209.165.200.225
        SharedSecret = secret
        Type = NAS
        Vendor =
        IncomingScript~ =
        OutgoingScript~ =
        UseDNIS = FALSE
        DeviceName = a_name
        DevicePassword = password

--> set vendor TechmWithODAP


Set Vendor TechmWithODAP
```

Save Your Configuration

Step 10 After completing the configuration, save your changes.

```
--> save


Validating //localhost...
Saving //localhost...
```

Chapter 6

Wireless Support

This chapter provides the following information about using Tech Mahindra Access Registrar for wireless support:

- Mobile Node-Home Agent Shared Key
- 3GPP2 Home Agent Support
- Session Correlation Based on User-Defined Attributes
- Managing Multiple Accounting Start/Stop Messages
- NULL Password Support
- 3GPP Compliance
- 5G Data Network-AAA (DN-AAA) Compliance

Mobile Node-Home Agent Shared Key

In a mobile wireless environment, a Home Agent (HA) can request a Mobile Node-Home Agent (MN-HA) shared key from the home Tech Mahindra Access Registrar RADIUS server during a mobile IP registration request (RRQ) from a Packet Data Serving Node (PDSN). Tech Mahindra Access Registrar supports distribution of the shared key in this environment. Tech Mahindra Access Registrar encrypts the shared key using MD5 encryption before sending the key back to the HA in an Access-Accept packet.

When an HA receives an RRQ from a PDSN, the HA authenticates the RRQ using a MN-HA shared key. If the HA does not have the MN-HA shared key, it retrieves the MN-HA shared key from the Tech Mahindra Access Registrar server by sending an Access-Request packet containing the 3GPP2 VSA CDMA-MN-HA-SPI (SPI attribute). Tech Mahindra Access Registrar then sends the CDMA-MN-HA-Shared-Key corresponding to the user if the user has been successfully authenticated. This section contains the following topics:

- Use Case Example
- Configuring User Attributes

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Use Case Example

When HA receives an RRQ from a PDSN, it authenticates the RRQ by using a MN-HA shared key. If the HA does not have the MN-HA shared key, it retrieves the MN-HA shared key from the Tech Mahindra Access Registrar server by sending an Access-Request packet containing the 3GPP2 vendor-specific attribute (VSA) CDMA-MN-HA-SPI, the Security Parameter Index (SPI attribute).

The Tech Mahindra Access Registrar server then sends the CDMA-MN-HA-Shared-Key corresponding to the user if the user has successfully authenticated subject to the following rules:

1. If there is an incoming SPI and no configured SPI, the Tech Mahindra Access Registrar server authenticates the user as usual and does not include a configured shared-key (if there is one) in the reply.
2. If the incoming SPI does not match the configured SPI, the Tech Mahindra Access Registrar server authenticates the user as usual, but does not include the configured shared-key (if there is one) in the reply.
3. If the incoming SPI matches the configured SPI, but there is no shared-key configured, the Tech Mahindra Access Registrar server proceeds with normal authentication. Since there is no shared-key, it will not be included in the reply.
4. If the incoming SPI matches the configured SPI and a configured shared-key exists, the Tech Mahindra Access Registrar server proceeds to encrypt the MCD5 shared-key and include it in the Access-Accept.

The key to including the shared key in an Access-Accept is in matching the values of the SPI attribute.

Configuring User Attributes

Tech Mahindra Access Registrar server supports user-specific attributes which enables the Tech Mahindra Access Registrar server to return attributes on a per-user or per-group basis without having to use profiles.

Configuring the User Attributes

To configure a user with the CDMA-MN-HA-SPI VSA to request a MN-HA shared key:

Step 1 Log into the Tech Mahindra Access Registrar server and launch **aregcmd**.

Log in as a user with administrative rights such as user **admin**.

Step 2 Change directory to the attribute directory of the user.

cd /Radius/UserLists/Default/bob/Attributes

Step 3 Set the CDMA-MN-HA-SPI VSA to the appropriate shared-key value.

set CDMA-MN-HA-SPI 1124

```
set CDMA-MN-HA-SPI 1124
```

Step 4 Set the CDMA-MN-HA-SPI VSA to the appropriate shared-key value.

set CDMA-MN-HA-Shared-Key secret112

```
set CDMA-MN-HA-Shared-Key secret112
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Step 5 Validate and save your changes.

validate

save

3GPP2 Home Agent Support

The Tech Mahindra Access Registrar server supports 3GPP2 home agents. This support enables mobile IP clients that authenticate through a Tech Mahindra Access Registrar RADIUS server to be told which home agent they should use.

Every Mobile IP client has a home domain that is served by a group of Home Agents (HA). The Mobile IP client sets up a tunnel to one (and only one) HA during a session while it roams. Typically, the domain can be determined by the Mobile IP client's network access identifier (NAI).

Note The NAI is the userID submitted by the client during PPP authentication. In roaming, the purpose of the NAI is to identify the user as well as to assist in the routing of the authentication request.

During the authentication and authorization phase for each Mobile IP client, the RADIUS server must decide which HA from a group of HAs should be chosen to serve the client. This is called dynamic HA assignment.

This section contains the following topics:

- Home-Agent Resource Manager
- Querying and Releasing Sessions
- Access Request Requirements
- New 3GPP2 VSAs in the Tech Mahindra Access Registrar Dictionary

Home-Agent Resource Manager

Tech Mahindra Access Registrar supports dynamic HA assignment with a new resource manager type called home-agent. You configure the home-agent resource manager with a list of IP addresses. The Tech Mahindra Access Registrar server assigns those addresses to clients whose request dictionary has the right attributes to indicate that an assignment should be done. This is similar to the *ip-dynamic* resource manager.

Unlike the ip-dynamic resource manager, HAs are not exclusively allocated to an individual session but are shared among a set of sessions.

Load Balancing

The goal of dynamic HA assignment is to have load balancing among HAs. The Tech Mahindra Access Registrar server achieves this by evenly distributing mobile clients among HAs. At the same time, the Tech Mahindra Access Registrar server ensures that the same HA is always assigned to the same Mobile IP client for the same session.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Configuring the Home Agent Resource Manager

To create a new resource manager using the **aregcmd** command:

Step 1 Use the **cd** command to change to the **Radius /ResourceManagers** level.

--> **cd /Radius/ResourceManagers**

```
[ //localhost/Radius/ResourceManagers ]

    Entries 0 to 0 from 0 total entries
    Current filter: <all>
```

Step 2 Use the **add** command to specify the name of a resource manager to create.

--> **add home-agent-pool**

```
--> Added home-agent-pool
```

Step 3 Use the **cd** command to change to the **Radius /ResourceManagers/home-agent-pool** level.

--> **cd home-agent-pool**

```
[ //localhost/Radius/ResourceManagers/home-agent-pool ]

    Name = home-agent-pool
    Description =
    Type =
```

Step 4 Use the **set** command to set the resource manager type to **home-agent**.

--> **set type home-agent**

Step 5 Use the **ls** command to view the subdirectories under home-agent-pool.

--> ls

```
[ //localhost/Radius/ResourceManagers/home-agent-pool ]

    Name = home-agent-pool
    Description =
    Type = home-agent
    Home-Agent-IPAddresses/
```

Step 6 Use the **cd** command to change to the **Radius/ResourceManagers/home-agent-pool/Home-Agent-IPAddresses** level.

--> **cd Home-Agent-IPAddresses**

```
[ //localhost/Radius/ResourceManagers/home-agent-pool/Home-Agent-IPAddresses ]
```

Step 7 Use the **add** command to add a single IP address or a range of IP addresses.

--> **add 209.165.200.200-209.165.200.254**

```
--> Added 209.165.200.200-209.165.200.254
```

Querying and Releasing Sessions

The **aregcmd** program has been modified to support a new filter for **query-session** and **release-session**. You can use this filter to restrict a request (either query or release) to just the sessions with a given home-agent IP address. For example, consider the following command line.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

--> **query-session /radius with-home-agent 10.10.10.1**

This command line will return all sessions that have a home-agent resource equal to the IP address 10.10.10.1.

Querying sessions using **aregcmd** displays the home-agent resource in each session as:

HA ddd.ddd.ddd.ddd

where each *ddd* is a decimal number from 0-255.

Access Request Requirements

When the home-agent resource manager receives an Access-Request that contains a CDMA-HA-IP-Addr attribute, the home-agent resource manager checks the response dictionary to see if it already has a CDMA-HA-IP-Addr attribute. If it does, then the Mobile IP client has been assigned a HA address already and the resource manager does not need to do anything.

If the value of the CDMA-HA-IP-Addr attribute in the request dictionary is 0.0.0.0, the home-agent resource manager assigns a HA and puts a new CDMA-HA-IP-Addr attribute whose value is the IP address of the HA in the response dictionary.

If the value of the CDMA-HA-IP-Addr attribute is not 0.0.0.0, the Mobile IP client has been assigned a HA address already. The home-agent resource manager copies the attribute (with its value) from the request dictionary into the response dictionary.

The Tech Mahindra Access Registrar server might select the session manager based on the domain (using the rule engine, dynamic properties, or scripting), and it allows each session manager to have its own home-agent resource manager.

New 3GPP2 VSAs in the Tech Mahindra Access Registrar Dictionary

Tech Mahindra Access Registrar supports 3GPP2 vendor-specfic attributes (VSAs) in the vendor-specific dictionary in **/Radius/Advanced/Attribute Dictionary**.

Note There is no planned support for the Accounting-Container (3GPP2/6) attribute because it has different syntax than other vendor-specfic attributes (VSAs) and requires special processing.

Session Correlation Based on User-Defined Attributes

All the session objects are maintained in one dictionary keyed by a string.

You can define the keying material to the session dictionary through a newly introduced environment variable, Session-Key. If the Session-Key is presented at the time of session manager process, it will be used as the key to the session object for this session. The Session-Key is of type string. By default, the Session-Key is not set. It's value should come from attributes in the incoming packet and is typically set by scripts. For example, CLID can be used to set the value of Session-Key.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Use the script UseCLIDAsSessionKey as defined in the script **rexscript.c** to specify that the Calling-Station-Id attribute that should be used as the session key to correlate requests for the same session. This is a typical case for 3G mobile user session correlation. You can provide your own script to define other attributes as the session key.

In the absence of the Session-Key variable, the key to the session will be created based on the string concatenated by the value of the NAS and the NAS-Port.

There is a new option *with-key* available in **aregcmd** for query-sessions and release-sessions to access sessions by Session-Key.

Managing Multiple Accounting Start/Stop Messages

Since the PDSN is aware when it sends a RADIUS stop followed by a start record, it inserts the new Session Continue attribute (3GPP2/48) into the stop record. The existence of the Session Continue attribute denotes that a start record will immediately be sent and the packet data session continues on the PDSN.

When Tech Mahindra Access Registrar receives an accounting stop packet, the following two conditions trigger a release of a session and its resources:

- There is no 3GPP2/48 Session Continue attribute in the stop packet and the number of accounting stops received is greater or equal to the starts received for this session
- The 3GPP2/48 Session Continue attribute is present in the stop packet, but its value is zero (0)

Note One of the conditions above must be true to release the session and its resources.

NULL Password Support

Tech Mahindra Access Registrar introduced a new Tech Mahindra Access Registrar environment variable, *Allow-NULL-Password*. At authentication time, if the following three conditions are met, user authentication is bypassed:

1. Allow-NULL-Password environment variable is set to TRUE.
2. The User-Password or CHAP-Password must be NULL in the incoming request. (If it is not NULL, normal password checking will occur.)
3. A user record exists for this user.

By default, the *Allow-NULL-Password* environment variable is not set.

Note You should be aware of the security impact when using the NULL Password feature.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

You can set this environment variable in three different ways:

1. For the user in local database, one new field ***AllowNullPassword*** is added in the user record. When Tech Mahindra Access Registrar fetches a user record for authentication, if this field is set to TRUE and Allow-NULL-Password environment variable does not exist, it sets *Allow-NULL-Password* environment variable to TRUE.
2. If the user record is in LDAP database, then the *LDAPToEnvironmentMappings* must be defined to map an attribute in LDAP user record to *Allow-NULL-Password* environment variable.
3. Through scripting which allows the decision to be made based on runtime conditions, such as attributes in the access-request or policies.

3GPP Compliance

Tech Mahindra Access Registrar supports 3GPP compliance by implementing the following (refer to RFC 29.273):

- SWa reference point between an untrusted non-3GPP IP access and a 3GPP AAA server/proxy. See SWa Access Authentication and Authorization.
- STa reference point between a trusted non-3GPP access and a 3GPP AAA server/proxy. See STa Access Authentication and Authorization.
- SWm reference point between an Evolved Packet Data Gateway (ePDG) and a 3GPP AAA server/proxy. See SWm Access Authentication and Authorization.
- SWd reference point between a 3GPP AAA server and a 3GPP AAA proxy. See SWd Access Authentication and Authorization.
- SWx reference point between a Home Subscriber Server (HSS) and a 3GPP AAA server. See SWx Authentication Procedure.
- S6b reference point between a PDN GW and a 3GPP AAA server/proxy. See S6b Authentication and Authorization Procedure.

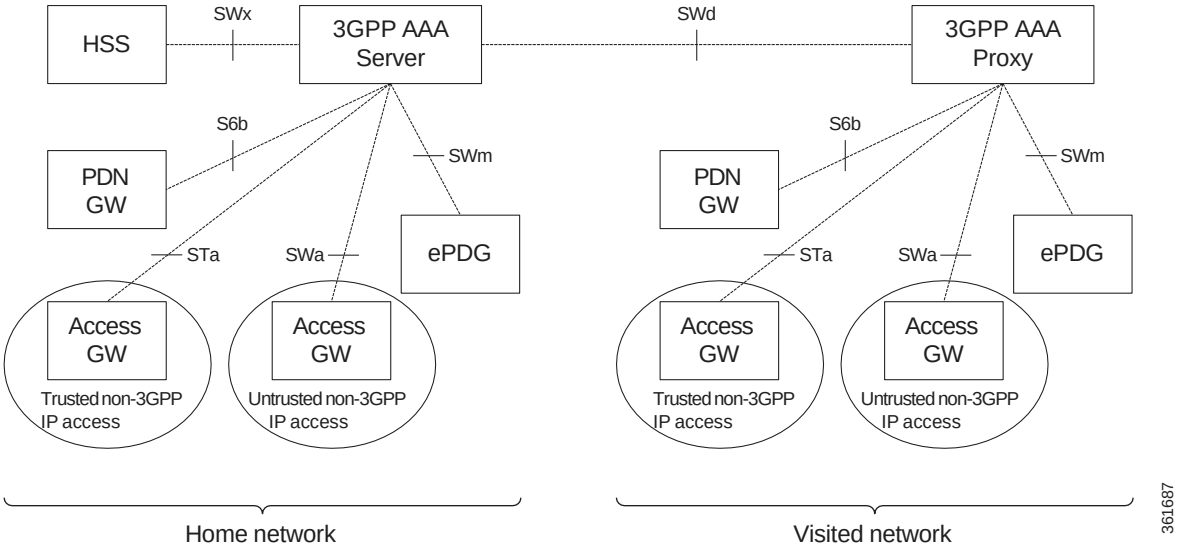
This topic also contains the following sections:

- 3GPP Call Flows
- Voice over Wi-Fi (VoWiFi) Location Based Authentication
- Mobile Equipment Identity Check Support in Tech Mahindra Access Registrar

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Figure 6-1 depicts the various interfaces used for 3GPP compliance in a mobile network.

Figure 6-1 3GPP Interfaces



SWa Access Authentication and Authorization

The SWa reference point is defined between a non-3GPP IP access and a 3GPP AAA server or between a non-3GPP IP access and a 3GPP AAA proxy.

The SWa access authentication and authorization procedure includes the following steps:

1. The 3GPP AAA server issues an unsolicited re-auth request towards the untrusted non-3GPP access, indicating that both re-authentication and re-authorization of the user is needed.
2. Upon receipt of such a request, the untrusted non-3GPP access responds to the request and indicates the disposition of the request. This procedure is mapped to the Diameter command codes Re-Auth-Request and Re-Auth-Answer.
3. Upon receiving the re-auth request, the untrusted non-3GPP access immediately invokes the SWa authentication and authorization procedure requesting the identity of the user through EAP and using DER/DEA commands, with the same session-ID.
4. If the re-authentication of the user is not successful, the untrusted non-3GPP access detaches the user.

STa Access Authentication and Authorization

The STa reference point is defined between a non-3GPP access network and a 3GPP AAA Server or between a non-3GPP access network and a 3GPP AAA Proxy.

Tech Mahindra Access Registrar decides whether a non-3GPP access network is trusted or untrusted by using the access authentication and authorization procedure executed between the non-3GPP access network and the 3GPP AAA server. This is implemented by the STa and SWa reference points sharing the same Diameter application and partly sharing the same authentication and authorization procedure.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

The STa and SWa reference points are clearly distinguished after the exchange of the first authentication and authorization messages, during which trusted/untrusted decision is made by the 3GPP AAA server and this decision is communicated to the non-3GPP access network.

The trusted non-3GPP access authentication and authorization requires DiaEAP with EAP-AKA or EAP-AKA`. Tech Mahindra Access Registrar implements the STa access authentication and authorization procedure based on the mobility parameters transported by the non-3GPP access network to the 3GPP AAA server.

This procedure follows the SWa authentication and authorization procedure, with the following differences:

- Information elements that reflect information about the user's service request and about the access network are mandatorily included in the authentication and authorization request.
- The information elements that describe the user's subscription profile are downloaded to the non-3GPP access network.

SWm Access Authentication and Authorization

The SWm reference point is defined between the ePDG and the 3GPP AAA server or between the ePDG and the 3GPP AAA proxy. It is used to authenticate and authorize a UE by transporting mobility parameters that are needed for the S2b interface. In particular this information may include the Packet Data Network (PDN) GW identity(s) and Access Point Name (APN(s)) currently allocated to a UE during a previous attach in a 3GPP access.

The SWm reference point performs authentication and authorization based on the reuse of the DER/DEA command set defined in the Diameter EAP application. The SWm access authentication and authorization procedure includes the following steps:

- The UE transmits a ‘tunnel establishment request’ message to the ePDG in order to establish a connection to the PDN.
- The ePDG initiates access authentication and authorization request to the 3GPP AAA server.
- During the access authentication and authorization procedure, the ePDG provides mobility parameters of the UE to the 3GPP AAA Server.
- The 3GPP AAA server performs IP mobility mode selection appropriately and upon successful authorization, it returns mobilty mode information back to the ePDG.

SWd Access Authentication and Authorization

The SWd reference point is defined between a 3GPP AAA proxy and a 3GPP AAA server. The SWd interface is used in roaming scenarios where the 3GPP AAA proxy is located in the visited network and the 3GPP AAA server is located in the home network. The 3GPP AAA proxy acts as a Diameter proxy agent and forwards Diameter commands between the Diameter client and the Diameter server.

When used in connection with an STa reference point, the SWd interface supports the trusted non-3GPP access authentication and authorization procedure. For this procedure, the 3GPP AAA proxy forwards the Diameter commands received from the 3GPP AAA server and the trusted non-3GPP access network as a stateful Diameter proxy.

When used in connection with the SWm reference point, the SWd interface supports the untrusted non-3GPP access authentication and authorization procedure. For this procedure, the 3GPP AAA proxy forwards the Diameter commands received from the 3GPP AAA server and the ePDG as a stateful Diameter proxy.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

SWx Authentication Procedure

The SWx is a reference point defined between a HSS and a 3GPP AAA server. It is used in AAA server registration of a new user.

The authentication procedure includes the following steps:

1. The 3GPP AAA server registers the current 3GPP AAA server address in the HSS for a given user when a new subscriber has been authenticated by the 3GPP AAA server.
2. The 3GPP AAA server informs the HSS about the current PDN GW identity and APN being used for a given UE, or that a certain PDN GW and APN pair is no longer used.
3. Accordingly, the 3GPP AAA server may de-register the currently registered 3GPP AAA server in the HSS for a given user and purge any related non-3GPP user status data in the HSS. This occurs if the UE for some reason has been disconnected from the non-3GPP access.

HSS Initiated Update of User Profile

The subscriber profile management procedures over SWx include the subscriber profile push and the subscriber profile request. The SWx reference point enables the following:

- Indication to the 3GPP AAA server of change of non-3GPP subscriber profile within HSS.
- Activation and deactivation of the subscriber and equipment trace in the PDN GW.

This procedure is used between the 3GPP AAA Server and the HSS and is invoked by the HSS during the following circumstances:

- When the subscriber profile has been modified and needs to be sent to the 3GPP AAA Server. This may happen due to a modification in the HSS.
- To update the 3GPP AAA Server with the identity of a dynamically allocated PDN GW, which is included in the APN-Configuration AVP in the user profile as a result of the first PDN connection establishment associated with an APN over 3GPP access.

This procedure is mapped to the Diameter command codes Push-Profile-Request (PPR) and Push-Profile-Answer (PPA). An IMSI Range based mechanism is provided to select the HSS server. In the CLI, if the MultiplePeersPolicy is IMSIRangeBased, then the ranges are configured as a list and from them the HSS server is selected.

S6b Authentication and Authorization Procedure

The S6b reference point is defined between a PDN GW and a 3GPP AAA server (for non-roaming case, or roaming with home routed traffic to PDN GW in home network) and between a PDN GW and a 3GPP AAA proxy.The S6b interface protocol is based on Diameter. It uses the Diameter base protocol and also supports Diameter EAP application. The EAP methods EAP-AKA and EAP-AKA` are used.

The authentication and authorization procedure includes the following steps:

1. The S6b interface enables authentication and authorization between the UE and the 3GPP AAA server/proxy.
2. When the UE performs the DSMIPv6 initial attach, it runs an IKEv2 exchange with the PDN GW. In this exchange, EAP AKA is used for UE authentication over IKEv2. The PDN GW acts as an IKEv2 responder and an EAP pass-through authenticator for this authentication.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

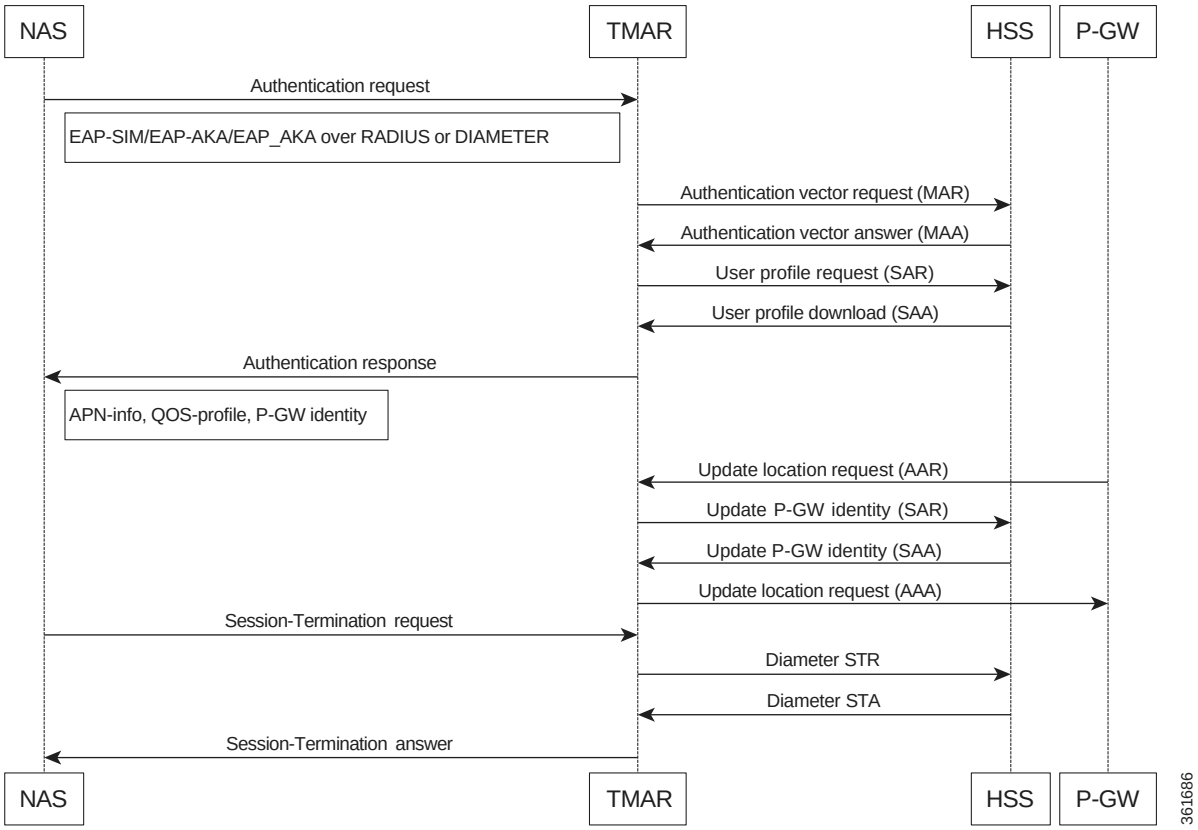
3. The S6b authentication and authorization procedure is invoked by the PDN GW after receiving an IKE_SA_AUTH message from the UE. The S6b reference point performs authentication based on reuse of the DER/DEA command set defined in Diameter EAP.

3GPP Call Flows

When Tech Mahindra Access Registrar receives an authentication or authorization request from any of the access points, it sends the packet to the rules and policy engine for processing. The rules and policies are added in the configuration of Tech Mahindra Access Registrar. Client, vendor, and server scripting points are provided in order to modify any AVPs in the packet or to decide upon the type of service that the packet requires. For example, if the service is Radius-to-Diameter translation, Tech Mahindra Access Registrar performs the translation of Radius packet to Diameter packet and sends it to the remote server. The service also has scripting points that can be used to modify the incoming packets. Once authentication or authorization is done for the packet session management can be performed for the packet by storing the user sessions in a session cache, if the authentication or authorization is successful. The server, client, vendor, and service outgoing scripting points can be used to modify the response packet.

Figure 6-2 depicts the call flows implemented for 3GPP.

Figure 6-2 3GPP Call Flows



This topic contains the following sections:

- CLI for 3GPP Authorization

- CLI for 3GPP Reverse Authorization

CLI for 3GPP Authorization

Following is the CLI for 3GPP authorization service:

```
[ //localhost/Radius/Services/3gpp-authz-diameter]
    Name = 3gpp-authz-diameter
    Description = STa to SWx authz (update-gw, get-profile , push-profile from HSS, de-reg
from HSS )
    Type = 3gpp-authorization
    Protocol = Diameter
    IncomingScript~ =
   OutgoingScript~=
   SessionManager =
   DiameterProxyService =

[ //localhost/Radius/Services/3gpp-authz-radius]
    Name = 3gpp-authz-radius
    Description = STa to SWx authz (update-gw, get-profile , push-profile from HSS, de-reg
from HSS )
    Type = 3gpp-authorization
    Protocol = Radius
    SessionManager =
    TranslationService =

[ //localhost/Radius/Services/3gpp-authz-radius]
    Name = 3gpp-authz-radius
    Description = STa to SWx authz (update-gw, get-profile , push-profile from HSS, de-reg
from HSS )
    Type = 3gpp-reverse-authorization
     Protocol = Radius
    PreRequestTranslationScript~ =
    PostRequestTranslationScript~ =
    PreResponseTranslationScript~ =
    PostResponseTranslationScript~ =
    EnvMapping/
    ForwardMapping/
    ReverseMapping/
    ResponseMapping/

[ //localhost/Radius/Services/3gpp-authz]
    Name = 3gpp-authz-radius
    Description = STa to SWx authz (update-gw, get-profile , push-profile from HSS, de-reg
from HSS )
    Type = 3gpp-reverse-authorization
    Protocol = Diameter
    Incoming~ =
   Outgoing~=
    SessionManager =
    RequestMapping/
    EnvMapping/
    ResponseMapping/
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

CLI for 3GPP Reverse Authorization

3GPP reverse authorization is used during RADIUS to Diameter translation. You can set the corresponding parameter to TRUE during the RADIUS to Diameter conversion. In this case, the request command mapping must not be defined because a new diameter request is created from the radius request by the 3GPP reverse authorization service. For more information about RADIUS<->Diameter translations, see "Diameter" chapter of the *Tech Mahindra Access Registrar 9.3 User Guide*.

Following is the CLI for 3GPP reverse authorization service:

```
[ //localhost/Radius/Services/reverse ]
Name = reverse
Description =
Type = 3gpp-reverse-authorization
IncomingScript~ =
OutgoingScript~ =
SessionManager = cache
TranslationService = diatorad
ProxyService =

[ //localhost/Radius/Services/diatorad ]
Name = diatorad
Description =
Type = diameter-radius
ProxyServiceName = rad-proxy
PreRequestTranslationScript~ =
PostRequestTranslationScript~ =
PreResponseTranslationScript~ =
PostResponseTranslationScript~ =
RequestMapping/
CommandMappings/
PPR = Radius-Access-Request
RAR = Radius-CoA-Request
AVPMappings/
Auth-Session-State = Techm-AVPair
user-name = user-name
AVPsToBeAdded/
EnvironmentMappings/
ResponseMapping/
ResultCodeMappings/
Radius-CoA-ACK = Diameter-Success
Radius-CoA-NAK = Diameter-Unable-To-Deliver
AVPMappings/
AVPsToBeAdded/
EnvironmentMappings/
```

Voice over Wi-Fi (VoWiFi) Location Based Authentication

Tech Mahindra Access Registrar allows or blocks access to voice over Wi-Fi (VoWiFi) based on location information of the user equipment (UE). Tech Mahindra Access Registrar uses Sh interface for fetching the location information of the UE. The workflow is as given below:

1. UE tries to establish connection to VoWiFi.
2. Request reaches Tech Mahindra Access Registrar server.
3. Upon successful authentication, Tech Mahindra Access Registrar sends a User Data Repository (UDR) request to HSS through Sh interface.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

4. If HSS has the location information, it sends a User-Data-Answer (UDA) response to Tech Mahindra Access Registrar through Sh interface in XML format.
    a. The UDA response contains a User-Data AVP, which contains location information of the UE.
    b. The AVP has various attributes including E-UTRANCellGlobalId, which carries the location information of the UE.
5. If HSS doesn't have the location information, it sends an Insert-Subscription-Data-Request (IDR) to the Mobility Management Entity (MME)/Serving GPRS Support Node (SGSN) requesting for the user identity information.
6. The MME/SGSN sends the user identity information to the HSS through an Insert-Subscription-Data-Answer (IDA) response.
7. The HSS communicates the received data to Tech Mahindra Access Registrar through Sh interface in XML format.
8. Upon receiving the user profile, Tech Mahindra Access Registrar parses the User-Data AVP, extracts the location information, and copies it to the E-UTRANCellGlobalId environment variable. Tech Mahindra Access Registrar can be configured to run the following script at 3GPP authorization service outgoing script to check the E-UTRANCellGlobalId variable and reject/accept the UE based on the location information.

```
proc test {request response environ} {

   if { [ $environ containsKey E-UTRANCellGlobalId ] } {

       set cellid [ $environ get E-UTRANCellGlobalId ]

       if { [ string compare $cellid sanjose ] == 0 } {
       #block the user send Reject
       $environ put Response-Type "Diameter-Access-Reject"
       #$environ put Response-Type "Access-Reject"
      }
   }
}
```

Following are sample CLI configurations for 3GPP authorization service with RADIUS and Diameter:

```
[ //localhost/Radius/Services/3gpp ]
    Name = 3gpp
    Description =
    Type = 3gpp-authorization
    Protocol = diameter
    IncomingScript~ =
    OutgoingScript~ = BlockorAcceptUE
    SessionManager = sm1
    DiameterProxyService = diaproxy
    FetchLocationInformation = True

[ //localhost/Radius/Services/3gpp-rad ]
    Name = 3gpp-rad
    Description =
    Type = 3gpp-authorization
    Protocol = radius
    IncomingScript~ =
    OutgoingScript~ = BlockorAcceptUE
    SessionManager = smrad
    TranslationService = rad-AA-SAR
    FetchLocationInformation = True
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Mobile Equipment Identity Check Support in Tech Mahindra Access Registrar

The Mobile Equipment Identity is used between the 3GPP AAA Server and the Equipment Identity Registrar (EIR) to check the identity status of a Mobile Equipment (ME) for e.g. to ensure the ME is not stolen or verify that the ME has no faults. This procedure is mapped to the commands ME-Identity-Check-Request/Answer (ECR/ECA).

In SWm interface, the IMEI number is retrieved by ePDG from the client and is sent in the Terminal-Information AVP of the DER packet.

In STa interface, Tech Mahindra Access Registrar retrieves the IMEI information using additional AVPs in the EAP call flows as shown in the sample configuration below.

```
[ //localhost/Radius/Services/eap-aka ,eap-aka-prime and eap-sim ]
    Name = eap-aka
    Description =
    Type = eap-aka
    NumberOfQuintets = 1
    AlwaysRequestIdentity = False
    EnableIdentityPrivacy = False
    EnableRollingPseudonymSecret = False
    PseudonymSecret = <encrypted>
    PseudonymRenewtime = "24 Hours"
    PseudonymLifetime = Forever
    NotificationService =
    Generate3GPPCompliantPseudonym = False
    EnableReauthentication = False
    UseOutagePolicyForReauth = False
    MaximumReauthentications = 16
    ReauthenticationTimeout = 3600
    ReauthenticationRealm =
    EnableEncryptedIMSI = FALSE
    QuintetCacheTimeout = 120
    AuthenticationTimeout = 120
    QuintetGenerationScript~ =
    UseProtectedResults = False
    EnableStateStickiness = False
    SendReAuthIDInAccept = False
    Subscriber_DBLookup = DiameterDB
    DiameterInterface = SWx
    ProxyService =
    MEIdentityLookup = TRUE/FALSE
    IMEIUnavailable = Continue/Terminate
    GreyListPolicy = Accept/Reject
    EIRProxyService =
    EmergencyServiceMEIdentityLookup = True
    MEIdentityLookupFailurePolicy = Continue
```

Table 6-1 lists the attributes added to support the EIR check feature in EAP-SIM, EAP-AKA, and EAP-AKA-PRIME services.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table 6-1 Equipment Identity Check Parameters

Attribute	Description
MEIdentityLookup	Set to TRUE to enable EIR check for the service.
IMEIUnavailable	Set this parameter to one of the following: • Continue—Tech Mahindra Access Registrar will continue the authentication/authorization even if the IMEI information is not received from the client. • Terminate—Tech Mahindra Access Registrar will terminate the authentication/authorization if the IMEI information is not received from the client.
GreyListPolicy	Set this parameter to one of the following: • Accept—Tech Mahindra Access Registrar will continue the authentication/authorization even if the equipment status is grey-listed from EIR check. • Reject—Tech Mahindra Access Registrar will reject the authentication/authorization if the equipment status is grey-listed from EIR check.
EIRProxyService	Separate proxy service for EIR that should be mapped with EIR remote servers.
EmergencyServiceMEIdentityLookup	Set to TRUE to perform MEIdentityLookup during emergency services based on the **EmergencyServicesPolicy** set up under Radius/Advanced/Diameter/General.
MEIdentityLookupFailurePolicy	Set this parameter to one of the following: • **Continue**—Tech Mahindra Access Registrar will continue the authentication for emergency ME Identity Lookup EIR failure cases. • **Terminate**—Tech Mahindra Access Registrar will terminate the authentication for emergency ME Identity Lookup EIR failure cases. This option is available only if **EmergencyServiceMEIdentityLookup** is checked.

5G Data Network-AAA (DN-AAA) Compliance

Tech Mahindra Access Registrar is 5G Data Network-AAA (DN-AAA) compliant based on the spec 3GPP TS 29.561 V15.1.0. Further enhancements are made to support this functionality as given below:

- DN-AAA server-specific RADIUS and Diameter attributes are added in the dictionary and carried in the corresponding messages.
- N6-specific AVPs and Experimental-Result-Code are added in the corresponding dictionary.
- With respect to accounting traffic, the release of IPv4 address and/or IPv6 prefix is notified to the DN-AAA server by sending RADIUS Accounting-Request Interim-Update without the Framed-IP-Address and/or Framed-Ipv6-Prefix attribute.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

- Tech Mahindra Access Registrar checks the 3GPP-Notification AVP and if the first bit of the third octet is set, then IP address is not allocated.
- Accounting ON and OFF is expected from Session Management Function (SMF) to ensure the synchronization of session information.
- Support is provided to trigger Re-Auth-Request (RAR) and Abort-Session-Request (ASR) when there is no integration with HSS for non-SIM based subscribers.
- **3GPP-Teardown-Indicator** is added to the RADIUS Disconnect Request message indicating the SMF that all QoS flows for this particular user and sharing the same user session will be deleted.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Chapter 7

Enforcement of Licensing Models

This chapter describes the enforcement of transactions per second (TPS) based licensing and session based licensing models introduced in Tech Mahindra Access Registrar .

In TPS based licensing model, the license is based on the number of transactions per second that are handled by the server. In session based licensing model, the license is managed based on the number of sessions that resides in Tech Mahindra Access Registrar. During Tech Mahindra Access Registrar startup, you can either load TPS based licensing or session based licensing, but not both at the same time.

This chapter contains the following sections:

- TPS Licensing Features
- Concurrent Session License Features

Note The type of licensing will determine the applicable features and its corresponding enforcement.

TPS Licensing Features

The following are the features of TPS licensing:

- License will enable features but with restriction enforced on the TPS.
- TPS is the number of packets flowing into Tech Mahindra Access Registrar. This is accounted by Tech Mahindra Access Registrar irrespective of the feature being used.

This section contains the following topics:

- Enforcement Rules
- Notification Logs
- Notification - SNMP Traps
- TPS Logging Feature

Enforcement Rules

Any license enforcement is triggered only after Tech Mahindra Access Registrar has observed increasing steady state in TPS. Increasing steady state is marked by the steady increase in incoming traffic (measured in TPS) beyond 80% of the licensed TPS for any 15 minutes of a 20 minute interval.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

The following are the enforcement rules applied on reaching increasing steady state:

- When the incoming traffic (measured in TPS) is greater than 80% of the licensed TPS, SNMP Trap will be generated for the first time on reaching the increased steady state. The warning message on the current license usage is logged for every 5 minutes.
- When the incoming traffic (measured in TPS) is greater than 90% of the licensed TPS, SNMP Trap will be generated for the first time on reaching the increased steady state. Warning message on the current license usage is logged for every 5 minutes.
- When the incoming traffic (measured in TPS) is greater than 100% of the licensed TPS, SNMP Trap will be generated for the first time on reaching the increased steady state. Error message on the current license usage is logged for every 5 minutes.
- When the incoming traffic (measured in TPS) is greater than 110% of the licensed TPS, SNMP Trap will be generated for the first time on reaching the increased steady state.

Note Steady state denotes continuous increase or decrease in the TPS within a given TPS range. For the purpose of enforcement of licensing in Tech Mahindra Access Registrar, the range is always 80% and above. The enforcement begins after TPS reaches and is greater than 80% for a steady state of 20 minutes.

Notification Logs

A warning message is logged for every 5 minutes when the TPS count reaches an increased steady state, where, the TPS count is in the range of 80% to 100% of the licensed TPS.

An error message is logged for every 5 minutes when the TPS count reaches an increased steady state, where, the TPS count is in the range of 100% to 110% of the licensed TPS.

Notification - SNMP Traps

The **carLicenseUsage** traps are generated only once in an increasing phase. The incoming traffic slabs are defined as 80%, 90%, 100%, and 110% of the licensed TPS. When the incoming traffic slabs reaches an increasing steady state of 80% or above for the first time, the respective trap is generated for the slab.

If the TPS count drops below 80% of the licensed TPS for a steady state period of 20 minutes, Tech Mahindra Access Registrar marks it as decreased or normal steady state. Traps will be regenerated again only if Tech Mahindra Access Registrar observes a decreased steady state followed by an increased steady state of TPS falling under the slab (say 80%).

