Trademarks

The symbol, NOMADIX™ and Nomadix Service Engine™ are trademarks of Nomadix, Inc. All other trademarks and brand names are marks of their respective holders.

Product Information

Telephone: +1.818.597.1500
Fax: +1.818.597.1502

For technical support information, see the Appendix in this User Guide.

Write your product serial number in this box:

S/N

Patent Information

Covered by one or more of the following U.S. and foreign patents: US6,130,892; AU740012, 中国发明专利 98805023.4, Israel 131831, Korea 528156, Mexico 222100, New Zealand 337772; US6,868,399; US7,117,526, EU1226687 (validated in: BE1226687, FI1226687, FR1226687, DE60028229.5, GB1226687, IE1226687, NL1226687, ES1226687, SE1226687, CH1226687); US7,197,556, EU1224788 (validated in: BE1224788, CH1224788, DE60011799.5-08, ES1224788, FI1224788, FR1224788, GB1224788, NL1224788, SE1224788); US6,636,894, EU1222791 (validated in: BE1222791, FI1222791, FR1222791, DE60020588.6, GB1222791, NL1222791, ES1222791, SE1222791, CH1222791); SG88575, 中国发明专利 00815828.2, AU2006207853; US6,789,110, Japan 3880856, Korea 559357, SG88483, 中国发明专利 00815982.3, EU1234425 (validated in: BE1234425, FI1234425, FR1234425, DE60029819.1, GB1234425, IE1234425, NL1234425, ES1234425, SE1234425, CH1234425); US7,088,727; US6,857,009; US7,194,554, AU779137, Korea 0687837, SG88465, 中国发明专利 00815827.4; US7,554,995; US7,698,432, EU1232610 (validated in: BE1232610, FI1232610, FR1232610, DE60041352.7, GB1232610, IE1232610, IT1232610, NL1232610, ES1232610, SE1232610, CH1232610); and US7,689,716. European patents (EU) only validated in the indicated states. Other U.S. and foreign patents pending or granted.

Disclaimer

Nomadix, Inc. makes no warranty, either express or implied, including but not limited to any implied warranties of merchantability and fitness for a particular purpose, regarding the product described herein. In no event shall Nomadix, Inc. be liable to anyone for special, collateral, incidental, or consequential damages in connection with or arising from the use of Nomadix, Inc. products.
WARNING
Risk of electric shock; do not open; no user-serviceable parts inside.

AVERTISSEMENT
Risque de choc électrique; ne pas ouvrir; ne pas tenter de demontre l’appareil.

WARNUNG
Nicht öffnen; elektrische Bauteile.

AVISO
Riesgo de shock eléctrico. No abrir. No hay piezas configurables dentro.

CAUTION
Read the instruction manual prior to operation.

ATTENTION
Lire le mode d’emploi avant utilisation.

ACHTUNG
Lesen Sie das Handbuch bevor Sie das Gerät in Betrieb nehmen.

PRECAUCIÓN
Leer el manual de instrucciones antes de poner en marcha el equipo.
# Table of Contents

**Chapter 1: Introduction**

- About this Guide ................................................................. 1
- Organization ........................................................................... 1

**Welcome to the Access Gateway** ................................................. 2

**Product Configuration and Licensing** ........................................... 2

**Key Features and Benefits** .......................................................... 3
- Platform Reliability ............................................................ 3
- Local Content and Services .................................................. 3
- Transparent Connectivity ...................................................... 4
- Billing Enablement ............................................................... 5
- Access Control and Authentication ...................................... 5
- Security .................................................................................. 5
- 5-Step Service Branding ....................................................... 5

**NSE Core Functionality** ............................................................ 7
- Access Control ................................................................. 8
- Bandwidth Management ...................................................... 8
- Billing Records Mirroring ................................................... 9
- Bridge Mode ......................................................................... 9
- Command Line Interface .................................................... 10
- Credit Card ........................................................................... 10
- Dynamic Address Translation™ ........................................... 10
- Dynamic Transparent Proxy ............................................... 10
- End User Licensee Count .................................................... 11
- External Web Server Mode ................................................ 11
- Home Page Redirect .......................................................... 11
- iNAT™ .................................................................................. 11
- Information and Control Console ....................................... 12
- Internal Web Server ............................................................ 13
- International Language Support ........................................ 14
- IP Upsell .............................................................................. 14
- Logout Pop-Up Window ....................................................... 14
- MAC Filtering ....................................................................... 15
- Multi-Level Administration Support ................................... 15
- NTP Support ......................................................................... 15
- Portal Page Redirect ............................................................ 15
- RADIUS-driven Auto Configuration .................................. 16
- RADIUS Client ................................................................. 16
- RADIUS Proxy ................................................................. 16
- Realm-Based Routing ......................................................... 17
Setting the System Date and Time {Time} ............................................................... 144
Setting up Traffic Descriptors .............................................................................. 146
Setting Up URL Filtering {URL Filtering} ............................................................. 147
Selecting User Agent Filtering Settings ................................................................. 148
Zone Migration ......................................................................................................... 149
Defining IPSec Tunnel Settings .............................................................................. 151
Network Info Menu .................................................................................................. 153
Displaying ARP Table Entries {ARP} ..................................................................... 153
Displaying DAT Sessions {DAT} ............................................................................. 153
Displaying the Host Table {Hosts} .......................................................................... 154
Displaying ICMP Statistics {ICMP} ......................................................................... 155
Displaying the Network Interfaces {Interfaces} ......................................................... 155
Displaying the IP Statistics {IP} .............................................................................. 157
Viewing IPSec Tunnel Status {IPSec} ..................................................................... 157
Displaying the Routing Tables {Routing} ................................................................. 157
Displaying the Active IP Connections {Sockets} ...................................................... 158
Displaying the Static Port Mapping Table {Static Port-Mapping} ......................... 159
Displaying TCP Statistics {TCP} ............................................................................. 160
Displaying UDP Statistics {UDP} ............................................................................. 161
Port-Location Menu .................................................................................................. 161
Adding and Updating Port-Location Assignments {Add} ....................................... 162
Deleting All Port-Location Assignments {Delete All} ............................................. 165
Deleting Port-Location Assignments by Location {Delete by Location} ............... 166
Deleting Port-Location Assignments by Port {Delete by Port} ............................... 167
Exporting Port-Location Assignments {Export} ............................................. 167
Finding Port-Location Assignments by Description {Find by Description} ............. 168
Finding Port-Location Assignments by Location {Find by Location} .................... 169
Finding Port-Location Assignments by Port {Find by Port} ..................................... 170
Importing Port-Location Assignments {Import} ................................................... 171
Displaying the Port-Location Mappings {List} ...................................................... 173
Subscriber Administration Menu ............................................................................ 173
Adding Subscriber Profiles {Add} .......................................................................... 173
Displaying Current Subscriber Connections {Current} ......................................... 179
Deleting Subscriber Profiles by MAC Address {Delete by MAC} ......................... 180
Deleting Subscriber Profiles by User Name {Delete by User} ............................... 181
Displaying the Currently Allocated DHCP Leases {DHCP Leases} ......................... 182
Deleting All Expired Subscriber Profiles {Expired} ............................................. 182
Finding Subscriber Profiles by MAC Address {Find by MAC} ............................... 183
Finding Subscriber Profiles by User Name {Find by User} ..................................... 183
Listing Subscriber Profiles by MAC Address {List by MAC} ................................. 184
Listing Subscriber Profiles by User Name {List by User} ....................................... 185
Viewing RADIUS Proxy Accounting Logs {RADIUS Session History} ................. 186
Displaying Current Profiles and Connections {Statistics} ..................................... 187
### Subscriber Interface Menu
- Defining the Billing Options (Billing Options) .......................................................... 187
- Setting Up the Information and Control Console (ICC Setup) ..................................... 194
- Defining Languages (Language Support) ..................................................................... 201
- Enable Serving of Local Web Pages (Local Web Server) ............................................ 203
- Defining the Subscriber’s Login UI (Login UI) ........................................................... 205
- Defining the Post Session User Interface (Post Session UI) ........................................... 209
- Defining Subscriber UI Buttons (Subscriber Buttons) .................................................. 212
- Defining Subscriber UI Labels (Subscriber Labels) ..................................................... 213
- Defining Subscriber Error Messages (Subscriber Errors) ........................................... 215
- Defining Subscriber Messages (Subscriber Messages) ................................................ 217

### System Menu
- Adding an ARP Table Entry (ARP Add) ........................................................................ 220
- Deleting an ARP Table Entry (ARP Delete) ................................................................. 221
- Configurable Gateway ARP Refresh Interval .............................................................. 221
- Enabling the Bridge Mode Option (Bridge Mode)........................................................ 222
- Exporting Configuration Settings to the Archive File (Export) ..................................... 223
- Importing the Factory Defaults (Factory) ..................................................................... 224
- Defining the Fail Over Options (Fail Over) .................................................................. 225
- Viewing the History Log (History) ............................................................................... 226
- Establishing ICMP Blocking Parameters (ICMP) ......................................................... 227
- Importing Configuration Settings from the Archive File (Import) ................................. 228
- Establishing Login Access Levels (Login) ..................................................................... 229
- Defining the MAC Filtering Options (Mac Filtering) ..................................................... 232
- Rebooting the System (Reboot) .................................................................................... 233
- Adding a Route (Route Add) ....................................................................................... 234
- Deleting a Route (Route Delete) .................................................................................. 235
- Establishing Session Rate Limiting (Session Limit) ..................................................... 235
- Adding Static Ports (Static Port-Mapping Add) ............................................................. 236
- Deleting Static Ports (Static Port-Mapping Delete) ....................................................... 238
- Blocking a Subscriber Interface (Subscriber Interfaces) ............................................. 239
- Updating the Access Gateway Firmware (Upgrade) .................................................... 239

### Chapter 4: The Subscriber Interface
- Overview ...................................................................................................................... 241
- Authorization and Billing ............................................................................................. 242
  - The AAA Structure ..................................................................................................... 243
  - Process Flow (AAA) .................................................................................................. 246
- Internal and External Web Servers .............................................................................. 247
- Language Support ........................................................................................................ 247
- Home Page Redirection ............................................................................................... 247
- Subscriber Management .............................................................................................. 248
  - Subscriber Management Models ............................................................................... 248
Chapter 6: Troubleshooting ........................................................................................ 305
   General Hints and Tips ............................................................................................ 305
   Management Interface Error Messages ..................................................................... 306
   Common Problems .................................................................................................... 308
   Contact Information .................................................................................................. 311
Introduction

About this Guide

This User Guide provides information and procedures that will enable system administrators to install, configure, manage, and use the Access Gateway product successfully and efficiently. Use this guide to take full advantage of the Access Gateway’s functionality and features.