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

TPS Logging Feature

The properties in Advanced Object such as TPSSamplingPeriodInSecs, LogTPSActivity, TPSLogFilenamePrefix and TPSLogFileCount enable logging of TPS in the Tech Mahindra Access Registrar server. TPS log file is located in **/techm-ar/**logs. It creates one file per day to hold the TPS information for the day. The TPS samples are collected for every TPSSamplingPeriodInSecs. The file is updated only once for every 10* TPSSamplingPeriodInSecs. If there is no inflowing traffic, Tech Mahindra Access Registrar logs zero TPS once for every 10* TPSSamplingPeriodInSecs. See the "Configuring and Monitoring the RADIUS Server" chapter of the *Tech Mahindra Access Registrar 9.2 Administrator Guide* for more information on TPSSamplingPeriodInSecs, LogTPSActivity, TPSLogFilenamePrefix, and TPSLogFileCount properties.

The following is the sample configuration of tps license:

```
/techm-ar/bin/aregcmd -s
set /Radius/Advanced/LogTPSActivity TRUE
set /Radius/Advanced/TPSLogFilenamePrefix tps
set /Radius/Advanced/TPSLogFileCount 5
set /Radius/Advanced/TPSSamplingPeriodInSecs 30
save
```

The following is the sample output of the log file:

```
[root@ar-lnx-vm020 logs]# tail -f sm-04-24-2016.csv
04-24-2016,18:36:30,2998,1000
04-24-2016,18:36:51,2997,1000
04-24-2016,18:37:11,996,408
04-24-2016,18:37:32,3532,1263
04-24-2016,18:37:53,2763,1000
04-24-2016,18:38:14,4749,1669
```

In the above example, the first numerical value (2998) in the log entry denotes the total TPS traffic and the second value (1000) denotes the SIGTRAN-M3UA traffic.

For TPS measurement in Tech Mahindra Access Registrar server, you can run the TPS calculator script when you want to monitor the TPS during the peak period or run the TPS for 24 hours.

Concurrent Session License Features

In Concurrent Session based license, the licensing is done based on the number of sessions that resides in Tech Mahindra Access Registrar.

Note During startup of the Tech Mahindra Access Registrar, the default session manager must be enabled for RADIUS and the EnableStickySession must be set to TRUE for Diameter. This is applicable only for session based license.

The sticky sessions is enabled during the initialization of Tech Mahindra Access Registrar for Diameter based license to track the session counts in the diameter service. The server level count is calculated by adding all the sessions maintained across all the session managers and the sticky sessions of all the diameter services in the server. This session count is used by licensing module for license enforcement. The session count is either increased or decreased based on the action performed.

This section contains the following topics:

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

- Sessions Enforcement Rules
- Notification Logs
- Notification - SNMP Traps
- Session Logging Feature

Sessions Enforcement Rules

The following are the enforcement rules applied on concurrent session based license:

- When the session count (measured in concurrent session) reaches 80% of the licensed sessions, SNMP Trap will be generated for the first time on reaching the increased steady state. The warning message on the current license usage is logged for every 5 minutes.
- When the session count (measured in concurrent session) reaches 90% of the licensed sessions, SNMP Trap will be generated for the first time on reaching the state. The warning message on the current license usage is logged for every 5 minutes.
- When the session count (measured in concurrent session) attains 100% of the licensed sessions, SNMP Trap will be generated for the first time on reaching the state. The error message on the current license usage is logged for every 5 minutes.
- When the session count (measured in concurrent session) attains 110% of the licensed sessions, SNMP Trap will be generated for the first time on reaching the state.

Note The steady state period is not applicable for Concurrency Session based licensing.

Notification Logs

A warning message is logged for every 5 minutes when the session count reaches 80% and 90% of the licensed Concurrent Session.

An error message is logged when the session count reaches the range of 100% to 110% of the licensed Concurrent Session.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Notification - SNMP Traps

The **carLicenseUsage** trap is generated when the Tech Mahindra Access Registrar server reaches 80%. The incoming traffic slabs defined for trap generation are 80%, 90%, 100%, and 110% of the licensed Concurrent Sessions. These traps are generated once for every slab during the increasing steady state.

Note Logging Feature is applicable for session based license as like TPS logging feature. The warning messages are displayed corresponding to session logging feature. See TPS Logging Feature for more information.

Session Logging Feature

The properties in Advanced Object such as SessionSamplingPeriodInSecs, LogSessionActivity, SessionLogFilenamePrefix and SessionLogFileCount enable logging of session count in the Tech Mahindra Access Registrar server. The session log file is located in **/techm-ar/**logs. It creates one file per day to hold the session information for the day. The session samples are collected for every SessionSamplingPeriodInSecs. The file is updated only once for every 10* SessionSamplingPeriodInSecs. See the "Configuring and Monitoring the RADIUS Server" chapter of the *Tech Mahindra Access Registrar 9.2 Administrator Guide* for more information on SessionSamplingPeriodInSecs, LogSessionActivity, SessionLogFilenamePrefix, and SessionLogFileCount properties.

The following is a sample configuration of session license:

```
/techm-ar/bin/aregcmd -s
set /Radius/Advanced/LogSessionActivity TRUE
set /Radius/Advanced/SessionLogFilenamePrefix sm
set /Radius/Advanced/SessionLogFileCount 5
set /Radius/Advanced/SessionSamplingPeriodInSecs 10
save
```

The following is the sample output of the log file:

```
[root@ar-lnx-vm020 logs]# tail -f sm-08-09-2016.csv

08-09-2016, 5:18:52,100, 20
08-09-2016, 5:19:22,130, 45
08-09-2016, 5:19:52,160, 60
08-09-2016, 5:20:22,175, 70
08-09-2016, 5:20:52,210, 85
08-09-2016, 5:21:22,195, 83
08-09-2016, 5:21:52,225, 95
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Chapter 8

Logging Syslog Messages

Logging messages via syslog provides centralized error reporting for Tech Mahindra Access Registrar. Local logging and syslog logging can be turned on or off at any time by modifying the control flags in the **$INSTALLPATH/conf/car.conf** file.

Logging syslog messages requires a UNIX host running a ***syslog daemon*** as a receiver for Tech Mahindra Access Registrar messages. Tech Mahindra Access Registrar and the syslog daemon can be running on the same host or different hosts.

This chapter contains the following sections:

- Syslog Messages
- Configuring Message Logging
- Configuring Syslog Daemon (syslogd)
- Changing Log Directory
- Managing the Syslog File
- Server Up/Down Status Change Logging
- Logging Subscriber Data
- Logging User IP Information
- Support for Logging Timeout Packets
- Logging System Statistics
- Logging Worker Queue Size

Syslog Messages

Messages sent to the following logs will be forwarded to **syslog** server in a slightly different format. The logs are:

- aregcmd_log
- config_mcd_[1..n]_log
- name_radius_[1..n]_log
- agent_server_[1..n]_log

Messages less than 1024 bytes in length display in the following format:

```
MMM DD hh:mm:ss hostname %Prime AR-[severity]-[mnemonic]: [#n], [System|Server]:
message_description
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Where:

MMM DD is the month and date that the message is received by the syslog server.

hh:mm:ss is the arrival time of the message.

hostname is the name of the syslog server.

severity is one of the following levels:

0 - emergency

1 - alert

2 - critical

3 - error

4 - warning

5 - notification

6 - informational

7 - debugging

mnemonic can be ***aregcmd***, ***name_radius***, ***agent_server*** and ***config_mcd*** for the identification of Tech Mahindra Access Registrar-relative subsystems.

#n is the id for the components: ***name_radius***, ***agent_server***, and ***config_mcd***

message_description provides detailed information of the message.

Messages greater than 1024 bytes in length display in multiple lines. At the end of each 1024 bytes line, three dots indicate a continuation of the message as follows:

```
MMM DD hh:mm:ss hostname %Prime AR-[severity]-[mnemonic]: [#n], [System|Server]:
message_description: Configuration: text and more message text and more message text
and more message text and more message text and more message text and more message
text and more message text and more message text and more message text and more
message text and more message text and more message text and more message text and
more message text and more message text and more message text and more message text
and more message text and more message text and more message text and more message
text and more message text and more message text and more message text ...
```

The continuation of a message begins with three dots as follows:

```
MMM DD hh:mm:ss hostname %Prime AR-[severity]-[mnemonic]: [#n], [System|Server]:
message_description: Configuration: ... text and more message text and more message
text and more message text and more message text and more message text and more
message text and more message text and more message text and more message text and
more message text and more message text and more message text
```

Example 1

```
May 19 14:28:44 dwlau-ultra2.techmahindra.com
%Prime AR-3-name_radius: #1, System: Remote LDAP Server.Unable to bind.
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Example 2

```
May 19 14:28:45 dwlau-ultra2.techmahindra.com
%Prime AR-6-name_radius: #1, Server: Stopping server
```

Configuring Message Logging

To enable **syslog** logging in Linux, you must modify the **syslog.conf** file in the **/etc/sysconfig** directory. The following is the default syslog file.

```
# Options to syslogd
# -m 0 disables 'MARK' messages.
# -r enables logging from remote machines
# -x disables DNS lookups on messages recieved with -r
# See syslogd(8) for more details
SYSLOGD_OPTIONS="-m 0"
# Options to klogd
# -2 prints all kernel oops messages twice; once for klogd to decode, and
#    once for processing with 'ksymoops'
# -x disables all klogd processing of oops messages entirely
# See klogd(8) for more details
KLOGD_OPTIONS="-x"
```

To enable logging of **syslog** messages, you must enable the **syslog** daemon to listen on port 514 by adding the -r flag to the SYSLOGD_OPTIONS line as follows:

```
SYSLOGD_OPTIONS=”-r -m 0”
```

For RHEL version 7.0 and above, you must update the /etc/rsyslog.conf file with the following information and restart the syslog service:

```
$ModLoad imudp.so
$UDPServerRun 514
SYSLOGD_OPTIONS="-r -m 0"
localn.info <tab> <tab> <tab> /var/log/filename.log
```

To restart the syslog service:

```
systemctl restart rsyslog.service
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Configuring Syslog Daemon (syslogd)

You must specify the facility from which *syslogd* will receive messages and the file into which the messages will be deposited.

In the syslog server's **/etc/syslog.conf** file, the following line might be needed.

```
local*n*.info <tab> <tab> <tab> /var/log/filename.log
```

Note Use at least one <tab> as a field separator.

Where:

local*n*—is the facility being used for syslogd; ***n*** must be a value from 0-7 and match the FACILITY_LOCAL_NUMBER used in Tech Mahindra Access Registrar's **car.conf** file.

/var/log/—is the path to the file that stores **syslogd** messages.

filename.log—is the file that stores **syslogd** messages. You can give this file a name of your choice.

Creating a Syslog Log File

To create a syslog log file:

Step 1 Log in as user ***root***.

Step 2 Enter the following command, where ***filename.log*** is a name you choose.

touch *filename.log*

Step 3 Change permissions on the syslog log file by entering the following:

chmod 664 *filename.log*

Changing Log Directory

You can change the directory where local log messages are stored by adding the following line in the **$INSTALLPATH/conf/car.conf** file.

```
LOGDIR full_path
```

Where *full_path* is a full path to the directory where you want to store the log messages. For example, to store all system logs in **/var/log/AICar1**, add the following line in the **$INSTALLPATH/conf/car.conf** file:

```
LOGDIR /var/log/AICar1
```

You must first stop the Tech Mahindra Access Registrar server prior to changing the **car.conf** file. After changing the **car.conf** file, copy all existing log files to the new directory, then restart the server.

Note Specifying a path for local logging does not affect the storage location of syslog messages.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Managing the Syslog File

Left unmanaged, the **syslog** file will grow in size over time and eventually fill all available disk space in its partition. Tech Mahindra Access Registrar writes log files and session data (to persist user sessions) in the same disk partition where Tech Mahindra Access Registrar is installed.

In normal operation, log files consume a large amount of disk space. If log files are not managed regularly, Tech Mahindra Access Registrar might not have sufficient disk space to write session data. To avoid this, you should move the Tech Mahindra Access Registrar log files directory to a different disk partition than the one where Tech Mahindra Access Registrar writes session data, as described in Changing Log Directory.

Using a cron Program to Manage the Syslog Files

We recommend that you use the **cron** program to manage the **syslog** files.

The following example **crontab** file performs a weekly archival of the existing **syslog** file (named **ar_syslog.log** in this example). This scheme keeps the previous two week's worth of **syslog** files.

```
#
#  At 02:01am on Sundays:
#  Move a weeks worth of 'ar_syslog.log' log messages to 'ar_syslog.log.1'.
#  If there was a 'ar_syslog.log.1' move it to 'ar_syslog.log.2'.
# If there was a 'ar_syslog.log.2' then it is lost.
01 02 * * 0 cd /var/log;
if [ -f ar_syslog.log ];
then if [ -f ar_syslog.log.1 ];
then /bin/mv ar_syslog.log.1 ar_syslog.log.2;
fi;
/usr/bin/cp ar_syslog.log ar_syslog.log.1;
>ar_syslog.log;
fi
```

Note Consider using move (**mv**) or copy (**cp**) commands to store the previous week's syslog files in a different disk partition to reserve space for the current syslog file.

Using a cron Program to Manage the Syslog Files

To add this **crontab** segment to the existing **cron** facility in **/usr/spool/cron/crontabs** directory, complete the following steps at the syslog server console:

Step 1 Log in as user ***root***.

Step 2 Enter the following command:

```
crontab -e
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Server Up/Down Status Change Logging

Tech Mahindra Access Registrar supports RADIUS server up/down detection and logging. The information messages are saved in the **$INSTALL/logs/name_radius_1_log** file where **$INSTALL** is the Tech Mahindra Access Registrar installation directory. Each message consists of a header and a message description.

Header Formats

The format of a header entry is:

mm/*dd*/*yyyy HH*:*MM*:*SS* name/radius/*n* Error Server 0

Example Log Messages

Following are the descriptions and types of messages that can be found within the *<AR_install_dir>***/logs/name_radius_1_log** file:

1. Tech Mahindra Access Registrar detects a Remote Server when it responds for the first time or after it is reentered into Tech Mahindra Access Registrar's server pool for retry. The format of the message is:

   Remote Server <*hostname*> (<*ipaddress*>:<*port*>) is UP!

   The following is an example header and message:

   ```
   10/12/2013 17:56:32 name/radius/1 Error Server 0
   Remote Server dave-ultra (171.69.127.99:1812) is UP!
   ```

   Tech Mahindra Access Registrar detects the Remote Server is not responding to its request. The format of the message is:

   Remote Server <*hostname*> (<*ipaddress*>:<*port*>) is DOWN!

   The following is an example header and message:

   ```
   10/12/2013 17:57:12 name/radius/1 Error Server 0 Remote
   server dave-ultra (171.69.127.99:1812) is DOWN!
   ```

2. Tech Mahindra Access Registrar receives no response from the Remote Server after the server is reentered into Tech Mahindra Access Registrar's server pool for retry. The format of the message is:

   Remote Server <*hostname*> (<*ipaddress*>:<*port*>) remains DOWN!

   The following is an example header and message:

   ```
   10/12/2013 17:56:32 name/radius/1 Error Server 0 Remote
   server dave-ultra (171.69.127.99:1812) remains DOWN!
   ```

3. The Remote Server is responding to the first retry but not the initial request. The format of the message is:

   Remote Server <*hostname*> (<*ipaddress*>:<*port*>) is UP but slow!

   The following is an example header and message:

   ```
   10/12/2013 17:56:32 name/radius/1 Error Server 0 Remote
   server dave-ultra (171.69.127.99:1812) is UP but slow!
   ```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

4. The Remote Server is responding to the second retry request but not the initial request or the first retry request. The format of the message is:

   Remote Server <*hostname*> (<*ipaddress*>:<*port*>) is UP but very slow!

   The following is an example header and message:

   ```
   10/12/2013 17:56:32 name/radius/1 Error Server 0 Remote
   server dave-ultra (171.69.127.99:1812) is UP but very slow!
   ```

5. The Remote Server has been marked inactive and is being put back into Tech Mahindra Access Registrar's server pool for later use. The format of the message is:

   Remote Server <*hostname*> (<*ipaddress*>:<*port*>) is being reactivated for later use.

   The following is an example header and message:

   ```
   10/12/2013 17:56:32 name/radius/1 Error Server 0 Remote
   server dave-ultra (209.165.200.224:1812) is being reactivated for later use.
   ```

Logging Subscriber Data

Tech Mahindra Access Registrar stores all subscriber message details including Diameter request and response in a separate log file called **Subscriber_log** under $INSTALLPATH/logs folder. To log subscriber data for a selected Diameter client or remote server, you must set the corresponding **UserLogEnabled** parameter to True.

Message Format:

```
Date|Time|Diameter-Message-Type|User-Name(IMSI) \
|MSISDN|Subscirption-Id|Origin-Host|Host-IP-Address|Product-Name|Origin-Realm|Destin\
ation-Host|APN-Name|Session-id|Result_Code|Result-Description|UELocalIPAddress|Non-3\
GPP-IP-Access
```

Logging User IP Information

Tech Mahindra Access Registrar provides an option to capture the username as part of the aregcmd_log during login failures. The following parameter is added under ***/Radius/Advanced*** to support this feature:

DisplayUserForFailedLogin—If this option is enabled, during login failures, username is captured along with the failure reason as part of the aregcmd_log.

Also, for all the configuration, login, and logout activities, Tech Mahindra Access Registrar displays the end user IP in the aregcmd_log. With this enhancement, Tech Mahindra Access Registrar will start logging the end user's IP address, which is the immediate first hop IP for every aregcmd activity.

Support for Logging Timeout Packets

With this enhancement, Tech Mahindra Access Registrar starts logging information about all packets that timeout i.e. packets which are not responded to within the specified timeout period.

A sample log file content is provided below:

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
07/04/2020 14:08:35.904 name/radius/1 Info System 0 Remote Server REM_76 has not responded
Cmd code: 303 request for user-name 97000000051 in 1 try
```

Logging System Statistics

With this enhancement, Tech Mahindra Access Registrar allows you to collect following statistics data for a configured duration:

- CPU Utilization
- Memory Utilization
- NFSIOstats
- Peak Worker Thread Queue / sec (for reporting of All Workers Temporarily Busy warning)

Global Statistics:

- TimedOut MAR/SAR/UDR
- Throttled Packets Count
- PacketsInUse Count
- DEA EAP Multi-Round Auth Success Responses
- DER Challenge Requests Count
- DuplicateSessionID Packets Count
- TimerQueue Entries Count

Per Connection Statistics:

- TimedOut MAR/SAR/UDR
- Throttled Packets Count
- Dropped DuplicateSessionID Packets Count
- Dropped Outgoing Responses for STA/AAA/DEA
- Dropped Incoming Responses for MAA/SAA/UDA/CEA/DWA
- Incoming Requests per Second
- Outgoing Requests per Second,
- Retransmitted Requests per Second
- Incoming Responses per Second
- Outgoing Responses per Second

A new parameter **SystemStatsLogFrequencyInSecs** is added under ***/Radius/Advanced/Diameter/TransportManagement***, which when set to a non-zero value, allows you to log the above statistics for the configured duration. By default this value is set to zero. The system statistics are saved in the **system_stats_log** file.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Logging Worker Queue Size

Reporting of **All Workers Temporarily Busy** warning has been added to the System Stats Log under the parameter **Peak Worker Thread Queue / sec,** and is only reported if the condition has occurred during the last statistics interval.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Chapter 9

Troubleshooting Tech Mahindra Access Registrar

This chapter provides information about techniques used when troubleshooting Tech Mahindra Access Registrar and highlights common problems.

This chapter contains the following sections:

- Gathering Basic Information
- Troubleshooting Quick Checks
- aregcmd and Tech Mahindra Access Registrar Configuration
- RADIUS Request Processing
- Other Troubleshooting Techniques and Resources
- Checking Tech Mahindra Access Registrar Server Health Status

Gathering Basic Information

Table 9-1 lists UNIX commands that provide basic and essential information to help you understand the Tech Mahindra Access Registrar installation environment.

Table 9-1 UNIX Commands to Gather Information

UNIX Command	Information Returned
/usr/bin/uname -r	Release level
/usr/bin/uname -i	Machine hardware name
/usr/bin/uname -v	OS version
/usr/bin/uname -a	All system information including hostname, operating system type and release, machine model and type
/usr/sbin/prtconf	System configuration information including memory capacity, machine type, and peripheral equipment
/usr/sbin/df -k	File system disk space usage including partitions, capacity, and space used
/usr/bin/ps -ef	Currently running processes

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table 9-1 UNIX Commands to Gather Information (continued)

UNIX Command	Information Returned
/usr/sbin/psinfo -v	Information about processors
/usr/bin/pkginfo -l TMar	Software package information about Tech Mahindra Access Registrar version number and installation directory

Note More information about these commands and their options is available using the **man** command in a terminal window on the Sun workstation.

Troubleshooting Quick Checks

Many of the most common problems can be diagnosed by doing the following:

- Check disk space
- Check for resource conflicts
- Check the Tech Mahindra Access Registrar log files

Disk Space

Running out of disk space can cause a number of problems including:

- Failure to process RADIUS requests
- Parts of the Tech Mahindra Access Registrar configuration *disappearing* in **aregcmd**
- Failure to log into **aregcmd**

Check that the Tech Mahindra Access Registrar installation partition (**$INSTALL**) and **/tmp** are not at capacity.

Resource Conflicts

Resource conflicts are a common reason for the Tech Mahindra Access Registrar server failing to start. The most common resource conflicts are the following:

- Cisco Prime Network Registrar is running on the Tech Mahindra Access Registrar server
- Another application is also using ports 1812 and 1813
- A network management application is using the Sun SNMP Agent

No Co-Existence With Cisco Prime Network Registrar

Cisco Prime Network Registrar cannot coexist on a machine running Tech Mahindra Access Registrar for this reason. You can determine if CNR is running by entering the following command line in a terminal window:

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

pkginfo | grep -i “network registrar”

Port Conflicts

The default ports used by the Tech Mahindra Access Registrar server are ports 1812 and 1813. You should check to determine that no other applications are listening on the same ports as Tech Mahindra Access Registrar.

You can check to see which TCP ports are in use by entering the following command line:

netstat -aP tcp

You can check to see which UDP ports are in use by entering the following command line:

netstat -aP udp

Note If you configure the Tech Mahindra Access Registrar server to use ports other than the default, you will have to specifically add those ports if you want to use them.

Tech Mahindra Access Registrar Log Files

Examining the Tech Mahindra Access Registrar log files can help you diagnose most Tech Mahindra Access Registrar issues. By default, the Tech Mahindra Access Registrar log files are located in **/opt/TMar/logs**. Table 9-2 lists the Tech Mahindra Access Registrar log files and the information stored in each log.

Table 9-2 Tech Mahindra Access Registrar Log Files

Log File	Information Recorded
agent_server_1_log	Log of the server agent process
ar-status	Log of Tech Mahindra Access Registrar stop and start using the **arserver** utility
aregcmd_log	Log of commands executed in aregcmd (very useful for tracing the steps that took place before a problem occurred)
config_mcd_1_log	Log of the mcd internal database
name_radius_1_log	Log of the radius server process
name_radius_1_trace	Debugging output of RADIUS request processing (only generated when the trace level, set in **aregcmd**, is greater than zero)

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table 9-2 Tech Mahindra Access Registrar Log Files (continued)

Log File	Information Recorded
m3ua	System logs related to stack including m3ua client and stack manager; and radius communication logs related to m3ua stack. These are typically low level debug logs
Subscriber_log	Log that records all subscriber messages including Diameter request and response in a separate log file in the $INSTALLPATH/logs folder.

Modifying File Sizes for Agent Server and MCD Server Logs

The two parameters added to the **car.conf** file under **$BASEDIR/conf** affect the **agent_server_logs** and **config_mcd_server_logs logs** files:

- AGENT_SERVER_LOG_SIZE (10 MB by default)
- AGENT_SERVER_LOG_FILES (2 by default)

You will find these new parameters at the beginning of the **car.conf** file. When the log file size reaches the value set in AGENT_SERVER_LOG_SIZE, a rollover of the **agent_server_log_file** occurs. The value set in AGENT_SERVER_LOG_FILES specifies the number of log files to be created.

Using xtail to Monitor Log File Activity

A useful way of monitoring all of the log files is to run **xtail**, a utility provided with Tech Mahindra Access Registrar. The **xtail** program monitors one or more files and displays all data written to a file since command invocation.

Run **xtail** in a dedicated terminal window. It is very useful for monitoring multiple logfiles simultaneously, such as with a command line like the following:

xtail $INSTALL/logs/*

Note Cisco Prime AR 4.1.5 and later include the millisecond field in the logs' timestamp.

Modifying the Trace Level

By modifying the trace level, you can gather more detailed information in the log files about what is happening in the Tech Mahindra Access Registrar server. There are five different trace levels. Each higher trace level also includes the information logged using lower trace levels. The different trace levels provide the following information:

- Level 0—No tracing occurs
- Level 1—Indicates when a packet is sent or received and when a status change occurs in a remote server (RADIUS Proxy and LDAP)
- Level 2—Information includes the following:
  - Which services and session managers are used to process

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

  - Which client and vendor objects are being used to process a packet
  - More details about remote servers (RADIUS Proxy and LDAP), packet transmission, and timeouts
  - Details about poorly-formed packets.
- Level 3—Information includes the following:
  - Tracing of errors in Tcl scripts when referencing invalid RADIUS attributes
  - Which scripts have been run
  - Details about local userlist processing
- Level 4—Information includes the following:
  - Advanced duplication detection processing
  - Details about creating, updating, and deleting sessions
  - Tracing of all APIs called during the running of a script
- Level 5—Provides information about policy engine operations

Installation and Server Process Start-up

The installation process installs the Tech Mahindra Access Registrar software to the specified installation directory and then starts the server processes. This process rarely fails but the following checks should always be performed:

- Ensure that there is an **installation success message** at the end of the **pkgadd** dialog, otherwise check the dialog for the problem
- Follow the installation instructions carefully especially when performing an upgrade. For example, when upgrading to 1.6R1, 1.6R2, or 1.6R3, a post-installation upgrade script needs to be run
- Pay attention to the information included in README files

At the end of a successful installation, **arstatus** should show the following four server processes:

> **$INSTALL/usrbin/arstatus**

```
AR RADIUS server running   (pid: 6285)
AR MCD lock manager running (pid: 6284)
AR MCD server running   (pid: 6283) AR
Server Agent running    (pid: 6277)
```

If any of the above processes are not displayed, check the log file of the failed process to determine the reason. The MCD processes might fail to start if Cisco Prime Network Registrar is installed on the same machine.

The manual method of starting and stopping the Tech Mahindra Access Registrar processes is using the **arserver** utility.

To start Tech Mahindra Access Registrar processes: **arserver start**

To stop Tech Mahindra Access Registrar processes: **arserver stop**

To restart Tech Mahindra Access Registrar processes: **arserver restart**

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

aregcmd and Tech Mahindra Access Registrar Configuration

While troubleshooting, you should always use the **aregcmd** command trace to turn on tracing. With tracing active, Tech Mahindra Access Registrar generates debugging output to the log file **name_radius_1_trace**.The syntax is:

trace [<server>] [<level>]

When you do not specify a server, Tech Mahindra Access Registrar sets the trace level for all servers in the current cluster. When you do not specify a trace level, the currently set level is used. The default trace level is 0.

Running and Stopped States

Tech Mahindra Access Registrar can be in two states, running or stopped. In either state, all four Tech Mahindra Access Registrar processes remain running. The state of Tech Mahindra Access Registrar will be displayed when logging into **aregcmd** or by using the **aregcmd status** command:

status

```
Server 'Radius' is Running, its health is 10 out of 10\
```

The **start** and **stop** commands allow Tech Mahindra Access Registrar to move between states. **Reload** is equivalent to a **stop** followed by a **start** if Tech Mahindra Access Registrar is already running, and just a **start** if it is already stopped.

stop

```
Stopping Server 'Radius'...
Server 'Radius' is Stopped
```

start

```
Starting Server 'Radius'...
Server 'Radius' is Running, its health is 10 out of 10
```

reload

```
Reloading Server 'Radius'...
Server 'Radius' is Running, its health is 10 out of 10
```

During the transition from running to stopped, Tech Mahindra Access Registrar stops processing new RADIUS requests and releases resources such memory, network and database connections and open files.

During the transition from stopped to running, Tech Mahindra Access Registrar reverses this process by opening a connection with its internal database, reading configuration data, claiming memory, establishing network connections, opening files, and initializing scripts. During this transition, problems can occur. Tech Mahindra Access Registrar might fail to start and display the following:

reload

```
Reloading Server 'Radius'...
310 Command failed
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Tech Mahindra Access Registrar failed to move from stopped state to running:

status

```
Server 'Radius' is Stopped
```

This might occur for a number of reasons including the following:

- An invalid configuration
- Insufficient memory
- Listening ports already in use by another application
- Unable to open files
- Unable to initialize scripts

Check the **name_radius_1_log** file for the one of these indications.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

RADIUS Request Processing

The main technique for troubleshooting RADIUS request processing in Tech Mahindra Access Registrar is to examine the **name_radius_1_trace** log file with the trace level set to 5. Most issues are fairly self-explanatory. Some issues that can arise are as follows:

- Tech Mahindra Access Registrar has marked a remote server as ***down***
- A resource manager has run out of resources (for example, user or group session limit has been reached or no more IP addresses are available)
- A configuration error (such as an accounting service not being set)
- A run time error in a script

Some issues are not immediately evident from the log files though, such as the following:

- Failure to save or reload Tech Mahindra Access Registrar after a configuration change
- Tech Mahindra Access Registrar is not listening on the correct UDP ports for RADIUS requests

Other Troubleshooting Techniques and Resources

aregcmd Stats Command

The **aregcmd** command **stats** provides statistics on request processing.

--> **stats**

```
Global Statistics for Radius:
serverStartTime = Tue Oct  2 10:28:02 2013
serverResetTime = Tue Oct  2 20:25:12 2013
serverState = Running
totalPacketsInPool = 1024
totalPacketsReceived = 0
totalPacketsSent = 0
totalRequests = 0
totalResponses = 0
totalAccessRequests = 0
totalAccessAccepts = 0
totalAccessChallenges = 0
totalAccessRejects = 0
totalAccessResponses = 0
totalAccountingRequests = 0
totalAccountingResponses = 0
totalStatusServerRequests = 0
totalAscendIPAAllocateRequests = 0
totalAscendIPAAllocateResponses = 0
totalAscendIPAReleaseRequests = 0
totalAscendIPAReleaseResponses = 0
totalUSRNASRebootRequests = 0
totalUSRNASRebootResponses = 0
totalUSRResourceFreeRequests = 0
totalUSRResourceFreeResponses = 0
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
totalUSRQueryResourceRequests = 0
totalUSRQueryResourceResponses = 0
totalUSRQueryReclaimRequests = 0
totalUSRQueryReclaimResponses = 0
totalPacketsInUse = 0
totalPacketsDrained = 0
totalPacketsDropped = 0
totalPayloadDecryptionFailures = 0

Global Statistics for Radius:
serverStartTime = Sat Dec 7 07:37:52 2013
serverResetTime = Sat Dec 7 07:37:52 2013
serverState = Running
cdbpLocalStatsTotalUpTime = 1486 seconds
cdbpLocalResetTime = 1486 seconds
cdbpLocalStatsTotalPacketsIn = 30
cdbpLocalStatsTotalPacketsOut = 30
cdbpLocalStatsTotalPacketsInUse = 0
```

Core Files

A core file in the Tech Mahindra Access Registrar installation directory is an indication that Tech Mahindra Access Registrar has crashed and restarted. Check that the radius server process generated the core file using the UNIX **file** command:

> **file core**