Refer to “Product Specifications” on page 266 for a list of Access Gateway Products that this document supports.

Organization

This User Guide is organized into the following sections:

Chapter 1 – Installing the Access Gateway. This section provides instructions for installing the Access Gateway and establishing the start-up configuration.

Chapter 2 – System Administration. This section provides all the instructions and procedures necessary to manage and administer the Access Gateway on the customer’s network, following a successful installation.

Chapter 3 – The Subscriber Interface. This section provides an overview and sample scenario for the Access Gateway’s subscriber interface. It also includes an outline of the authorization and billing processes utilized by the system, and the Nomadix Information and Control Console.

Chapter 4 – Quick Reference Guide. This section contains product reference information, organized by topic and functionality. It also contains a full listing of all product configuration elements, sorted alphabetically and by menu.

Chapter 5 – Troubleshooting. This section provides information to help you resolve common hardware and software problems. It also contains a list of error messages associated with the management interface.

Appendix A: Technical Support. The appendix informs you how to obtain technical support. Refer to Troubleshooting before contacting Nomadix, Inc. directly.

Glossary of Terms. The glossary provides an explanation of terms directly related to Nomadix product technology. Glossary entries are organized alphabetically.

Index. The index is a valuable information search tool. Use the index to locate specific topics and categories contained in this User Guide.
Welcome to the Access Gateway

The Access Gateway is a freestanding, fully featured network appliance that enables public access service providers to offer broadband Internet connectivity to their customers.

The Access Gateway handles transparent connectivity, advanced security, policy-based traffic shaping, and service placement supporting thousands of users simultaneously in a broadband environment. The Access Gateway also offers a unique set of security and connectivity features for deploying metro wireless 802.11 networks, including Mesh and WiMAX technologies.

The Access Gateway yields a complete solution to a set of complex issues in the Enterprise, Public-LAN, and Residential segments.

Product Configuration and Licensing

All Nomadix Access Gateway products are powered by our patented and patent-pending suite of embedded software, called the Nomadix Service Engine™ (NSE). The Access Gateway employs our NSE core software package and comes pre-packaged with the option to purchase additional modules to expand the product’s functionality.

This User Guide covers all features and functionality provided with the NSE core package, as well as additional optional modules. Your product license must support the optional NSE modules if you want to take advantage of the expanded functionality. The following note will preface procedures that directly relate to optional modules.

See also:

- NSE Core Functionality
- Optional NSE Modules
Key Features and Benefits

The Access Gateway is a 1U high, free-standing or rack-mountable Access Gateway that employs three fast Ethernet ports to interface with the router (one for network side) and the aggregation equipment (two for subscriber side) within the network. It also incorporates an RS232 serial port for connecting to a Property Management System (PMS) and for system management and administration, while maintaining one billing relationship with their chosen provider.

The Access Gateway enables a wide variety of network deployment options for different venue types. For example:

- Allows for flexible WAN Connectivity (T1/E1, Cable, xDSL, and ISDN).
- Supports 802.11a/b/g and hybrid networks utilizing wired Ethernet.
- Supports key requirements needed to be compliant with the Wi-Fi ZONE™ program.
- Allows you to segment your existing network into public and private sections using VLANs, then leverage your existing network investment to create new revenue streams.
- Enables you to provide Wi-Fi access as a billable service or as an amenity to augment the main line of business for your venue.
- Contains an advanced XML interface for accepting and processing XML commands, allowing the implementation of a variety of service plans and offerings.
- Offers three user-friendly ways of remote management—through a Web interface, SNMP MIBs, and Telnet interfaces—allowing for scalable, large public access deployments.

Platform Reliability

The Access Gateway is designed as a network appliance, providing maximum uptime and reliability unlike competitive offerings that use a server-based platform.

Local Content and Services

The Access Gateway’s Portal Page feature intercepts the user’s browser settings and directs them to a designated Web site to securely sign up for service or log in if they have a pre-existing account.

- Allows the provider to present their customers with local services or have the user sign up for service at zero expense.
Offers both pre and post authentication redirects of the user’s browser, providing maximum flexibility in service branding.

**Transparent Connectivity**

Resolving configuration conflicts is difficult and time consuming for network users who are constantly on the move, and costly to the solution provider. In fact, most users are reluctant to make changes to their computer’s network settings and won’t even bother. This fact alone has prevented the widespread deployment of broadband network services.

Our patented Dynamic Address Translation™ (DAT) functionality offers a true “plug and play” solution by enabling a seamless and transparent experience and the tools to acquire new customers on-site.