```
core:           ELF 32-bit MSB core file SPARC Version 1, from 'radius'
```

Check the timestamp on the core file and look for corresponding log messages in the **name_radius_1_log** file in **$INSTALL/logs**. The word *assertion* commonly appears in core messages. Try to establish what caused the problem and contact Tech Mahindra TAC.

radclient

The Tech Mahindra Access Registrar package provides a utility called **radclient** that allows RADIUS requests to be generated. Use **radclient** to test configurations and troubleshoot problems.

Tech Mahindra Access Registrar Replication

For more information about using Tech Mahindra Access Registrar replication, see Chapter 4, “Replication Log.”

Checking Tech Mahindra Access Registrar Server Health Status

To check the server’s health, use the **aregcmd** command **status**. The following issues decrement the server’s health:

- Multiple occurrences of Access-Request rejection

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Note One of the parameters in the calculation of the Tech Mahindra Access Registrar server's health is the percentage of responses to Access-Accepts that are rejections. In a healthy environment, the rejection percentage will be fairly low. An extremely high percentage of rejections could be an indication of a Denial of Service attack.

- Configuration errors
- Running out of memory
- Errors reading from the network
- Dropping packets that cannot be read (because the server ran out of memory)
- Errors writing to the network.

Tech Mahindra Access Registrar logs all of these conditions. Sending multiple successful responses to any packet, increments the server's health.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Appendix A

Tech Mahindra Access Registrar Tcl, REX, and Java Dictionaries

This appendix describes the Tcl and REX dictionaries that are used when writing Incoming or Outgoing scripts.

A dictionary is a data structure that contains key/value pairs. Two types of dictionaries exist: the Attribute dictionaries (used by the Request and Response dictionaries), and the Environment dictionary.

This section contains the dictionaries you reference when writing a Tcl script and the dictionaries you reference when you write a script using the shared libraries (REX—RADIUS EXtension).

This appendix section also describes the following Java attribute dictionary:

- Tcl Attribute Dictionaries
- REX Attribute Dictionary
- Java Attribute Dictionary

Tcl Attribute Dictionaries

An *Attribute dictionary* is a dictionary in which the keys are constrained to be the names of attributes as defined in the Tech Mahindra Access Registrar server configuration, and the values are the string representation of the legal values for that particular attribute. For example, IP addresses are specified by the dotted-decimal string representation of the address, and enumerated values are specified by the name of the enumeration. This means numbers are specified by the string representation of the number.

Attribute dictionaries have the unusual feature that there can be more than one instance of a particular key in the dictionary. These instances are ordered, with the first instance at index zero. Some of the methods of an Attribute dictionary allow an index to be specified to indicate a particular instance or position in the list of instances to be referenced. This section contains the following topics:

- Attribute Dictionary Methods
- Tcl Environment Dictionary

Attribute Dictionary Methods

Attribute dictionaries use active commands, called *methods*, that allow you to change and access the values in the dictionaries. Table A-1 lists of all of the methods you can use with the Request and Response dictionaries.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table A-1 Tcl Attribute Dictionary Methods

Name	Syntax	Description
addProfile	**$dict addProfile** <*profile*> [<*mode*>]	Copies all of the attributes in the profile <*profile*> into the dictionary. Note, <*profile*> must be the name of one of the profiles listed in the server configuration. When <*mode*> is not provided or when <*mode*> equals the special value **REPLACE**, any duplicate instances of the attributes in the dictionary are replaced with the attribute from <*profile*>. When <*mode*> is provided and equals the special value **APPEND**, new instances of the attributes are appended to the attributes already in the dictionary. When <*mode*> is provided and equals the special value **AUGMENT**, only add the attribute when it does not already exist.
clear	**$dict clear**	Removes all entries from the dictionary.
containsKey	**$dict containsKey** <*attribute*>	Returns 1 when the dictionary contains the attribute <*attribute*>, otherwise returns 0.
firstKey	**$dict firstKey**	Returns the name of the first attribute in the dictionary. Note, the attributes are not stored in a sorted order of name.
get	**$dict get** <*attribute*> [<*index*> [**bMore**]]	Returns the value of the <*attribute*> attribute from the dictionary, represented as a string. When the dictionary does not contain the <*attribute*>, an empty string is returned. When <*index*> is provided, return the <*index*>'th instance of the attribute. Some attributes can appear more than once in the request (or response) packet. The <*index*> argument is used to select which instance to return. When **bMore** is provided, the **get** method sets **bMore** to 1 when more attributes exist after the one returned, and to 0 otherwise. You can use this to determine whether another call to **get** should be made to retrieve other instances of the attribute.
isEmpty	**$dict isEmpty**	Returns 1 when the dictionary has no entries, otherwise returns 0.
log	**$dict log** <*level*> <*message*> …	Outputs a message into the RADIUS server's logging system. The <*level*> should be either **LOG_ERROR**, **LOG_WARNING**, or **LOG_INFO**. The remaining arguments are concatenated together and sent to the logging system at the specified level.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table A-1 Tcl Attribute Dictionary Methods (continued)

Name	Syntax	Description
nextKey	**$dict nextKey**	Returns the name of the next attribute in the dictionary that follows the attribute returned in the last call to **firstKey** or **nextKey**.
put	**$dict put** <*attribute*> <*value*> [<*index*>]	Associates <*value*> with the attribute <*attribute*> in the dictionary. When <*index*> is not provided or when <*index*> equals the special value **REPLACE**, any existing instances of <*attribute*> are replaced with the single value. When <*index*> is provided and equals the special value **APPEND**, a new instance of <*attribute*> is appended to the end of the list of instances of the <*attribute*>. When <*index*> is provided and is a number, a new instance of <*attribute*> is inserted at the position indicated. When <*index*> is provided and equals the special value **AUGMENT**, only put the attribute when it does not already exist.
remove	**$dict remove** <*attribute*> [<*index*>]	Removes the <*attribute*> attribute from the dictionary. When <*index*> is not provided or when <*index*> equals the special value **REMOVE_ALL**, remove any existing instances of <*attribute*>. When <*index*> is provided and is a number, remove the instance of <*attribute*> at the position indicated. Always returns 1, even when the dictionary did not contain the <*attribute*> at that <*index*>.
size	**$dict size**	Returns the number of entries in the dictionary.
trace	**$dict trace** <*level*> <*message*> ...	Outputs a message into the packet tracing system used by the RADIUS server. At level 0, no tracing occurs. At level 1, only an indication the server received the packet and sent a reply is output. As the number gets higher, the amount of information output increases, until at level 4, where everything is traced as output. The remaining arguments are concatenated and sent to the tracing system at the specified level.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Tcl Environment Dictionary

A dictionary is a data structure that contains key/value pairs. An Environment dictionary is a dictionary in which the keys and values are constrained to be strings. The Tcl Environment dictionary is used to communicate information from the script to the server and from script to script within the processing of a particular request. Note, there can be only one instance of a key in the Environment dictionary.

Table A-2 lists of all the methods you can use with the Request and Response dictionaries.

Table A-2 Tcl Environment Dictionary Methods

Name	Syntax	Description
clear	**$dict clear**	Removes all entries from the dictionary.
containsKey	**$dict containsKey** *<key>*	Returns 1 when the dictionary contains the *<key>* key, otherwise returns 0.
firstKey	**$dict firstKey**	Returns the name of the first key in the dictionary. Note, the keys are not stored sorted by name.
get	**$dict get** *<key>*	Returns the value of *<key>* from the dictionary. When the dictionary does not contain the *<key>*, an empty string is returned.
isEmpty	**$dict isEmpty**	Returns 1 when the dictionary has no entries, otherwise returns 0.
log	**$dict log** *<level> <message> …*	Outputs a message into the logging system used by the RADIUS server. *<level>* should be one of **LOG_ERROR**, **LOG_WARNING**, or **LOG_INFO**. The remaining arguments are concatenated together and sent to the logging system at the specified level.
nextKey	**$dict nextKey**	Returns the name of the next key in the dictionary that follows the key returned in the last call to **firstKey** or **nextKey**.
put	**$dict put** *<key> <value>*	Associates *<value>* with the *<key>* key in the dictionary, replacing an existing instance of *<key>* with the new value.
remove	**$dict remove** *<key>*	Removes the *<key>* key from the dictionary. Always returns 1, even when the dictionary did not contain the *<key>*.
size	**$dict size**	Returns the number of entries in the dictionary.
trace	**$dict** *<level> <message> …*	Outputs a message into the packet tracing system used by the RADIUS server. At level 0, no tracing occurs. At level 1, only an indication the server received the packet and sent a reply is output. As the number gets higher, the amount of information output is greater, until at level 4, where everything the is traced as output. The remaining arguments are concatenated together and sent to the tracing system at the specified level.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

REX Attribute Dictionary

A dictionary is a data structure that contains key/value pairs. An Attribute dictionary is a dictionary in which the keys are constrained to be the attributes as defined in the RADIUS server configuration and the values are constrained to be legal values for that particular attribute. Attribute dictionaries have the unusual feature that there can be more than one instance of a particular key in the dictionary. These instances are ordered, with the first instance at index 0. Some of the methods of an Attribute dictionary allow an index to be specified to indicate a particular instance or position in the list of instances to be referenced.

When writing REX scripts, you can specify keys as the string representation of the name of the attribute or by type, which is a byte sequence defining the attribute. The values can also be specified as the string representation of the value or as the byte sequence, which is the attribute. These options mean some of these access methods have four different variations that are the combinations of string or type for the key, and string or bytes for the value. This section contains the following topics:

- Attribute Dictionary Methods
- REX Environment Dictionary

Attribute Dictionary Methods

Attribute dictionaries use active commands, called *methods*, that allow you to change and access the values in the dictionaries.

Table A-3 lists all of the methods you can use with the Request and Response dictionaries.

Table A-3 REX Attribute Dictionary Methods

Name	Syntax	Description
addProfile	**abool_t pDict->addProfile(rex_AttributeDictionary_t* pDict, const char*** *<pszProfile>***, int** *<iMode>***)**	Copies all of the attributes in the *<pszProfile>* profile into the dictionary. Note, *<pszProfile>* must be the name of one of the profiles listed in the server configuration. When *<iMode>* equals the special value **REX_REPLACE**, it replaces any duplicate instances of the attributes in the dictionary with the attribute from the profile. When *<iMode>* equals the special value **REX_APPEND**, it appends a new instance of the attributes to any attributes already in the dictionary. When *<iMode>* equals the special value. When the mode is **REX_AUGMENT**, it adds the attribute in the dictionary, if it does not already exist in the dictionary.
allocateMemory	**void* pDict->allocateMemory(rex_AttributeDictionary_t* pDict, unsigned int** *<iSize>***)**	Allocates memory for use in scripts that persist only for the lifetime of this request. This memory is released when processing for this request is complete.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table A-3 REX Attribute Dictionary Methods (continued)

Name	Syntax	Description
clear	**void pDict->clear(rex_AttributeDictionary_t* pDict)**	Removes all entries from the dictionary.
containsKey	**abool_t pDict->containsKey(rex_AttributeDictionary_t* pDict, const char*** *<pszAttribute>***)**	Returns TRUE when the dictionary contains *<pszAttribute>*, otherwise returns FALSE.
containsKeyByType	**abool_t pDict->containsKeyByType(rex_AttributeDictionary_t* pDict, const abytes_t*** *<pAttribute>***)**	Returns TRUE when the dictionary contains *<pAttribute>*, otherwise returns FALSE.
firstKey	**const char* pDict->firstKey(rex_AttributeDictionary_t* pDict)**	Returns the name of the first attribute in the dictionary. Note, the attributes are not stored in a sorted order of name.
firstKeyByType	**const abytes_t* pDict->firstKeyByType (rex_AttributeDictionary_t* pDict)**	Returns a pointer to the byte sequence defining the first attribute in the dictionary. Note, attributes are not stored sorted by name.
get	**const char* pDict->get(rex_AttributeDictionary_t* pDict, const char* pszAttribute, int** *<iIndex>***, abool_t*** *<pbMore>***)**	Returns the value of the **<***iIndex***>**'d instance of the attribute from the dictionary, represented as a string. When the dictionary does not contain the attribute (or that many instances of the attribute), an empty string is returned. When *<pbMore>* is non-zero, the **get** method sets *<pbMore>* to TRUE when more instances of the attribute exist after the one returned, and to FALSE otherwise. This can be used to determine whether another call to **get** should be made to retrieve other instances of the attribute.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table A-3 REX Attribute Dictionary Methods (continued)

Name	Syntax	Description
getBytes	**const abytes_t* pDict->getBytes(rex_AttributeDictionary_t* pDict, const char* pszAttribute, int** <*iIndex*>**, abool_t*** <*pbMore*>**)**	Returns the value of the <*iIndex*>'d instance of the attribute from the dictionary, as a sequence of bytes. When the dictionary does not contain the attribute (or that many instances of the attribute), 0 is returned. When <*pbMore*> is non-zero, the **getBytes** method sets <*pbMore*> to TRUE when more instances of the attribute exist after the one returned, and to FALSE otherwise. This can be used to determine whether another call to **getBytes** should be made to retrieve other instances of the attribute.
getBytesByType	**const abytes_t* pDict->getBytesByType (rex_AttributeDictionary_t* pDict, const abytes_t* pAttribute, int** <*iIndex*>**, abool_t*** <*pbMore*>**)**	Returns the value of the <*iIndex*>'d instance of the attribute from the dictionary, as a sequence of bytes. When the dictionary does not contain the attribute (or that many instances of the attribute), 0 is returned instead. When <*pbMore*> is non-zero, sets the variable pointed to TRUE when more instances of the attribute exist after the one returned, and to FALSE otherwise. This can be used to determine whether another call to **get** should be made to retrieve other instances of the attribute.
getByType	**const char* pDict->get(rex_AttributeDictionary_t* pDict,** const abytes_t* <*pszAttribute*>, int <*iIndex*>, abool_t* <*pbMore*>)	Returns the value of the <*iIndex*>'d instance of the attribute from the dictionary, as represented as a string. When the dictionary does not contain the attribute (or that many instances of the attribute), returns an empty string. When <*pbMore*> is non-zero, the **getByType** method sets <*pbMore*> to TRUE when more instances of the attribute exist after the one returned, and to FALSE otherwise. This can be used to determine whether another call to **getByType** should be made to retrieve other instances of the attribute.
getType	**const char* pDict->getByType(rex_AttributeDictionary_t* pDict, const abytes_t*** <*pAttribute*>**)**	Returns a pointer to the byte sequence defining the attribute, when the attribute name matches a configured attribute, zero otherwise.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table A-3 REX Attribute Dictionary Methods (continued)

Name	Syntax	Description
isEmpty	**abool_t pDict->isEmpty(rex_AttributeDictionary_t* pDict)**	Returns TRUE when the dictionary has 0 entries, FALSE otherwise.
log	**abool_t pDict->log(rex_AttributeDictionary_t* pDict, int** <*iLevel*>**, const char*** <*pszFormat*>**, ...)**	Outputs a message into the logging system used by the RADIUS server. <*iLevel*> should be one of **REX_LOG_ERROR**, **REX_LOG_WARNING**, or **REX_LOG_INFO**. The **pszFormat** argument is treated as a **printf**-style format string, and it, along with the remaining arguments, are formatted and sent to the logging system at the specified level.
nextKey	**const char* pDict->nextKey(rex_AttributeDictionary_t* pDict)**	Returns the name of the *next* attribute in the dictionary that follows the attribute returned in the last call to **firstKey** or **nextKey**.
nextKeyByType	**const abytes_t* pDict->nextKeyByType(rex_AttributeDictionary_t* pDict)**	Returns a pointer to the byte sequence defining the next attribute in the dictionary that follows the attribute returned in the last call to **firstKeyByType** or **nextKeyByType**.
put	**abool_t pDict->put(rex_AttributeDictionary_t* pDict, const char*** <*pszAttribute*>**, const char*** <*pszValue*>**, int <***iIndex***>)**	Converts <*pszValue*> to a sequence of bytes, according to the definition of <*pszAttribute*> in the server configuration. Associates that sequence of bytes with <*pszAttribute*> in the dictionary. When **<***iIndex***>** equals the special value **REX_REPLACE**, it replaces any existing instances of <*pszAttribute*> with a single value. When **<***iIndex***>** equals the special value **REX_APPEND**, it appends a new instance of <*pszAttribute*> to the end of the list of existing instances of <*pszAttribute*>. Otherwise, a new instance of <*pszAttribute*> is inserted at the position indicated. This method returns TRUE unless <*pszAttribute*> does not match any configured attributes or the value could not be converted to a legal value. When **<***iIndex***>** equals the special value **REX_AUGMENT**, only **put** <*pszAttribute*> when it does not already exist.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table A-3 REX Attribute Dictionary Methods (continued)

Name	Syntax	Description
putBytes	**abool_t pDict->putBytes(rex_AttributeDictionary_t* pDict, const char*** <*pszAttribute*>**, const abytes_t*** <*pValue*>**, int** <*iIndex*>**)**	Associates <*pValue*> with the attribute <*pszAttribute*> in the dictionary. When <*iIndex*> equals the special value **REX_REPLACE**, it replaces any existing instances of the <*pszAttribute*> with a single new value. When <*iIndex*> equals the special value **REX_APPEND**, it appends a new instance of <*pszAttribute*> to the end of the list of existing instances of <*pszAttribute*>. When <*iIndex*> equals the special value **REX_AUGMENT**, only put the <*pszAttribute*> when it does not already exist. Otherwise, a new instance of <*pszAttribute*> is inserted at the position indicated. This method returns TRUE unless the attribute name does not match any configured attributes.
putBytesByType	**abool_t pDict->putBytesByType(rex_AttributeDictionary_t* pDict, const abytes_t*** <*pAttribute*>**, const abytes_t*** <*pValue*>**, int** <*iIndex*>**)**	Associates <*pValue*> with the attribute <*pAttribute*> in the dictionary. When <*iIndex*> equals the special value **REX_REPLACE**, it replaces any existing instances of <*pAttribute*> with the new value. When <*iIndex*> equals the special value **REX_APPEND**, it appends a new instance of <*pAttribute*> to the end of the list of existing instances of <*pAttribute*>. When <*iIndex*> equals the special value **REX_AUGMENT**, only **put** <*pAttribute*> when it does not already exist. Otherwise, insert a new instance of <*pAttribute*> at the position indicated. This method returns TRUE unless the attribute name does not match any configured attributes.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table A-3 REX Attribute Dictionary Methods (continued)

Name	Syntax	Description
putByType	**abool_t pDict->putByType(rex_AttributeDictionary_t* pDict, const abytes_t*** *<pszAttribute>***, const char*** *<pszValue>***, int** *<iIndex>***)**	Converts *<pszValue>* to a sequence of bytes, according to the definition of *<pszAttribute>* in the server configuration. Associates that sequence of bytes with *<pszAttribute>* in the dictionary. When *<iIndex>* equals the special value **REX_REPLACE**, it replaces any existing instances of *<pszAttribute>* with a single new value. When *<iIndex>* equals the special value **REX_APPEND**, it appends a new instance of *<pszAttribute>* to the end of the list of existing instances of *<pszAttribute>*. Otherwise, it inserts a new instance of *<pszAttribute>* at the position indicated. This method returns TRUE unless *<pszAttribute>* does not match any configured attributes, or the value could not be converted to a legal value.
remove	**abool_t pDict->remove(rex_AttributeDictionary_t* pDict, const char*** *<pszAttribute>***, int** *<iIndex>***)**	Removes the *<pszAttribute>* from the dictionary. When *<iIndex>* equals the special value **REX_REMOVE_ALL**, removes any existing instances of *<pszAttribute>*. Otherwise, it removes the instance of *<pszAttribute>* at the position indicated. Returns TRUE, even when the dictionary did not contain *<pszAttribute>* at the *<iIndex>*, unless *<pszAttribute>* does not match any configured attribute.
removeByType	**abool_t pDict->removeByType(rex_AttributeDictionary_t* pDict, const abytes_t*** *<pAttribute>***, int** *<iIndex>***)**	Removes the *<pAttribute>* from the dictionary. When *<iIndex>* equals the special value **REX_REMOVE_ALL**, it removes any existing instances of *<pszAttribute>*. Otherwise, the instance of *<pAttribute>* at the position indicated is removed. Always returns TRUE, even when the dictionary did not contain *<pAttribute>* at the *<iIndex>*.
reschedule	**abool_t pDict->reschedule(rex_AttributeDictionary_t* pDict)**	Enables control over asynchronous activities. It enables you to collect similar activities and mark them as pending. You can then process them and reschedule them. You can only use this attribute with multithreaded services. Use caution when employing this method.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table A-3 REX Attribute Dictionary Methods (continued)

Name	Syntax	Description
size	**int pDict->size(rex_AttributeDictionary_t* pDict)**	Returns the number of entries in the dictionary.
trace	**abool_t pDict->trace(rex_AttributeDictionary_t* pDict, int** *<iLevel>***, const char*** *<pszFormat>***, ...)**	Outputs a message into the packet tracing system used by the RADIUS server. At level 0, no tracing occurs. At level 1, only an indication the packet was received and a reply was sent is output. As the number gets higher, the amount of information output is greater, until at level 4, where everything traceable is output. The remaining arguments are formatted and sent to the tracing system at the specified level.

REX Environment Dictionary

A dictionary is a data structure that contains key/value pairs. An Environment dictionary is a dictionary in which the keys and values are constrained to be strings. The REX Environment dictionary is used to communicate information from the script to the server and from script to script within the processing of a particular request. Note, there can be only one instance of a key in the Environment dictionary.

REX Environment Dictionary Methods

The Environment dictionary uses active commands, called *methods*, to allow you to change and access the values in the dictionary. Table A-4 lists all of the methods you can use with the REX Environment dictionary.

Table A-4 REX Environment Dictionary Methods

Name	Syntax	Description
allocateMemory	**void* pDict->allocateMemory(rex_EnvironmentDictionary_t* pDict, unsigned int** *<iSize>***)**	Allocate memory for use in scripts that persist only for the lifetime of this request. This memory is released when processing for this request is complete.
clear	**void pDict->clear(rex_EnvironmentDictionary_t* pDict)**	Removes all entries from the dictionary.
containsKey	**abool_t pDict->containsKey(rex_EnvironmentDictionary_t* pDict, const char*** *<pszKey>*)	Returns TRUE when the dictionary contains *<pszKey>*, otherwise returns FALSE.
firstKey	**const char* pDict->firstKey(rex_EnvironmentDictionary_t* pDict)**	Returns the name of the first key in the dictionary. Note, the keys are not stored sorted by name.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table A-4 REX Environment Dictionary Methods (continued)

Name	Syntax	Description
get	**const char* pDict->get(rex_EnvironmentDictionary_t* pDict, const char*** *<pszKey>***)**	Returns the value associated with *<pszKey>* from the dictionary. When the dictionary does not contain *<pszKey>*, an empty string is returned.
isEmpty	**abool_t pDict->isEmpty(rex_EnvironmentDictionary_t* pDict)**	Returns TRUE when the dictionary has 0 entries, FALSE otherwise.
log	**abool_t pDict->log(rex_EnvironmentDictionary_t* pDict, int** *<iLevel>***, const char*** *<pszFormat>***, ...)**	Outputs a message into the logging system used by the RADIUS server. *<iLevel>* should be one of **REX_LOG_ERROR**, **REX_LOG_WARNING**, or **REX_LOG_INFO**. The *<pszFormat>* argument is treated as a **printf**-style format string, and it, along with the remaining arguments, are formatted and sent to the logging system at the specified level.
nextKey	**const char* pDict->nextKey(rex_EnvironmentDictionary_t* pDict)**	Returns the name of the next key in the dictionary that follows the key returned in the last call to **firstKey** or **nextKey**.
put	**abool_t pDict->put(rex_EnvironmentDictionary_t* pDict, const char*** *<pszValue>***, const char*** *<pszKey>***)**	Associates the value with *<pszKey>* in the dictionary, replacing any existing instance of *<pszKey>* with the new *<pszValue>*.
remove	**abool_t pDict->remove(rex_EnvironmentDictionary_t* pDict, const char*** *<pszKey>***)**	Removes *<pszKey>* and the associated value from the dictionary. Always returns TRUE, even when the dictionary did not contain *<pszKey>*
reschedule	**abool_t pDict->reschedule(rex_AttributeDictionary_t* pDict)**	Enables control over asynchronous activities. It enables you to collect similar activities and mark them as pending. You can then process them and reschedule them. You can only use this attribute with multithreaded services. Use caution when employing this method.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table A-4 REX Environment Dictionary Methods (continued)

Name	Syntax	Description
size	**int pDict->size(rex_EnvironmentDictionary_t* pDict)**	Returns the number of entries in the dictionary.
trace	**abool_t pDict->trace(rex_EnvironmentDictionary_t* pDict, int** *<iLevel>***, const char*** *<pszFormat>***, ...)**	Outputs a message into the packet tracing system used by the RADIUS server. At level 0, no tracing occurs. At level 1, only an indication the packet was received and a reply was sent is output. As the number gets higher, the amount of information output is greater, until at level 4, where everything traceable is output. The remaining arguments are formatted and sent to the tracing system at the specified level.

Java Attribute Dictionary

The AttributeDictionary is a dictionary of attributes, where the keys are the attribute types and the values are the data fields in the attribute. Both keys and values must conform to the definition of attributes in the server's Attribute Dictionary. Keys (types) can be either strings or byte arrays. If strings, they are the names of attributes. If byte arrays, they are the binary type. The type associated with a name can be retrieved by calling the static method getType(java.lang.String). Using byte arrays is slightly more efficient - methods that take String keys must do the mapping from String to byte array in the course of executing the method. Similarly, values can be strings or byte arrays. Again, string values are converted to the appropriate binary representation when stored in an AttributeDictionary and back again when retrieved into a string variable.

Keys in an AttributeDictionary can be associated with multiple values. Each of the values associated with a key is ordered with an integer index denoting its position in the list of values. Given an AttributeDictionary, a key and an index, each value associated with a key can be looked up. This section contains the following topics:

- Java Environment Dictionary Methods
- Interface Extension Methods
- Interface Extensionforsession Methods
- Interface Extensionwithinitialization Methods
- Interface Extensionforsessionwithinitialization Methods
- Variables in the Marker Extension Interface
- Session Record Methods

Java Attribute Dictionary Methods

Attribute dictionaries use active commands called methods, that allow you to change and access the values in the dictionaries.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table A-5 lists all of the methods you can use with the Request and Response dictionaries.

Table A-5 Java Attribute Dictionary Methods

Name	Syntax	Description
size	**public int size()**	Returns the number of distinct keys in the dictionary.
isEmpty	**public boolean isEmpty()**	Tests if the dictionary contains any entries.
clear	**public void clear()**	Removes all entries from the dictionary.
containsKey	**public boolean containsKey(java.lang.String key)**	Returns true if an entry exists for key.
get	**public java.lang.String get(java.lang.String key)**	Returns the first value associated with the key.
get	**public java.lang.String get(java.lang.String key, int index)**	Returns the value at position index associated with the key.
put	**public boolean put(java.lang.String key, java.lang.String value)**	Associates key with a value. Any existing values associated with the key are removed before adding this association.
put	**public boolean put(java.lang.String key, java.lang.String value, int index)**	Associates key with a value depending on the value of index. If index equals **Extension.EXT_REPLACE**, any existing values are removed before adding this new association. If index equals **Extension.EXT_APPEND**, a new value is added at the end of the list of existing values. If index equals **Extension.EXT_AUGMENT**, the new association is only made if the dictionary does not already have an entry for key. If index is a number greater than or equal to 0 and less than the number of entries in the list, the value is inserted at that position in the list. Otherwise, the value is appended at the end of the list.
getBytes	**public byte[] getBytes(java.lang.String key)**	Returns the first value associated with the key.
getBytes	**public byte[] getBytes(java.lang.String key, int index)**	Returns the value at position index associated with key.
putBytes	**public boolean putBytes(java.lang.String key, byte[] value)**	Associates key with value. Any existing values associated with key are removed before adding this association.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table A-5 Java Attribute Dictionary Methods (continued)

Name	Syntax	Description
putBytes	**public boolean putBytes(java.lang.String key, byte[] value, int index)**	Associates key with a value depending on the value of index. If index equals **Extension.EXT_REPLACE**, any existing values are removed before adding this new association. If index equals **Extension.EXT_APPEND**, a new value is added at the end of the list of existing values. If index equals **Extension.EXT_AUGMENT**, the new association is only made if the dictionary does not already have an entry for key. If index is a number greater than or equal to 0 and less than the number of entries in the list, the value is inserted at that position in the list. Otherwise, the value is appended at the end of the list.
remove	**public void remove(java.lang.String key)**	Removes key (and all corresponding values) from the dictionary. This method does nothing if key is not in the dictionary.
remove	**public void remove(java.lang.String key, int index)**	Removes value at the position index that is associated with key. If the index equals **Extension.EXT_REMOVE_ALL** or if the value being removed is the last value associated with key, the key is removed from the dictionary. This method does nothing if key is not in the dictionary.
addProfile	**public boolean addProfile(java.lang.String profileName)**	Adds all the attributes contained in the specified profile into the dictionary. Any existing attributes that have the same keys as attributes in the profile are removed before adding the new attributes.
Addprofile	**boolean addProfile(java.lang.String profileName, int mode)**	Adds all the attributes contained in the specified profile into the dictionary. Any existing attributes that have the same keys as attributes in the Profile will be treated depending on the mode value. For each attribute in the Profile, if mode equals **Extension.EXT_REPLACE**, any values associated with the attribute in the dictionary are removed before adding the attribute. If index equals **Extension.EXT_APPEND**, a new value is added at the end of the list of existing values. If index equals **Extension.EXT_AUGMENT**, a new value is added only if the dictionary does not already have an entry for the given key.
getType	**public static byte[] getType(java.lang.String key)**	Takes the name of the attribute (as a string) and returns the binary form of key.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table A-5 Java Attribute Dictionary Methods (continued)

Name	Syntax	Description
keys	**public java.util.Enumeration keys()**	Returns an enumeration of the keys in the dictionary. The general contract for the keys method is that an Enumeration object is returned that will generate all the keys for which the dictionary contains entries.
elements	**public java.util.Enumeration elements()**	Returns an enumeration of the entries in the dictionary. The general contract for the elements method is that an Enumeration object is returned that will generate all the elements contained in entries in the dictionary. Keys with multiple values will result in multiple elements being returned.
keysByType	**public java.util.Enumeration keysByType()**	Returns an enumeration of the keys in the dictionary. The general contract for the keys method is that an Enumeration object is returned that will generate all the keys for which the dictionary contains entries.

Java Environment Dictionary

The Environment Dictionary can be used to store information between Extensions invoked subsequently on a given request or can be used to pass information between the Extension and the server properly.

The Environment Dictionary maps keys to values, where the keys and values are strings. In any one instance of the Environment Dictionary, every key is associated with at most one value. Given an Environment Dictionary and a key, the associated value can be looked up. Any non-null string can be used as a key and value.

Java Environment Dictionary Methods

The Environment dictionary uses active commands called methods, to allow you to change and access the values in the dictionary. Table A-6 lists all of the methods you can use with the java Environment dictionary.

Table A-6 Java Environment Dictionary Methods

Name	Syntax	Description
size	**public int size()**	Returns the number of entries (distinct keys) in the dictionary.
isEmpty	**public boolean isEmpty()**	Tests if the dictionary contains no entries.
clear	**public void clear()**	Removes all entries from the dictionary.
containsKey	**public boolean containsKey(java.lang.String key)**	Returns true if the dictionary contains an entry for key.
get	**public java.lang.String get(java.lang.String key)**	Returns the value associated with key in the dictionary.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table A-6 Java Environment Dictionary Methods (continued)

Name	Syntax	Description
put	**public boolean put(java.lang.String key, java.lang.String value)**	Associates key with value.
remove	**public void remove(java.lang.String key)**	Removes key (and its corresponding value) from this dictionary. This method does nothing if key is not in the dictionary.
keys	**public java.util.Enumeration keys()**	Returns an enumeration of the keys in the dictionary. The general contract for the keys method is that an Enumeration object is returned that will generate all the keys for which the dictionary contains entries.
elements	**public java.util.Enumeration elements()**	Returns an enumeration of the entries in the dictionary. The general contract for the elements method is that an Enumeration object is returned that will generate all the elements contained in entries in the dictionary.
log	**public static void log(int level,java.lang.String message)**	Prints a message in the server log at the specified level.
trace	**public void trace(int level, java.lang.String message)**	Prints a message in the server trace file at the specified level.
reschedule	**public void reschedule()**	Informs the server that it should take back ownership of the request associated with the dictionary and continue processing it.

Interface Extension

Classes that are going to be used as scripts or services from Access Registrar must implement the Extension interface. When a Java scripting point or service is encountered during the processing of a request, the server will call the runExtension method defined in this interface and implemented by the appropriate class.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Interface Extension Methods

Table A-7 lists the methods you can use for interface extension

Table A-7 Interface Extension Methods

Name	Syntax	Description
runExtension	**int runExtension(int iExtensionPoint, AttributeDictionary request, AttributeDictionary response,EnvironmentDictionary environment)**	This method is called whenever a Java scripting point or service is encountered during the processing of a request. When runExtension is used as a script, it should process requests as quickly as possible, without blocking. This is because the server has a limited number of threads that it is using to process requests and if any one extension takes too long to run, it is likely that many requests will be delayed as each one calls the extension. runExtension must return either **EXT_OK** to indicate that processing of this request should continue or **EXT_ERROR** to indicate that an error occurred while processing this request and that the request should be dropped. Extensions should always log an error before returning **EXT_ERROR** so that the administrator has a way to determine the problem that was encountered. When runExtension is used as a service, it will be called once before requests start coming in (with the iExtensionPoint parameter set to **EXT_START_SERVICE**) to give the extension the opportunity to initialize resources needed to process requests, and once after the last request has been received (with the iExtensionPoint parameter set to **EXT_STOP_SERVICE**) to give the extension the opportunity to release those resources before stopping. runExtension must return one of the following values: **EXT_OK, EXT_ERROR** or **EXT_PENDING. EXT_PENDING** should be returned to inform the server that the extension has taken ownership of the request, will process the request on a background thread, and will inform the server when it is time to continue processing the request by calling reschedule() on one of the request's dictionaries.

Interface ExtensionforSession

Classes that are going to be used as scripts at Session Manager level from Tech Mahindra Access Registrar must implement the ExtensionForSession interface. When a Java scripting point or service is encountered during the processing of a request, the server will call the runExtension method defined in this interface and implemented by the appropriate class.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Interface Extensionforsession Methods

Table A-8 lists the methods you can use for interface extensionforsession

Table A-8 Interface Extensionforsession Methods

Name	Syntax	Description