DAT greatly reduces provisioning and technical support costs and enables providers to deliver an easy to use, customer-friendly service.
Billing Enablement
The Access Gateway supports billing plans using credit cards, scratch cards, or monthly subscriptions, or direct billing to a hotel’s Property Management System (PMS) and can base the billable event on a number of different parameters such as time, volume, IP address type, or bandwidth.

Access Control and Authentication
The Access Gateway ensures that all traffic to the Internet is blocked until authentication has been completed, creating an additional level of security in the network. Also, the Access Gateway allows service providers to create their own unique “walled garden,” enabling users to access only certain predetermined Web sites before they have been authenticated.

Nomadix simultaneously supports the secure browser-based Universal Access Method (UAM), IEEE 802.1x, and Smart Clients for companies such as Adjuno Networks, Boingo Wireless, GRIC and iPass. MAC-based authentication is also available.

Security
The patented iNAT™ (Intelligent Network Address Translation) feature creates an intelligent mapping of IP Addresses and their associated VPN tunnels—by far the most reliable multi-session VPN passthrough to be tested against diverse VPN termination servers from companies such as Cisco, Checkpoint, Nortel and Microsoft. Nomadix’ iNAT feature allows multiple tunnels to be established to the same VPN server, creating a seamless connection for all users on the network.

The Access Gateway provides fine-grain management of DoS (Denial of Service) attacks through its Session Rate Limiting (SRL) feature, and MAC filtering for improved network reliability.

5-Step Service Branding
A network enabled with the Nomadix Access Gateway offers a 5-Step service branding methodology for service providers and their partners, comprising:

1. Initial Flash Page branding.

2. Initial Portal Page Redirect (Pre-Authentication). Typically, this is used to redirect the user to a venue-specific Welcome and Login page.

3. Home Page Redirect (Post-Authentication). This redirect page can be tailored to the individual user (as part of the RADIUS Reply message, the URL is received by the NSE) or set to re-display itself at freely configurable intervals.
4. The Information and Control Console (ICC) contains multiple opportunities for an operator to display its branding or the branding of partners during the user’s session. As an alternative to the ICC, a simple pop-up window provides the opportunity to display a single logo.

5. The “Goodbye” page is a post-session page that can be defined either as a RADIUS VSA or be driven by the Internal Web Server (IWS) in the NSE. Using the IWS option means that this functionality is also available for other post-paid billing mechanisms (for example, post-paid PMS).
NSE Core Functionality

Powering Nomadix’ family of Access Gateways, the Nomadix Service Engine (NSE) delivers a full range of features needed to successfully deploy public access networks. These “core” features solve issues of connectivity, security, billing, and roaming in a Wi-Fi public access network.

The NSE’s core package of features includes:

- Access Control
- Bandwidth Management
- Billing Records Mirroring
- Bridge Mode
- Command Line Interface
- Credit Card
- Dynamic Address Translation™
- Dynamic Transparent Proxy
- End User Licensee Count
- External Web Server Mode
- Home Page Redirect
- iNAT™
- Information and Control Console
- Internal Web Server
- International Language Support
- IP Upsell
- Logout Pop-Up Window
- MAC Filtering
- Multi-Level Administration Support
- NTP Support
- Portal Page Redirect
- RADIUS Client
- RADIUS-driven Auto Configuration
Introduction

- RADIUS Proxy
- Realm-Based Routing
- Remember Me and RADIUS Re-Authentication
- Secure Management
- Secure Socket Layer (SSL)
- Secure XML API
- Session Rate Limiting (SRL)
- Session Termination Redirect
- Smart Client Support
- SNMP Nomadix Private MIB
- Static Port Mapping
- Tri-Mode Authentication
- URL Filtering
- Walled Garden
- Web Management Interface

Access Control

For IP-based access control, the NSE incorporates a master access control list that checks the source (IP address) of administrator logins. A login is permitted only if a match is made with the master list contained within the NSE. If a match is not made, the login is denied, even if a correct login name and password are supplied.

The access control list supports up to 50 (fifty) entries in the form of a specific IP address or range of IP addresses.

The NSE also offers access control based on the interface being used. This feature allows administrators to block access from Telnet, Web Management, and FTP sources.

Administration can now be performed after unblocking the interfaces for the Subscriber side of the NSE. The Administrative ports are configurable as well. See Establishing Secure Administration {Access Control}.

Bandwidth Management

The NSE optimizes bandwidth by limiting bandwidth usage symmetrically or asymmetrically on a per device (MAC address / User) basis, and manages the WAN Link traffic to provide
complete bandwidth management over the entire network. You can ensure that every user has a quality experience by placing a bandwidth ceiling on each device accessing the network, so every user gets a fair share of the available bandwidth.

With the Nomadix ICC feature enabled, subscribers can increase or decrease their own bandwidth and pricing plans for their service dynamically.

**Billing Records Mirroring**

NSE-powered devices can send copies of credit card billing records (and optionally, PMS) to external servers that have been previously defined by system administrators. The NSE assumes control of billing transmissions and the saving of billing records. By effectively “mirroring” the billing data, the NSE can send copies of billing records to predefined “carbon copy” servers. Additionally, if the primary and secondary servers are not responding, the NSE can store up to 2,000 billing records. The NSE regularly attempts to connect with the primary and secondary servers. When a connection is re-established (with either server), the NSE sends the cached information to the server. Customers can be confident that their billing information is secure and that no transaction records are lost.