runExtension	**int runExtension(int iExtensionPoint, AttributeDictionary request, AttributeDictionary response, EnvironmentDictionary environment, SessionRecord session)**	This method is called whenever a Java scripting point or service is encountered during the processing of a request. When runExtension is used as a script, it should process requests as quickly as possible, without blocking. This is because the server has a limited number of threads that it is using to process requests and if any one extension takes too long to run, it is likely that many requests will be delayed as each one calls the extension. runExtension must return either **EXT_OK** to indicate that processing of this request should continue or **EXT_ERROR** to indicate that an error occurred while processing this request and that the request should be dropped. Extensions should always log an error before returning **EXT_ERROR** so that the administrator has a way to determine the problem that was encountered. When runExtension is used as a service, it will be called once before requests start coming in (with the iExtensionPoint parameter set to **EXT_START_SERVICE**) to give the extension the opportunity to initialize resources needed to process requests, and once after the last request has been received (with the iExtensionPoint parameter set to **EXT_STOP_SERVICE**) to give the extension the opportunity to release those resources before stopping. runExtension must return one of the following values: **EXT_OK, EXT_ERROR** or **EXT_PENDING**. **EXT_PENDING** should be returned to inform the server that the extension has taken ownership of the request, will process the request on a background thread, and will inform the server when it is time to continue processing the request by calling reschedule() on one of the request's dictionaries.

Interface Extensionwithinitialization

Classes that are going to be used as scripts or services from Access Registrar implements the ExtensionWithInitialization interface. ExtensionWithInitialization extends the Extension interface with methods to initialize and destroy the extension. initialize(java.lang.String) is called when the extension is first loaded, with the string argument being set from the InitializeArg property that was defined in the server configuration when the extension was defined (either as a Script or a Service). Destroy() is called before the extension is unloaded.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Interface Extensionwithinitialization Methods

Table A-9 lists the methods you can use for Interface Extensionwithinitialization.

Table A-9 Interface Extensionwithinitialization Methods

Name	Syntax	Description
initialize	**void initialize(java.lang. String initializeArg)**	This method is called by the server when the extension is first loaded.
destroy	**void destroy()**	This method is called by the server when the extension is going to be unloaded.

Interface ExtensionforSessionwithinitialization

Classes that are going to be used as scripts from Access Registrar at Session Manager level implement the ExtensionForSessionWithInitialization interface. ExtensionForSessionWithInitialization extends the ExtensionForSession interface with methods to initialize and destroy the extension. initialize(java.lang.String) is called when the extension is first loaded, with the string argument being set from the InitializeArg property that was defined in the server configuration when the extension was defined (either as a script or a service). Destroy () is called before the extension is unloaded.

Interface Extensionforsessionwithinitialization Methods

Table A-10 lists the methods you can use for Interface Extensionforsessionwithinitialization.

Table A-10 Interface Extensionforsessionwithinitialization Methods

Name	Syntax	Description
initialize	**void initialize(java.la ng.String initializeArg)**	This method is called by the server when the extension is first loaded.
destroy	**void destroy()**	This method is called by the server when the extension is going to be unloaded.

Interface MarkerExtension

This is just going to be a marker interface containing various member variables which can be used in interfaces/classes extending from this interface. Extension and ExtensionForSession interfaces will extend this interface.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Variables in the Marker Extension Interface

Table A-11 lists the variables in the marker extension interface.

Table A-11 Marker Extension Interface Variables

Name	Syntax	Description
EXT_OK	**static final int EXT_OK**	Returns **EXT_OK** by implementation of runExtension() to indicate that the extension operated correctly and processing of the request should continue.
EXT_ERROR	**static final int EXT_ERROR**	Returns **EXT_ERROR** by implementation of runExtension() to indicate that the extension failed in some way and processing of the request should NOT continue.
EXT_PENDING	**static final int EXT_PENDING**	Returns **EXT_PENDING** by implementations of runExtension() to indicate that the extension operated correctly and the extension wants to take ownership of the request for a while. Further processing of the request by the server will be postponed until the extension indicates that it can do so by calling the reschedule method on any of the dictionaries.
EXT_LOG_ERROR	**static final int EXT_LOG_ERROR**	Indicates that the message should be logged with a severity of ERROR, when passed to log() in the level parameter.
EXT_LOG_WARNING	**static final int EXT_LOG_WARNING**	Indicates that the message should be logged with a severity of WARNING, when passed to log() in the level parameter.
EXT_LOG_INFO	**static final int EXT_LOG_INFO**	Indicates that the message should be logged with a severity of INFO, when passed to log() in the level parameter.
EXT_REMOVE_ALL	**static final int EXT_REMOVE_ALL**	Indicates that all values associated with the specified key should be removed, when passed to AttributeDictionary::remove() in the index parameter.
EXT_REPLACE	**static final int EXT_REPLACE**	Indicates that all existing values associated with the specified key(s) should be removed before adding the new value(s), when passed to AttributeDictionary::put() (and its variants) in the index parameter or to AttributeDictionary::addProfile() in the mode parameter.
EXT_APPEND	**static final int EXT_APPEND**	Indicates that the new value(s) should be appended to the end of the list of any existing values associated with the specified key(s), when passed to AttributeDictionary::put() (and its variants) in the index parameter or to AttributeDictionary::addProfile() in the mode parameter.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table A-11 Marker Extension Interface Variables (continued)

Name	Syntax	Description
EXT_AUGMENT	**static final int EXT_AUGMENT**	Indicates that the new association(s) should only be added if the dictionary does not already have an entry for the given key(s), when passed to AttributeDictionary::put() (and its variants) in the index parameter or to AttributeDictionary::addProfile() in the mode parameter.
EXT_START_SERVICE	**static final int EXT_START_SERVICE**	Indicates that the extension should do whatever is necessary to prepare to offer service, when passed to extensions used as services. This may include starting background threads, opening database connections, and so on.
EXT_AUTHENTICATION_SERVICE	**static final int EXT_AUTHENTICATION_SERVICE**	Indicates that the extension should authenticate the current request, when passed to extensions used as services. To indicate whether the request was authenticated or not, the extension should set the EnvironmentDictionary entry for "Response-Type" to either "Access-Accept" or "Access-Reject".
EXT_AUTHORIZATION_SERVICE	**static final int EXT_AUTHORIZATION_SERVICE**	Indicates that the extension should authorize the current request, when passed to extensions used as services.
EXT_AUTHENTICATION_AND_AUTHORIZATION_SERVICE	**static final int EXT_AUTHENTICATION_AND_AUTHORIZATION_SERVICE**	Indicates that the extension should both authenticate and authorize the current request, when passed to extensions used as services. To indicate whether the request was authenticated or not, the extension should set the EnvironmentDictionary entry for "Response-Type" to either "Access-Accept" or "Access-Reject".
EXT_ACCOUNTING_SERVICE	**static final int EXT_ACCOUNTING_SERVICE**	Indicates that the extension should produce an accounting record for the current request, when passed to extensions used as services.
EXT_STOP_SERVICE	**static final int EXT_STOP_SERVICE**	Indicates that the extension should do whatever is necessary to shut down, when passed to extensions used as services. This may include stopping background threads, closing database connections and so on.
EXT_NAS_STARTED_ACCOUNTING_SERVICE	**static final int EXT_NAS_STARTED_ACCOUNTING_SERVICE**	Indicates that the NAS identified in the EnvironmentDictionary (by either the "NAS-Identifier" or "NAS-IP-Address" entries) has indicated that it is starting up, when passed to extensions used as services. This may be used by extensions to prepare to receive requests from this particular NAS if the extension treats requests from different NASs differently.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table A-11 Marker Extension Interface Variables (continued)

Name	Syntax	Description
EXT_NAS_STOPPED_ACCOUNTING_SERVICE	**static final int EXT_NAS_STOPPED_ACCOUNTING_SERVICE**	Indicates that the NAS identified in the EnvironmentDictionary (by either the "NAS-Identifier" or "NAS-IP-Address" entries) has indicated that it is shutting down, when passed to extensions used as services. This may be used by extensions to recover any resources associated with this NAS if the extension treats requests from different NASs differently.
EXT_INCOMING_SERVER_SCRIPTING_POINT	**static final int EXT_INCOMING_SERVER_SCRIPTING_POINT**	Indicates that the extension is being called from the script **/Radius/IncomingScript**, when passed to extensions used as scripts.
EXT_INCOMING_VENDOR_SCRIPTING_POINT	**static final int EXT_INCOMING_VENDOR_SCRIPTING_POINT**	Indicates that the extension is being called from the script **/Radius/Vendors/**<*vendor*>**/IncomingScript**. when passed to extensions used as scripts.
EXT_INCOMING_CLIENT_SCRIPTING_POINT	**static final int EXT_INCOMING_CLIENT_SCRIPTING_POINT**	Indicates that the extension is being called from the script **/Radius/Clients/**<*client*>**/IncomingScript** or from the script **/Radius/RemoteServers/**<*server*>**/IncomingScript**, when passed to extensions used as scripts.
EXT_INCOMING_SERVICE_SCRIPTING_POINT	**static final int EXT_INCOMING_SERVICE_SCRIPTING_POINT**	Indicates that the extension is being called from the script **/Radius/Services/**<*service*>**/IncomingScript**, when passed to extensions used as scripts.
EXT_USERGROUP_AUTHENTICATION_SCRIPTING_POINT	**static final int EXT_USERGROUP_AUTHENTICATION_SCRIPTING_POINT**	Indicates that the extension is being called from the script **/Radius/UserGroups/**<*group*>/**AuthenticationScript**, when passed to extensions used as scripts.
EXT_USERRECORD_AUTHENTICATION_SCRIPTING_POINT	**static final int EXT_USERRECORD_AUTHENTICATION_SCRIPTING_POINT**	Indicates that the extension is being called from the script **/Radius/UserLists/**<*userlist*>/<*user*>/**AuthenticationScript**, when passed to extensions used as scripts.
EXT_USERGROUP_AUTHORIZATION_SCRIPTING_POINT	**static final int EXT_USERGROUP_AUTHORIZATION_SCRIPTING_POINT**	Indicates that the extension is being called from the script **/Radius/UserGroups/**<*group*>/**AuthorizationScript**, when passed to extensions used as scripts.
EXT_USERRECORD_AUTHORIZATION_SCRIPTING_POINT	**static final int EXT_USERRECORD_AUTHORIZATION_SCRIPTING_POINT**	Indicates that the extension is being called from the script **/Radius/UserLists/**<*userlist*>/<*user*>/**AuthorizationScript**, when passed to extensions used as scripts.
EXT_OUTGOING_SERVICE_SCRIPTING_POINT	**static final int EXT_OUTGOING_SERVICE_SCRIPTING_POINT**	Indicates that the extension is being called from the script **/Radius/Services/**<*service*>/**OutgoingScript**, when passed to extensions used as scripts.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table A-11 Marker Extension Interface Variables (continued)

Name	Syntax	Description
EXT_OUTGOING_CLIENT_SCRIPTING_POINT	**static final int EXT_OUTGOING_CLIENT_SCRIPTING_POINT**	Indicates that the extension is being called from the script **/Radius/Clients/**<*client*>**/OutgoingScript** or from the script **/Radius/RemoteServers/**<*server*>**/OutgoingScript**, when passed to extensions used as scripts.
EXT_OUTGOING_VENDOR_SCRIPTING_POINT	**static final int EXT_OUTGOING_VENDOR_SCRIPTING_POINT**	Indicates that the extension is being called from the script **/Radius/Vendors/**<*vendor*>**/OutgoingScript**. when passed to extensions used as scripts.
EXT_OUTGOING_SERVER_SCRIPTING_POINT	**static final int EXT_OUTGOING_SERVER_SCRIPTING_POINT**	Indicates that the extension is being called from the script **/Radius/OutgoingScript**, when passed to extensions used as scripts.
EXT_REMOTE_SERVER_OUTAGE_SCRIPTING_POINT	**static final int EXT_REMOTE_SERVER_OUTAGE_SCRIPTING_POINT**	Indicates that the extension is being called from the script **/Radius/Services/**<*service*>**/OutageScript**, when passed to extensions used as scripts.
EXT_INCOMING_SESSIONMANAGER_SCRIPTING_POINT	**static final int EXT_INCOMING_SESSIONMANAGER_SCRIPTING_POINT**	Indicates that the extension is being called from the script **/Radius/SessionManagers/**<*sessionmgr*>**/Incoming Script**, when passed to extensions used as scripts.
EXT_OUTGOING_SESSIONMANAGER_SCRIPTING_POINT	**static final int EXT_OUTGOING_SESSIONMANAGER_SCRIPTING_POINT**	Indicates that the extension is being called from the script **/Radius/SessionManagers/**<*sessionmgr*>**/Outgoing Script**, when passed to extensions used as scripts.

Class Sessionrecord

Each request processed by an Extension will have a corresponding session. The methods present in this class operate on the attributes cached in that session record. Group of attributes are cached as an AttributeDictionary in the session record.

Session Record Methods

Table A-12 lists the methods you can use for Session record.

Table A-12 Session Record Methods

Name	Syntax	Description
get	**public java.lang.String get(java.lang.String key)**	Returns the first value associated with key.
get	**public java.lang.String get(java.lang.String key,int index)**	Returns the value at position index associated with key.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table A-12 Session Record Methods (continued)

Name	Syntax	Description
put	**public boolean put(java.lang.String key,java.lang.String value)**	Associates key with value and stores it to the session record. Any existing values associated with key are removed before adding this association. The value can be retrieved by calling the get method with a key that is equal to the original key.
put	**public boolean put(java.lang.String key,java.lang.String value, int index)**	Associates key with value depending on the value of index and stores it in the session record. If index equals **ExtensionForSession.EXT_REPLACE**, any existing values are removed before adding this new association. If index equals **ExtensionForSession.EXT_APPEND**, the new value is added at the end of the list of existing values. If index equals **ExtensionForSession.EXT_AUGMENT**, the new association is only made if the session record does not already have an entry for key. If index is a number greater than or equal to 0 and less than the number of entries in the list, the value is inserted at that position in the list. Otherwise, the value is appended at the end of the list. The value can be retrieved by calling the get method with a key that is equal to the original key and the appropriate index.
remove	**public boolean remove(java.lang.String key)**	Removes key (and all corresponding values) from the session record. This method does nothing if key is not in the session record.
remove	**public boolean remove(java.lang.String key, int index)**	Removes value at the position index that is associated with key. If the index equals **ExtensionForSession.EXT_REMOVE_ALL** or if the value being removed is the last value associated with key, the key is removed from the session record. This method does nothing if key is not in the session record.
getSessionInfo	**public java.lang.String getSessionInfo()**	Returns Session-ID, Session-Start-Time and Session-Last-Accessed-Time of the session record.

Note A sample java script is available in the following path "/techm-ar/examples/java" after the installation of AR.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Appendix B

Environment Dictionary

This appendix describes the environment variables the scripts use to communicate with Tech Mahindra Access Registrar or to communicate with other scripts.

Tech Mahindra Access Registrar sets the **arguments** variable in the Environment dictionary, before calling the **InitEntryPoint** of each script. The **arguments** variable is set to the value of the **InitEntryPointArgs** property corresponding to that script, and it allows the administrator to pass (possibly unique) information to each script initialization function.

Environment variables that are set and read for resource management override provide scripts further control over session management. These environment variables, including the following **Acquire-User-Session-Limit**, **Acquire-Group-Session-Limit**, **Acquire-IP-Dynamic**, **Acquire-IP-Per-NAS-Port**, **Acquire-IPX-Dynamic**, and **Acquire-USR-VPN**, can be set at any point before session management is invoked. These environment variables are read as the packet flows through each Resource Manager that the chosen Session Manager calls. The default setting for these environment variables is TRUE. See the "Configuring and Monitoring the RADIUS Server" chapter of the *Tech Mahindra Access Registrar 9.2 Administrator Guide* for additional information about Resource Managers.

This appendix has the following major sections:

- Tech Mahindra Access Registrar Environment Dictionary Variables

  This section lists environment variables you can use in scripts to communicate with Tech Mahindra Access Registrar or to communicate with other scripts.

- Internal Variables

  This section lists environment variables used by the Tech Mahindra Access Registrar server for internal operations. The environment variables listed in this section must not be modified by scripts.

Tech Mahindra Access Registrar Environment Dictionary Variables

The following variables are text strings stored in the Environment dictionary passed to each scripting point.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Accepted-Profiles

Accepted-Profiles is read during authorization after calling server and client incoming scripts (not set by Tech Mahindra Access Registrar code). If set, the authorization done by local user lists checks to see if the given user's profile as specified in the user record is one of those in the separated list of profiles. If it is not in the separated list of profiles, the request is rejected.

Accounting-Service

Accounting-Service is set after calling server and client incoming scripts and is used to determine which accounting service is used for this request. If set, the server directs the request to be processed by the specified accounting service.

When **Accounting-Service** is not set, the **DefaultAccountingService** (as defined in the server configuration) is used instead.

Acquire-Dynamic-DNS

Acquire-Dynamic-DNS is set and read for resource management override. **Acquire-Dynamic-DNS** is set to FALSE to skip DNS updating during resource management processing.

Acquire-Group-Session-Limit

Acquire-Group-Session-Limit is set and read for resource management override.
Acquire-Group-Session-Limit is set to FALSE to override the use of group session limit resource management.

Acquire-Home-Agent

Acquire-Home-Agent is set and read for resource management override. **Acquire-Home-Agent** is set to FALSE to override the allocation of the home agent IP address during resource management processing.

Acquire-IP-Dynamic

Acquire-IP-Dynamic is set and read for resource management override. **Acquire-IP-Dynamic** is set to FALSE to override the use of a managed pool of IP addresses resource management.

Acquire-IPX-Dynamic

Acquire-IPX-Dynamic is set and read for resource management override. **Acquire-IPX-Dynamic** is set to FALSE to override the use of a managed pool of IPX addresses resource management.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Acquire-IP-Per-NAS-Port

Acquire-IP-Per-NAS-Port is set and read for resource management override.
Acquire-IP-Per-NAS-Port is set to FALSE to override the use of ports associated with specific IP addresses resource management.

Acquire-Subnet-Dynamic

Acquire-Subnet-Dynamic is not always used. If set to FALSE, subnet-dynamic resource managers are skipped.

Acquire-User-Session-Limit

Acquire-User-Session-Limit set and read for resource management override.
Acquire-User-Session-Limit is set to FALSE to override the use of user session limit resource management.

Acquire-USR-VPN

Acquire-USR-VPN is set and read for resource management override. **Acquire-USR-VPN** is set to FALSE to override the use of Virtual Private Networks (VPNs) that use USR NAS Clients resource management.

Allow-Null-Password

Allow-Null-Password is read during password matching and set in local userlist password matching if not set prior. If **Allow-Null-Password** is set to TRUE, the Tech Mahindra Access Registrar server accepts requests with null passwords.

Authentication-Service

Authentication-Service is set and read for authentication service selection and is used to determine which service is used to authenticate the user. If set, the server directs the request to be processed by the specified authentication service. When **Authentication-Service** is not set, the **DefaultAuthenticationService** is used instead.

Authorization-Service

Authorization-Service is set and read for authorization service selection and is used to determine which service to use to authorize the user. If set, the server directs the request to be processed by the specified authorization service. When **Authorization-Service** is not set, the **DefaultAuthorizationService** is used instead.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

AuthorizationInfo

The MSISDN information is copied to **AuthorizationInfo** that is fetched by M3UA service.

BackingStore-Env-Vars

BackingStore-Env-Vars overrides the BackingStoreEnvironmentVariables property of remote servers of type *odbc-accounting* only when the property BufferAccountingPackets is set to TRUE. The value is a comma separated list of environment variables to be stored along with the packet contents in the local disk.

Blacklisted-IMSI

This variable is configured on a SIGTRAN-M3UA remote server. For any incoming request with an IMSI value, if the variable is set as TRUE, then that IMSI value is blacklisted and will not forwarded to the HLR. For more information, see the "SIGTRAN-M3UA" chapter of the *Tech Mahindra Access Registrar 9.3 User Guide*.

Broadcast-Accounting-Packet

If set to TRUE, **Broadcast-Accounting-Packet** enables broadcasting of Accounting-on or Accounting-off packets to all remote servers of type *radius*.

Cache-Attributes-In-Session

Cache-Attributes-In-Session is set and read for resource management override. **Cache-Attributes-In-Session** is set to FALSE to override the caching of attributes by the *session-cache* type of resource manager.

Current-Group-Count

Current-Group-Count is set and read for group session management. If set, the group-session-limit resource manager sets **Current-Group-Count** to be the new value of the group-session-limit counter.

Cache-Outer-Identity

Cache-Outer-Identity value is set to enable identifying session of an user. If it is set to TRUE, WiMAX session manager will cache the outer identity. If it is set to FALSE, the WiMAX session manager will cache the inner identity. The value is set to FALSE by default.

Destination-IP-Address

Destination-IP-Address is a read only value which is set to the receiver IP address. **Destination-IP-Address** contains the IP address of the request packet receiver.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Destination-Port

Destination-port is a read only value which is set to the receiving port number. **Destination-port** contains the port number of the receiver of the request.

Dest-Translation-Type

Dest-Translation-Type is configured through the GlobalTitleTranslationScript. When the RoutingIndicator is set to **RTE_GT**, Tech Mahindra Access Registrar server reads the value that is set in Dest-Translation-Type and sets the TranslationType field of the Called Party Address. The value in this environment variable overrides the value that is configured in the DestinationGTAddress/DestTranslationType property of a remote server, SIGTRAN-M3UA.

Dest-Numbering-Plan

Dest-Numbering-Plan is configured through the GlobalTitleTranslationScript. When the RoutingIndicator is set to **RTE_GT**, Tech Mahindra Access Registrar server reads the value that is set in Dest-Numbering-Plan and sets the NumberingPlan field of the Called Party Address. The value in this environment variable overrides the value that is configured in the DestinationGTAddress/Dest-Numbering-Plan property of a remote server, SIGTRAN-M3UA.

The following are the only values that are used for Dest-Numbering-Plan environment variable:

- DATA
- GENERIC
- ISDN
- ISDNMOB
- LANMOB
- MARMOB
- NWSPEC
- TEL
- TELEX
- UNKN

If you set any variable other than the above ones, Tech Mahindra Access Registrar server sets the NumberingPlan that is configured in DestinationGTAddress/Dest-Numbering-Plan property of a remote server of type SIGTRAN-M3UA.

Dest-Encoding-Scheme

Dest-Encoding-Scheme is configured through the GlobalTitleTranslationScript. When the RoutingIndicator is set to **RTE_GT**, Tech Mahindra Access Registrar server reads the value that is set in Dest-Encoding-Scheme environment variable and sets the EncodingScheme field of the Called Party Address. The value in this environment variable overrides the value that is configured in the DestinationGTAddress/ DestEncodingScheme property of a remote server, SIGTRAN-M3UA.

The following are the only values that are used for Dest-Encoding-Scheme environment variab

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

- BCDEVEN
- BCDODD

If you set any variable other than the above ones, Tech Mahindra Access Registrar server sets the EncodingScheme that is configured in the DestinationGTAddress/ DestEncodingScheme property of a remote server of type SIGTRAN-M3UA.

Dest-Nature-Of-Address

Dest-Nature-Of-Address is configured through the GlobalTitleTranslationScript. When the RoutingIndicator is set to **RTE_GT**, Tech Mahindra Access Registrar server reads the value that is set in Dest-Nature-Of-Address environment variable and sets the NatureOfAddress field of the Called Party Address. The value in this environment variable overrides the value that is configured in the DestinationGTAddress/ DestNatureofAddress property of a remote server, SIGTRAN-M3UA.

The following are the only values that are used for Dest-Nature-Of-Address environment variable:

- ADDR_NOTPRSNT
- INTNUM
- NATSIGNUM
- SUBNUM

If you set any variable other than the above ones, Tech Mahindra Access Registrar server sets the NatureOfAddress that is configured in the DestinationGTAddress/ DestNatureofAddress property of a remote server of type SIGTRAN-M3UA.

Dest-GT-Format

Dest-GT-Format configured through the GlobalTitleTranslationScript. When the RoutingIndicator is set to **RTE_GT**, Tech Mahindra Access Registrar server reads the value that is set in Dest-GT-Format environment variable and uses this format specified for the Global Title Digits(Address Information). The value in this environment variable overrides the value that is configured in the DestinationGTAddress/ DestGTFormat property of a remote server, SIGTRAN-M3UA.

The following are the only values that are used for Dest-GT-Format environment variable:

- GTFRMT_0
- GTFRMT_1
- GTFRMT_2
- GTFRMT_3
- GTFRMT_4
- GTFRMT_5

If you set any variable other than the above ones, Tech Mahindra Access Registrar server sets the GTFormat that is configured in the DestinationGTAddress/ DestGTFormat property of a remote server of type SIGTRAN-M3UA.

Diameter-Application-Id

Diameter-Application-Id is set to get the application ID in the Diameter packet.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Diameter-Command-Code

Diameter-Command-Code is set to get the command codes in the Diameter packet.

Disable-Accounting-On-Off-Broadcast

If set to TRUE, **Disable-Accounting-On-Off-Broadcast** disables broadcasting of Accounting-On and Accounting-Off packets to all remote servers of type 'radius'.

DSA-Response-Cache

DSA-Response-Cache is used while performing DSA(Dynamic Service Authorization) feature in Tech Mahindra Access Registrar. It is FALSE by default, which will clear the response dictionary before Re-Authentication. If DSA-Response-Cache is set to TRUE, Tech Mahindra Access Registrar will not clear the response dictionary before Re-Authenticating with next service configured.

DSA-Response-Cache must be set to TRUE for enabling delivery of location information from the client to RADIUS/Diameter server.

Dynamic-DNS-HostName

Dynamic-DNS-HostName is read while constructing the forward hostname during resource management processing to update DNS entries. If set, the name will be used as forward hostname instead of constructing one.

Dynamic-Search-Filter

Dynamic-Search-Filter overrides the Filter property in remote servers of type *ldap*. The format of the value set for **Dynamic-Search-Filter** should be similar to that of the Filter property.

Dynamic-Search-Path

Dynamic-Search-Path is read for LDAP searching. If set, the server uses it as its LDAP search path rather than the value set in the remote server configuration.

Dynamic-Search-Scope

Dynamic-Search-Scope is used to dynamically set the SearchScope property of an LDAP remote server configuration on a per-packet basis.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Dynamic-Service-Loop-Limit

Dynamic-Service-Loop-Limit variable is used to change loop counts. When using the same service for reauthentication and reauthorization, a loop can occur in these services. The loop count, by default is 10. You can change the loop count using this variable.

Dynamic-User-Password-Attribute

Dynamic-User-Password-Attribute is read for LDAP authentication and overrides the UserPasswordAttribute. If set, the server uses it to retrieve the password field as its LDAP UserPassword attribute instead of the value set in the remote server configuration.

EAP-Actual-Identity

EAP-Actual-Identity is a read-only variable that contains the International Mobile Subscriber Identity (IMSI) of the user after a successful EAP-SIM authentication.

EAP-Authentication-Mode

EAP-Authentication-Mode is a read-only variable, set after a successful EAP-SIM authentication, that indicates whether the EAP-SIM authentication was a reauthentication or a full authentication.

EnableMatchingServiceSelection5GFlag

EnableMatchingServiceSelection5GFlag variable provides a flexibility to decide if you want to check the Interworking-5GS-Indicator AVP in the APN configuration of matching Service-Selection. The value must be set to 1 in the remote server incoming script to enable this flag.

Enforce-Traffic-Throttling

By default, the value is set to FALSE. When set to TRUE, the traffic throttling check for the packet will be executed.

E-UTRANCellGlobalId

Variable that carries location information of a user equipment (UE) that tries to access a network. For more information, see Chapter 6, “Wireless Support.”

FetchAuthorizationInfo

When set to TRUE, this variable fetches MSISDN value from the HLR.

Do not use **FetchAuthorizationInfo** for authorization. We recommend that you use the authorization service of m3ua instead.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Generate-BEK

Generate-BEK is read when WiMax provisioning service is enabled. If this is set, Tech Mahindra Access Registrar will generate the Bootstrap Encryption Key in the WiMax flow.

Group-Session-Limit

Group-Session-Limit is set and read for group session management. The group-session-limit resource manager sets this environment variable to be the limit of the group-session-limit counter as set by the configuration.

HLR-GlobalTitle-Address

HLR-GlobalTitle-Address is configured through the GlobalTitleTranslationScript. When the RoutingIndicator is set to **RTE_GT** in SIGTRAN-M3UA remote server, Tech Mahindra Access Registrar server reads the value that is set in HLR-GlobalTitle-Address and sets the Destination GT Digits(Address Information field) of the Called Party Address.

HLR-GlobalTitle-Cached

HLR-GlobalTitle-Cached is set as TRUE to indicate the HLR GT is cached.

The Home Location Registry (HLR) Global Title address (GT address in calling party address (CgPA)) from the SendAuthenticationInfo (SAI) response is cached and used for subsequent authorization request. This cached HLR GT is added to the environment dictionary of the packet to be available for the authorization flow.

The cached HLR GT overrides both the configured destination GT values and GT script provided GT values. The HLR GT caching works by default for RTE_GT. The cached HLR GT can be overridden by updating the environment variable HLR-GlobalTitle-Cached to FALSE (or anything other than TRUE) in the GT script.

This HLR GT will not be cached for:

- reauthentication flow
- authorize only flow when authentication vectors are already available in cache (as there will not be SAI request.

HLR-Translated-IMSI

HLR-Translated-IMSI is configured through the IMSITranslationScript. Tech Mahindra Access Registrar server reads the value in HLR-Translated-IMSI and sets the value as IMSI before sending the request to STP/HLR. The value that is configured in the HLR-Translated-IMSI environment variable overrides the IMSI received in EAP-AKA/EAP-SIM request packet.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Ignore-Accounting-Signature

Ignore-Accounting-Signature is set after calling server and client incoming scripts and is used to ignore missing or incorrect accounting signatures from NASs. If set, Tech Mahindra Access Registrar does not check whether the account request packet has been signed with the same shared secret as the NAS.

Ignore-Accounting-Signature is used to work with RADIUS implementations that did not sign Accounting-Requests. A script was provided in the distribution (for USR NASs) that could be set in the IncomingScript extension point for the USR Vendor that simply set this environment variable.

IMSI

International Mobile System Identifier (IMSI) that is fetched from the response from HLR.

Incoming-Translation-Groups

Incoming-Translation-Groups is read for authentication while processing responses from a remote RADIUS server. If set, **Incoming-Translation-Groups** specifies the translation groups to be used to filter attributes on requests.

Location-Capability

Location-Capability must be set to TRUE to enable delivery of location information from the client to RADIUS/Diameter server.

Master-URL-Fragment

Used with the Windows Provisioning Service feature, **Master-URL-Fragment** specifies the fragment within the Master URL to be sent back to the provisioning server. **Master-URL-Fragment** can be set to any of the following four values: *signup*, *renewal*, *passwordchange*, and *forceupdate*. If **Master-URL-Fragment** is not set and is required to send the URL, *signup* will be sent by default.

The environmental variable **Send-PEAP-URL-TLV** indicates whether or not to send the URL.

Misc-Log-Message-Info

Misc-Log-Message-Info is read for packet event logging. If a log message is generated, the value of **Misc-Log-Message-Info** is inserted into the middle of the log message.

MSISDN

The Mobile Subscriber ISDN Number (MSISDN) that is fetched from the response from HLR.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Notification-Code

The Notification-Code variable is set up to indicate the reason for an authentication or authorization failure for EAP-SIM, EAP-AKA, and EAP-AKA' services. The common authorization/authentication failure reasons as received from the HLR are:

- Unknown subscriber
- System failure
- Data missing
- Unexpected data value
- Reject / Return with unknown error

Tech Mahindra Access Registrar reads this environment variable and sends an appropriate message to the client.

Notification-Service

Notification-Service is an authorization service and is used to send a notification code to the client in case of authorization failure.

This can be any of the services configured under /radius/services/ except eap services, accounting services, radius-session, radius-query, and diameter.

Outgoing-Translation-Groups

Outgoing-Translation-Groups is read while proxying to a remote radius server. If set, **Outgoing-Translation-Groups** specifies the translation groups to be used to filter attributes.

Pager

The **aregcmd** command supports the **Pager** environment variable. When the **aregcmd** command **stats** is used and the **Pager** environment variable is set, the output of the **stats** command is displayed using the program specified by the **Pager** environment variable.

PoD/CoA

The **PoD/CoA** variable is set and read for the CoA/PoD packet processing and used to determine whether the incoming PoD/CoA request must be translated to the corresponding PoD/CoA request. Table B-1 lists the PoD/CoA values and the corresponding functions.

Table B-1 PoD/CoA Values and Functions

PoD/CoA Value	Function
PoD-CoA	Converts Disconnect-Request to CoA
CoA-PoD	Converts CoA-Request to PoD
PoDACK-CoAACK	Converts the Disconnect-ACK to CoA-ACK

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table B-1 PoD/CoA Values and Functions

PoD/CoA Value	Function
CoAACK-PoDACK	Converts the CoA-ACK to Disconnect-ACK
PoDNAK-CoANAK	Converts the Disconnect-NAK to CoA-NAK
CoANAK-PoDNAK	Converts the CoA-NAK to Disconnect-NAK

Query-Service

The Query-Service variable is set and read for the *radius-query* service selection type. The Query-Service variable must be set before authentication phase begins at the server, vendor, or client incoming scripting point or using the policy engine. If set, the server directs requests to be processed by the specified *radius-query* service. After the Query-Service variable is set, no AAA processing will be done.

Re-Accounting-Service

Re-Accounting-Service is configured, through script, for dynamic service authorization. When the Re-Accounting-Service is set, the server directs the request to the specified reaccounting service for processing.

Re-Authentication-Service

Re-Authentication-Service is configured, through script, for dynamic service authorization. When the Re-Authentication-Service is set, the server directs the request to the specified reauthentication service for processing.

Re-Authorization-Service

Re-Authorization-Service is configured, through script, for dynamic service authorization. When the Re-Authorization-Service is set, the server directs the request to the specified reauthorization service for processing.

Re-Authorization Service must be set to the local service, which contains the profiles that must be added to the EAP Access-Challenge message for delivery of location information from the client to the RADIUS/Diameter server.

Reject-Reason

Reject-Reason is set when a request is being rejected and contains the **Reject-Reason**. Tech Mahindra Access Registrar uses the value of **Reject-Reason** to look up the reject reason in the reply message table.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

If **Reject-Reason** is set to one of: UnknownUser, UserNotEnabled, UserPasswordInvalid, UnableToAcquireResource, ServiceUnavailable, InternalError, MalformedRequest, ConfigurationError, IncomingScriptFailed, OutgoingScriptFailed, IncomingScriptRejectedRequest, OutgoingScriptRejectedRequest, or TerminationAction, then the value set in the configuration under **/Radius/Advanced/ReplyMessages** will be returned.

Remote-Server

Remote-Server is set and read for logging a rejected packet from a remote server. **Remote-Server** records the name and IP address of the remote server to which the request has been forwarded.

Remove-Session-On-Acct-Stop

When set to TRUE, server removes the session on receiving an accounting stop packet.

Remote-Servers-Tried

Remote-Servers-Tried contains a list of remote servers that were tried before a request was accepted or rejected (in the case of a Failover multiple remoteserver policy). The list of servers is a comma-separated list of remote server names.

Request-Authenticator

Request-Authenticator is set for every packet upon reception. Getting the **Request-Authenticator** from a script returns the value of the request authenticator.

Request-Type

Request-Type is set when a request is first received to the type of request, such as one of Access-Request, Access-Accept, Access-Reject, Accounting-Request, Accounting-Response, or Access-Challenge before calling any extension points.

The request contains a string representation of the RADIUS packet type (code). When Tech Mahindra Access Registrar does not recognize the packet type, it is represented as "Unknown-Packet-Type-<*N*>, where <*N*> is the numeric value of the packet type (for example "Unknown-Packet-Type-9). The known packet types are listed in Table B-2.

Table B-2 Request-Type Packets

String	Packet Code
Access-Request	(1)
Access-Accept	(2)
Access-Reject	(3)
Accounting-Request	(4)
Accounting-Response	(5)

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table B-2 Request-Type Packets (continued)

String	Packet Code
Access-Challenge	(11)
Status-Server	(12)
Status-Client	(13)
USR-Resource-Free-Request	(21)
USR-Resource-Free-Response	(22)
USR-Resource-Query-Request	(12)
USR-Resource-Query-Response	(24)
USR-NAS-Reboot-Request	(26)
USR-NAS-Reboot-Response	(27)
Ascend-IPA-Allocate	(50)
Ascend-IPA-Release	(51)
USR-Enhanced-Radius	(254)

Note **Request-Type** is to be used as a read-only variable by scripts.

Require-User-To-Be-In-Authorization-List

Require-User-To-Be-In-Authorization-List is read for authorization. If we are authorizing with a different service than we authenticated with (not usually done) and the user is not known by the authorization service, the default is to continue on unless this environment variable is set, in which case we reject the request with a cause of Unknown-user.

Response-Type

Response-Type is set and read throughout processing and used to determine whether the request should be accepted, rejected, or challenged. When **Response-Type** is set to “Access-Reject at any time during the processing of a request, no more processing of the request is done, and an Access-Reject response is sent. For other valid values for **Response-Type**, see Table B-2.

Retrace-Packet

If set, **Retrace-Packet** causes a trace of the packet to be displayed during the incoming and outgoing scripts. If set, will cause a second trace of the request packet's contents after running all the incoming scripts and/or a second trace of the response packet's contents before running the ou

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Send-PEAP-URI-TLV

When set to TRUE, the URI PEAP-TLV is included along with the Result PEAP-TLV in the access-challenge packet. The authenticating user service (of type userlist, LDAP, or WDA) can set this to TRUE using an extension point script or attribute mapping so that the PEAP-v0 service can send the URI PEAP-TLV. The default value for this is FALSE.

Note This variable is used with the Windows Provisioning Service (WPS) feature.

Session-Key

Session-Key is read for session management. If set, the server uses it as the key to look up the session associated with the current request, if any. If not set, the server uses the NAS IP Address and NAS Port to create a session key.

Session-Manager

Session-Manager is read after user authorization and determines which dynamic resources to allocate for this user, when one is needed. If set, the server directs the request to be processed by the specified session manager. When not set, the SessionManager (as defined in **DefaultSessionManager**) is used when needed.

Session-Notes

Session-Notes is a comma-separated list set to make session information available to scripts. **Session-Notes** contains the names of other environment variables. If set, these variables are stored on a Session as notes.

Session-Service

Session-Service is set and read during session management. If set, the server will direct the request to be processed by the specified session service.

Set-Session-Mgr-And-Key-Upon-Lookup

When **Set-Session-Mgr-And-Key-Upon-Lookup** is set to TRUE, a session-cache resource manager sets the session-manager and session-key environment variable during a query-lookup, and the Tech Mahindra Access Registrar server does not cache the response dictionary attributes.
Set-Session-Mgr-And-Key-Upon-Lookup is set to TRUE by a query-service IncomingScript.

Skip-Session-Management

When set to TRUE in a request, **Skip-Session-Management** causes session management to be skipped for the request, even if session management might normally occur.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Skip-Overriding-Username-With-LDAP-UID

Skip-Overriding-Username-With-LDAP-UID is used to decide if the username should be replaced with the UID from the LDAP server. When Skip-Overriding-Username-With-LDAP-UID is set to TRUE, the username is not replaced with the UID from the LDAP server.

You can use Skip-Overriding-Username-With-LDAP-UID to retain case sensitivity in usernames when the username given logging into the network is in a different case that the UID in the LDAP server database, such as *User1* and *user1*.

Skip-Overriding-UserName-With-PEAPIdentity

Skip-Overriding-Username-With-PEAPIdentity is used to decide if the username should be replaced with the PEAP Identity. When Skip-Overriding-Username-With-PEAPIdentity is set to TRUE, the username is not replaced with the PEAP Identity.

Source-IP-Address

Source-IP-Address is set when a request is first received to the IP address from which the IP request was received before calling any extension points. **Source-IP-Address** contains the IP address of the NAS or proxy server that sent the request to this server.

Note **Source-IP-Address** is to be used as a read-only variable by scripts.

Source-Port

Source-Port is set when a request is first received to the port from which the request was received. Source-Port is set for each request before calling any extension points and contains the port on the NAS or proxy server that was used to send the request to this server.

Note **Source-Port** is to be used as a read-only variable by scripts.

SQL-Sequence

SQL-Sequence variable is set with a list of SQL statement names, separated by a semicolon (;). For example, the SQL statement names ‘sql3’, ‘sql4’, and ‘sql5’ are denoted as sql3;sql4;sql5. If the variable is set, Tech Mahindra Access Registrar picks the SQL statements and executes them in the order specified.

Subnet-Size-If-No-Match

Subnet-Size-If-No-Match is set to one of BIGGER, SMALLER or EXACT, determines the behavior of the subnet-dynamic resource manager if a pool of the requested size is not available.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Trace-Level

Trace-Level is set for each request before calling any extension points. **Trace-Level** is set to the current trace level as specified through **aregcmd**. If set by a script, Trace-Level changes the trace level used to determine what level of information is traced.

Unavailable-Resource

Unavailable-Resource is set during session management. If the request is being rejected because one of the resource managers failed to allocate a resource, **Unavailable-Resource** is set to the name of the resource manager that failed.

Unavailable-Resource-Type

Unavailable-Resource-Type is set during session management. If the request is being rejected because one of the resource managers failed to allocate a resource, **Unavailable-Resource-Type** is set to the type of the resource manager that failed.

UserDefined1

UserDefined1 is set to the value of the UserDefined1 property of the user from a local user list during password matching of local users.

User-Authorization-Script

User-Authorization-Script is read in local services during authorization. If set, the server calls the specified script to do additional user authorization after authentication succeeds.

User-Group

User-Group is read in local services during authorization. If set, species the UserGroup to which the current user belongs.

User-Group-Session-Limit

User-Group-Session-Limit is read during session management. If set, **User-Group-Session-Limit** overrides the limit specified for the group-session-limit resource manager.

User-Name

User-Name is read by a local service during authentication. When **User-Name** is set, it is the name used to authenticate or authorize the request and overrides the **User-Name** in the Request dictionary.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

User-Profile

User-Profile is read in local services during authorization. If set, **User-Profile** specifies the Profile from which the current user should receive attributes.

User-Session-Limit

User-Session-Limit is read during session management. If set, **User-Session-Limit** overrides the limit specified for the user-session-limit resource manager.

Virtual-Server-Outgoing-Script

Virtual-Server-Outgoing-Script is read when LawfulIntercept script object is enabled to use virtual script object. If this is set, the configured script will be executed after server outgoing script.

X509- Subject-Name

X509- Subject-Name reads the value of the subject in the SSL certificate. This is read while processing the access request.

Internal Variables

The following environment variables are used by the server for internal operation. The values for these environment variables must not be modified.

- Add-Message-Authenticator
- Calling-Service-Name
- Cleartext-Password
- Current-Service-Name
- Dynamic-Search-UID
- Duplicate-Req
- EAP-Internal-Services
- Group-Service
- Group-Service-State-ID
- Hidden-Attrib
- IMSI
- Local-Port-type
- Message-Authenticator-Present
- MSCHAP-Account-Name
- MS-ChapV2-Message
- NAS-Name-And-IPAddress

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

- Notify-Service-Session-Key
- Notify-Service-State-ID
- Number-Requested-Quintets
- Number-Requested-Triplets
- Proxied-Dynamic-Auth (named Proxied-POD in earlier releases)
- Provider-Identifier
- Rcd-NT-Password-Hash-Hash (named Rcd-NT-Password-Hash in earlier releases)
- Remote-Session
- Return-Data
- Roaming
- Script-Level
- Session-ID
- Session-Accounting-Counter
- Session-Generation-Tag
- Session-Last-Accessed-Time
- Session-Manager-Key
- Session-NAS-Identifier
- Session-NAS-Port
- Session-Resource-Count
- Session-Resource-%d
- Session-Reuse
- Session-Start-Time
- Session-Survives-NAS-Reboot
- Session-User-Name
- User-Name-Used-For-Lookup
- WiMax-Authentication
- WiMax-SessionManager-Exists

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Appendix C

RADIUS Attributes

This appendix lists the attributes Tech Mahindra Access Registrar supports with their names and values. RADIUS attributes carry the specific authentication, authorization information, and configuration details for requests and replies. For more detailed information about specific attributes, see the appropriate RFC as listed Table C-1.

Table C-1 RFCs for RADIUS Attributes

RFC Subject	RFC Number
Standard RADIUS Attributes	2865
RADIUS Accounting Attributes	2866
Accounting Modifications for Tunnel Protocol Support	2867
Attributes for Tunnel Protocol Support	2868
RADIUS Extensions	2869

This appendix has two sections:

- RADIUS Attributes—This section provides an alphabetic list of all RADIUS attributes Tech Mahindra Access Registrar supports and a list of all RADIUS attributes in numeric order.
- Vendor-Specific Attributes—This section provides lists of RADIUS vendor-specific attributes (VSAs).

RADIUS Attributes

This section lists the RADIUS attributes supported in Tech Mahindra Access Registrar. RADIUS attributes carry specific authentication, authorization, information, and configuration details in the Access-Request and the RADIUS server response.

Tech Mahindra Access Registrar Attributes

Table C-2 provides an alphabetical list of all attributes used in Tech Mahindra Access Registrar and the attribute number.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-2 RADIUS Attributes Alphabetical List

Attribute Name	Attribute Number
Acct-Authentic	45
Acct-Delay-Time	41
Acct-Input-Gigawords	52
Acct-Input-Octets	42
Acct-Input-Packets	47
Acct-Interim-Interval	85
Acct-Link-Count	51
Acct-Multi-Session-Id	50
Acct-Output-Gigawords	53
Acct-Output-Octets	43
Acct-Output-Packets	48
Acct-Session-Id	44
Acct-Session-Time	46
Acct-Status-Type	40
Acct-Terminate-Cause	49
Acct-Tunnel-Connection	68
Acct-Tunnel-Packets-Lost	86
Acquire-Group-Session-Limit	280
ARAP-Challenge-Response	84
ARAP-Features	71
ARAP-Password	70
ARAP-Security	73
ARAP-Security-Data	74
ARAP-Zone-Access	72
Callback-Id	20
Callback-Number	19
Called-Station-Id	30
Calling-Station-Id	31
Change-Password	17
CHAP-Challenge	60
CHAP-Password	3
Class	25
Configuration-Token	78
Connect-Info	77
Digest-Attributes	207
Digest-Response	206

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-2 RADIUS Attributes Alphabetical List (continued)

Attribute Name	Attribute Number
EAP-Message	79
Error-Cause	101
Event-Timestamp	55
Filter-Id	11
Framed-AppleTalk-Link	37
Framed-AppleTalk-Network	38
Framed-AppleTalk-Zone	39
Framed-Compression	13
Framed-Interface-Id	96
Framed-IP-Address	8
Framed-IP-Netmask	9
Framed-IPv6-Pool	100
Framed-IPv6-Prefix	97
Framed-IPv6-Route	99
Framed-IPX-Network	12
Framed-MTU	12
Framed-Pool	88
Framed-Protocol	7
Framed-Route	22
Framed-Routing	10
Idle-Timeout	28
Login-IP-Host	14
Login-IPv6-Host	98
Login-LAT-Group	36
Login-LAT-Node	35
Login-LAT-Port	63
Login-LAT-Service	34
Login-Service	15
Login-TCP-Port	16
Message-Authenticator	80
NAS-Identifier	32
NAS-IP-Address	4
NAS-IPv6-Address	95
NAS-Port	5
NAS-Port-ID	87
NAS-Port-Type	61

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-2 RADIUS Attributes Alphabetical List (continued)

Attribute Name	Attribute Number
Originating-Line-Info	94
Password-Expiration	21
Password-Retry	75
Port-Limit	62
Prompt	76
Proxy-State	33
Reply-Message	18
Service-Type	6
Session-Timeout	27
State	24
Termination-Action	29
Text-Ascend-Data-Filter	225
Tunnel-Assignment-ID	82
Tunnel-Client-Auth-ID	90
Tunnel-Client-Endpoint	66
Tunnel-Medium-Type	65
Tunnel-Password	69
Tunnel-Preference	83
Tunnel-Private-Group-ID	81
Tunnel-Server-Auth-ID	91
Tunnel-Server-Endpoint	67
Tunnel-Type	64
User-Name	1
User-Password	2
Vendor-Specific Attributes	26

RADIUS Attributes Numeric List

Table C-3 lists all RFC-defined RADIUS attributes in numeric order.

Table C-3 RADIUS Attributes Numeric List

Number	Attribute Name
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-3 RADIUS Attributes Numeric List (continued)

Number	Attribute Name
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
9	Framed-IP-Netmask
10	Framed-Routing
11	Filter-Id
12	Framed-MTU
13	Framed-Compression
14	Login-IP-Host
15	Login-Service
16	Login-TCP-Port
17	Change-Password
18	Reply-Message
19	Callback-Number
20	Callback-Id
21	Password-Expiration
22	Framed-Route
12	Framed-IPX-Network
24	State
25	Class

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-3 RADIUS Attributes Numeric List (continued)

Number	Attribute Name
26	Vendor-Specific Attributes (VSAs) See Vendor-Specific Attributes, or the specific vendor's VSA list: • 3GPP VSAs • 3GPP2 VSAs • ACC VSAs • Altiga VSAs • Ascend VSAs • Bay Networks VSAs • Cabletron VSAs • Tech Mahindra Access Registrar Internal VSAs • Tech Mahindra VSAs • Compatible VSAs • Microsoft VSAs • Nomadix VSAs • RedBack VSAs • RedCreek VSAs • Telebit VSAs • Unisphere VSAs • USR VSAs • WiMax • WISPr • XML
27	Session-Timeout
28	Idle-Timeout
29	Termination-Action
30	Called-Station-ID (DNIS)
31	Calling-Station-ID (CLID)
32	NAS-Identifier
33	Proxy-State
34	Login-LAT-Service
35	Login-LAT-Node
36	Login-LAT-Group
37	Framed-AppleTalk-Link

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-3 RADIUS Attributes Numeric List (continued)

Number	Attribute Name
38	Framed-AppleTalk-Network
39	Framed-AppleTalk-Zone
40	Acct-Status-Type
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-Id
45	Acct-Authentic
46	Acct-Session-Time
47	Acct-Input-packets
48	Acct-Output-packets
49	Acct-Terminate-Cause
50	Acct-Multi-Session-Id
51	Acct-Link-Count
52	Acct-Input-Gigawords
53	Acct-Output-Gigawords
54	unassigned
55	Event-Timestamp
56	unassigned
57	unassigned
58	unassigned
59	unassigned
60	CHAP-Challenge
61	NAS-Port-Type
62	Port-Limit
63	Login-LAT-PortNo
64	Tunnel-Type
65	Tunnel-Medium-Type
66	Tunnel-Client-Endpoint
67	Tunnel-Server-Endpoint
68	Acct-Tunnel-Connection
68	Tunnel-ID
69	Tunnel-Password
70	ARAP-Password
71	ARAP-Features
72	ARAP-Zone-Access

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-3 RADIUS Attributes Numeric List (continued)

Number	Attribute Name
73	ARAP-Security
74	ARAP-Security-Data
75	Password-Retry
76	Prompt
77	Connect-Info
78	Configuration-Token
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID
81	Ascend-Auth-Type
82	Tunnel-Assignment-ID
83	Tunnel-Preference
84	ARAP-Challenge-Response
85	Acct-Interim-Interval
85	Ascend-IP-Pool-Chaining
86	Acct-Tunnel-Packets-Lost
87	NAS-Port-ID
88	Framed-Pool
88	Ascend-IP-TOS
89	Ascend-IP-TOS-Precedence
90	Tunnel-Client-Auth-ID
90	Ascend-IP-TOS-Apply-To
91	Tunnel-Server-Auth-ID
91	Ascend-Filter
92	Ascend-Dsl-Rate-Type
93	Ascend-Redirect-Number
94	Originating-Line-Info
95	Ascend-ATM-Vci
96	Ascend-Source-IP-Check
97	Ascend-Dsl-Rate-Mode
98	Ascend-Dsl-Upstream-Limit
99	Ascend-Dsl-Downstream-Limit
100	Ascend-Dsl-CIR-Recv-Limit
101	Error-Cause
102	EAP-Key-Name
103	Ascend-Source-Auth

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-3 RADIUS Attributes Numeric List (continued)

Number	Attribute Name
104	Ascend-Private-Route
105	unassigned
106	Ascend-FR-Link-Status-DLCI
107	unassigned
108	Ascend-Callback-Delay
109	unassigned
110	unassigned
111	Ascend-Multicast-GLeave-Delay
112	Ascend-CBCP-Enable
113	Ascend-CBCP-Mode
114	unassigned
115	Ascend-CBCP-Trunk-Group
116	Ascend-Appletalk-Route
117	Ascend-Appletalk-Peer-Mode
118	Ascend-Route-Appletalk
119	unassigned
120	Ascend-Modem-PortNo
121	Ascend-Modem-SlotNo
122	unassigned
112	unassigned
124	unassigned
125	Ascend-Maximum-Call-Duration
126	Ascend-Preference
127	Tunneling-Protocol
128	Ascend-Shared-Profile-Enable
129	Ascend-Primary-Home-Agent
130	Ascend-Secondary-Home-Agent
131	Ascend-Dialout-Allowed
132	Ascend-Client-Gateway
133	Ascend-BACP-Enable
134	Ascend-DHCP-Maximum-Leases
135	Ascend-Client-Primary-DNS
136	Ascend-Client-Secondary-DNS
137	Ascend-Client-Assign-DNS
138	Ascend-User-Acct-Type
139	Ascend-User-Acct-Host

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-3 RADIUS Attributes Numeric List (continued)

Number	Attribute Name
140	Ascend-User-Acct-Port
141	Ascend-User-Acct-Key
142	Ascend-User-Acct-Base
143	Ascend-User-Acct-Time
144	Ascend-Assign-IP-Client
145	Ascend-Assign-IP-Server
146	Ascend-Assign-IP-Global-Pool
147	Ascend-DHCP-Reply
148	Ascend-DHCP-Pool-Number
149	Ascend-Expect-Callback
150	Ascend-Event-Type
151	Ascend-Session-Svr-Key
152	Ascend-Multicast-Rate-Limit
153	Ascend-IF-Netmask
154	Ascend-Remote-Addr
155	Ascend-Multicast-Client
156	Ascend-FR-Circuit-Name
157	Ascend-FR-LinkUp
158	Ascend-FR-Nailed-Grp
159	Ascend-FR-Type
160	Ascend-FR-Link-Mgt
161	Ascend-FR-N391
162	Ascend-FR-DCE-N392
163	Ascend-FR-DTE-N392
164	Ascend-FR-DCE-N393
165	Ascend-FR-DTE-N393
166	Ascend-FR-T391
167	Ascend-FR-T392
168	Ascend-Bridge-Address
169	Ascend-TS-Idle-Limit
170	Ascend-TS-Idle-Mode
171	Ascend-DBA-Monitor
172	Ascend-Base-Channel-Count
173	Ascend-Minimum-Channels
174	Ascend-IPX-Route
175	Ascend-FT1-Caller

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-3 RADIUS Attributes Numeric List (continued)

Number	Attribute Name
176	Ascend-backup
177	Ascend-Call-Type
178	Ascend-Group
179	Ascend-FR-DLCI
180	Ascend-FR-Profile-Name
181	Ascend-Ara-PW
182	Ascend-IPX-Node-Addr
183	Ascend-Home-Agent-IP-Addr
184	Ascend-Home-Agent-Password
185	Ascend-Home-Network-Name
186	Ascend-Home-Agent-UDP-Port
187	Ascend-Multilink-ID supported
188	Ascend-Num-In-Multilink
189	Ascend-First-Dest (Not supported)
190	Ascend-Pre-Input-Octets
191	Ascend-Pre-Output-Octets
192	Ascend-Pre-Input-packets
193	Ascend-Pre-Output-packets
194	Ascend-Maximum-Time
195	Ascend-Disconnect-Cause
196	Ascend-Connect-Progress
197	Ascend-Data-Rate
198	Ascend-PreSession-Time
199	Ascend-Token-Idle
200	Ascend-Token-Immediate
201	Ascend-Require-Auth
202	Ascend-Number-Sessions
203	Ascend-Authen-Alias
204	Ascend-Token-Expiry
205	Ascend-Menu-Selector
206	Digest-Response
207	Digest-Attributes
208	Ascend-PW-Lifetime
209	Ascend-IP-Direct
210	Ascend-PPP-VJ-Slot-Comp
211	Ascend-PPP-VJ-1172

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-3 RADIUS Attributes Numeric List (continued)

Number	Attribute Name
212	Ascend-PPP-Async-Map
213	Ascend-Third-Prompt
214	Ascend-Send-Secret
215	Ascend-Receive-Secret
216	Ascend-IPX-Peer-Mode
217	Ascend-IP-Pool-Definition
218	Ascend-Assign-IP-Pool
219	Ascend-FR-Direct
220	Ascend-FR-Direct-Profile
221	Ascend-FR-Direct-DLCI
222	Ascend-Handle-IPX
212	Ascend-Netware-timeout
224	Ascend-IPX-Alias
225	Ascend-Metric
226	Ascend-PRI-Number-Type
227	Ascend-Dial-Number
228	Ascend-Route-IP
229	Ascend-Route-IPX
120	Ascend-Bridge
121	Ascend-Send-Auth
122	Ascend-Send-Passwd
123	Ascend-Link-Compression
124	Ascend-Target-Util
125	Ascend-Maximum-Channels
126	Ascend-Inc-Channel-Count
127	Ascend-Dec-Channel-Count
128	Ascend-Seconds-Of-History
129	Ascend-History-Weigh-Type
240	Ascend-Add-Seconds
241	Ascend-Remove-Seconds
242	Ascend-Data-Filter
243	Ascend-Call-Filter
244	Ascend-Idle-Limit
245	Ascend-Preempt-Limit
246	Ascend-Callback
247	Ascend-Data-Svc

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-3 RADIUS Attributes Numeric List (continued)

Number	Attribute Name
248	Ascend-Force-56
249	Ascend-Billing-Number
250	Ascend-Call-By-Call
251	Ascend-Transit-Number
252	Ascend-Host-Info
253	Ascend-PPP-Address
254	Ascend-MPP-Idle-Percent
255	Ascend-Xmit-Rate
256	HNB Parameters
257	Macro-Coverage-Information
258	Geographical Location
259	HNB Internet Information
260	Reject Cause
270	White-List
271	State Value

Vendor-Specific Attributes

This section lists all vendor-specific attributes (VSAs) supported by Tech Mahindra Access Registrar.

3GPP VSAs

Table C-4 lists the 3GPP VSAs. The vendor ID for 3GPP VSAs is 10415.

Table C-4 3GPP VSAs

SubAttr	VSA Name	Type	Min-Max Value
1	3GPP-IMSI	String	0-15
2	3GPP-Charging-Id	UINT	0-65535
3	3GPP-PDPType	ENUM	0-2 0 = IPv4 1 = PPP 2 = IPv6
4	3GPP-OG-Address	IP Address	
5	3GPP-GPRS-QoS-Profile	String	0-31
6	3GPP-SGSN-Address	IP Address	

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-4 3GPP VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
7	3GPP-GGSN-Address	IP Address	
8	3GPP-IMSI-MCC-MNC	String	6-6
9	3GPP-GGSN-MCC-MNC	String	6-6
10	3GPP-NSAPI	String	1-1
11	3GPP-Session-Stop-Indicator	String	2-2
12	3GPP-Selection-Mode	String	1-1
13	3GPP-Charging-Characteristics	String	4-4
14	3GPP-CG-IPv6-Address	String	16-16
15	3GPP-SGSN-IPv6-Address	String	16-16
16	3GPP-GGSN-IPv6-Address	String	6-6
17	3GPP-IPv6-DNS-Servers	String	16-253
18	3GPP-SGSN-MCC-MNC	String	0-1
19	3GPP-Teardown-Indicator	UINT32	0-1
20	3GPP-IMEISV	String	16-16
21	3GPP-RAT-Type	String	1-1
22	3GPP-User-Location-Info	String	0-253
12	3GPP-MS-Timezone	String	2-2
24	3GPP-Camel-Charging-Info	String	0-253
25	3GPP-Packet-Filter	String	0-253
26	3GPP-Negotiated-DSCP	String	1-1

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

3GPP2 VSAs

Table C-5 lists the 3GPP2 VSAs. The vendor ID for 3GPP2 VSAs is 5535 with 8-bit VendorTypeSize.

Table C-5 3GPP2 VSAs

SubAttr	VSA Name	Type	Min-Max Value
1	CDMA-IKE-Pre-Shared-Secret-Request	ENUM	1-2; 1 = The PDSN requests a pre-shared secret for IKE 2 = The PDSN does not request a pre-shared secret for IKE
2	CDMA-Security-Level	ENUM	1-4; 1 = IPSec for registration messages 2 = IPSec for tunnels 3= IPSec for tunnels and registration messages 4 = No IPSec security
3	CDMA-Pre-Shared-Secret	String	0-24
4	CDMA-Reverse-Tunnel-Spec	ENUM	0-1; 0 = Reverse tunneling is not required 1 = Reverse tunneling is required
5	CDMA-Diff-Svc-Class-Opt	ENUM	0-46; 0 = Best Effort 10 = AF11 12 = AF12 14 = AF13 18 = AF21 20 = AF22 22 = AF12 26 = AF31 28 = AF32 30 = AF33 34 = AF41 36 = AF42 38 = AF43 46 = EF
6	CDMA-Container	String	0-253
7	CDMA-HA-IP-Addr	IPADDR	
8	CDMA-KeyID-Attribute	String	0-28
9	CDMA-PCF-IP-Addr	IP Address	
10	CDMA-BS-MSC-Addr	String	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-5 3GPP2 VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
11	CDMA-User-ID	UINT32	0-0
12	CDMA-Forward-MUX	UINT32	0-0
13	CDMA-Reverse-MUX	UINT32	0-0
14	CDMA-Forward-Rate	UINT32	0-0
15	CDMA-Reverse-Rate	UINT32	0-0
16	CDMA-Service-Option	UINT32	0-0
17	CDMA-Forward-Type	ENUM	0-1; 0 = Primary 1 = Secondary
18	CDMA-Reverse-Type	ENUM	0-1; 0 = Primary 1 = Secondary
19	CDMA-Frame-Size	ENUM	0-2; 0 = No Fundamental 1 = 5 ms Frame and 20ms Mixed Frame 2 = 20 ms Frame
20	CDMA-Forward-RC	UINT32	0-0
21	CDMA-Reverse-RC	UINT32	0-0
22	CDMA-IP-Technology	ENUM	1-3; 1 = Simple-IP 2 = Mobile-IP 3 = Proxy-Mobile-IP
12	CDMA-Comp-Flag	ENUM	0-2; 0 = None 1 = Non-secure 2 = Secure

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-5 3GPP2 VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
24	CDMA-Release-Ind	ENUM	0-14; 0 = Unknown 1 = PPP/Service timeout 2 = Handoff 3 = PPP termination 4 = Mobile IP registration failure 5 = Abnormal Terminations 6 = Termination due to Resource management 7 = Service instance released 8 = Volume Quota reached, service instance released 9 = Duration Quota reached, Service instance released 10 = Incompatible PrePaid accounting information 11 = Airlink Parameter Change 12 = Time of Day Timer expiration 13 = Dormant by Accounting-Stop-triggered-by-Active-Stop 14 = Hot-Line status changed
25	CDMA-Dropped-Octets	UINT32	0-0
26	CDMA-Start-Date	String	0-253
27	CDMA-Start-Time	String	0-253
28	CDMA-Stop-Date	String	0-253
29	CDMA-Stop-Time	String	0-253
30	CDMA-Num-Active	UINT32	0-0
31	CDMA-SDB-Input-Octets	UINT32	0-0
32	CDMA-SDB-Output-Octets	UINT32	0-0
33	CDMA-NumSDB-Input	UINT32	0-0
34	CDMA-NumSDB-Output	UINT32	0-0
35	CDMA-Alt-Billing	UINT32	0-0

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-5 3GPP2 VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
36	CDMA-IP-QoS	UINT32	0-0
37	CDMA-Interconnect-IP	UINT32	0-0
38	CDMA-Interconnect-QoS	UINT32	0-0
39	CDMA-Air-QoS	UINT32	0-0
40	CDMA-Airlink-Record-Type	ENUM	1-4; 1 = Connection Setup 2 = Active Start 3 = Active Stop 4 = SDB Record
41	CDMA-R-P-Link-ID	UINT32	0-0
42	CDMA-Airlink-Record-Type	UINT32	0-0
43	CDMA-PPP-Bytes-Received	UINT32	0-0
44	CDMA-Correlation-ID	String	0-253
45	CDMA-Mobile-Terminate-Originated-Ind	UINT32	0-0
46	CDMA-Inbound-Mobile-IP-Signalling-Octets	UINT32	0-0
47	CDMA-Outbound-Mobile-IP-Signalling-Octets	UINT32	0-0
48	CDMA-Session-Continue	ENUM	0-1; 0 = False 1 = True
49	CDMA-Active-Time	UINT32	0-0
50	CDMA-DCCH-Frame-Format	UINT32	0-3
51	CDMA-Beginning-Session	ENUM	0-1; 0 = False 1 = True
52	CDMA-ESN	String	0-253
54	CDMA-S-Attribute	String	0-253
55	CDMA-S-Request-Attribute	ENUM	0-1; 0 = The HA does not request a S secret for IKE 1 = The HA requests a S secret for IKE

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-5 3GPP2 VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
56	CDMA-S-Lifetime-Attribute	UINT32	0-0
57	CDMA-MN-HA-SPI	String	0-4
58	CDMA-MN-HA-Shared-Key	String	0-253
59	CDMA-Remote-IPv4-Address	String	12-253
60	CDMA-HRPD-Access-Authentication	ENUM	1-1; 1 = HRPD Access Authentication
70	CDMA-Remote-IPv6-Address	String	68-253
71	CDMA-Remote-Address-Table-Index	UINT32	0-253
72	CDMA-Remote-IPv4-Address-Octet-Count	String	24-253
73	CDMA-Allowed-Differentiated-Service-Marking	String	12-253
74	CDMA-Service-Option-Profile	String	8-253
75	CDMA-DNS-Update-Required	ENUM	0-1; 0 = HA does not need to send DNS Update 1 = HA does need to send DNS Update
78	CDMA-Always-On	ENUM	0-1; 0 = Inactive 1 = Active
79	CDMA-Foreign-Agent-Address	IP Address	
80	CDMA-Last-User-Activity	UINT32	0-0
81	CDMA-MN-AAA-Removal-Indication	ENUM	1-1; 1 = MN-AAA not required
82	CDMA-RN-Packet-Data-Inactivity-Timer	UINT32	0-0
83	CDMA-Forward-PDCH-RC	UINT32	0-0
84	CDMA-Forward-DCCH-Mux-Option	UINT32	0-0
85	CDMA-Reverse-DCCH-Mux-Option	UINT32	0-0
86	CDMA-Forward-DCCH-RC	UINT32	0-0
87	CDMA-Reverse-DCCH-RC	UINT32	0-0

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-5 3GPP2 VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
88	CDMA-Session-Termination-Capability	UINT32	0-0
89	CDMA-Allowed-Persistent-TFTs	UINT32	0-0
90	CDMA-PrePaid-Accounting-Quota	String	0-253
91	CDMA-PrePaid-Accounting-Capability	String	0-253
92	CDMA-MIP-Lifetime	String	0-253
93	CDMA-Accounting-Stop-Triggered-By-Active-Stop-Indication	ENUM	1-1; 1 = Accounting report at active/ dormant transitions
94	CDMA-Service-Reference-ID	String	0-253
95	CDMA-DNS-Update-Capability	ENUM	1-1: 1 = HA is capable of dynamic DNS Update
96	CDMA-Disconnect-Reason	ENUM	1-1: 1 = MS Mobility Detection
97	CDMA-Remote-IPv6-Address-Octet-Count	String	36-253
98	CDMA-PrePaid-Tariff-Switching	String	0-253
99	CDMA-Authorization-Parameters	String	0-253
100	CDMA-BCMCS-Flow-ID	String	0-253
101	CDMA-BCMCS-Capability	String	0-253
102	CDMA-Common-Session-Info	String	0-253
103	CDMA-BSN-Session-Info	String	0-253
104	CDMA-RN-Session-Info	String	0-253
105	CDMA-Reason-Code	String	0-253
106	CDMA-Physical-Channel	String	0-253
107	CDMA-BCMCS-Flow-Transmission-Time	String	0-253
108	CDMA-Subnet	String	0-253
109	CDMA-Multicast-IP-Address	String	0-253
110	CDMA-Port	String	0-253
111	CDMA-Auth-Key	String	0-253
112	CDMA-TK-Info	String	0-253
113	CDMA-BAK-ID	String	0-253
114	CDMA-Reverse-PDCH-RC	UINT32	0-0
115	CDMA-Acq-Info-Timestamp	UINT32	0-0

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-5 3GPP2 VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
116	CDMA-MEID	String	0-16
117	CDMA-DNS-Server-IP-Address	String	0-22
118	CDMA-MIP6-Home-Agent-from-BU	String	0-18
119	CDMA-MIP6-CoA	String	0-22
120	CDMA-MIP6-HoA-Not-Authorized	ENUM	1-1; 1 = The HoA is not authorized
121	CDMA-MIP6-Session-Key	String	0-253
122	CDMA-Hot-Line-Accounting-Indicatio n	String	0-253
112	CDMA-Hot-Line-Profile-ID	String	0-253
124	CDMA-Filter-Rule	String	0-253
125	CDMA-HTTP-Redirection-Rule	String	0-253
126	CDMA-IP-Redirection-Rule	String	0-253
127	CDMA-Hot-Line-Capability	UINT3 2	0-0
128	CDMA-MIP6-Home-Link-Prefix	String	0-253
129	CDMA-MIP6-Home-Address	String	0-253
130	CDMA-Maximum-Authorized-Aggrega te-Bandwidth-for-Best-Effort-Traffic	UINT3 2	0-0
131	CDMA-Authorized-QoS-Profile-IDs-fo r-the-User	String	0-253
132	CDMA-Granted-QoS-Parameters	String	0-253
133	CDMA-Maximum-Per-Flow-Priority-fo r-the-User	UINT3 2	0-15
134	CDMA-MIP6-Authenticator	String	0-253
135	CDMA-Source-IPv6-Address	String	0-253
136	CDMA-Program-ID	String	0-253
137	CDMA-Program-Name	String	0-253
138	CDMA-MIP6-MAC-Mobility-Data	String	0-253
139	CDMA-Inter-User-Priority	UINT3 2	0-3
140	CDMA-MIP6-Home-Agent-Attribute-B	String	0-253
141	CDMA-MIP6-HoA	String	0-253
142	CDMA-Carrier-ID	String	0-8
143	CDMA-GMT-Time-Zone-Offset	String	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

ACC VSAs

Table C-6 lists the ACC VSAs. The vendor ID for ACC VSAs is 5.

Table C-6 ACC VSAs

SubAttr	VSA Name	Type	Min-Max Value
1	Acc-Reason-Code	ENUM: no reason given/no failure resource shortage protocol error invalid attribute invalid service type invalid framed protocol invalid attribute value invalid user information invalid IP address invalid integer syntax invalid NAS port	0-56
1	Acc-Reason-Code *(Continued)*	ENUM: requested by user session already open network disconnect service interruption physical port error idle timeout session timeout administrative reset NAS reload or reset NAS error NAS request	0-56
1	Acc-Reason-Code *(Continued)*	ENUM: undefined reason given too many RADIUS users conflicting attributes port limit exceeded facility not available internal configuration error bad route specification	0-56

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-6 ACC VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
1	Acc-Reason-Code *(Continued)*	Access Partition bind failure security violation request type conflict configuration disallowed missing attribute no authentication server invalid request missing parameter invalid parameter call cleared with cause inopportune config request invalid config parameter missing config parameter incompatible service profile administrative reset	0-56
1	Acc-Reason-Code *(Continued)*	administrative reload no authentication response port unneeded port preempted port suspended service unavailable callback user error host request no accounting server no accounting response access denied temporary buffer shortage	0-56
2	Acc-Ccp-Option	ENUM: Disabled Enabled	1-2
3	Acc-Input-Errors	UINT32	0-253
4	Acc-Output-Errors	UINT32	0-253
5	Acc-Access-Partition	String	0-253
6	Acc-Customer-Id	String	0-253
7	Acc-Ip-Gateway-Pri	IPADDR	0-253
8	Acc-Ip-Gateway-Sec	IPADDR	0-253
9	Acc-Route-Policy	ENUM : Funnel Direct	1-2
10	Acc-ML-MLX-Admin-State	ENUM: Enabled Disabled	1-2
11	Acc-ML-Call-Threshold	UINT32	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-6 ACC VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
12	Acc-ML-Clear-Threshold	UINT32	0-253
13	Acc-ML-Damping-Factor	UINT32	0-253
14	Acc-Tunnel-Secret	String	0-253
15	Acc-Clearing-Cause	ENUM: cause unspecified unassigned number invalid information element c message incompatible with sta recovery on timer expiration mandatory information element protocol error interworking normal clearing user busy no user responding user alerted no answer	0-127
15	Acc-Clearing-Cause *(Continued)*	ENUM: no route to transit network call rejected number changed non selected user clearing destination out of order invalid or incomplete number facility rejected no route to destination response to status inquiry normal unspecified cause no circuit or channel availab network out of order	0-127
15	Acc-Clearing-Cause *(Continued)*	ENUM: temporary failure switching equipment congestio access information discarded circuit or channel unavailabl circuit or channel preempted resources unavailable quality of service unavailabl facility not subscribed outgoing calls barred incoming calls barred bearer capability unauthorize bearer capability not availab	0-127

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-6 ACC VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
15	Acc-Clearing-Cause *(Continued)*	ENUM: channel unacceptable service not available bearer capability not impleme channel type not implemented facility not implemented call awarded being delivered restricted digital informatio service not implemented invalid call reference identified channel does not e call identity does not exist call identity in use no call suspended	0-127
15	Acc-Clearing-Cause *(Continued)*	ENUM: suspended call cleared incompatible destination invalid transit network selec invalid message mandatory information element message not implemented inopportune message information element not imple	0-127
16	Acc-Clearing-Location	ENUM: local or remote user private network serving local beyond interworking point public network serving local transit network private network serving remot public network serving remote international network	0-10
17	Acc-Service-Profile	String	0-253
18	Acc-Request-Type	ENUM: Ring Indication Dial Request User Authentication Tunnel Authentication User Accounting Tunnel Accounting	1-6
19	Acc-Framed-Bridge	ENUM : Disabled Enabled	0-1
20	Acc-Vpsm-Oversubscribed	ENUM : False True	1-2

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-6 ACC VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
21	Acc-Acct-On-Off-Reason	ENUM : NAS Reset NAS Reload Configuration Reset Configuration Reload Enabled Disabled	0-5
22	Acc-Tunnel-Port	UINT32	0-253
12	Acc-Dns-Server-Pri	IPADDR	0-253
24	Acc-Dns-Server-Sec	IPADDR	0-253
26	Acc-Nbns-Server-Sec	IPADDR	0-253
27	Acc-Dial-Port-Index		
28	Acc-Ip-Compression	ENUM: Disabled Enabled	0-1
29	Acc-Ipx-Compression	ENUM: Disabled Enabled	0-1
30	Acc-Connect-Tx-Speed	UINT32	0-253
31	Acc-Connect-Rx-Speed	UINT32	0-253
32	Acc-Modem-Modulation-Type	String	0-253
33	Acc-Modem-Error-Protocol	String	0-253
34	Acc-Callback-Delay	UINT32	0-253
35	Acc-Callback-Num-Valid	String	0-253
36	Acc-Callback-Mode	ENUM: User-Auth User-Specified-E-164 CBCP-Callback CLI-Callback	0-7
37	Acc-Callback-CBCP-Type	ENUM: CBCP-None CBCP-User-Specified CBCP-Pre-Specified	1-3
38	Acc-Dialout-Auth-Mode	ENUM: PAP CHAP CHAP-PAP NONE	1-4
39	Acc-Dialout-Auth-Password	String	0-253
40	Acc-Dialout-Auth-UserName	String	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-6 ACC VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
42	Acc-Access-Community	ENUM: PUBLIC NETMAN	1-2
43	Acc-Vpsm-Reject-Cause	ENUM: No-Access-Partition Access-Partition-Disabled Partition-Portlimit-Exceeded License-Portlimit-Exceeded Home-Server-Down Rejected-By-Home-Server NAS-Administratively-Disabled	1-7
44	Acc-Ace-Token	String	0-253
45	Acc-Ace-Token-Ttl	UINT	0-253
46	Acc-Ip-Pool-Name	String	0-253
47	Acc-Igmp-Admin-State	ENUM : Enabled Disabled	1-2
48	Acc-Igmp-Version	ENUM : V1 V2	1-2

Altiga VSAs

Table C-7 lists the Altiga VSAs. The vendor ID for Altiga VSAs is 3076.

Table C-7 Altiga VSAs

SubAttr	VSA Name	Type	Min-Max Value
1	Altiga-General-Acces-Hours	String	0-253
2	Altiga-General-Simultaneous-Logic	UINT32	0-253
3	Altiga-General-Minimum-Password-Length	UINT32	0-253
4	Altiga-General-All-Alphabetic-Only-Passwords	ENUM	0-1
5	Altiga-General-Primary-DNS	IP Address	0-253
6	Altiga-General-Secondary-DNS	IP Address	0-253
8	Altiga-General-Secondary-WINS	IP Address	0-253
9	Altiga-General-SEP-Card-Assignment	UINT32	0-253
10	Altiga-General-Priority-On-SEP	UINT32	0-253
11	Altiga-General-Tunneling-Protoco	UNIT32	0-253
12	Altiga-IPSec-Security-Associatio	String	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-7 Altiga VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
13	Altiga-IPSec-Authentication	ENUM: None RADIUS LDAP NT Domain SDI Internal	0-5
15	Altiga-IPSec-Banner	String	0-253
16	Altiga-IPSec-Allow-Password-Storage-On-Client	ENUM: False True	0-1
17	Altiga-PPTP-L2TP-Use-Client-Specified-Addres s	ENUM: False True	0-1
18	Altiga-PPTP-Minimal-Authentication-Protocol	UINT32	0-253
19	Altiga-L2TP-Minimal-Authentication	UINT32	0-253
20	Altiga-PPTP-Encryption	UINT32	0-253
21	Altiga-L2TP-Encryption	UINT32	0-253
22	Altiga-Argument-Authentication-Server-Type	ENUM: First Active Server RADIUS LDAP NT SDI Internal	0-5
12	Altiga-Argument-Authentication-Server-Passwor d	String	0-253
24	Altiga-Argument-Request-Authenticatior-Vector	String	0-253
25	Altiga-IPSec-LTL-Keepalives	ENUM: False True	0-1
26	Altiga-Argument-IPSec-Group-Name	String	0-253
27	Altiga-IPSec-Split-Tunneling	String	0-253
28	Altiga-IPSec-Default-Domain	String	0-253
28	Altiga-IPSec-Secondary-Domain-List	String	0-253
30	Altiga-IPSec-Tunnel-Type	ENUM: LAN to LAN Remote Access	1-2

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-7 Altiga VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
31	Altiga-IPSec-Mode-Configuration	ENUM: False True	0-1
32	Altiga-Argument-Authentication-Server-Priority	UINT32	0-253
33	Altiga-IPSec-Group-Lock-Of-User	ENUM: False True	0-1
34	Altiga-IPSec-IPSec-Over-UDP	ENUM: False True	0-1
35	Altiga-IPSec-UDP-Port-For-IPSec	UINT32	0-253
128	Altiga-Partitioning-Primary-DHCP		
129	Altiga-Partitioning-Secondary-DHCP	IP Address	0-253
131	Altiga-Partitioning-Premise-Rout	IP Address	0-253
132	Altiga-Partitioning-Partition-Max-Sessions	String	0-253
133	Altiga-Partitioning-Mobile-IP-Key	String	0-253
134	Altiga-Partitioning-Mobile-IP-Address	IP Address	0-253
135	Altiga-Partitioning-Mobile-IP-SPI	IP Address	0-253
136	Altiga-Partitioning-Strip-Realm	ENUM: False True	0-1
137	Altiga-Partitioning-Group-ID	UINT32	0-253
250	Altiga-Group-Name	String	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Ascend VSAs

Table C-8 lists the Ascend VSAs. The vendor ID for Ascend VSAs is 529.

Table C-8 Ascend VSAs

SubAttr	VSA Name	Type	Min-Max Value
17	Ascend-Change-Password	String	0 - 253
18	Ascend-Session-Type	ENUM: Unused Unknown G711-Ulaw G711-Alaw G712 G729 G712-64KPS G728 RT24	0 - 8
19	Ascend-H312-Gatekeeper	IP Address	0 - 253
21	Ascend-H312-Conference-ID	String	0-253
22	Ascend-H312-Destination-NAS-ID	IP Address	0-65535
12	Ascend-H312-Dialed-Time	UINT32	0-253
24	Ascend-H312-Dialed-Number	String	0-253
25	Ascend-Inter-Arrival-Jitter	UINT32	0-253
26	Ascend-Dropped-Octets	UINT32	0-253
27	Ascend-Dropped-Packets	UINT32	0-253
48	Ascend-Call-Direction	ENUM: Incoming Outgoing	0-1

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-8 Ascend VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
49	Ascend-Service-Type	ENUM	0 - 12; NotUsed None EuUi Telnet TelnetBin RawTcp TermServer MP VirtualConn X25DChan PseuTun PPP IpFax Other ATM HdlcNrm VoIp Visa2 PPP Slip MPP X25 Combinet FR EuRaw
68	Ascend-Tunnel-ID	String	0 - 253
126	Ascend-Route-Preference	ENUM: Interface, OSPF-Internal, RIP, Down-WAN, OSPF-ASE, Infinite, ICMP	0-225
132	Ascend-Client-Gateway	IP Address	0 - 253
144	Ascend-Assign-IP-Client	IP Address	0-0
145	Ascend-Assign-IP-Server	IP Address	0-0
152	Ascend-Multicast-Rate-Limit	UINT32	0-65535
162	Ascend-FR-DCE-N392	UINT32	0-65535

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-8 Ascend VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
163	Ascend-FR-DTE-N392	UINT32	0-65535
164	Ascend-FR-DCE-N393	UINT32	0-65535
165	Ascend-FR-DTE-N393	UINT32	0-65535
166	Ascend-FR-T391	UINT32	0-65535
167	Ascend-FR-T392	UINT32	0-65535
168	Ascend-Bridge-Address	UINT32	1-253
169	Ascend-TS-Idle-Limit	UINT32	0-65535
170	Ascend-TS-Idle-Mode	ENUM; TS-Idle-None TS-Idle-Input TS-Idle-Input-Output	0-2
171	Ascend-DBA-Monitor	ENUM; Transmit Transmit-Receive None	0-2
172	Ascend-Base-Channel-Count	UINT32	0-65535
173	Ascend-Minimum-Channels	UINT32	0-65535
174	Ascend-IPX-Route	String	1-253
175	Ascend-FT1-Caller	ENUM; FT1-No FT1-Yes	0-1
176	Ascend-Backup	String	1-253
177	Ascend-Call-Type	ENUM; Nailed Nailed/MPP Perm/Switched	0-2
178	Ascend-Group	String	1-253
179	Ascend-FR-DLCI	UINT32	0-65535
180	Ascend-FR-Profile-Name	String	1-253
181	Ascend-Ara-PW	String	1-253
182	Ascend-IPX-Node-Address	String	1-253
183	Ascend-Home-Agent-IP-Addr	IP Address	0-0
184	Ascend-Home-Agent-Password	String	1-253
185	Ascend-Home-Network-Name	String	1-253
186	Ascend-Home-Agent-UDP-Port	UINT32	0-65535
187	Ascend-Multilink-ID	UINT32	0-65535

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-8 Ascend VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
188	Ascend-Num-In-Multilink	UINT32	0-65535
189	Ascend-First-Dest	IP Address	0-0
190	Ascend-Pre-Input-Octets	UINT32	0-65535
191	Ascend-Pre-Output-Octets	UINT32	0-65535
192	Ascend-Pre-Input-Packets	UINT32	0-65535
193	Ascend-Pre-Output-Packets	UINT32	0-65535
194	Ascend-Maximum-Time	UINT32	0-65535

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-8 Ascend VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
195	vAscend-Pre-Output-Packets (continued)	ENUM: No-Reason, Not-Applicable, Modem-No-DCD, Session-Timeout, Invalid-Incoming-User, Disconnect-Due-To-Callback, DCD-Detected-Then-Inactive, Modem-Invalid-Result-Codes, Protocol-Disabled-Or-Unsuppor, Disconnect-Req-By-RADIUS, Disconnect-Req-By-Local-Admin, V110-Timeout-Or-Sync-Retry-Ex, PPP-Auth-Timeout-Exceeded, User-Executed-Do-Hangup, Remote-End-Hung-Up, Resource-Has-Been-Quiesced, Max-Call-Duration-Reached, Unknown, (continued)	0-195

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-8 Ascend VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