**Bridge Mode**

This feature allows complete and unconditional access to devices. When Bridge Mode is enabled, your NSE-powered product is effectively transparent to the network in which it is located.

The NSE forwards any and all packets (except those addressed to the NSE network interface). The packets are unmodified and can be forwarded in both directions. The Bridge Mode function is a very useful feature when troubleshooting your entire network as it allows...
administrators to effectively “remove” your product from the network without physically disconnecting the unit.

**Command Line Interface**

The Command Line Interface (CLI) is a character-based user interface that can be accessed remotely or via a direct cable connection. Until your Nomadix product is up and running on the network, the CLI is the Network Administrator’s window to the system. Software upgrades can only be performed from the CLI.

See also “The Management Interfaces (CLI and Web)” on page 31.

**Credit Card**

The Credit Card provides a secure interface over SSL to enable billing via a credit card for High Speed Internet Access (HSIA). This module also includes the Bill Mirror functionality for posting of billing records to multiple sources.

See also:
- “Secure Socket Layer (SSL)” on page 18.

**Dynamic Address Translation™**

Dynamic Address Translation (DAT) enables transparent broadband network connectivity, covering all types of IP configurations (static IP, DHCP, DNS), regardless of the platform or the operating system used—ensuring that everyone gets access to the network without the need for changes to their computer’s configuration settings or client-side software. The NSE supports both PPTP and IPSec VPNs in a manner that is transparent to the user and that provides a more secure standard connection. See also, **Transparent Connectivity**.

**Dynamic Transparent Proxy**

The NSE directs all HTTP and HTTPS proxy requests through an internal proxy which is transparent to subscribers (no need for users to perform any reconfiguration tasks). Uniquely, the NSE also supports clients that dynamically change their browser status from non-proxy to proxy, or vice versa. In addition, the NSE supports proxy ports 80, 800-900, 911 and 990 as well as all unassigned ports (for example, ports above 1024), thus ensuring far fewer proxy related support calls than competitive products.
**End User Licensee Count**

The NSE supports a range of simultaneous user counts depending on the Nomadix Access Gateway you choose. In addition, depending on your platform, various user count upgrades are available for each of our NSE-powered products that allow you to increase the simultaneous user count.

**External Web Server Mode**

The External Web Server (EWS) interface is for customers who want to develop and use their own content. It allows you to create a “richer” environment than is possible with your product’s embedded Internal Web Server.

The advantages of using an External Web Server are:

- Manage frequently changing content from one location.
- Serve different pages depending on site, sub-location (for example, VLAN), and user.
- Take advantage of the comprehensive Nomadix XML API to implement more complex billing plans.
- Recycle existing Web page content for the centrally hosted portal page.

If you choose to use the EWS interface, Nomadix Technical Support can provide you with sample scripts. See also, “Contact Information” on page 311.

**Home Page Redirect**

The NSE supports a comprehensive HTTP redirect logic that allows network administrators to define multiple instances to intercept the browser’s request and replace it with freely configurable URLs.

Portal page redirect enables redirection to a portal page before the authentication process. This means that anyone will get redirected to a Web page to establish an account, select a service plan, and pay for access. Home Page redirect enables redirection to a page after the authentication process (for example, to welcome a specific user to the service—after the user has been identified by the authentication process. See also, Portal Page Redirect.

**iNAT™**

Nomadix invented a new way of intelligently supporting multiple VPN connections to the same termination at the same time (iNAT™), thus solving a key problem of many public access networks.
Nomadix’ patented iNAT™ (intelligent Network Address Translation) feature contains an advanced, real-time translation engine that analyzes all data packets being communicated between the private address realm and the public address realm.

The NSE performs a defined mode of network address translation based on packet type and protocol (for example, GRE, ISAKMP etc.). UDP packet fragmentation is supported to provide more seamless translation engine for certificate-based VPN connections.

If address translation is needed to ensure the success of a specific application (for example, multiple users trying to access the same VPN termination server at the same time), the packet engine selects an IP address from a freely definable pool of publicly routable IP addresses. The same public IP address can be used as a source IP to support concurrent tunnels to different termination devices—offering unmatched efficiency in the utilization of costly public IP addresses. If the protocol type can be supported without the use of a public IP (for example, HTTP, FTP), our proven Dynamic Address Translation™ functionality continues to be used.

Some of the benefits of iNAT™ include:

- Improves the success rate of VPN connectivity by misconfigured users, thus reducing customer support costs and boosting customer satisfaction.
- Maintains the security benefits of traditional address translation technologies while enabling secure VPN connections for mobile workers accessing corporate resources from a public access location.
- Dynamically adjusts the mode of address translation during the user's session, depending on the packet type.
- Supports users with static private IP addresses (for example, 192.168.x.x) or public (different subnet) IP addresses without any changes to the client IP settings.
- Dramatically heightens the reusability factor of costly public IP addresses.