195	vAscend-Pre-Output-Packets	ENUM: TermSrv-User-Quit, TermSrv-Idle-Timeout, TermSrv-Exit-Telnet, TermSrv-No-IPaddr, TermSrv-Exit-Raw-TCP, TermSrv-Exit-Login-Failed, TermSrv-Exit-Raw-TCP-Disabled, TermSrv-CTRL-C-In-Login, TermSrv-Destroyed, TermSrv-User-Closed-VCon, Call-Disconnected, TermSrv-VCon-Destroyed, TermSrv-Exit-Rlogin, TermSrv-Bad-Rlogin-Option, TermSrv-Not-Enough-Resources, MPP-No-NULL-Msg-Timeout, CLID-Authentication-Failed, (continued)	0-195

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-8 Ascend VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
195	vAscend-Pre-Output-Packets	ENUM: PPP-LCP-Timeout, PPP-LCP-Negotion-Failed, PPP-PAP-Auth-Failed, PPP-CHAP-Auth-Failed, PPP-Rmt-Auth-Failed, PPP-Rcv-Terminate-Req, PPP-Rcv-Close-Event, PPP-No-NCPs-Open, PPP-MP-Bundle-Unknown,. PPP-LCP-Close-MP-Add-Fail, CLID-RADIUS-Timeout (continued)	0-195

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-8 Ascend VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
195	vAscend-Pre-Output-Packets (*continued*)	Out-Of-Resources, Invalid-IP-Address, Hostname-Resolution-Failed, Bad-Or-Missing-Port-Number, Host-Reset, Connection-Refused, Connection-Timeout, Connection-Closed, Network-Unreachable, Host-Unreachable, Network-Unreachable-Admin, Host-Unreachable-Admin, Port-Unreachable,	

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-8 Ascend VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
196	Ascend-Connect-Progress	ENUM: No-Progress, unknown1, Call-Up, unknown2, Modem-Up, Modem-Awaiting-DCD, Modem-Awaiting-Codes, TermSrv-Started, TermSrv-Raw-TCP-Started, TermSrv-Telnet-Started, TermSrv-Raw-TCP-Connected, TermSrv-Telnet-Connected, TermSrv-Rlogin-Started, TermSrv-Rlogin-Connected, TermSrv-Authentication-Begin, Modem-Outdial-Call-Up	0-94

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-8 Ascend VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
196	Ascend-Connect-Progress	ENUM: LAN-Session-Up, LCP-Opening, CCP-Opening, IPNCP-Opening, NCP-Opening, LCP-Opened, CCP-Opened, IPNCP-Opened, BNCP-Opened, LCP-State-Initial, LCP-State-Starting, LCP-State-Closed, LCP-State-Stopped, BACP-Opened, LCP-State-Stopping, LCP-State-Request-Sent, LCP-State-Ack-Received, LCP-State-Ack-Sent, IPXNCP-Opened, ATNCP-Opened, BACP-Opening, V110-Up, V110-State-Opened, V110-State-Carrier, V110-State-Reset, V110-State-Closed	0-94
197	Ascend-Data-Rate	UINT32	0-65535

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-8 Ascend VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
198	Ascend-PreSession-Time	UINT32	0-65535
199	Ascend-Token-Idle	UINT32	0-65535
200		ENUM: Tok-Imm-No, Tok-Imm-Yes	0-1
201	Ascend-Require-Auth	ENUM: Not-Require-Auth Require-Auth Pap-Only Pap-Only Pap-Login-Only Pap-Framed-Only Pap-Outbound-Only CHAP-Only CHAP-Only CHAP-Login-Only CHAP-Framed-Only CHAP-Outbound-Only MS-CHAP-Only MS-CHAP-Only MS-CHAP-Login-Only MS-CHAP-Framed-Only MS-CHAP-Outbound-Only	0-55
210	Ascend-PPP-VJ-Slot-Comp	ENUM: VJ-Slot-Comp-No	1-1
211	Ascend-PPP-VJ-1172	ENUM: PPP-VJ-1172	1-1
212	Ascend-PPP-Async-Map	UINT32	0-65535
213	Ascend-Third-Prompt	String	1-253
214	Ascend-Send-Secret	String	1-253
215	Ascend-Receive-Secret	String	1-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-8 Ascend VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
216	Ascend-IPX-Peer-Mode	ENUM: IPX-Peer-Router, IPX-Peer-Dialin	1-1
217	Ascend-IP-Pool-Definition	String	1-253
218	Ascend-Assign-IP-Pool	UINT32	0-65535
219	Ascend-FR-Direct	ENUM: FR-Direct-No, FR-Direct-Yes	1-1
220	Ascend-FR-Direct-Profile	String	1-253
221	Ascend-FR-Direct-DLCI	UINT32	0-65535
222	Ascend-Handle-IPX	ENUM: Handle-IPX-None, Handle-IPX-Client, Handle-IPX-Server	0-2
212	Ascend-Netware-timeout	UINT32	0-65535
224	Ascend-IPX-Alias	UINT32	0-65535
225	Ascend-Metric	UINT32	0-65535
226	Ascend-PRI-Number-Type	ENUM: Unknown-Number, Intl-Number, National-Number, Local-Number Abbrev-Number	0-5
227	Ascend-Dial-Number	String	1-253
228	Ascend-Route-IP	ENUM: Unknown-Number, Intl-Number, National-Number, Local-Number, Abbrev-Number	0-5

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-8 Ascend VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
229	Ascend-Route-IPX	ENUM: Route-IPX-No Route-IPX-Yes	0-1
120	Ascend-Bridge	ENUM: Bridge-No, Bridge-Yes	0-1
121	Ascend-Send-Auth	ENUM: Send-Auth-None, end-Auth-PAP, Send-Auth-CHAP	0-2
122	Ascend-Send-Passwd	String	1-253
123	Ascend-Link-Compression	ENUM: Link-Comp-None, Link-Comp-Stac, Link-Comp-Stac-Draft-9, Link-Comp-MS-Stac	0-3
124	Ascend-Target-Util	UINT32	0-65535
125	Ascend-Maximum-Channels	UINT32	0-65535
126	Ascend-Inc-Channel-Count	UINT32	0-65535
127	Ascend-Dec-Channel-Count	UINT32	0-65535
128	Ascend-Seconds-Of-History	UINT32	0-65535
129	Ascend-History-Weigh-Type	ENUM: History-Constant, History-Linear, History-Quadratic	0-2
240	Ascend-Add-Seconds	UINT32	0-65535
241	Ascend-Remove-Seconds	UINT32	0-65535
242	Ascend-Data-Filter	String	1-253
243	Ascend-Call-Filter	String	1-253
244	Ascend-Idle-Limit	UINT32	0-65535
245	Ascend-Idle-Limit	UINT32	0-65535

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-8 Ascend VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
246	Ascend-Callback	ENUM: Callback-No, Callback-Yes	0-1

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

SubAttr	VSA Name	Type	Min-Max Value
247	Ascend-Data-Svc	ENUM: Switched-Voice-Bearer, Switched-56KR, Switched-192K, Switched-256K, Switched-320K, Switched-384K-MR, Switched-448K, Switched-512K, Switched-566K, Switched-640K, Switched-704K, Switched-768K, Switched-64K, Switched-832K, Switched-896K, Switched-960K, Switched-1024K, Switched-1088K, Switched-1152K, Switched-1216K,. Switched-1280K, Switched-1344K, Switched-1408K, Switched-64KR, Switched-1472K, Switched-160	0-43

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-8 Ascend VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
248	Ascend-Force-56	ENUM: Force-56-No, Force-56-Yes	0-1
249	Ascend-Billing-Number	String	1-253
250	Ascend-Call-By-Call	UINT32	0-65535
251	Ascend-Transit-Number	String	1-253
252	Ascend-Host-Info	String	1-253
253	Ascend-PPP-Address	IP Address	0-0
254	Ascend-MPP-Idle-Percent	UINT32	0-65535

Bay Networks VSAs

Table C-9 lists the Bay Networks VSAs. The vendor ID for Bay Networks VSAs is 1584.

Table C-9 Bay Networks VSAs

SubAttr	VSA Name	Type	Min-Max Value
28	Annex-Filter	String	1-253
29	Annex-CLI-Command	String	1-253
30	Annex-CLI-Filter	String	1-253
31	Annex-Host-Restrict	String	1-253
32	Annex-Host-Allow	String	1-253
33	Annex-Product-Name	String	1-253
34	Annex-SW-Version	String	1-253
35	Annex-Local-IP-Address	IPADDR	1-253
36	Annex-Callback-Portlist	UINT32	0-0
44	Annex-System-Disc-Reason	UINT32	0-0
45	Annex-Modem-Disc-Reason	UINT32	0-0
46	Annex-Disconnect-Reason	UINT32	0-0
50	Annex-Transmit-Speed	UINT32	0-0
51	Annex-Receive-Speed	UINT32	0-0

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Cabletron VSAs

Table C-10 lists the Cabletron VSAs. The vendor ID for Cabletron VSAs is 52.

Table C-10 Cabletron VSAs

SubAttr	VSA Name	Type	Min-Max Value
192	Cabletron-Framed-Data-Rate	ENUM: Rate-56KB Rate-64KB Rate-112KB Rate-128KB	0-4
193	Cabletron-Phone-Number	String	0-253
194	Cabletron-Caller-Id	String	0-253
196	Cabletron-Connection-Reference	UINT32	0-253
198	Cabletron-Initial-Rate	UINT32	0-253
199	Cabletron-Maximum-Rate	UINT32	0-253
192	Cabletron-Framed-Data-Rate	Enum: Rate-56KB Rate-64KB Rate-112KB Rate-128KB	192

Tech Mahindra Access Registrar Internal VSAs

Table C-11 lists the Tech Mahindra Access Registrar Internal VSAs. The vendor ID for Tech Mahindra Access Registrar internal VSAs is 1760.

Table C-11 Tech Mahindra Access Registrar Internal VSAs

SubAttr	VSA Name	Type	Min-Max Value
1	Realm	String	1-253
2	Incoming-Translation-Groups	String	1-253
3	Client-IP-Address	IP Address	1-253
4	Subnet-Mask	IP Address	1-253
5	Outgoing-Translation-Groups	String	1-253
6	Authentication-Service	String	1-253
7	Authorization-Service	String	1-253
8	DNIS	String	1-253
9	CLID	String	1-253
10	UserFilterMask	String	1-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-11 Tech Mahindra Access Registrar Internal VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
11	Session-Manager	String	1-253
12	Accounting-Service	String	1-253
13	TimeRange	String	1-253
14	AcceptedProfiles	String	1-253
15	Policy	String	1-253
16	Prefix	String	1-253
17	Delimiters	String	1-253
18	StripPrefix	String	1-253
19	ODBC-Reply-Attribs	String	1-253
20	ODBC-Check-Attribs	String	1-253
21	Session-Service	String	1-253
22	Prepaid	ENUM: 0 = False 1 = True	0-1
12	Suffix	String	0-253
12	Implicit-Auth-Enabled	ENUM: 0 = False 1 = True	0-1
24	StripSuffix	ENUM: 0 = False 1 = True	0-1
24	Query-Service	String	0-253
92	RepSourceIP	String	1-253
93	RepTargetIP	String	1-253
94	RepTxnNum	String	1-253
95	RepTxnCRC	String	1-253
96	RepTxnElementCount	String	1-253
97	RepNeedsFullSync	UINT32	0-253
98	RepNeedsReSync	UINT32	0-253
99	RepLastRxTxnNum	UINT32	0-253
100	RepLastRxTxnCRC	UINT32	0-253
101	RepNeedsMember	UINT32	0-253
102	RepMemberName	String	1-253
103	RepMemberIP	IP Address	0-253
104	RepMemberPort	UINT32	0-253
105	RepMemberOrdinal	UINT32	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-11 Tech Mahindra Access Registrar Internal VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
106	RepWorkLoad	UINT32	0-253
107	RepTxTime	UINT32	0-253
108	RepElementPath	String	1-253
109	RepElementValue	String	1-253
110	RepElementOrdinal	UINT32	0-253
111	RepElementCRC	UINT32	0-253
112	RepElementType	UINT32	0-253
113	RepElementMode	UINT32	0-253
114	RepPartialElement	Undefined	0-253

Tech Mahindra VSAs

Table C-12 lists the Tech Mahindra VSAs. The vendor ID for Tech Mahindra VSAs is 9.

Table C-12 Tech Mahindra VSAs

SubAttr	VSA Name	Type	Min-Max Value
1	Techm-AVPair	String	0-253
2	Techm-NAS-Port	String	0-253
3	Techm-Fax-Account-ID-Origin	String	0-253
4	Techm-Fax-Message-ID	String	0-253
5	Techm-Fax-Pages	String	0-253
6	Techm-FAX Cover Page Flag	String	0-253
7	Techm-Fax-Modem-Time	String	0-253
8	Techm-Fax-Connect-Speed	String	0-253
9	Techm-Fax-Recipient-Count	String	0-253
10	Techm-Fax-Process-Abort-Flag	String	0-253
11	Techm-Fax-DSN-Address	String	0-253
12	Techm-Fax-DSN-Flag	String	0-253
13	Techm-Fax-MDN-Address	String	0-253
14	Techm-Fax-MDN-Flag	String	0-253
15	Techm-Fax-Auth-Status	String	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-12 Tech Mahindra VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
16	Techm-Email-Server-Address	IP Address	
17	Techm-Email-Server-ACK Flag	String	0-253
18	Techm-Gateway-ID	String	0-253
19	Techm-Call-Type	String	0-253
20	Techm-Port-Used	String	0-253
21	Techm-Abort-Cause	String	0-253
22	Techm-CRS-Info	String	0-253
12	Techm-h312-Remote-Address	String	0-253
24	Techm-h312-Conf-ID	String	0-253
25	Techm-h312-Setup-Time	String	0-253
26	Techm-h312-Call-Origin	String	0-253
27	Techm-h312-Call-Type	String	0-253
28	Techm-h312-Connect- Time	String	0-253
29	Techm-h312-Disconnect-Time	String	0-253
30	Techm-h312-Disconnect-Cause	String	0-253
31	Techm-h312-Voice-Quality	String	0-253
32	Techm-h312-Generic-IVR-Out	String	0-253
33	Techm-h312-Gateway-ID	String	0-253
34	Techm-3GPP2-AVPair	String	0-253
35	Techm Connection ID-h312-incoming-connection-ID	String	0-253
100	Techm-h312-Generic-IVR-In	String	0-253
101	Techm-h312-Amount-Balance		
102	Techm-h312-Time-Balance	String	0-253
103	Techm-h312-Return-Code	String	0-253
104	Techm-h312-Prompt-ID	String	0-253
105	Techm-h312-Time-of-Day	String	0-253
106	Techm-h312-Redirect-Number	String	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-12 Tech Mahindra VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
107	Techm-h312-Preferred-Language	String	0-253
108	Techm-h312-Redirect-IP-Address	String	0-253
109	Techm-h312-Billing-Model	ENUM: postpaid prepaid	0-1
110	Techm-h312-Currency	String	0-253
128	Techm-UCP-IP-Pool-ID	String	0-253
129	Techm-UCP-User-Max-Sessions	String	0-253
130	Techm-UCP-User-Session-Count	String	0-253
131	Techm-UCP-Next-Session-ID	String	0-253
132	Techm-UCP-VPDN-Max-Sessions	String	0-253
133	Techm-UCP-VPDN-Session-Count	String	0-253
134	Techm-UCP-B-Channel-Max-Sessions	String	0-253
135	Techm-UCP-B-Channel-Session-Coun	String	0-253
136	Techm-UCP-Status	String	0-253
137	Techm-UCP-BLOB-Attribute-Length	String	0-253
138	Techm-UCP-Disable-Statu	String	0-253
139	Techm-UCP-Block-Access-Range	String	0-253
140	Techm-UCP-Home-POP-ID	String	0-253
175	Techm-UCP-IP-Addresses	IP Address	0-253
176	Techm-UCP-Session-Info	String	0-253
211	Techm-Ascend AV pairs	String	0-253
250	Techm-SSG-Account-Info	String	0-253
251	Techm-SSG-Service-Info	String	0-253
252	Techm-SSG-Command-Code	String	0-253
253	Techm-SSG-Control-Info	String	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Compatible VSAs

Table C-13 lists the Compatible VSAs. The vendor ID for Compatible VSAs is 255.

Table C-13 Compatible VSAs

SubAttr	VSA Name	Type	Min-Max Value
0	Compatible-Tunnel-Delay	UNIT32	0-253
1	Compatible-Tunnel-Throughput	UNIT32	0-253
3	Compatible-Tunnel-Server-Endpoint	IP Address	0-253
4	Compatible-Tunnel-Group-Info	String	0-253
5	Compatible-Tunnel-Password	String	0-253
6	Compatible-Echo	UNIT32	0-253
7	Compatible-Tunnel-Client-IPX	UNIT32	0-253

Microsoft VSAs

Table C-14 lists the Microsoft VSAs. The vendor ID for Microsoft VSAs is 311.

Table C-14 Microsoft VSAs

SubAttr	VSA Name	Type	Min-Max Value
1	MS-CHAP-Response	String	50-50
2	MS-CHAP-Error	String	0-253
3	MS-CHAP-CPW1	String	70-70
4	MS-CHAP-CPW2	String	84-84
5	MS-CHAP-LM-Enc-PW	String	4-253
6	MS-CHAP-NT-Enc-PW	String	4-253
7	MS-MPPE-Encryption-Policy	ENUM: Encryption-Allowed Encryption-Required	1-2
8	MS-MPPE-Encryption-Types	String	0-4
9	MS-RAS-Vendor	UINT32	0-253
10	MS-CHAP-Domain	String	0-253
11	MS-CHAP-Challenge	String	0-253
12	MS-CHAP-MPPE-Keys	String	32-32
13	MS-BAP-Usage	ENUM: Not allowed Allowed Required	0-2

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-14 Microsoft VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
14	MS-Link-Utilization-Threshold	UINT32	0-253
15	MS-Link-Drop-Time-Limit	String	0-253
16	MS-MPPE-Send-Key	String	0-253
17	MS-MPPE-Recv-Key	String	0-253
18	MS-RAS-Version	String	0-253
19	MS-Old-ARAP-Password	String	0-253
20	MS-New-ARAP-Password	String	0-253
21	MS-ARAP-Password-Change-Reason	ENUM: Just-Change-Password Expired-Password Admin-Requires-Password-Chang Password-Too-Short	1-4
22	MS-Filter	String	0-253
12	MS-Acct-Auth-Type	ENUM: PAP CHAP MS-CHAP-1 MS-CHAP-2 EAP	1-5
26	MS-CHAP2-Success	String	43-43
27	MS-CHAP2-CPW8	String	68-68
29	MS-Secondary-DNS-Server	IP Address	68-68
31	MS-Secondary-NBNS-Server	IP Address	70-70
33	MS-ARAP-Challenge	String	8-8

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Nomadix VSAs

Table C-15 lists the Nomadix VSAs. The vendor ID for Nomadix VSAs is 3309.

Table C-15 Nomadix VSAs

SubAttr	VSA Name	Type	Min-Max Value
1	Nomadix-Bw-Up 0 253	UINT32	0-253
2	Nomadix-Dw-Down	UINT32	0-253

RedBack VSAs

Table C-16 lists the RedBack VSAs. The vendor ID for RedBack VSAs is 1252.

Table C-16 RedBack VSAs

SubAttr	VSA Name	Type	Min-Max Value
1	RedBack-Client-DNS-Pri	String	0-253
2	RedBack-Client-DNS-Sec	String	0-253
3	RedBack-DHCP-Max-Leases	String	0-253
4	RedBack-Context-Name	String	0-253
5	RedBack-Bridge-Group	String	0-253
6	RedBack-BG-Aging-Time	String	0-253
7	RedBack-BG-Path-Cost	String	0-253
8	RedBack-BG-Span-Dis	String	0-253
9	RedBack-BG-Trans-BPDU	String	0-253
10	RedBack-Rate-Limit-Rate	String	0-253
11	RedBack-Rate-Limit-Burst	String	0-253
12	RedBack-Police-Rate	String	0-253
13	RedBack-Police-Burst	String	0-253
14	RedBack-Source-Validation	String	0-253
15	RedBack-Tunnel-Domain	String	0-253
16	RedBack-Tunnel-Local-Name	String	0-253
17	RedBack-Tunnel-Remote-Name	String	0-253
18	RedBack-Tunnel-Function	String	0-253
21	RedBack-Tunnel-Max-Sessions	String	0-253
22	RedBack-Tunnel-Max-Tunnels	String	0-253
12	RedBack-Tunnel-Session-Auth	String	0-253
24	RedBack-Tunnel-Window	String	0-253
25	RedBack-Tunnel-Retransmit	String	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-16 RedBack VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
26	RedBack-Tunnel-Cmd-Timeout	String	0-253
27	RedBack-PPPOE-URL	String	0-253
28	RedBack-PPPOE-MOTM	String	0-253
29	RedBack-Tunnel-Group	String	0-253
30	RedBack-Tunnel-Context	String	0-253
31	RedBack-Tunnel-Algorithm	String	0-253
32	RedBack-Tunnel-Deadtime	String	0-253
33	RedBack-Mcast-Send	String	0-253
34	RedBack-Mcast-Receive	String	0-253
35	RedBack-Mcast-MaxGroups	String	0-253
36	RedBack-Ip-Address-Pool-Name	String	0-253
37	RedBack-Tunnel-DNIS	String	0-253
38	RedBack-Medium-Type	String	0-253
39	RedBack-PVC-Encapsulation-Type	String	0-253
40	RedBack-PVC-Profile-Name	String	0-253
41	RedBack-PVC-Circuit-Padding	String	0-253
42	RedBack-Bind-Type	String	0-253
43	RedBack-Bind-Auth-Protocol	String	0-253
44	RedBack-Bind-Auth-Max-Sessions	String	0-253
45	RedBack-Bind-Bypass-Bypass	String	0-253
46	RedBack-Bind-Auth-Context	String	0-253
47	RedBack-Bind-Auth-Service-Grp	String	0-253
48	RedBack-Bind-Bypass-Context	String	0-253
49	RedBack-Bind-Int-Context	String	0-253
50	RedBack-Bind-Tun-Context	String	0-253
51	RedBack-Bind-Ses-Context	String	0-253
52	RedBack-Bind-Dot1q-Slot	String	0-253
53	RedBack-Bind-Dot1q-Port	String	0-253
54	RedBack-Bind-Dot1q-Vlan-Tag-Id	String	0-253
55	RedBack-Bind-Int-Interface-Name	String	0-253
56	RedBack-Bind-L2TP-Tunnel-Name	String	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-16 RedBack VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
57	RedBack-Bind-L2TP-Flow-Control	String	0-253
58	RedBack-Bind-Sub-User-At-Context	String	0-253
59	RedBack-Bind-Sub-Password	String	0-253
60	RedBack-Ip-Host-Addr	String	0-253
61	RedBack-IP-TOS-Field	String	0-253
62	RedBack-NAS-Real-Port	String	0-253
63	RedBack-Tunnel-Session-Auth-Ctx	String	0-253
64	RedBack-Tunnel-Session-Auth-Service-Grp	String	0-253
65	RedBack-Tunnel-Rate-Limit-Rate	String	0-253
66	RedBack-Tunnel-Rate-Limit-Burst	String	0-253
67	RedBack-Tunnel-Police-Rate	String	0-253
68	RedBack-Tunnel-Police-Burst	String	0-253
69	RedBack-Tunnel-L2F-Second-Password	String	0-253
128	RedBack-Acct-Input-Octets-64	String	0-253
129	RedBack-Acct-Output-Octets-64	String	0-253
130	RedBack-Acct-Input-Packets-64	String	0-253
131	RedBack-Acct-Output-Packets-64	String	0-253
132	RedBack-Assigned-IP-Address	String	0-253
133	RedBack-Acct-Mcast-In-Octets	String	0-253
134	RedBack-Acct-Mcast-Out-Octets	String	0-253
135	RedBack-Acct-Mcast-In-Packets	String	0-253
136	RedBack-Acct-Mcast-Out-Packets	String	0-253
137	RedBack-LAC-Port	String	0-253
138	RedBack-LAC-Real-Port	String	0-253
139	RedBack-LAC-Port-Type	String	0-253
140	RedBack-LAC-Real-Port-Type	String	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

RedCreek VSAs

Table C-17 lists the RedCreek VSAs. The vendor ID for RedCreek VSAs is 1958.

Table C-17 RedCreek VSAs

SubAttr	VSA Name	Type	Min-Max Value
6	RedCreek-Tunneled-IP-Netmask	IP Address	0-253
7	RedCreek-Tunneled-Gateway	IP Address	0-253
9	RedCreek-Tunneled-WINS-Server1	String	0-253
10	RedCreek-Tunneled-WINS-Server2	String	0-253
11	RedCreek-Tunneled-HostName	String	0-253
12	RedCreek-Tunneled-DomainName	String	0-253
13	RedCreek-Tunneled-Search-List	String	0-253

TACACS+ VSAs

Table C-18 lists the TACACS+ VSAs. The vendor ID for TACACS+ VSAs is 268435456.

Table C-18 TACACS+ VSAs

SubAttr	VSA Name	Type	Min-Max Value
1	Tacacs-Version	ENUM: 192 = 12.0 193 = 12.1	0-255
2	Tacacs-Type	ENUM: 1 = Authentication 2 = Authorization 3 = Accounting	1-3
3	Tacacs-Sequence-Number	UINT32	0-1
4	Tacacs-Session-Id	UINT32	0-2147483647
5	Tacacs-Action	ENUM: 1 = Login 2 = ChPass 3 = SendPass 4 = SendAuth	0-253
6	Tacacs-Privilege-Level	UINT32	0-15
7	Tacacs-Authentication-Type	ENUM: 1 = ASCII 2 = PAP 3 = CHAP 4 = ARAP 5 = MSCHAP	1-5

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-18 TACACS+ VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
8	Tacacs-Service	ENUM: 1 = Login 2 = Enable 3 = PPP 4 = ARAP 5 = PT 6 = RCMD 7 = X25 8 = NASI 9 = FWPROXY	1-9
9	Tacacs-User-Name	String	0-253
10	Tacacs-Port	String	0-253
11	Tacacs-Remote-Address	String	0-253
12	Tacacs-Data	String	0-253
13	Tacacs-User-Message	String	0-253
14	Tacacs-User-Data	String	0-253
15	Tacacs-Authentication-Continue-Flag	ENUM: 0 = Continue 1 = Abort	0-1
16	Tacacs-Authentication-Reply-Flag‘	ENUM: 0 = Echo 1 = NoEcho	0-1
17	Tacacs-Authentication-Reply-Status	ENUM: 1 = Pass 2= Fail 3 = GetData 4 = GetUser 5 = GetPass 6 = Restart 7 = Error 33 = Follow	0-33
18	Tacacs-Authorization-Reply-Status	ENUM: 1 = PassAdd 2 = PassRepl 16 = Fail 17 = Error 33 = Follow	0-33
19	Tacacs-Server-Message	String	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-18 TACACS+ VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
20	Tacacs-Authentication-Method	ENUM: 0 = NotSet 1 = None 2 = KRB5 3 = Line 4 = Enable 5 = Local 6 = TacacsPlus 7 = Guest 16 = Radius 17 = KRB4 32 = RCMD	0-32
21	Tacacs-AVPair	String	0-253
22	Tacacs-Accounting-Reply-Status	ENUM: 1 = Success 2 = Fail 33 = Follow	0-33
12	Tacacs-Header-Flag	ENUM: 0 = Encrypted 1 = Unencrypted 4 = Encrypted + ReuseConnection 5 = Unencrypted + ReuseConnection	0-5
24	Tacacs-User-Password	String	0-253
25	Tacacs-Accounting-Request-Flag	ENUM: 1 = More 2 = Start 3 = Start 4 = Stop 5 = Stop 6 = Start 7 = Start 8 = Update 9 = More 10 = Start 11 = Start 12 = Stop 13 = Stop 14 = Start 15 = Start	0-33
26	Tacacs-CHAP-Password	CHAP_PASSWORD	17-17
27	Tacacs-CHAP-Challenge	String	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-18 TACACS+ VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
28	Tacacs-MSCHAP-Response	String	50-50
29	Tacacs-MSCHAP-Challenge	String	0-253

Telebit VSAs

Table C-19 lists the Telebit VSAs. The vendor ID for Telebit VSAs is 117.

Table C-19 Telebit VSAs

SubAttr	VSA Name	Type	Min-Max Value
1	Telebit-Login-Command	String	0-253
2	Telebit-Port-Name	String	0-253
3	Telebit-Activate-Command	String	0-253
4	Telebit-Accounting-Info	String	0-253
5	Telebit-Login-Option	String	0-253

Unisphere VSAs

Table C-20 lists the Unisphere VSAs. The vendor ID for RedBack VSAs is 4874.

Table C-20 Unisphere VSAs

SubAttr	VSA Name	Type	Min-Max Value
1	Unisphere-Virtual-Router	String	0-253
2	Unisphere-Local-Address-Pool	String	0-253
3	Unisphere-Local-Interface	String	0-253
4	Unisphere-Primary-DNS	String	0-253
5	Unisphere-Secondary-DNS	String	0-253
6	Unisphere-Primary-WINS	String	0-253
7	Unisphere-Secondary-WINS	String	0-253
8	Unisphere-Tunnel-Virtual-Router	String	0-253
9	Unisphere-Tunnel-Password	String	0-253
10	Unisphere-Ingress-Policy-Name	String	0-253
11	Unisphere-Egress-Policy-Name	String	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-20 Unisphere VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
12	Unisphere-Ingress-Statistics	String	0-253
13	Unisphere-Egress-Statistics	String	0-253
14	Unisphere-Service-Category	String	0-253
15	Unisphere-PCR	String	0-253
16	Unisphere-SCR	String	0-253
17	Unisphere-MBS	String	0-253
18	Unisphere-Init-CLI-Access-Level	String	0-253
19	Unisphere-Allow-All-VR-Access	String	0-253
20	Unisphere-Alt-CLI-Access-Level	String	0-253
21	Unisphere-Alt-CLI-VRouter-Name	String	0-253
22	Unisphere-SA-Validate	String	0-253
12	Unisphere-IGMP-enable	String	0-253
24	Unisphere-PPPoE-Description	String	0-253
25	Unisphere-Redirect-VRouter-Name	String	0-253

USR VSAs

Table C-21 lists the USR VSAs. The vendor ID for USR VSAs is 429.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs

SubAttr	VSA Name	Type	Min-Max Value
1	USR-DTE-Data-Idle-Timeout	UINT32	0-0
2	USR-Default-DTE-Data-Rate	ENUM: 110_BPS 300_BPS 600_BPS 1200_BPS 2400_BPS 4800_BPS 7200_BPS 9600_BPS 12K_BPS 14.4K_BPS 16.8_BPS 19.2K_BPS 38.4K_BPS 75_BPS 450_BPS UNKNOWN_BPS 57.6K_BPS 21.6K_BPS 24K_BPS 26K_BPS 28K_BPS 115K_BPS 31K_BPS 33K_BPS 25333_BPS 110_BPS 300_BPS 600_BPS 1200_BPS 2400_BPS 26666_BPS 28000_BPS 29333_BPS 30666_BPS 32000_BPS	1-54

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
2	USR-Default-DTE-Data-Rate	33333_BPS 34666_BPS 36000_BPS 37333_BPS 38666_BPS 40000_BPS 41333_BPS 42666_BPS 44000_BPS 45333_BPS 46666_BPS 48000_BPS 49333_BPS 50666_BPS 52000_BPS 53333_BPS 54666_BPS 56000_BPS 57333_BPS 58666_BPS 60000_BPS 61333_BPS 62666_BPS 64000_BPS	
3	USR-Last-Number-Dialed-Out	String	1-253
4	USR-Sync-Async-Mode	ENUM: Asynchronous Synchronous	1-2
5	USR-Originate-Answer-Mode	ENUM: Originate_in_Originate_Mode Originate_in_Answer_Mode Answer_in_Originate_Mode Answer_in_Answer_Mode	1-4
6	USR-Failure-to-Connect-Reason	ENUM:	1-67

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

7	USR-Initial-Tx-Link-Data-Rate	ENUM: 110_BPS 14.4K_BPS 16.8_BPS 19.2K_BPS 38.4K_BPS 75_BPS 450_BPS UNKNOWN_BPS 57.6K_BPS 21.6K_BPS 24K_BPS 300_BPS 26K_BPS 28K_BPS 115K_BPS 31K_BPS 33K_BPS 25333_BPS 26666_BPS 28000_BPS 29333_BPS 30666_BPS 600_BPS 32000_BPS 33333_BPS 34666_BPS 36000_BPS 37333_BPS 38666_BPS 40000_BPS 41333_BPS 42666_BPS 44000_BPS 1200_BPS 45333_BPS 46666_BPS 48000_BPS 49333_BPS 50666_BPS 52000_BPS 53333_BPS 54666_BPS 56000_BPS 57333_BPS 2400_BPS 58666_BPS 60000_BPS	1-54

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
7	USR-Initial-Tx-Link-Data-Rate (*continued*)	61333_BPS 62666_BPS 64000_BPS 4800_BPS 7200_BPS 9600_BPS 12K_BPS	
8	USR-Final-Tx-Link-Data-Rate	ENUM: 110_BPS 14.4K_BPS 16.8_BPS 19.2K_BPS 38.4K_BPS 75_BPS 450_BPS UNKNOWN_BPS 57.6K_BPS 21.6K_BPS 24K_BPS 300_BPS 26K_BPS 28K_BPS 115K_BPS 31K_BPS 33K_BPS 25333_BPS 26666_BPS 28000_BPS 29333_BPS 30666_BPS 600_BPS	1-54

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
8	USR-Final-Tx-Link-Data-Rate	32000_BPS 33333_BPS 34666_BPS 36000_BPS 37333_BPS 38666_BPS 40000_BPS 41333_BPS 42666_BPS 44000_BPS 1200_BPS 45333_BPS 46666_BPS 48000_BPS 49333_BPS 50666_BPS 52000_BPS 53333_BPS	1-54
8	USR-Final-Tx-Link-Data-Rate	54666_BPS 56000_BPS 57333_BPS 2400_BPS 58666_BPS 60000_BPS 61333_BPS 62666_BPS 64000_BPS 4800_BPS 7200_BPS 9600_BPS	

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
9	USR-Modulation-Type	ENUM: usRoboticsHST bell208b v21FaxClass1 v27FaxClass1 v29FaxClass1 v17FaxClass1 v21FaxClass2 v27FaxClass2 v29FaxClass2 v17FaxClass2 v32Terbo ccittV32 v34 vFC v34plus x2 v110 v120 x75 ayncSyncPPP clearChannel ccittV22bis bell103 ccittV21 bell212 ccittV32bis ccittV12 negotiationFailed	1-28
9	USR-Modulation-Type	ENUM:	
10	USR-Equalization-Type	ENUM: Long Short	1-2
112	USR-Characters-Sent	UINT32	0-0
13	USR-Characters-Received	UINT32	0-0
14	USR-Blocks-Sent	UINT32	0-0
15	USR-Blocks-Received 0	UINT32	0-0
16	USR-Blocks-Resent	UINT32	0-0
17	USR-Retrains-Requested	UINT32	0-0
18	USR-Retrains-Granted	UINT32	
19	USR-Line-Reversals	UINT32	
20	USR-Number-Of-Characters-Lost0	UINT32	0-0

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
21	USR-Back-Channel-Data-Rate	ENUM : 450BPS 300BPS None	1-3
22	USR-Number-of-Blers	UINT32	0-0
12	USR-Number-of-Link-Timeouts	UINT32	0-0
24	USR-Number-of-Fallbacks	UINT32	0-0
25	USR-Number-of-Upshifts	UINT32	0-0
26	USR-Number-of-Link-NAKs	UINT32	0-0
27	USR-Simplified-MNP-Levels	ENUM: Unknown NON_ARQ MNP10ec LAPMAC V42ETC2 V42SREJ PIAFS V120 X75 MNP3 MNP4 V42 HST synchronous MNP2 MNP10(Cellular) V42ETC	0-16

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
28	USR-Connect-Term-Reason	ENUM: dtrDrop retransmitLimit linkDisconnectMsgReceived noLoopCurrent invalidSpeed unableToRetrain managementCommand noDialTone keyAbort lineBusy noAnswer escapeSequence voice noAnswerTone noCarrier undetermined v42SabmeTimeout v42BreakTimeout v42DisconnectCmd v42IdExchangeFail v42BadSetup v42InvalidCodeWord athCommand v42StringToLong v42InvalidCommand none v32Cleardown dialSecurity	1-67

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
28	USR-Connect-Term-Reason	remoteAccessDenied loopLoss ds0Teardown promptNotEnabled noPromptingInSync carrierLoss nonArqMode modeIncompatible noPromptInNonARQ dialBackLink linkAbort autopassFailed pbGenericError pbLinkErrTxPreAck pbLinkErrTxTardyACK pbTransmitBusTimeout inactivityTimout pbReceiveBusTimeout pbLinkErrTxTAL pbLinkErrRxTAL pbTransmitMasterTimeout pbClockMissing pbReceivedLsWhileLinkUp pbOutOfSequenceFrame pbBadFrame pbAckWaitTimeout pbReceivedAckSeqErr mnpIncompatible pbReceiveOvrflwRNRFail pbReceiveMsgBufOvrflw rcvdGatewayDiscCmd tokenPassingTimeout dspInterruptTimeout mnpProtocolViolation	
28	USR-Connect-Term-Reason	class2FaxHangupCmd hstSpeedSwitchTimeout undefined remotePassword linkPassword	
29	USR-DTR-False-Timeout	UINT32	0-0
30	USR-Fallback-Limit	UINT32	0-0
31	USR-Block-Error-Count-Limit	UINT32	0-0
32	USR-Simplified-V42bis-Usage	ENUM: None ccittV42bis mnpLevel5	1-3

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
33	USR-DTR-True-Timeou	UINT32	0-0
34	USR-Last-Number-Dialed-In-DNIS	String	1-253
35	USR-Last-Callers-Number-ANI	String	1-253
36	USR-Mbi-Ct-PRI-Card-Slot	UINT32	0-0
37	USR-Mbi-Ct-TDM-Time-Slot	UINT32	0-0
38	USR-Mbi-Ct-PRI-Card-Span-Line	UINT32	0-0
39	USR-Mbi-Ct-BChannel-Used	UINT32	0-0
40	USR-IP-Input-Filter	String	1-253
41	USR-IPX-Input-Filter	String	1-253
42	USR-IP-Output-Filter	String	1-253
43	USR-IPX-Output-Filter	String	1-253
44	USR-SAP-Output-Filter	String	1-253
45	USR-VPN-ID	UINT32	0-0
46	USR-VPN-Name	String	1-253
47	USR-VPN-Neighbor	String	1-253
48	USR-Framed-Routing-V2	ENUM: RIP-V2-Off RIP-V2-On	1-2
49	USR-VPN-Gateway	String	1-253
50	USR-Tunnel-Authenticato	String	1-253
51	USR-Packet-Index	String	1-253
52	USR-Cutoff	String	1-253
53	USR-Access-Accept-Packet	String	1-253
54	USR-Primary-DNS-Server	String	1-253
55	USR-Secondary-DNS-Server	String	1-253
56	USR-Primary-NBNS-Server	String	1-253
57	USR-Secondary-NBNS-Server	String	1-253
58	USR-Syslog-Tap	UINT32	0-0
59	USR-Chassis-Call-Slot	UINT32	0-0
60	USR-Chassis-Call-Span	UINT32	0-0
61	-Chassis-Call-Channel	UINT32	0-0
62	USR-Keypress-Timeout	UINT32	0-0
63	USR-Unauthenticated-Time	UINT32	0-0
64	USR-Bearer-Capabilities	UINT32	0-0

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
65	USR-Speed-Of-Connection	UINT32	0-0
66	USR-Max-Channels	UINT32	0-0
67	USR-Channel-Expansion	UINT32	0-0
68	USR-Channel-Decrement	UINT32	0-0
69	USR-Expansion-Algorithm	UINT32	0-0
70	USR-Compression-Algorithm	UINT32	0-0
71	USR-Receive-Acc-Map	UINT32	0-0
72	USR-Transmit-Acc-Map	UINT32	0-0
73	USR-Compression-Reset-Mode	UINT32	0-0
74	USR-Min-Compression-Size	UINT32	0-0
75	USR-IP	UINT32	0-0
76	USR-IPX	UINT32	0-0
77	USR-Filter-Zones	UINT32	0-0
78	USR-Appletalk	UINT32	0-0
79	USR-Bridging	UINT32	0-0
80	USR-Spoofing	UINT32	0-0
81	USR-Host-Type	String	1-253
82	USR-Send-Name	UINT32	0-0
83	USR-Send-Password	String	1-253
84	USR-Start-Time	UINT32	0-0
85	USR-End-Time	UINT32	0-0
86	USR-Send-Script1	String	1-253
87	USR-Reply-Script1	String	1-253
88	USR-Send-Script2	String	1-253
89	USR-Reply-Script2	String	1-253
90	USR-Send-Script3	String	1-253
91	USR-Send-Script3 USR-Reply-Script3	String	1-253
92	USR-Send-Script4	String	1-253
93	USR-Reply-Script4	String	1-253
94	USR-Send-Script5	String	1-253
95	USR-Reply-Script5	String	1-253
96	USR-Send-Script6	String	1-253
97	USR-Reply-Script6	String	1-253
98	USR-Terminal-Type	String	1-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
99	USR-Appletalk-Network-Range	UINT32	0-0
100	USR-Local-IP-Address	String	1-253
101	USR-Routing-Protocol	UINT32	0-0
102	USR-Modem-Group	UINT32	0-0
103	USR-IPX-Routing	UINT32	0-0
104	USR-IPX-Wan	UINT32	0-0
105	USR-IP-RIP-Policies	UINT32	0-0
106	USR-IP-RIP-Simple-Auth-Password	String	0-253
107	USR-IDS0-Call-Type	UINT32	0-0
108	USR-Call-Terminate-in-GMT	UINT32	0-0
109	USR-Call-Connect-in-GMT	UINT32	0-0
110	USR-Call-Arrival-in-GMT	UINT32	0-0
111	USR-Channel-Connected-To	UINT32	0-0
112	USR-Slot-Connected-To	UINT32	0-0
113	USR-Device-Connected-To	ENUM: None isdnGateway quadModem	1-3
114	USR-NFAS-ID	UINT32	0-0
115	USR-Q931-Call-Reference-Value	UINT32	0-0

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
116	USR-Call-Event-Code	ENUM: notSupported noFreeIGW igwRejectCall igwSetupTimeout noFreeTdmts bcReject ieReject chidReject progReject callingPartyReject calledPartyReject setup blocked analogBlocked digitalBlocked outOfService busy congestion protocolError noFreeBchannel inOutCallCollision usrSetup telcoDisconnect usrDisconnect noFreeModem modemsNotAllowed modemsRejectCall modemSetupTimeout	1-28
117	USR-DS0	UINT32	0-0
118	USR-DS0s	String	1-253
119	USR-Gateway-IP-Address	IP Address	0-0
120	USR-Physical-State	UINT32	0-0
121	USR-Chassis-Temp-Threshold	UINT32	0-0

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
122	USR-Card-Type	ENUM: SlotEmpty QuadV32DigitalModemNAC DualT1NIC DualAlogMdmNIC QuadDgtlMdmNIC QuadAlogDgtlMdmNIC TokenRingNIC SingleT1NIC EthernetNIC ShortHaulDualT1NIC DualAlogMgdIntlMdmNIC X25NIC	
122	USR-Card-Type (continued)	ENUM: QuadAlogNonMgdMdmNIC QuadAlogMgdIntlMdmNIC QuadAlogNonMgdIntlMdmNIC QuadLsdLiMgdMdmNIC QuadLsdLiNonMgdMdmNIC QuadLsdLiMgdIntlMdmNIC QuadLsdLiNonMgdIntlMdmNIC EthernetWithV35NIC HSEthernetWithoutV35NIC DualHighSpeedV35NIC QuadV35RS122LowSpeedNIC DualE1NIC ShortHaulDualE1NIC BellcoreLongHaulDualT1NIC BellcoreShrtHaulDualT1NIC SCSIEdgeServerNIC QuadV32AnalogModemNAC QuadV32DigAnlModemNAC QuadV34DigModemNAC QuadV34AnlModemNAC QuadV34DigAnlModemNAC SingleT1NAC EthernetGatewayNAC AccessServer 486TrGatewayNAC SlotUnknown	

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
122	USR-Card-Type *(continued)*	ENUM: 486EthernetGatewayNAC DualRS122NAC 486X25GatewayNAC ApplicationServerNAC ISDNGatewayNAC ISDNpriT1NAC ClkedNetMgtCard ModemPoolManagementNAC NetwMgtCard ModemPoolNetserverNAC (continued)	1-1027
122	USR-Card-Type *(continued)*	ModemPoolV34ModemNAC ModemPoolISDNNAC NTServerNAC QuadV34DigitalG2NAC QuadV34AnalogG2NAC QuadV34DigAnlgG2NAC NETServerFrameRelayNAC NETServerTokenRingNAC X2524ChannelNAC DualT1NAC WirelessGatewayNac EnhancedAccessServer EnhancedISDNGatewayNAC DualModemNAC QuadModemNAC TrGatewayNAC X25GatewayNAC DualV34ModemNAC	
112	USR-Security-Login-Limit	UINT32	0-0
124	USR-Security-Resp-Limit	UINT32	0-0
125	USR-Packet-Bus-Session	UINT32	0-0
126	USR-DTE-Ring-No-Answer-Limit	UINT32	0-0

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
127	USR-Final-Rx-Link-Data-Rate	ENUM: 110_BPS 14.4K_BPS 16.8_BPS 19.2K_BPS 38.4K_BPS 75_BPS 450_BPS UNKNOWN_BPS 57.6K_BPS 21.6K_BPS 24K_BPS 300_BPS 6K_BPS 28K_BPS 115K_BPS 31K_BPS 33K_BPS 25333_BPS 26666_BPS 28000_BPS 62666_BPS 9333_BPS 30666_BPS 600_BPS (continued)	1-54

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
127	USR-Final-Rx-Link-Data-Rate (continued)	32000_BPS 33333_BPS 34666_BPS 36000_BPS 37333_BPS 38666_BPS 40000_BPS 41333_BPS 42666_BPS 44000_BPS 1200_BPS 45333_BPS 46666_BPS 48000_BPS 49333_BPS 50666_BPS 52000_BPS 53333_BPS 54666_BPS 56000_BPS 57333_BPS 2400_BPS 58666_BPS 60000_BPS 61333_BPS 64000_BPS 800_BPS 7200_BPS 9600_BPS 12K_BPS	

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
128	USR-Initial-Rx-Link-Data-Rate	ENUM: 110_BPS 14.4K_BPS 16.8_BPS 19.2K_BPS 38.4K_BPS 75_BPS 450_BPS UNKNOWN_BPS 57.6K_BPS 21.6K_BPS 24K_BPS 300_BPS 26K_BPS 28K_BPS 115K_BPS 31K_BPS 33K_BPS 25333_BPS 26666_BPS	1-54
128	USR-Initial-Rx-Link-Data-Rate	28000_BPS 29333_BPS 30666_BPS 600_BPS 32000_BPS 33333_BPS 34666_BPS 36000_BPS 37333_BPS 38666_BPS 40000_BPS 41333_BPS 42666_BPS 44000_BPS 1200_BPS 45333_BPS 46666_BPS 48000_BPS 49333_BPS 50666_BPS 52000_BPS 53333_BPS	

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
128	USR-Initial-Rx-Link-Data-Rate	54666_BPS 56000_BPS 57333_BPS 2400_XBPS 58666_BPS 60000_BPS 61333_BPS 62666_BPS 64000_BPS 4800_BPS 7200_BPS 9600_BPS 12K_BPS	
129	USR-Event-Date-Time	UINT32	0-0
130	USR-Chassis-Temperature	UINT32	0-0
131	USR-Actual-Voltage	UINT32	0-0
132	USR-Expected-Voltage	UINT32	0-0
133	USR-Power-Supply-Number	UINT32	0-0
134	USR-Channel	UINT32	0-0
135	USR-Chassis-Slot	UINT32	0-0

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value

136	USR-Event-Id	ENUM: HUB_Temp_Out_of_Range Fan_Failed Watchdog_Timeout Mgmt_Bus_Failure In_Connection_Est Out_Connection_Est In_Connection_Term Out_Connection_Term Connection_Failed Connection_Timeout DTE_Transmit_Idle DTR_True DTR_False Block_Error_at_Threshold Fallbacks_at_Threshold No_Dial_Tone_Detected No_Loop_Current_Detected Yellow_Alarm Red_Alarm Loss_Of_Signal Rcv_Alrm_Ind_Signal Timing_Source_Switch Modem_Reset_by_DTE Modem_Ring_No_Answer DTE_Ring_No_Answer Pkt_Bus_Session_Active Pkt_Bus_Session_Congestion Pkt_Bus_Session_Lost Pkt_Bus_Session_Inactive User_Interface_Reset Gateway_Port_Out_of_Service Gateway_Port_Link_Active Dial_Out_Login_Failure Dial_In_Login_Failure Dial_Out_Restricted_Number Dial_Back_Restricted_Number User_Blacklisted Attempted_Login_Blacklisted Response_Attempt_Limit_Exceed Login_Attempt_Limit_Exceeded Dial_Out_Call_Duration Dial_In_Call_Duration Pkt_Bus_Session_Err_Status NMC_AutoRespnse_Trap (*Continued*)	

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
136	USR-Event-Id (*Continued*)	Acct_Server_Contact_Loss Yellow_Alarm_Clear Red_Alarm_Clear Loss_Of_Signal_Clear Rcv_Alrm_Ind_Signal_Clear Incoming_Connection_Establish Module_Inserted Outgoing_Connection_Establish Incoming_Connection_Terminate Outgoing_Connection_Terminate Connection_Attempt_Failure Continuous_CRC_Alarm Continuous_CRC_Alarm_Clear Physical_State_Change Module_Removed Gateway_Network_Failed Gateway_Network_Restored Packet_Bus_Clock_Lost Packet_Bus_Clock_Restored D_Channel_In_Service D_Channel_Out_of_Service DS0s_In_Service DS0s_Out_of_Service T1/T1PRI/E1PRI_Call_Event PSU_Voltage_Alarm Psu_Incompatible T1,T1-E1/PRI-Call-Arrive-Even T1,T1-E1/PRI-Call-Connect-Ev e T1,T1-E1/PRI-Call-Termina-Ev e T1,T1-E1/PRI-Call-Failed-Even	6-84
137	USR-Number-of-Rings-Limit	UINT32	0-0
138	USR-Connect-Time-Limit	UINT32	0-0
139	USR-Call-End-Date-Time	UINT32	0-0
140	USR-Call-Start-Date-Time	UINT32	0-0
141	USR-Server-Time	UINT32	0-0

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
142	USR-Request-Type	ENUM: Access-Request Access-Challenge Status-Server Status-Client Access-Accept Reserved Access-Reject Accounting-Request Accounting-Response Access-Password-Change Access-Password-Ack Access-Password-Reject	1-255
143	USR-Old-Password	String	0-253
144	USR-Expiration	UINT32	0-0
145	USR-Prompt	UINT32	0-1
146	USR-Char-Noecho	UINT32	0-0
147	USR-User-Group-Name	String	0-253
148	148 USR-Call-Reference-Number	UINT32	0-253
149	USR-Dial-In-Sec-Mode	UNIT32	0-0
150	USR-Req-Db-Mdm-Sel	UINT32	0-0
151	USR-Req-Db-Login-Valid	UINT32	0-0
152	USR-Dialback-Group-Names	String	0-253
153	USR-Dial-In-Call-Rest	String	0-253
154	USR-Dial-Out-Call-Rest	String	0-253
155	USR-Logins-Before-Blacklist	UINT32	0-0
156	USR-Failed-Logins	UINT32	0-0
157	USR-Allowed-DB-Modems	String	0-253
158	USR-VPN-Encrypter	String	0-253
159	USR-Acct-VPN-Gateway	String	0-253
160	USR-Re-CHAP-Timeout	UINT32	0-0
161	USR-RMMIE-Manufacutere-ID	String	0-253
162	USR-RMMIE-Product-Code	String	0-253
163	USR-RMMIE-Serial-Number	String	0-253
164	USR-RMMIE-Firmware-Version	String	0-253
165	USR-RMMIE-Firmware-Build-Date	String	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
166	USR-RMMIE-Status	ENUM: notEnabledInLocalModem notDetectedInRemoteModem ok	1-3
170	USR-RMMIE-Last-Update-Time	UINT32	0-253
171	USR-RMMIE-Last-Update-Event	ENUM: None initialConnection retrain speedShift plannedDisconnect	1-5
172	USR-RMMIE-Rcv-Tot-PwrLvl	UNIT32	0-253
173	USR-RMMIE-Rcv-PwrLvl-3300Hz	UNIT32	0-253
174	USR-RMMIE-Rcv-PwrLvl-3750Hz	UNIT32	0-253
175	USR-RMMIE-PwrLvl-NearEcho-Canc	UNIT32	0-253
176	USR-RMMIE-PwrLvl-FarEcho-Canc	UNIT32	0-253
177	USR-RMMIE-PwrLvl-Noise-Lvl	UNIT32	0-253
178	USR-RMMIE-PwrLvl-Xmit-Lvl	UNIT32	0-253
179	USR-IPX-SAP	String	0-253
180	USR-MIC	UNIT32	0-253
181	USR-Call-Tracking-ID	UNIT32	0-253
182	USR-Log-Filter-Packet	UNIT32	0-253
183	USR-CCP-Algorithm	UNIT32	0-253
184	USR-ACCM-Type	UNIT32	0-253
185	USR-Connect-Speed	UNIT32	0-253
186	USR-Framed-IP-Address-Pool-Name	UNIT32	0-253
187	USR-MP-EDO	String	0-253
188	USR-Local-Framed-IP-Addr	UNIT32	0-253
189	USR-IP-RIP-Input-Filter	String	0-253
190	USR-IP-Call-Input-Filter	String	0-253
191	USR-IPX-Call-Input-Filter	String	0-253
192	USR-AT-Input-Filter	String	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table C-21 USR VSAs (continued)

SubAttr	VSA Name	Type	Min-Max Value
193	USR-AT-RTMP-Input-Filter	String	0-253
194	USR-AT-Zip-Input-Filter	String	0-253
195	USR-AT-Call-Input-Filter	String	0-253
196	USR-ET-Bridge-Input-Filter	String	0-253
197	USR-IP-RIP-Output-Filter	String	0-253
198	USR-IP-Call-Output-Filter	String	0-253
199	USR-IPX-RIP-Output-Filter	String	0-253
200	USR-IPX-Call-Output-Filter	String	0-253
201	USR-AT-Output-Filter	String	0-253
202	USR-ET-RTMP-Output-Filter	String	0-253
203	USR-AT-Zip-Output-Filter	String	0-253
204	USR-AT-Call-Output-Filter	String	0-253
205	USR-ET-Bridge-Output-Filter	String	0-253
206	USR-ET-Bridge-Call-Output-Filter	String	0-253
207	USR-IP-Default-Route-Option	UINT32	0-253
208	USR-MP-EDO-HIPER	String	0-253
209	USR-MP-MRRU	UINT32	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

WiMax

Table C-22 lists the WiMax VSAs. The vendor ID for WiMax VSAs is 24757.

Table C-22 WiMax VSAs

SubAttr	VSA Name	Type	Min-Max Value
1	HA-IP-MIP4	IPAddress	0-253
2	HA-IP-MIP6	IPAddress	0-253
3	GMT-Time-Zone-Offet	String	0-253
4	NAP-ID	String	0-253
5	NSP-ID	String	0-253
6	Hotline-Indicator	String	0-253
7	BS-ID	String	0-253

WISPr

Table C-23 lists the WISPr VSAs. The vendor ID for WISPr VSAs is 14122.

Table C-23 WISPr VSAs

SubAttr	VSA Name	Type	Min-Max Value
1	WISPr-Location-ID	String	0-65535
2	WISPr-Location-Name	String	0-253
3	WISPr-Logoff-URL	String	0-253
4	WISPr-Redirection-URL	String	0-253
5	WISPr-Bandwidth-Min-Up	UINT32	0-65535
6	WISPr-Bandwidth-Min-Down	UINT32	0-65535
7	WISPr-Bandwidth-Max-Up	UINT32	0-65535
8	WISPr-Bandwidth-Max-Down	UINT32	0-65535
9	WISPr-Session-Terminate-Time	UINT32	0-65535
10	WISPr-Session-Terminate-End-Of-Day	UINT32	0-65535
11	WISPr-Billing-Class-Of-Service	String	0-253

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

XML

Table C-24 lists the XML VSAs, attributes for XML tags. The vendor ID for XML VSAs is 5842.

Table C-24 XML VSAs

SubAttr	VSA Name	Type	Min-Max Value
1	XML-Address-format-IPv4	IPADDR	0-253
2	XML-Association	String	0-253
3	XML-Request	String	0-253
4	XML-Response	String	0-253
5	XML-UserId-id_type-subscriber_id	String	0-253
6	XML-UserIdRequest	String	0-253

Configuring Unique TAG number for Vendor-Specific Sub Attributes

Tech Mahindra Access Registrar allows you to configure a unique tag number for each of the multiple vendor-specific sub-attributes available for a user profile. This enhancement is applicable for multi-tag valued vendor-specific attributes with type as TAG_STRING and TAG_INT.

A sample configuration is shown below:

```
[ //localhost/Radius/Profiles/base-avp/Attributes ]
    unisphere-activate = HQOS-RES
    unisphere-activate-2 = DHCP-IPOE-DATA-PROFILE
    unisphere-activate-3 = DHCP-IPOE-VIDEO-PROFILE

[ //localhost/Radius/UserLists/Default/jane ]
    Name = jane
    Description =
    Password = <encrypted>
    Enabled = TRUE
    Group~ = Telnet-users
    BaseProfile~ = base-avp
    AuthenticationScript~ =
    AuthorizationScript~ =
    UserDefined1 =
    AllowNullPassword = FALSE
    Attributes/
    CheckItems/
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Appendix D

Support for REST API in Tech Mahindra Access Registrar

This appendix provides information about the REpresentational State Transfer (REST) APIs supported in Tech Mahindra Access Registrar. The purpose of this appendix is to provide a developer, system or network administrator, or system integrator with basic guidelines for using the outlined REST APIs within the Tech Mahindra Access Registrar deployment.

This chapter contains the following sections:

- REST API Framework
- CSRF Token Implementation using REST

REST API Framework

REST is a resource-based architectural style to create web services. A resource is an object, which could be a user, address, and so on. Each resource is identified by a Unique Resource Identifier (URI) and is manipulated by representations that pass back and forth between client and server. Representations can be in the form of XML, JSON, Plain, TEXT, or HTML. However, Tech Mahindra Access Registrar supports only the JSON format.

Table D-1 lists the common operations supported in Tech Mahindra Access Registrar for REST APIs.

Table D-1 Common Operations Used in REST APIs

Method	Crud Operation
ADD	Create a resource
GET	Read and retrieve a representation of a resource
EDIT	Update an existing representation
DELETE	Delete a resource

This topic contains the following sections:

- REST API Services
- CoA and PoD REST APIs
- REST API Support for Query and Release Sessions
- Support for RADIUS to JSON and JSON to RADIUS Translation

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

REST API Services

You can use any client for creating the APIs and must pass the following information as inputs for the APIs:

- Content-Type—application/json
- username—username to access the service
- password—password to access the service

Table D-1 lists the REST APIs used in Tech Mahindra Access Registrar.

Table D-2 REST API Services

Object -> Type ID	ADD	EDIT	GET	DELETE

Script -> 1	`http://<hostname>:8080/RESTAPI/service/addobject`
	
	Pass the object and the object name as data.
	
	Example:
	
	`{"Script":{"Name":"test,..}}`
		`http://<hostname>:8080/RESTAPI/service/editobject?typeid=1&name=<object name>`	`http://<hosktname>:8080/RESTAPI/service/getobject?typeid=1&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/deleteobject?typeid=1&name=<object name>`

Client -> 2	`http://<hostname>:8080/RESTAPI/service/addobject` Pass the object and the object name as data.	`http://<hostname>:8080/RESTAPI/service/editobject?typeid=2&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/getobject?typeid=2&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/deleteobject?typeid=2&name=<object name>`
Service -> 3	`http://<hostname>:8080/RESTAPI/service/addobject` Pass the object and the object name as data.	`http://<hostname>:8080/RESTAPI/service/editobject?typeid=3name=<object name>`	`http://<hostname>:8080/RESTAPI/service/getobject?typeid=3&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/deleteobject?typeid=3&name=<object name>`
Policy -> 4	`http://<hostname>:8080/RESTAPI/service/addobject` Pass the object and the object name as data.	`http://<hostname>:8080/RESTAPI/service/editobject?typeid=4&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/getobject?typeid=4&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/deleteobject?typeid=4&name=<object name>`
ResourceManager -> 5	`http://<hostname>:8080/RESTAPI/service/addobject` Pass the object and the object name as data.	`http://<hostname>:8080/RESTAPI/service/editobject?typeid=5&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/getobject?typeid=5&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/deleteobject?typeid=5&name=<object name>`

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table D-2 REST API Services (continued)

Object -> Type ID	ADD	EDIT	GET	DELETE
Administrator -> 6	`http://<hostname>:8080/RESTAPI/service/addobject` Pass the object and the object name as data.	`http://<hostname>:8080/RESTAPI/service/editobject?typeid=6&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/getobject?typeid=6&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/deleteobject?typeid=6&name=<object name>`
RemoteServer -> 7	`http://<hostname>:8080/RESTAPI/service/addobject` Pass the object and the object name as data.	`http://<hostname>:8080/RESTAPI/service/editobject?typeid=7&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/getobject?typeid=7&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/deleteobject?typeid=7&name=<object name>`
UserGroup -> 8	`http://<hostname>:8080/RESTAPI/service/addobject` Pass the object and the object name as data.	`http://<hostname>:8080/RESTAPI/service/editobject?typeid=8&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/getobject?typeid=8&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/deleteobject?typeid=8&name=<object name>`
Profile -> 9	`http://<hostname>:8080/RESTAPI/service/addobject` Pass the object and the object name as data.	`http://<hostname>:8080/RESTAPI/service/editobject?typeid=9&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/getobject?typeid=9&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/deleteobject?typeid=9&name=<object name>`
Replication -> 10	`http://<hostname>:8080/RESTAPI/service/addobject` Pass the object and the object name as data.	`http://<hostname>:8080/RESTAPI/service/editobject?typeid=10&name=<name of Repmember>`	`http://<hostname>:8080/RESTAPI/service/getobject?typeid=10&name=<name of Repmember>`	`http://<hostname>:8080/RESTAPI/service/deleteobject?typeid=10&name=Replication/Rep+Members/<name of Repmember>`
Rule -> 11	`http://<hostname>:8080/RESTAPI/service/addobject` Pass the object and the object name as data.	`http://<hostname>:8080/RESTAPI/service/editobject?typeid=11&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/getobject?typeid=11&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/deleteobject?typeid=11&name=<object name>`
SessionManager -> 12	`http://<hostname>:8080/RESTAPI/service/addobject` Pass the object and the object name as data.	`http://<hostname>:8080/RESTAPI/service/editobject?typeid=12&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/getobject?typeid=12&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/deleteobject?typeid=12&name=<object name>`

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table D-2 REST API Services (continued)

Object -> Type ID	ADD	EDIT	GET	DELETE
Snmp -> 13	`http://<hostname>:8080/RESTAPI/service/addobject` Pass the object and the object name as data.	—	—	—
RemoteODBCSession Server -> 14	`http://<hostname>:8080/RESTAPI/service/addobject` Pass the object and the object name as data.	—	—	—
UserList -> 16	`http://<hostname>:8080/RESTAPI/service/addobject` Pass the object and the object name as data.	`http://<hostname>:8080/RESTAPI/service/editobject?typeid=16&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/getobject?typeid=16&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/deleteobject?typeid=16&name=<object name>`
EncryptedIMSI-PrivateKeys -> 18	`http://<hostname>:8080/RESTAPI/service/addobject`	`http://<hostname>:8080/RESTAPI/service/editobject?typeid=18&name=<name of key>`	`http://<hostname>:8080/RESTAPI/service/getobject?typeid=18&name=<name of key>`	`http://<hostname>:8080/RESTAPI/service/deleteobject?typeid=18&name=EncryptedIMSI-PrivateKeys/keys/<name of key>`
ODBCDataSource -> 44	`http://<hostname>:8080/RESTAPI/service/addobject` Pass the object and the object name as data.	`http://<hostname>:8080/RESTAPI/service/editobject?typeid=44&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/getobject?typeid=44&name=<object name>`	`http://<hostname>:8080/RESTAPI/service/deleteobject?typeid=44&name=<object name>`

Table D-3 provides a list of other REST APIs used in Tech Mahindra Access Registrar.

Table D-3 Other APIs used in Tech Mahindra Access Registrar

Operation	URL
Tacacs Statistics	http://<hostname>:8080/RESTAPI/service/Tacacsstatistics
Diameterstatistics	http://<hostname>:8080/RESTAPI/service/Diameterstatistics
Statistics	http://<hostname>:8080/RESTAPI/service/Statistics
RemoteServerStats	http://<hostname>:8080/RESTAPI/service/RemoteServerStats
DiameterPeerStats	http://<hostname>:8080/RESTAPI/service/DiameterPeerStats
DiaRemoteServerStats	http://<hostname>:8080/RESTAPI/service/DiaRemoteServerStats
ClientStats	http://<hostname>:8080/RESTAPI/service/ClientStats

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table D-3 Other APIs used in Tech Mahindra Access Registrar (continued)

Operation	URL
Reload	http://<hostname>:8080/RESTAPI/service/Reload
AddUser	http://<hostname>:8080/RESTAPI/service/adduser?UserListName=<nameofUsernameList>
GetUser	http://<hostname>:8080/RESTAPI/service/getuser?name=<nameof user>&UserListName=<nameofuserlist>
EditUser	http://<hostname>:8080/RESTAPI/service/edituser?name=< nameof user >&UserListName=<nameofuserlist>
DeleteUser	http://<hostname>:8080/RESTAPI/service/deleteuser?name=< nameof user>&UserListName=<nameofuserlist>

Example for adding a user using REST interface:

```
curl http://hostname:8080/RESTAPI/service/adduser?UserListName=new -H "Content-Type:
application/json" -H "Authorization: Basic YWRtaW46YWljdXNlcg==" --data
"{\"User\":{\"Name\":\"TestUser\",\"Description\":\"\",\"Password\":\"testuser\",\"Enabled
\"=\"TRUE\",\"AllowNullPassword\":\"FALSE\",\"Attributes\":{\"User-Name\":\"joe\",\"Nas-Po
rt\":\"3\"}}"
```

Always the JSON input must start with name of the objects while editing sub objects. A sample is given below:

```
curl -k -X PUT -H "Authorization: Basic YWRtaW46YWljdXNlcg==" -H "Content-Type:
application/json" 'https://<hostname>:8443/RESTAPI/service/editobject?typeid=18&name=key1' -
data
"{\"AllowedKeyIdentifiers\":\"hello\",\"keys\":[{\"Name\":\"key1\",\"identifier\":\"100\",
\"PrivateKey\":\"test456\"}]}"
```

Note REST interface can also be accessed using HTTPS through the 8443 port.

CoA and PoD REST APIs

The Change of Authorization (CoA) and Packet of Disconnect (PoD) API calls allow you to send session reauthentication and session disconnect commands for a specified session.

You can use any client for creating the APIs and must pass the following information as inputs for the APIs:

- URL—URL to access the PoD/CoA service. Example:
  - For PoD—http://<hostname>:8080/RESTAPI/service/PoD
  - For CoA—http://<hostname>:8080/RESTAPI/service/CoA
- Content-Type—application/json
- username—username to access the service
- password—password to access the service
- data—API body with syntax as listed in Table D-4

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Examples

The following example shows a sample PoD API written using cURL client:

```
http://ar-lnx-vm054:8080/RESTAPI/service/PoD -H "Content-Type: application/json" -H
"username:admin -H "password:aicuser --data
"{"parameter":"S21","value":"","type":"with-id"}"
```

Tech Mahindra Access Registrar supports basic authentication with Base64 encoding support for username and password.

A sample header on encryption is provided in the example below:

```
-H "Authorization: Basic YWRtaW46YWljdXNlcg=="
```

The following example shows a sample CoA API:

```
curl http://10.197.95.187:8080/RESTAPI/service/CoA -H "Authorization: Basic
YWRtaW46YWljdXNlcg==" -H "Content-Type: alication/json" --data
"{\"parameter\":\"bob\",\"value\":\"\",\"type\":\"with-user\"}"
```

Note REST interface can also be accessed using HTTPS through the 8443 port.

We can also send CoA using **with-profile** option along with the existing parameters using REST API.

The parameters supported for REST API for CoA with-profile option are: **with-id**, **with-user**, **with-key**, **with-nas**, **with-ip-address**, **with-ipx-network**, **with-age**, **with-usr-vpn**, **with-attribute**, **with-Home-Agent**, and **with-IP-Subnet**.

Example:

```
curl 'http://10.197.95.162:8080/RESTAPI/service/CoA' -H "Authorization: Basic
YWRtaW46YWljdXNlcg==" -H "Content-Type: application/json" --data
"{\"parameter\":\"bob1\",\"value\":\"bob1\",\"type\":\"with-user\",\"profileType\":\"with-
profile\",\"profileValue\":\"cap\"}"
```

Table D-4 Parameter and Data Syntax for APIs

Parameter	Data Syntax/Example
with-profile	"{"profileType":"with-profile","profileValue":"cap"}"
with-id	"{"parameter":"S21","value":"","type":"with-id"}"
with-user	"{"parameter":"bob","value":"","type":"with-user"}"
with-key	"{"parameter":"bob","value":"","type":"with-key"}"
with-nas	"{"parameter":"localhost","value":"","type":"with-nas"}"
with-ip-address	"{"parameter":"192.168.0.4","value":"","type”:”with-ip-address"}"
with-ipx-network	"{"parameter":"0x6","value":"","type":"with-ipx-network"}"
with-age	"{"parameter":"1S","value":"","type":"with-age"}"
with-usr-vpn	"{"parameter":"1","value":"","type":"with-usr-vpn"}"
with-attribute	"{"parameter":"Framed-IP-Address","value":"192.168.0.1","type":"with-attrib ute"}"
with-Home-Agent	"{"parameter":"","value":"","type":"with-Home-Agent"}"
with-IP-Subnet	"{"parameter":"","value":"","type":" with-IP-Subnet "}"

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Tech Mahindra Access Registrar supports **send-CoA** using CLI interface as well. For configuring **send-CoA** using CLI, see the "query-sessions" section in the "Setting the Tech Mahindra Access Registrar Configurable Option" chapter of the *Tech Mahindra Access Registrar 9.3 Administrator Guide*.

REST API Support for Query and Release Sessions

The REST interface allows you to perform the following:

- Query the server about the currently active user sessions
- Release the currently active user sessions

You can request information about those sessions that match a specified filter type, which could be one of the following:

- with-id
- with-user
- with-key
- with-nas
- with-ip-address
- with-ipx-network
- with-age
- with-usr-vpn
- with-attribute
- with-Home-Agent
- with-IP-Subnet

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table D-5 lists the details of REST APIs for query and release session services.

Table D-5 REST APIs for Query and Release Sessions

Service	URL	Inputs	Sample API

Query Session	`http://<hostname>:8080/RESTAPI/service/querySessions?path=/r&filterType=with-user&filterValue=bob`	• Content-Type—application/json
		• username—username to access the services
		• password—password to access the service
		• filterType—as listed above
			`curl -H "username:admin" -H "password:aicuser" 'http://ar-lnx-vm038:8080/RESTAPI/service/querySessions?path=/r&filterType=with-user&filterValue=bob'`
			`{"session-mgr-1":{"S3":{"Username":"bob","Key":"localhost:1","Nas":"localhost","IP":"192.168.0.0","IPX":"0x1","GSL":"1","USL":"1","UserVPN":"1","Nas-port":"1","Time":"00:01:17","User-Name":"bob"}}}`
			`[root@ar-lnx-vm049 ~]#`

Release Session	`http://<hostname>:8080/RESTAPI/service/releasesessions?path=/r&filterType=with-user&filterValue=bob`		`curl -X GET -H "username:admin" -H "password:aicuser" -H "Content-Type: application/json" 'http://ar-lnx-vm041:8080/RESTAPI/service/releasesessions?path=/r/SessionManagers/&filterType=with-user&filterValue=bob'` `Released 1 session(s) Successfully in /Radius/SessionManagers`

Support for RADIUS to JSON and JSON to RADIUS Translation

Tech Mahindra Access Registrar allows you to translate incoming radius requests to JSON format and vice versa.

The REST interface is extended to accommodate this functionality. This translation is supported for the following scenarios:

- Authorization
- Accounting (Start/Interim-Update/Stop)
- Change of Authorization/Packet of Disconnect (CoA/PoD)
- Session manager

Note This translation is not supported for authentication.

The following are CLI configurations to support this feature:

```
--> ls -R /r/services/restproxy

[ restproxy ]
Name = restproxy
Description =
Type = rest
IncomingScript~ =
OutgoingScript~ =
OutagePolicy~ = RejectAll
OutageScript~ = myscript
MultipleServersPolicy = Failover
RemoteServers/
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
1. restRM


--> ls -R

[ //localhost/Radius/RemoteServers/rest ]
Name = rest
Description =
Protocol = rest
ReactivateTimerInterval = 300000
Timeout = 5000
MaxTimeOuts = 3
RESTSourceConnections = 16
RequestURL =
http://10.81.78.143:8080/eapauth/IMSI/TECHMAHINDRA/NASId/NASIP/Port/authorization
HTTPVersion = HTTP2
UserName = eapAuth32TMUS
Password = <encrypted>
KeepAliveTimerInterval = 0
RequestToJSONRequestMappings/
RequestToQueryMappings/
TECHMAHINDRA = Techm-AVPair
IMSI = User-Name
NASId = NAS-Identifier
NASIP = NAS-IP-Address
Port = NAS-Port
```

CSRF Token Implementation using REST

Tech Mahindra Access Registrar supports Cross-Site Request Forgery (CSRF) check for enhanced security. A CSRF token is introduced to handle a CSRF request. This is an optional feature and is backward compatible.

To use the CSRF token:

1. Enable CSRF Token in RestCSRF.properties under /techm-ar/apache-tomcat-9.0.31/webapps/RESTAPI/WEB-INF/classes/RestCSRF.properties

   Set the value to **YES** as shown below. Default is NO.

   ```
   CSRF-TOKENS=YES
   ```

2. Set the timer for the CSRF token in RestCSRF.properties. The token expires based on the timer value. Default time value is 5 mins.
3. Generate CSRF tokens based on the authentication parameters. See the sample command below:

   ```
   curl
   [http://%3cIpaddress:port%3e/RESTAPI/service/getlogin]http://<Ipaddress:port>/RESTAPI/
   service/getlogin -H "Authorization:Basic < Authentication paramert>"

   Output:

   {CSRF tokens :< csrf-token >}
   ```

4. You can perform curl operations using the CSRF token. See the sample command below:

   ```
   curl 'http:// ://<Ipaddress:port>/RESTAPI/service/addobject' -H "csrf-token: <
   csrf-token >" -H "Content-Type: application/json" --data
   "{\"Service\":{\"Name\":\"null\",\"Description\":\"\",\"Type\":\"null\",\"IncomingScri
   pt\":\"\",\"OutgoingScript\":\"\"}"
   ```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Appendix E

Supported Counters and Error Statistics

This appendix lists the supported counters and error statistics used in Tech Mahindra Access Registrar.

This appendix contains the following sections:

- Interface-Level KPI Counters
- Error Statistics (error-stats)

Interface-Level KPI Counters

Tech Mahindra Access Registrar allows you to view the Diameter peer statistics at the interface level. Applicable statistics will be listed for interfaces such as SWm, S6b, STa, SWx, NASREQ, and so on.

The following is a sample CLI that shows the Diameter statistics for a client with interface level counters:

Note The generic statistics counters are also displayed along with the interface-level counters.

Diameter Peer statistics for client: client1, 10.81.79.79 With Origin-Host 10.81.79.79, And port 4994

```
cdbpPeerStatsState = Closed
cdbpPeerStatsACRsIn = 0
cdbpPeerStatsACRsOut = 0
cdbpPeerStatsACAsIn = 0
cdbpPeerStatsACAsOut = 0
cdbpPeerStatsCERsIn = 0
cdbpPeerStatsCERsOut = 0
cdbpPeerStatsCEAsIn = 0
cdbpPeerStatsCEAsOut = 0
cdbpPeerStatsDWRsIn = 0
cdbpPeerStatsDWRsOut = 0
cdbpPeerStatsDWAsIn = 0
cdbpPeerStatsDWAsOut = 0
cdbpPeerStatsDPRsIn = 0
cdbpPeerStatsDPRsOut = 0
cdbpPeerStatsDPAsIn = 0
cdbpPeerStatsDPAsOut = 0
cdbpPeerStatsRedirectEvents = 0
cdbpPeerStatsAccDupRequests = 0
cdbpPeerStatsMalformedReqsts = 0
cdbpPeerStatsAccsNotRecorded = 0
cdbpPeerStatsWhoInitDisconnect = 0
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

cdbpPeerStatsAccRetrans = 0
cdbpPeerStatsTotalRetrans= 0
cdbpPeerStatsAccPendReqstsOut = 0
cdbpPeerStatsAccReqstsDropped = 0
cdbpPeerStatsHByHDropMessages = 0
cdbpPeerStatsEToEDupMessages= 0
cdbpPeerStatsUnknownTypes= 0
cdbpPeerStatsProtocolErrors = 0
cdbpPeerStatsTransientFailures = 0
cdbpPeerStatsPermanentFailures = 0
cdbpPeerStatsDWCurrentStatus= 0
cdbpPeerStatsTransportDown = 0
cdbpPeerStatsTimeoutConnAtmpts = 0
cdbpPeerStatsFailedCERs = 0
cdbpPeerStatsFailedDWRs = 0
cdbpPeerStatsFailedDPRs = 0

Stats Interface = SWm
cdbpPeerStatsASAsOut = 0
cdbpPeerStatsRARsOut = 0
cdbpPeerStatsRAAsIn = 0
cdbpPeerStatsRAAsOut = 0
cdbpPeerStatsRstRARsOut = 0
cdbpPeerStatsRstRAAsIn = 0
cdbpPeerStatsSTRsIn= 0
cdbpPeerStatsSTRsOut = 0
cdbpPeerStatsSTAsIn = 0
cdbpPeerStatsSTAsOut = 0
cdbpPeerStatsASRsIn= 0
cdbpPeerStatsASRsOut= 0
cdbpPeerStatsASAsIn = 0
cdbpPeerStatsDERsIn = 0
cdbpPeerStatsDERsOut = 0
cdbpPeerStatsDEAsIn = 0
cdbpPeerStatsDEAsOut = 0
cdbpPeerStatsAARsIn = 0
cdbpPeerStatsAARsOut = 0
cdbpPeerStatsAAAsIn = 0
cdbpPeerStatsAAAsOut = 0
cdbpPeerStatsMARsIn = 0
cdbpPeerStatsMARsOut = 0
cdbpPeerStatsMAAsIn = 0
cdbpPeerStatsMAAsOut = 0
cdbpPeerStatsSARsIn = 0
cdbpPeerStatsSARsOut = 0
cdbpPeerStatsSAAsIn = 0
cdbpPeerStatsSAAsOut = 0
cdbpPeerStatsUDRsIn = 0
cdbpPeerStatsUDRsOut = 0
cdbpPeerStatsUDAsIn = 0
cdbpPeerStatsUDAsOut = 0
cdbpPeerStatsRTRsIn = 0
cdbpPeerStatsRTRsOut = 0
cdbpPeerStatsRTAsIn = 0
cdbpPeerStatsRTAsOut = 0
cdbpPeerStatsPPRsIn = 0
cdbpPeerStatsPPRsOut = 0
cdbpPeerStatsPPAsIn = 0
cdbpPeerStatsPPAsOut = 0
cdbpPeerStatsFailedAARs = 0
cdbpPeerStatsFailedDERs = 0
cdbpPeerStatsFailedMARs = 0
cdbpPeerStatsFailedSARs = 0
cdbpPeerStatsFailedPPRs = 0

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
cdbpPeerStatsFailedRARs = 0
cdbpPeerStatsRstFailedRARs = 0
cdbpPeerStatsFailedRTRs = 0
cdbpPeerStatsFailedASRs = 0
cdbpPeerStatsFailedSTRs = 0
cdbpPeerStatsMultiRoundDEAs = 0
cdbpPeerStatsFailedUDRs = 0

Stats Interface = S6b
cdbpPeerStatsASAsOut = 0
cdbpPeerStatsRARsOut = 0
cdbpPeerStatsRAAsIn = 0
cdbpPeerStatsRAAsOut = 0
cdbpPeerStatsRstRARsOut = 0
cdbpPeerStatsRstRAAsIn = 0
cdbpPeerStatsSTRsIn= 0
cdbpPeerStatsSTRsOut = 0
cdbpPeerStatsSTAsIn = 0
cdbpPeerStatsSTAsOut = 0
cdbpPeerStatsASRsIn= 0
cdbpPeerStatsASRsOut= 0
cdbpPeerStatsASAsIn = 0
cdbpPeerStatsDERsIn = 0
cdbpPeerStatsDERsOut = 0
cdbpPeerStatsDEAsIn = 0
cdbpPeerStatsDEAsOut = 0
cdbpPeerStatsAARsIn = 0
cdbpPeerStatsAARsOut = 0
cdbpPeerStatsAAAsIn = 0
cdbpPeerStatsAAAsOut = 0
cdbpPeerStatsMARsIn = 0
cdbpPeerStatsMARsOut = 0
cdbpPeerStatsMAAsIn = 0
cdbpPeerStatsMAAsOut = 0
cdbpPeerStatsSARsIn = 0
cdbpPeerStatsSARsOut = 0
cdbpPeerStatsSAAsIn = 0
cdbpPeerStatsSAAsOut = 0
cdbpPeerStatsUDRsIn = 0
cdbpPeerStatsUDRsOut = 0
cdbpPeerStatsUDAsIn = 0
cdbpPeerStatsUDAsOut = 0
cdbpPeerStatsRTRsIn = 0
cdbpPeerStatsRTRsOut = 0
cdbpPeerStatsRTAsIn = 0
cdbpPeerStatsRTAsOut = 0
cdbpPeerStatsPPRsIn = 0
cdbpPeerStatsPPRsOut = 0
cdbpPeerStatsPPAsIn = 0
cdbpPeerStatsPPAsOut = 0
cdbpPeerStatsFailedAARs = 0
cdbpPeerStatsFailedDERs = 0
cdbpPeerStatsFailedMARs = 0
cdbpPeerStatsFailedSARs = 0
cdbpPeerStatsFailedPPRs = 0
cdbpPeerStatsFailedRARs = 0
cdbpPeerStatsRstFailedRARs = 0
cdbpPeerStatsFailedRTRs = 0
cdbpPeerStatsFailedASRs = 0
cdbpPeerStatsFailedSTRs = 0
cdbpPeerStatsMultiRoundDEAs = 0
cdbpPeerStatsFailedUDRs = 0

Stats Interface = STa
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
cdbpPeerStatsASAsOut = 0
cdbpPeerStatsRARsOut = 0
cdbpPeerStatsRAAsIn = 0
cdbpPeerStatsRAAsOut = 0
cdbpPeerStatsRstRARsOut  = 0
 cdbpPeerStatsRstRAAsIn =  0
cdbpPeerStatsSTRsIn= 0
cdbpPeerStatsSTRsOut = 0
cdbpPeerStatsSTAsIn = 0
cdbpPeerStatsSTAsOut = 0
cdbpPeerStatsASRsIn= 0
cdbpPeerStatsASRsOut= 0
cdbpPeerStatsASAsIn = 0
cdbpPeerStatsDERsIn = 0
cdbpPeerStatsDERsOut = 0
cdbpPeerStatsDEAsIn = 0
cdbpPeerStatsDEAsOut = 0
cdbpPeerStatsAARsIn = 0
cdbpPeerStatsAARsOut = 0
cdbpPeerStatsAAAsIn = 0
cdbpPeerStatsAAAsOut = 0
cdbpPeerStatsMARsIn = 0
cdbpPeerStatsMARsOut = 0
cdbpPeerStatsMAAsIn = 0
cdbpPeerStatsMAAsOut = 0
cdbpPeerStatsSARsIn = 0
cdbpPeerStatsSARsOut = 0
cdbpPeerStatsSAAsIn = 0
cdbpPeerStatsSAAsOut = 0
cdbpPeerStatsUDRsIn = 0
cdbpPeerStatsUDRsOut = 0
cdbpPeerStatsUDAsIn = 0
cdbpPeerStatsUDAsOut = 0
cdbpPeerStatsRTRsIn = 0
cdbpPeerStatsRTRsOut = 0
cdbpPeerStatsRTAsIn = 0
cdbpPeerStatsRTAsOut = 0
cdbpPeerStatsPPRsIn = 0
cdbpPeerStatsPPRsOut = 0
cdbpPeerStatsPPAsIn = 0
cdbpPeerStatsPPAsOut = 0
cdbpPeerStatsFailedAARs  = 0
cdbpPeerStatsFailedDERs  = 0
cdbpPeerStatsFailedMARs  = 0
cdbpPeerStatsFailedSARs  = 0
cdbpPeerStatsFailedPPRs  = 0
cdbpPeerStatsFailedRARs  = 0
cdbpPeerStatsRstFailedRARs = 0
cdbpPeerStatsFailedRTRs = 0
cdbpPeerStatsFailedASRs = 0
cdbpPeerStatsFailedSTRs = 0
cdbpPeerStatsMultiRoundDEAs = 0
cdbpPeerStatsFailedUDRs = 0
```

For remote server statistics, the interface is listed as a combination of the source (front-end) and destination (back-end) interfaces e.g. SWx-SWm. In certain cases, where there is a failure of requests initiated from HSS, there will not be any front-end interface. Those requests are grouped under SWx interface.