**Information and Control Console**

The Nomadix ICC is a HTML-based pop-up window that is presented to subscribers with their Web browser. The ICC allows subscribers to select their bandwidth and billing options quickly.
and efficiently from a simple pull-down menu. For credit card accounts, the ICC displays a dynamic “time” field to inform subscribers of the time remaining on their account.

Additionally, the ICC contains multiple opportunities for an operator to display its branding or the branding of partners during the user’s session, as well as display advertising banners and present a choice of redirection options to their subscribers.

See also:

- 5-Step Service Branding
- Logout Pop-Up Window
- Information and Control Console

**Internal Web Server**

The NSE offers an embedded Internal Web Server (IWS) to deliver Web pages stored in flash memory. These Web pages are configurable by the system administrator by selecting various parameters to be displayed on the internal pages. When providers or HotSpot owners do not want to develop their own content, the IWS is the answer. A banner at the top of each IWS page is configurable and contains the customer's company logo or any other image file they desire.

To support PDAs and other hand-held devices, the NSE automatically formats the IWS pages to a screen size that is optimal for the particular device being used.

See also:

- 5-Step Service Branding.
- International Language Support.
**International Language Support**

The NSE allows you to define the text displayed to your users by the IWS without any HTML or ASP knowledge. The language you select determines the language encoding that the IWS instructs the browser to use. See also, Internal Web Server.

The available language options are:

- English
- Chinese (Big 5)
- French
- German
- Japanese (Shift_JIS)
- Spanish
- Other, with drop-down menu

**IP Upsell**

System administrators can set two different DHCP pools for the same physical LAN. When DHCP subscribers select a service plan with a public pool address, the NSE associates their MAC address with their public IP address for the duration of the service level agreement. The opposite is true if they select a plan with a private pool address. This feature enables a competitive solution and is an instant revenue generator for ISPs.

The IP Upsell feature solves a number of connectivity problems, especially with regard to L2TP and certain video conferencing and online gaming applications.

**Logout Pop-Up Window**

As an alternative to the ICC, the NSE delivers a HTML-based pop-up window with the following functions:

- Provides the opportunity to display a single logo.
- Displays the session’s elapsed/count-down time.
- Presents an explicit Logout button.

See also, Information and Control Console.
**MAC Filtering**

MAC Filtering enhances Nomadix’ access control technology by allowing system administrators to block malicious users based on their MAC address. Up to 50 MAC addresses can be blocked at any one time. See also, Session Rate Limiting (SRL).

**Multi-Level Administration Support**

The NSE allows you to define 2 concurrent access levels to differentiate between managers and operators, where managers are permitted read/write access and operators are restricted to read access only.

Once the logins have been assigned, managers have the ability to perform all write commands (Submit, Reset, Reboot, Add, Delete, etc.), but operators cannot change any system settings. When Administration Concurrency is enabled, one manager and three operators can access the Access Gateway platform at any one time.

**NTP Support**

The NSE supports Network Time Protocol (NTP), an Internet standard protocol that assures accurate synchronization (to the millisecond) of computer clock times in a network of computers. NTP synchronizes the client’s clock to the U.S. Naval Observatory master clocks. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock.

**Portal Page Redirect**

The NSE contains a comprehensive HTTP page redirection logic that allows for a page redirect before (Portal Page Redirect) and/or after the authentication process (Home Page Redirect). As part of the Portal Page Redirect feature, the NSE can send a defined set of parameters to the portal page redirection logic that allows an External Web Server to perform a redirection based on:

- Access Gateway ID and IP Address
- Origin Server
- Port Location
- Subscriber MAC address
- Externally hosted RADIUS login failure page

This means that the network administrator can now perform location-specific service branding (for example, an airport lounge) from a centralized Web server.

See also, Home Page Redirect.
**RADIUS-driven Auto Configuration**

Nomadix’ unique RADIUS-driven Auto Configuration functionality utilizes the existing infrastructure of a mobile operator to provide an effortless and rapid method for configuring devices for fast network roll-outs. Once configured, this methodology can also be effectively used to centrally manage configuration profiles for all Nomadix devices in the public access network.

Two subsequent events drive the automatic configuration of Nomadix devices:

1. A flow of RADIUS Authentication Request and Reply messages between the Nomadix gateway and the centralized RADIUS server that specifies the location of the meta configuration file (containing a listing of the individual configuration files and their download frequency status) are downloaded from an FTP server into the flash of the Nomadix device.

2. Defines the automated login into the centralized FTP server and the actual download process into the flash.

Optionally, the RADIUS authentication process and FTP download can be secured by sending the traffic through a peer-to-peer IPSec tunnel established by the Nomadix gateway and terminated at the NOC (Network Operations Center). See also, Secure Management.

**RADIUS Client**

Nomadix offers an integrated RADIUS (Remote Authentication Dial-In User Service) client with the NSE allowing service providers to track or bill users based on the number of connections, location of the connection, bytes sent and received, connect time, etc. The customer database can exist in a central RADIUS server, along with associated attributes for each user. When a customer connects into the network, the RADIUS client authenticates the customer with the RADIUS server, applies associated attributes stored in that customer's profile, and logs their activity (including bytes transferred, connect time, etc.). The NSE's RADIUS implementation also handles vendor specific attributes (VSAs), required by WISPs that want to enable more advanced services and billing schemes, such as a per device/per month connectivity fee. See also, RADIUS Proxy.