For details about the Diameter peer and remote server statistics, see the *Tech Mahindra Access Registrar 9.3 User Guide*.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Sample CLI configuration is given below:

```
--> cd /r/remoteServers/

[ //localhost/Radius/RemoteServers ]
Entries 1 to 1 from 1 total entries
Current filter: <all>

remserver/

--> dia-stats /r/RemoteServers/remserver

Diameter Remote server statistics for: remserver, 10.81.78.165, port 3869
active = FALSE
cDiaRemSvrRTTAverage = 0ms
cDiaRemSvrRTTDeviation = 0ms
cDiaRemSvrServerType = Diameter
cDiaRemSvrTotalRequestsPending = 0
cDiaRemSvrTotalRequestsOutstanding = 0
cDiaRemSvrTotalRequestsAcknowledged = 0
cDiaRemSvrStatsState = Closed
cDiaRemSvrStatsACRsIn = 0
cDiaRemSvrStatsACRsOut = 0
cDiaRemSvrStatsACAsIn = 0
cDiaRemSvrStatsACAsOut = 0
cDiaRemSvrStatsCERsIn = 0
cDiaRemSvrStatsCERsOut = 11
cDiaRemSvrStatsCEAsIn = 0
cDiaRemSvrStatsCEAsOut = 0
cDiaRemSvrStatsDWRsIn = 0
cDiaRemSvrStatsDWRsOut = 0
cDiaRemSvrStatsDWAsIn = 0
cDiaRemSvrStatsDWAsOut = 0
cDiaRemSvrStatsDPRsIn = 0
cDiaRemSvrStatsDPRsOut = 0
cDiaRemSvrStatsDPAsIn = 0
cDiaRemSvrStatsDPAsOut = 0
cDiaRemSvrStatsRedirectEvents = 0
cDiaRemSvrStatsAccDupRequests = 0
cDiaRemSvrStatsMalformedRequests = 0
cDiaRemSvrStatsAccsNotRecorded = 0
cDiaRemSvrStatsWhoInitDisconnect = 2
cDiaRemSvrStatsAccRetrans = 0
cDiaRemSvrStatsTotalRetrans= 0
cDiaRemSvrStatsAccPendRequestsOut = 0
cDiaRemSvrStatsAccReqstsDropped = 0
cDiaRemSvrStatsHByHDropMessages = 0
cDiaRemSvrStatsEToEDupMessages= 0
cDiaRemSvrStatsUnknownTypes= 0
cDiaRemSvrStatsProtocolErrors = 0
cDiaRemSvrStatsTransientFailures = 0
cDiaRemSvrStatsPermanentFailures = 0
cDiaRemSvrStatsDWCurrentStatus= 2
cDiaRemSvrStatsTransportDown = 1
cDiaRemSvrStatsTimeoutConnAtmpts = 0
cDiaRemSvrStatsFailedCERs = 11
cDiaRemSvrStatsFailedDWRs = 0
cDiaRemSvrStatsFailedDPRs = 0

Stats for Interface= SWx-SWm
cDiaRemSvrStatsASRsIn= 0
cDiaRemSvrStatsASRsOut= 0
cDiaRemSvrStatsASAsIn = 0
cDiaRemSvrStatsASAsOut = 0
```

```
cDiaRemSvrStatsRARsIn = 0
cDiaRemSvrStatsRARsOut = 0
cDiaRemSvrStatsRAAsIn = 0
cDiaRemSvrStatsRAAsOut = 0
cDiaRemSvrStatsSTRsIn= 0
cDiaRemSvrStatsSTRsOut = 0
cDiaRemSvrStatsSTAsIn = 0
cDiaRemSvrStatsSTAsOut = 0
cDiaRemSvrStatsMARsIn = 0
cDiaRemSvrStatsMARsOut = 0
cDiaRemSvrStatsMAAsIn= 0
cDiaRemSvrStatsMAAsOut = 0
cDiaRemSvrStatsSARsIn = 0
cDiaRemSvrStatsSARsOut = 0
cDiaRemSvrStatsSAAsIn = 0
cDiaRemSvrStatsSAAsOut = 0
cDiaRemSvrStatsUDRsIn = 0
cDiaRemSvrStatsUDRsOut = 0
cDiaRemSvrStatsUDAsIn = 0
cDiaRemSvrStatsUDAsOut = 0
cDiaRemSvrStatsRTRsIn= 0
cDiaRemSvrStatsRTRsOut = 0
cDiaRemSvrStatsRTAsIn = 0
cDiaRemSvrStatsRTAsOut = 0
cDiaRemSvrStatsPPRsIn= 0
cDiaRemSvrStatsPPRsOut = 0
cDiaRemSvrStatsPPAsIn = 0
cDiaRemSvrStatsPPAsOut = 0
cDiaRemSvrStatsDERsIn= 0
cDiaRemSvrStatsDERsOut = 0
cDiaRemSvrStatsDEAsIn = 0
cDiaRemSvrStatsDEAsOut = 0
cDiaRemSvrStatsAARsIn= 0
cDiaRemSvrStatsAARsOut = 0
cDiaRemSvrStatsAAAsIn = 0
cDiaRemSvrStatsAAAsOut = 0
cDiaRemSvrStatsFailedAARs  = 0
cDiaRemSvrStatsFailedDERs  = 0
cDiaRemSvrStatsFailedMARs  = 0
cDiaRemSvrStatsFailedSARs  = 0
cDiaRemSvrStatsFailedPPRs  = 0
cDiaRemSvrStatsFailedRARs  = 0
cDiaRemSvrStatsFailedRTRs  = 0
cDiaRemSvrStatsFailedASRs  = 0
cDiaRemSvrStatsFailedSTRs  = 0
cDiaRemSvrStatsFailedUDRs  = 0

Stats for Interface= SWx-S6b
cDiaRemSvrStatsASRsIn= 0
cDiaRemSvrStatsASRsOut= 0
cDiaRemSvrStatsASAsIn = 0
cDiaRemSvrStatsASAsOut = 0
cDiaRemSvrStatsRARsIn = 0
cDiaRemSvrStatsRARsOut = 0
cDiaRemSvrStatsRAAsIn = 0
cDiaRemSvrStatsRAAsOut = 0
cDiaRemSvrStatsSTRsIn= 0
cDiaRemSvrStatsSTRsOut = 0
cDiaRemSvrStatsSTAsIn = 0
cDiaRemSvrStatsSTAsOut = 0
cDiaRemSvrStatsMARsIn = 0
cDiaRemSvrStatsMARsOut = 0
cDiaRemSvrStatsMAAsIn= 0
cDiaRemSvrStatsMAAsOut = 0
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
cDiaRemSvrStatsSARsIn = 0
cDiaRemSvrStatsSARsOut = 0
cDiaRemSvrStatsSAAsIn = 0
cDiaRemSvrStatsSAAsOut = 0
cDiaRemSvrStatsUDRsIn = 0
cDiaRemSvrStatsUDRsOut = 0
cDiaRemSvrStatsUDAsIn = 0
cDiaRemSvrStatsUDAsOut = 0
cDiaRemSvrStatsRTRsIn= 0
cDiaRemSvrStatsRTRsOut = 0
cDiaRemSvrStatsRTAsIn = 0
cDiaRemSvrStatsRTAsOut = 0
cDiaRemSvrStatsPPRsIn= 0
cDiaRemSvrStatsPPRsOut = 0
cDiaRemSvrStatsPPAsIn = 0
cDiaRemSvrStatsPPAsOut = 0
cDiaRemSvrStatsDERsIn= 0
cDiaRemSvrStatsDERsOut = 0
cDiaRemSvrStatsDEAsIn = 0
cDiaRemSvrStatsDEAsOut = 0
cDiaRemSvrStatsAARsIn= 0
cDiaRemSvrStatsAARsOut = 0
cDiaRemSvrStatsAAAsIn = 0
cDiaRemSvrStatsAAAsOut = 0
cDiaRemSvrStatsFailedAARs = 0
cDiaRemSvrStatsFailedDERs = 0
cDiaRemSvrStatsFailedMARs = 0
cDiaRemSvrStatsFailedSARs = 0
cDiaRemSvrStatsFailedPPRs = 0
cDiaRemSvrStatsFailedRARs = 0
cDiaRemSvrStatsFailedRTRs = 0
cDiaRemSvrStatsFailedASRs = 0
cDiaRemSvrStatsFailedSTRs = 0
cDiaRemSvrStatsFailedUDRs = 0

Stats for Interface= SWx-STa
cDiaRemSvrStatsASRsIn= 0
cDiaRemSvrStatsASRsOut= 0
cDiaRemSvrStatsASAsIn = 0
cDiaRemSvrStatsASAsOut = 0
cDiaRemSvrStatsRARsIn = 0
cDiaRemSvrStatsRARsOut = 0
cDiaRemSvrStatsRAAsIn = 0
cDiaRemSvrStatsRAAsOut = 0
cDiaRemSvrStatsSTRsIn= 0
cDiaRemSvrStatsSTRsOut = 0
cDiaRemSvrStatsSTAsIn = 0
cDiaRemSvrStatsSTAsOut = 0
cDiaRemSvrStatsMARsIn = 0
cDiaRemSvrStatsMARsOut = 0
cDiaRemSvrStatsMAAsIn= 0
cDiaRemSvrStatsMAAsOut = 0
cDiaRemSvrStatsSARsIn = 0
cDiaRemSvrStatsSARsOut = 0
cDiaRemSvrStatsSAAsIn = 0
cDiaRemSvrStatsSAAsOut = 0
cDiaRemSvrStatsUDRsIn = 0
cDiaRemSvrStatsUDRsOut = 0
cDiaRemSvrStatsUDAsIn = 0
cDiaRemSvrStatsUDAsOut = 0
cDiaRemSvrStatsRTRsIn= 0
cDiaRemSvrStatsRTRsOut = 0
cDiaRemSvrStatsRTAsIn = 0
cDiaRemSvrStatsRTAsOut = 0
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
cDiaRemSvrStatsPPRsIn=  )
cDiaRemSvrStatsPPRsOut =  0
cDiaRemSvrStatsPPAsIn = 0
cDiaRemSvrStatsPPAsOut =  0
cDiaRemSvrStatsDERsIn=  )
cDiaRemSvrStatsDERsOut =  0
cDiaRemSvrStatsDEAsIn = 0
cDiaRemSvrStatsDEAsOut =  0
cDiaRemSvrStatsAARsIn=  )
cDiaRemSvrStatsAARsOut =  0
cDiaRemSvrStatsAAAsIn = 0
cDiaRemSvrStatsAAAsOut =  0
cDiaRemSvrStatsFailedAARs  = 0
cDiaRemSvrStatsFailedDERs  = 0
cDiaRemSvrStatsFailedMARs  = 0
cDiaRemSvrStatsFailedSARs  = 0
cDiaRemSvrStatsFailedPPRs  = 0
cDiaRemSvrStatsFailedRARs  = 0
cDiaRemSvrStatsFailedRTRs  = 0
cDiaRemSvrStatsFailedASRs  = 0
cDiaRemSvrStatsFailedSTRs  = 0
cDiaRemSvrStatsFailedUDRs  = 0

Stats for Interface= SH
cDiaRemSvrStatsASRsIn= 0
cDiaRemSvrStatsASRsOut= 0
cDiaRemSvrStatsASAsIn = 0
cDiaRemSvrStatsASAsOut =  0
cDiaRemSvrStatsRARsIn = 0
cDiaRemSvrStatsRARsOut =  0
cDiaRemSvrStatsRAAsIn = 0
cDiaRemSvrStatsRAAsOut =  0
cDiaRemSvrStatsSTRsIn= 0
cDiaRemSvrStatsSTRsOut =  0
cDiaRemSvrStatsSTAsIn = 0
cDiaRemSvrStatsSTAsOut =  0
cDiaRemSvrStatsMARsIn = 0
cDiaRemSvrStatsMARsOut =  0
cDiaRemSvrStatsMAAsIn= 0
cDiaRemSvrStatsMAAsOut =  0
cDiaRemSvrStatsSARsIn = 0
cDiaRemSvrStatsSARsOut =  0
cDiaRemSvrStatsSAAsIn = 0
cDiaRemSvrStatsSAAsOut =  0
cDiaRemSvrStatsUDRsIn = 0
cDiaRemSvrStatsUDRsOut =  0
cDiaRemSvrStatsUDAsIn = 0
cDiaRemSvrStatsUDAsOut =  0
cDiaRemSvrStatsRTRsIn= 0
cDiaRemSvrStatsRTRsOut =  0
cDiaRemSvrStatsRTAsIn = 0
cDiaRemSvrStatsRTAsOut =  0
cDiaRemSvrStatsPPRsIn= 0
cDiaRemSvrStatsPPRsOut =  0
cDiaRemSvrStatsPPAsIn = 0
cDiaRemSvrStatsPPAsOut =  0
cDiaRemSvrStatsDERsIn= 0
cDiaRemSvrStatsDERsOut =  0
cDiaRemSvrStatsDEAsIn = 0
cDiaRemSvrStatsDEAsOut =  0
cDiaRemSvrStatsAARsIn= 0
cDiaRemSvrStatsAARsOut =  0
cDiaRemSvrStatsAAAsIn = 0
cDiaRemSvrStatsAAAsOut = 0
```

```
cDiaRemSvrStatsFailedAARs  = 0
cDiaRemSvrStatsFailedDERs  = 0
cDiaRemSvrStatsFailedMARs  = 0
cDiaRemSvrStatsFailedSARs  = 0
cDiaRemSvrStatsFailedPPRs  = 0
cDiaRemSvrStatsFailedRARs  = 0
cDiaRemSvrStatsFailedRTRs  = 0
cDiaRemSvrStatsFailedASRs  = 0
cDiaRemSvrStatsFailedSTRs  = 0
cDiaRemSvrStatsFailedUDRs  = 0
```

Error Statistics (error-stats)

Tech Mahindra Access Registrar aggregates the error counters in case of failure of requests. Error statistic is the list of error codes with the number of failures for each command. These statistics are also listed at the interface level.

To enable error-stats, you must place the **errorstats.xml** file in the following location:

/opt/TMar/conf

The xml file must contain the error codes to be monitored. Error statistics will be displayed only for the error codes mentioned in the xml file.

A sample errorstats.xml file content is shown below:

```
[root@tmar-rhel-93 conf]# cat errorstats.xml <?xml version="1.0"?> <Application>
<Command>
<ErrorCode Name="Diameter-Command-Unsupported">3001</ErrorCode>
<ErrorCode Name="Diameter-Unable-To-Deliver">3002</ErrorCode>
<ErrorCode Name="Diameter-Realm-Not-Served">3003</ErrorCode>
<ErrorCode Name="Diameter-Too-Busy">3004</ErrorCode>
<ErrorCode Name="Diameter-Loop-Detected">3005</ErrorCode>
<ErrorCode Name="Diameter-Redirect-Indication">3006</ErrorCode>
<ErrorCode Name="Diameter-Application-Unsupported">3007</ErrorCode>
<ErrorCode Name="Diameter-Invalid-Hdr-Bits">3008</ErrorCode>
<ErrorCode Name="Diameter-Invalid-Avp-Bits">3009</ErrorCode>
<ErrorCode Name="Diameter-Unknown-Peer">3010</ErrorCode>
<ErrorCode Name="Diameter-Authentication-Rejected">4001</ErrorCode>
<ErrorCode Name="Diameter-Out-Of-Space">4002</ErrorCode>
<ErrorCode Name="Diameter-Election-Lost">4003</ErrorCode>
<ErrorCode Name="Diameter-Error-User-Unknown">5001</ErrorCode>
<ErrorCode Name="Diameter-Unknown-Session-Id">5002</ErrorCode>
<ErrorCode Name="Diameter-Error-Identity-Not-Registered">5003</ErrorCode>
<ErrorCode Name="Diameter-Error-Roaming-Not-Allowed">5004</ErrorCode>
<ErrorCode Name="Diameter-Error-Identity-Already-Registered">5005</ErrorCode>
<ErrorCode Name="Diameter-Unable-To-Comply">5012</ErrorCode>
<ErrorCode Name="Diameter-Error-User-No-Non-3gpp-Subscription">5450</ErrorCode>
<ErrorCode Name="Diameter-Error-User-No-Apn-Subscription">5451</ErrorCode>
<ErrorCode Name="Diameter-Error-Rat-Type-Not-Allowed">5452</ErrorCode>
<ErrorCode Name="Diameter-Error-Late-Overlapping-Request">5453</ErrorCode>
<ErrorCode Name="Diameter-Error-Timed-Out-Request">5454</ErrorCode>
<ErrorCode Name="Diameter-Error-Illegal-Equipment">5554</ErrorCode>
</Command>
</Application>
```

Following is the sample CLI of the error statistics:

```
--> error-stats /r/RemoteServers/remserver SWx-SWm

Diameter Error Stats for RemoteServer : remserver, Interface: SWx-SWm
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
Command Code = CER
Diameter-Command-Unsupported = 0
Diameter-Unable-To-Deliver = 0
Diameter-Realm-Not-Served = 0
Diameter-Too-Busy = 0
Diameter-Loop-Detected = 0
Diameter-Redirect-Indication = 0
Diameter-Application-Unsupported = 0
Diameter-Invalid-Hdr-Bits = 0
Diameter-Invalid-Avp-Bits = 0
Diameter-Unknown-Peer = 0
Diameter-Authentication-Rejected = 0
Diameter-Out-Of-Space = 0
Election-Lost = 0
Diameter-Error-User-Unknown = 0
Diameter-Unknown-Session-Id = 0
Diameter-Error-Identity-Not-Registered = 0
Diameter-Error-Roaming-Not-Allowed = 0
Diameter-Error-Identity-Already-Registered = 0
Diameter-Unable-To-Comply = 0
Diameter-Error-User-No-Non-3gpp-Subscription = 0
Diameter-Error-User-No-Apn-Subscription = 0
Diameter-Error-Rat-Type-Not-Allowed = 0
Diameter-Error-Late-Overlapping-Request = 0
Diameter-Error-Timed-Out-Request = 0
Diameter-Error-Illegal-Equipment = 0

Command Code = DWR
Diameter-Command-Unsupported = 0
Diameter-Unable-To-Deliver = 0
Diameter-Realm-Not-Served = 0
Diameter-Too-Busy = 0
Diameter-Loop-Detected = 0
Diameter-Redirect-Indication = 0
Diameter-Application-Unsupported = 0
Diameter-Invalid-Hdr-Bits = 0
Diameter-Invalid-Avp-Bits = 0
Diameter-Unknown-Peer = 0
Diameter-Authentication-Rejected = 0
Diameter-Out-Of-Space = 0
Election-Lost = 0
Diameter-Error-User-Unknown = 0
Diameter-Unknown-Session-Id = 0
Diameter-Error-Identity-Not-Registered = 0
Diameter-Error-Roaming-Not-Allowed = 0
Diameter-Error-Identity-Already-Registered = 0
Diameter-Unable-To-Comply = 0
Diameter-Error-User-No-Non-3gpp-Subscription = 0
Diameter-Error-User-No-Apn-Subscription = 0
Diameter-Error-Rat-Type-Not-Allowed = 0
Diameter-Error-Late-Overlapping-Request = 0
Diameter-Error-Timed-Out-Request = 0
Diameter-Error-Illegal-Equipment = 0

Command Code = DPR
Diameter-Command-Unsupported = 0
Diameter-Unable-To-Deliver = 0
Diameter-Realm-Not-Served = 0
Diameter-Too-Busy = 0
Diameter-Loop-Detected = 0
Diameter-Redirect-Indication = 0
Diameter-Application-Unsupported = 0
Diameter-Invalid-Hdr-Bits = 0
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
Diameter-Invalid-Avp-Bits = 0
Diameter-Unknown-Peer = 0
Diameter-Authentication-Rejected = 0
Diameter-Out-Of-Space = 0
Election-Lost = 0
Diameter-Error-User-Unknown = 0
Diameter-Unknown-Session-Id = 0
Diameter-Error-Identity-Not-Registered = 0
Diameter-Error-Roaming-Not-Allowed = 0
Diameter-Error-Identity-Already-Registered = 0
Diameter-Unable-To-Comply = 0
Diameter-Error-User-No-Non-3gpp-Subscription = 0
Diameter-Error-User-No-Apn-Subscription = 0
Diameter-Error-Rat-Type-Not-Allowed = 0
Diameter-Error-Late-Overlapping-Request = 0
Diameter-Error-Timed-Out-Request = 0
Diameter-Error-Illegal-Equipment = 0

Command Code = AAR
Diameter-Command-Unsupported = 0
Diameter-Unable-To-Deliver = 0
Diameter-Realm-Not-Served = 0
Diameter-Too-Busy = 0
Diameter-Loop-Detected = 0
Diameter-Redirect-Indication = 0
Diameter-Application-Unsupported = 0
Diameter-Invalid-Hdr-Bits = 0
Diameter-Invalid-Avp-Bits = 0
Diameter-Unknown-Peer = 0
Diameter-Authentication-Rejected = 0
Diameter-Out-Of-Space = 0
Election-Lost = 0
Diameter-Error-User-Unknown = 0
Diameter-Unknown-Session-Id = 0
Diameter-Error-Identity-Not-Registered = 0
Diameter-Error-Roaming-Not-Allowed = 0
Diameter-Error-Identity-Already-Registered = 0
Diameter-Unable-To-Comply = 0
Diameter-Error-User-No-Non-3gpp-Subscription = 0
Diameter-Error-User-No-Apn-Subscription = 0
Diameter-Error-Rat-Type-Not-Allowed = 0
Diameter-Error-Late-Overlapping-Request = 0
Diameter-Error-Timed-Out-Request = 0
Diameter-Error-Illegal-Equipment = 0

Command Code = DER
Diameter-Command-Unsupported = 0
Diameter-Unable-To-Deliver = 0
Diameter-Realm-Not-Served = 0
Diameter-Too-Busy = 0
Diameter-Loop-Detected = 0
Diameter-Redirect-Indication = 0
Diameter-Application-Unsupported = 0
Diameter-Invalid-Hdr-Bits = 0
Diameter-Invalid-Avp-Bits = 0
Diameter-Unknown-Peer = 0
Diameter-Authentication-Rejected = 0
Diameter-Out-Of-Space = 0
Election-Lost = 0
Diameter-Error-User-Unknown = 0
Diameter-Unknown-Session-Id = 0
Diameter-Error-Identity-Not-Registered = 0
Diameter-Error-Roaming-Not-Allowed = 0
Diameter-Error-Identity-Already-Registered = 0
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
Diameter-Unable-To-Comply = 0
Diameter-Error-User-No-Non-3gpp-Subscription = 0
Diameter-Error-User-No-Apn-Subscription = 0
Diameter-Error-Rat-Type-Not-Allowed = 0
Diameter-Error-Late-Overlapping-Request = 0
Diameter-Error-Timed-Out-Request = 0
Diameter-Error-Illegal-Equipment = 0

Command Code = MAR
Diameter-Command-Unsupported = 0
Diameter-Unable-To-Deliver = 0
Diameter-Realm-Not-Served = 0
Diameter-Too-Busy = 0
Diameter-Loop-Detected = 0
Diameter-Redirect-Indication = 0
Diameter-Application-Unsupported = 0
Diameter-Invalid-Hdr-Bits = 0
Diameter-Invalid-Avp-Bits = 0
Diameter-Unknown-Peer = 0
Diameter-Authentication-Rejected = 0
Diameter-Out-Of-Space = 0
Election-Lost = 0
Diameter-Error-User-Unknown = 0
Diameter-Unknown-Session-Id = 0
Diameter-Error-Identity-Not-Registered = 0
Diameter-Error-Roaming-Not-Allowed = 0
Diameter-Error-Identity-Already-Registered = 0
Diameter-Unable-To-Comply = 0
Diameter-Error-User-No-Non-3gpp-Subscription = 0
Diameter-Error-User-No-Apn-Subscription = 0
Diameter-Error-Rat-Type-Not-Allowed = 0
Diameter-Error-Late-Overlapping-Request = 0
Diameter-Error-Timed-Out-Request = 0
Diameter-Error-Illegal-Equipment = 0

Command Code = SAR
Diameter-Command-Unsupported = 0
Diameter-Unable-To-Deliver = 0
Diameter-Realm-Not-Served = 0
Diameter-Too-Busy = 0
Diameter-Loop-Detected = 0
Diameter-Redirect-Indication = 0
Diameter-Application-Unsupported = 0
Diameter-Invalid-Hdr-Bits = 0
Diameter-Invalid-Avp-Bits = 0
Diameter-Unknown-Peer = 0
Diameter-Authentication-Rejected = 0
Diameter-Out-Of-Space = 0
Election-Lost = 0
Diameter-Error-User-Unknown = 0
Diameter-Unknown-Session-Id = 0
Diameter-Error-Identity-Not-Registered = 0
Diameter-Error-Roaming-Not-Allowed = 0
Diameter-Error-Identity-Already-Registered = 0
Diameter-Unable-To-Comply = 0
Diameter-Error-User-No-Non-3gpp-Subscription = 0
Diameter-Error-User-No-Apn-Subscription = 0
Diameter-Error-Rat-Type-Not-Allowed = 0
Diameter-Error-Late-Overlapping-Request = 0
Diameter-Error-Timed-Out-Request = 0
Diameter-Error-Illegal-Equipment = 0

Command Code = PPR
Diameter-Command-Unsupported = 0
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
Diameter-Unable-To-Deliver = 0
Diameter-Realm-Not-Served = 0
Diameter-Too-Busy = 0
Diameter-Loop-Detected = 0
Diameter-Redirect-Indication = 0
Diameter-Application-Unsupported = 0
Diameter-Invalid-Hdr-Bits = 0
Diameter-Invalid-Avp-Bits = 0
Diameter-Unknown-Peer = 0
Diameter-Authentication-Rejected = 0
Diameter-Out-Of-Space = 0
Election-Lost = 0
Diameter-Error-User-Unknown = 0
Diameter-Unknown-Session-Id = 0
Diameter-Error-Identity-Not-Registered = 0
Diameter-Error-Roaming-Not-Allowed = 0
Diameter-Error-Identity-Already-Registered = 0
Diameter-Unable-To-Comply = 0
Diameter-Error-User-No-Non-3gpp-Subscription = 0
Diameter-Error-User-No-Apn-Subscription = 0
Diameter-Error-Rat-Type-Not-Allowed = 0
Diameter-Error-Late-Overlapping-Request = 0
Diameter-Error-Timed-Out-Request = 0
Diameter-Error-Illegal-Equipment = 0

Command Code = RAR
Diameter-Command-Unsupported = 0
Diameter-Unable-To-Deliver = 0
Diameter-Realm-Not-Served = 0
Diameter-Too-Busy = 0
Diameter-Loop-Detected = 0
Diameter-Redirect-Indication = 0
Diameter-Application-Unsupported = 0
Diameter-Invalid-Hdr-Bits = 0
Diameter-Invalid-Avp-Bits = 0
Diameter-Unknown-Peer = 0
Diameter-Authentication-Rejected = 0
Diameter-Out-Of-Space = 0
Election-Lost = 0
Diameter-Error-User-Unknown = 0
Diameter-Unknown-Session-Id = 0
Diameter-Error-Identity-Not-Registered = 0
Diameter-Error-Roaming-Not-Allowed = 0
Diameter-Error-Identity-Already-Registered = 0
Diameter-Unable-To-Comply = 0
Diameter-Error-User-No-Non-3gpp-Subscription = 0
Diameter-Error-User-No-Apn-Subscription = 0
Diameter-Error-Rat-Type-Not-Allowed = 0
Diameter-Error-Late-Overlapping-Request = 0
Diameter-Error-Timed-Out-Request = 0
Diameter-Error-Illegal-Equipment = 0

Command Code = RstRAR
Diameter-Command-Unsupported = 0
Diameter-Unable-To-Deliver = 0
Diameter-Realm-Not-Served = 0
Diameter-Too-Busy = 0
Diameter-Loop-Detected = 0
Diameter-Redirect-Indication = 0
Diameter-Application-Unsupported = 0
Diameter-Invalid-Hdr-Bits = 0
Diameter-Invalid-Avp-Bits = 0
Diameter-Unknown-Peer = 0
Diameter-Authentication-Rejected = 0
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
Diameter-Out-Of-Space = 0
Election-Lost = 0
Diameter-Error-User-Unknown = 0
Diameter-Unknown-Session-Id = 0
Diameter-Error-Identity-Not-Registered = 0
Diameter-Error-Roaming-Not-Allowed = 0
Diameter-Error-Identity-Already-Registered = 0
Diameter-Unable-To-Comply = 0
Diameter-Error-User-No-Non-3gpp-Subscription = 0
Diameter-Error-User-No-Apn-Subscription = 0
Diameter-Error-Rat-Type-Not-Allowed = 0
Diameter-Error-Late-Overlapping-Request = 0
Diameter-Error-Timed-Out-Request = 0
Diameter-Error-Illegal-Equipment = 0

Command Code = RTR
Diameter-Command-Unsupported = 0
Diameter-Unable-To-Deliver = 0
Diameter-Realm-Not-Served = 0
Diameter-Too-Busy = 0
Diameter-Loop-Detected = 0
Diameter-Redirect-Indication = 0
Diameter-Application-Unsupported = 0
Diameter-Invalid-Hdr-Bits = 0
Diameter-Invalid-Avp-Bits = 0
Diameter-Unknown-Peer = 0
Diameter-Authentication-Rejected = 0
Diameter-Out-Of-Space = 0
Election-Lost = 0
Diameter-Error-User-Unknown = 0
Diameter-Unknown-Session-Id = 0
Diameter-Error-Identity-Not-Registered = 0
Diameter-Error-Roaming-Not-Allowed = 0
Diameter-Error-Identity-Already-Registered = 0
Diameter-Unable-To-Comply = 0
Diameter-Error-User-No-Non-3gpp-Subscription = 0
Diameter-Error-User-No-Apn-Subscription = 0
Diameter-Error-Rat-Type-Not-Allowed = 0
Diameter-Error-Late-Overlapping-Request = 0
Diameter-Error-Timed-Out-Request = 0
Diameter-Error-Illegal-Equipment = 0

Command Code = ASR
Diameter-Command-Unsupported = 0
Diameter-Unable-To-Deliver = 0
Diameter-Realm-Not-Served = 0
Diameter-Too-Busy = 0
Diameter-Loop-Detected = 0
Diameter-Redirect-Indication = 0
Diameter-Application-Unsupported = 0
Diameter-Invalid-Hdr-Bits = 0
Diameter-Invalid-Avp-Bits = 0
Diameter-Unknown-Peer = 0
Diameter-Authentication-Rejected = 0
Diameter-Out-Of-Space = 0
Election-Lost = 0
Diameter-Error-User-Unknown = 0
Diameter-Unknown-Session-Id = 0
Diameter-Error-Identity-Not-Registered = 0
Diameter-Error-Roaming-Not-Allowed = 0
Diameter-Error-Identity-Already-Registered = 0
Diameter-Unable-To-Comply = 0
Diameter-Error-User-No-Non-3gpp-Subscription = 0
Diameter-Error-User-No-Apn-Subscription = 0
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
Diameter-Error-Rat-Type-Not-Allowed = 0
Diameter-Error-Late-Overlapping-Request = 0
Diameter-Error-Timed-Out-Request = 0
Diameter-Error-Illegal-Equipment = 0

Command Code = STR
Diameter-Command-Unsupported = 0
Diameter-Unable-To-Deliver = 0
Diameter-Realm-Not-Served = 0
Diameter-Too-Busy = 0
Diameter-Loop-Detected = 0
Diameter-Redirect-Indication = 0
Diameter-Application-Unsupported = 0
Diameter-Invalid-Hdr-Bits = 0
Diameter-Invalid-Avp-Bits = 0
Diameter-Unknown-Peer = 0
Diameter-Authentication-Rejected = 0
Diameter-Out-Of-Space = 0
Election-Lost = 0
Diameter-Error-User-Unknown = 0
Diameter-Unknown-Session-Id = 0
Diameter-Error-Identity-Not-Registered = 0
Diameter-Error-Roaming-Not-Allowed = 0
Diameter-Error-Identity-Already-Registered = 0
Diameter-Unable-To-Comply = 0
Diameter-Error-User-No-Non-3gpp-Subscription = 0
Diameter-Error-User-No-Apn-Subscription = 0
Diameter-Error-Rat-Type-Not-Allowed = 0
Diameter-Error-Late-Overlapping-Request = 0
Diameter-Error-Timed-Out-Request = 0
Diameter-Error-Illegal-Equipment = 0

Command Code = UDR
Diameter-Command-Unsupported = 0
Diameter-Unable-To-Deliver = 0
Diameter-Realm-Not-Served = 0
Diameter-Too-Busy = 0
Diameter-Loop-Detected = 0
Diameter-Redirect-Indication = 0
Diameter-Application-Unsupported = 0
Diameter-Invalid-Hdr-Bits = 0
Diameter-Invalid-Avp-Bits = 0
Diameter-Unknown-Peer = 0
Diameter-Authentication-Rejected = 0
Diameter-Out-Of-Space = 0
Election-Lost = 0
Diameter-Error-User-Unknown = 0
Diameter-Unknown-Session-Id = 0
Diameter-Error-Identity-Not-Registered = 0
Diameter-Error-Roaming-Not-Allowed = 0
Diameter-Error-Identity-Already-Registered = 0
Diameter-Unable-To-Comply = 0
Diameter-Error-User-No-Non-3gpp-Subscription = 0
Diameter-Error-User-No-Apn-Subscription = 0
Diameter-Error-Rat-Type-Not-Allowed = 0
Diameter-Error-Late-Overlapping-Request = 0
Diameter-Error-Timed-Out-Request = 0
Diameter-Error-Illegal-Equipment = 0
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Appendix F

Health Monitoring in Tech Mahindra Access Registrar

This appendix briefs about enhanced health monitoring in Tech Mahindra Access Registrar and lists the supported statistics.

Tech Mahindra Access Registrar supports regular health monitoring for RADIUS server. A new parameter **EnableHealthMonitoring** is introduced to support enhanced health monitoring for RADIUS and Diameter.

You can monitor the health of Tech Mahindra Access Registrar server using the following parameters:

- CPU Utilization
- Memory
- Packet Buffer
- Worker Threads count
- Packet Rejects
- Packet Drops
- Packet Time Outs
- Peer Connectivity

You have an option to set threshold limits against which the individual health check parameters are monitored. The threshold limits are entered in percentage unit. You can also set the monitoring frequency.

Table F-1 lists and describes the configuration details of health monitoring counters.

Table F-1 Health Monitoring Counters

Fields	Description
EnableHealthMonitoring	Set to TRUE to enable health monitoring for RADIUS/Diameter in Tech Mahindra Access Registrar.
CPUUtilizationWarning-Threshold	Warning threshold for CPU utilization. If the CPU utilization hits the warning threshold, the corresponding health is decremented and a warning trap is initiated.
CPUUtilizationErrorThresh-old	Error threshold for CPU utilization. If the CPU utilization drops below the error threshold value, an error trap is initiated.

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

Table F-1 Health Monitoring Counters

Fields	Description
MemoryWarningThreshold	Warning threshold for memory utilization. If the memory utilization hits the warning threshold, the corresponding health is decremented and a warning trap is initiated.
MemoryErrorThreshold	Error threshold for memory utilization. If the memory utilization drops below the error threshold value, an error trap is initiated.
PacketsInUseWarningThreshold	Warning threshold for packet buffer. If the packet buffer hits the warning threshold, the corresponding health is decremented and a warning trap is initiated.
PacketsInUseErrorThreshold	Error threshold for packet buffer. If the packet buffer drops below the error threshold value, an error trap is initiated.
WorkerThreadsWarningThreshold	Warning threshold for worker threads. If the worker thread count hits the warning threshold, the corresponding health is decremented and a warning trap is initiated.
WorkerThreadsErrorThreshold	Error threshold for worker threads. If the worker thread count drops below the error threshold value, an error trap is initiated.
PacketRejectsWarningThreshold	Warning threshold for packet rejects. If the packet reject count hits the warning threshold, the corresponding health is decremented and a warning trap is initiated.
PacketRejectsErrorThreshold	Error threshold for packet rejects. If the packet reject count drops below the error threshold value, an error trap is initiated.
PacketTimedOutsWarningThreshold	Warning threshold for packet timeouts. If the packet timeout count hits the warning threshold, the corresponding health is decremented and a warning trap is initiated.
PacketTimedOutsErrorThreshold	Error threshold for packet timeouts. If the packet timeout count drops below the error threshold value, an error trap is initiated.
PacketDropsWarningThreshold	Warning threshold for packet drops. If the packet dropout count hits the warning threshold, the corresponding health is decremented and a warning trap is initiated.
PacketDropsErrorThreshold	Error threshold for packet drops. If the packet dropout count drops below the error threshold value, an error trap is initiated.
PeerConnectivityWarningThreshold	Warning threshold for peer connectivity. If the peer connectivity count hits the warning threshold, the corresponding health is decremented and a warning trap is initiated.
PeerConnectivityErrorThreshold	Error threshold for peer connectivity. If the peer connectivity count drops below the error threshold value, an error trap is initiated.
HealthMonitorFreqInsecs	The frequency, in seconds, to monitor the health parameters.

Note All the above parameters are represented in percentage values from 0 - 100. You can choose to set up a value more than zero only for those parameters for which you wish to enable monitoring.

The following is a sample CLI that shows the health monitoring counters:

```
[ //localhost/Radius/Advanced/HealthMonitor ]
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
EnableHealthMonitoring = TRUE
CPUUtilizationWarningThreshold = 90
CPUUtilizationErrorThreshold = 0
MemoryWarningThreshold = 0
MemoryErrorThreshold = 0
PacketsInUseWarningThreshold = 0
PacketsInUseErrorThreshold = 0
WorkerThreadsWarningThreshold = 0
WorkerThreadsErrorThreshold = 0
PacketRejectsWarningThreshold = 0
PacketRejectsErrorThreshold = 0
PacketTimedOutsWarningThreshold = 0
PacketTimedOutsErrorThreshold = 0
PacketDropsWarningThreshold = 0
PacketDropsErrorThreshold = 0
HealthMonitorLogFreqInsecs = 0
```

The status of the health monitoring parameters are displayed as one of the following in the statistics:

- GOOD—If the parameter is within the limits.
- REDUCING—If the parameter is hitting the warning threshold value.
- CRITICAL—If the parameter is dropping below the error threshold value.
- UNMONITORED—If the parameter is unmonitored (no threshold values are set for the parameter).

You can use the **health** command in CLI to display the health statistics of all the parameters. You can use the **status** command to display the overall health status of Tech Mahindra Access Registrar.

The following traps are triggered for each of the health monitoring parameters in Tech Mahindra Access Registrar:

- HealthMonitoringWarningTrap—Triggered when the parameter health hits the warning threshold limit.
- HealthMonitoringErrorTrap—Triggered when the parameter health hits the error threshold limit.
- HealthMonitoringResetTrap—Triggered to indicate that the parameter health has reached the configured error/warning threshold percentage limit and falls behind the error/warning threshold percentage limit. After this notification is sent, this type of notification will not be sent again until the parameter health on the server increases above the configured error/warning threshold percentage limit.

The following is an example of the health monitoring statistics:

```
--> health

Diameter Health Detailed Report:

CPU Utilization Health = GOOD
Memory Health = GOOD
Packet Buffer Health = GOOD
Worker Threads Health = GOOD
Packet Rejects = GOOD
Packet Drops = GOOD
Packets TimedOuts = GOOD

Radius Health Detailed Report:

CPU Utilization Health = GOOD
Memory Health = GOOD
Packet Buffer Health = GOOD
Worker Threads Health = GOOD
Packet Rejects = GOOD
Packet Drops = GOOD
```

Company Confidential | Copyright © 2024, Tech Mahindra. All rights reserved.

```
Packets Timedouts = GOOD
```