**RADIUS Proxy**

The RADIUS Proxy feature relays authentication and accounting packets between the parties performing the authentication process. Different realms can be set up to directly channel RADIUS messages to the various RADIUS servers. This functionality can be effectively deployed to:

- Support a wholesale WISP model directly from the edge without the need for any centralized AAA proxy infrastructure.
Support EAP authenticators (for example, WLAN APs) on the subscriber-side of the NSE to transparently proxy all EAP types (TLS, SIM, etc.) and to allow for the distribution of per-session keys to EAP authenticators and supplicants.

Complementing the RADIUS Proxy functionality is the ability to route RADIUS messages depending on the Network Access Identifier (NAI). Both prefix-based (for example, ISP/username@ISP.net) and suffix-based (username@ISP.net) NAI routing mechanisms are supported. Together, the RADIUS Proxy and Realm-Based Routing further support the deployment of the Wholesale Wi-Fi™ model allowing multiple providers to service one location. See also, RADIUS Client.

**Realm-Based Routing**

Realm-Based Routing provides advanced NAI (Network Access Identifier) routing capabilities, enabling multiple service providers to share a HotSpot location, further supporting a Wi-Fi wholesale model. This functionality allows users to interact only with their chosen provider in a seamless and transparent manner.

**Remember Me and RADIUS Re-Authentication**

The NSE’s Internal Web Server (IWS) stores encrypted login cookies in the browser to remember logins, using usernames and passwords. This “Remember Me” functionality creates a more efficient and better user experience in wireless networks.

The RADIUS Re-Authentication buffer has been expanded to 720 hours, allowing an even more seamless and transparent connection experience for repeat users.

**Secure Management**

There are many different ways to configure, manage and monitor the performance and up-time of network devices. SNMP, Telnet, HTTP and ICMP are all common protocols to accomplish network management objectives. And within those objectives is the requirement to provide the highest level of security possible.

While several network protocols have evolved that offer some level of security and data encryption, the preferred method for attaining maximum security across all network devices is to establish an IPSec tunnel between the NOC (Network Operations Center) and the edge device (early VPN protocols such as PPTP have been widely discredited as a secure tunneling method).

As part of Nomadix’ commitment to provide outstanding carrier-class network management capabilities to its family of public access gateways, we offer secure management through the NSE’s standards-driven, peer-to-peer IPSec tunneling with strong data encryption. Establishing the IPSec tunnel not only allows for the secure management of the Nomadix
gateway using any preferred management protocol, but also the secure management of third party devices (for example, WLAN Access Points and 802.3 switches) on private subnets on the subscriber side of the Nomadix gateway. See also, Defining IPSec Tunnel Settings.

Two subsequent events drive the secure management function of the Nomadix gateway and the devices behind it:

1. Establishing an IPSec tunnel to a centralized IPSec termination server (for example, Nortel Contivity). As part of the session establishment process, key tunnel parameters are exchanged (for example, Hash Algorithm, Security Association Lifetimes, etc.).

2. The exchange of management traffic, either originating at the NOC or from the edge device through the IPSec tunnel. Alternatively, AAA data such as RADIUS Authentication and Accounting traffic can be sent through the IPSec tunnel. See also, RADIUS-driven Auto Configuration.

The advantage of using IPSec is that all types of management traffic are supported, including the following typical examples:

- ICMP - PING from NOC to edge devices
- Telnet - Telnet from NOC to edge devices
- Web Management - HTTP access from NOC to edge devices
- SNMP
  - SNMP GET from NOC to subscriber-side device (for example, AP)
  - SNMP SET from NOC to subscriber-side device (for example, AP)
  - SNMP Trap from subscriber-side device (for example, AP) to NOC

**Secure Socket Layer (SSL)**

This feature allows for the creation of an end-to-end encrypted link between your NSE-powered product and wireless clients by enabling the Internal Web Server (IWS) to display pages under a secure link—important when transmitting AAA information in a wireless network when using RADIUS.

SSL requires service providers to obtain digital certificates to create HTTPS pages. Instructions for obtaining certificates are provided by Nomadix.

**Secure XML API**

XML (eXtensible Markup Language) is used by the subscriber management module for user administration. The XML interface allows the NSE to accept and process XML commands from an external source. XML commands are sent over the network to your NSE-powered product which executes the commands, and returns data to the system that initiated the
command request. XML enables solution providers to customize and enhance their product installations.

This feature allows the operator to use Nomadix' popular XML API using the built-in SSL certificate functionality in the NSE so that parameters passed between the Gateway and the centralized Web server are secured via SSL.

If you plan to implement XML for external billing, please contact technical support for the XML specification of your product. Refer to “Contact Information” on page 311.

**Session Rate Limiting (SRL)**

Session Rate Limiting (SRL) significantly reduces the risk of “Denial of Service” attacks by allowing administrators to limit the number of sessions any one user can take over a given time period and, if necessary, then block malicious users.

**Session Termination Redirect**

Once connected to the public access network, the NSE will automatically redirect the customer to a Web site for local or personalized services if the customer logs out or the customer’s account expires while online and the goodbye page is enabled. In addition, the NSE also provides pre- and post-authentication redirects as well as one at session termination.

**Smart Client Support**

The NSE supports authentication mechanisms used by Smart Clients by companies such as Adjungo Networks, Boingo Wireless, GRIC and iPass.

**SNMP Nomadix Private MIB**

Nomadix’ Access Gateways can be easily managed over the Internet with an SNMP client manager (for example, HP OpenView or Castle Rock).

To take advantage of the functionality provided with Nomadix’ private MIB (Management Information Base), simply import the nomadix.mib file from the Accessories CD (supplied with the product) to view and manage SNMP objects on your product.

See also:

- Using an SNMP Manager
- Installing the Nomadix Private MIB
**Static Port Mapping**

This feature allows the network administrator to setup a port mapping scheme that forwards packets received on a specific port to a particular static IP (typically private and misconfigured) and port number on the subscriber side of the NSE. The advantage for the network administrator is that free private IP addresses can be used to manage devices (such as Access Points) on the subscriber side of the NSE without setting them up with Public IP addresses.

**Tri-Mode Authentication**

The NSE enables multiple authentication models providing the maximum amount of flexibility to the end user and to the operator by supporting any type of client entering their network and any type of business relationship on the back end. For example, in addition to supporting the secure browser-based Universal Access Method (UAM) via SSL, Nomadix is the only company to simultaneously support port-based authentication using IEEE 802.1x and authentication mechanisms used by Smart Clients. MAC-based authentication is also available.

See also:
- Access Control and Authentication
- Smart Client Support

**URL Filtering**

The NSE can restrict access to specified Web sites based on URLs defined by the system administrator. URL filtering will block access to a list of sites and/or domains entered by the administrator using the following three methods:

- Host IP address (for example, 1.2.3.4).
- Host DNS name (for example, www.yahoo.com).
- DNS domain name (for example, *.yahoo.com, meaning all sites under the yahoo.com hierarchy, such as finance.yahoo.com, sports.yahoo.com, etc.).

The system administrator can dynamically add or remove up to 300 specific IP addresses and domain names to be filtered for each property.

**Walled Garden**

The NSE provides up to 300 IP passthrough addresses (and/or DNS entries), allowing you to create a “Walled Garden” within the Internet where unauthenticated users can be granted or denied access to sites of your choosing.
**Web Management Interface**

Nomadix’ Access Gateways can be managed remotely via the built-in Web Management Interface where various levels of administration can be established. See also, *Using the Web Management Interface (WMI).*
Optional NSE Modules

**Hospitality Module**

The optional Hospitality Module provides the widest range of Property Management System (PMS) interfaces to enable in-room guest billing for High Speed Internet Access (HSIA) service. This module also includes 2-Way PMS interface capability for in-room billing in a Wi-Fi enabled network. In addition, the Hospitality Module includes the Bill Mirror functionality for posting of billing records to multiple sources. With this module, the NSE also supports billing over a TCP/IP connection to select PMS interfaces.

**PMS Integration**

*Your product license may not support this feature.*

*Some Property Management Systems may require you to obtain a license before integrating the PMS with the Access Gateway. Check with the PMS vendor.*

By integrating with a hotel’s PMS, your NSE-powered product can post charges for Internet access directly to a guest’s hotel bill. In this case, the guest is billed only once. The NSE outputs a call accounting record to the PMS system whenever a subscriber purchases Internet service and decides to post the charges to their room. Nomadix’ Access Gateways are equipped with a serial PMS interface port to facilitate connectivity with a customer’s Property Management System.

**High Availability Module**

*Your product license may not support this feature.*

The optional High Availability Module offers enhanced network uptime and service availability when delivering high-quality Wi-Fi service by providing Fail-Over functionality. This module allows a secondary Nomadix Access Gateway to be placed in the network that can take over if the primary device fails, ensuring Wi-Fi service remains uninterrupted.
Network Architecture (Sample)

The Access Gateway can be deployed effectively in a variety of wireless and wired broadband environments where there are many users—usually mobile—who need high speed access to the Internet.

The following example shows a potential Hospitality application:
Online Help (WebHelp)

The Access Gateway incorporates an online Help system called “WebHelp” which is accessible through the Web Management Interface (when a remote Internet connection is established following a successful installation). WebHelp can be viewed on any platform (for example, Windows, Macintosh, or UNIX-based platforms) using either Internet Explorer or Netscape Navigator (see note).

WebHelp is useful when you have an Internet connection to the Access Gateway and you want to access information quickly and efficiently. It contains all the information you will find in this User Guide.

For more information about WebHelp and other online documentation resources, go to “Online Documentation and Help” on page 35.

Notes, Cautions, and Warnings

The following formats are used throughout this User Guide:

General notes and additional information that may be useful are indicated with a Note.

Cautions and warnings are indicated with a Caution. Cautions and warnings provide important information to eliminate the risk of a system malfunction or possible damage.
Installing the Access Gateway

This section provides installation instructions for the hardware and software components of the Access Gateway. It also includes an overview of the management interface, some helpful hints for system administrators, a Quick Reference Guide, and procedures for the following tasks:

- “Unpacking the Access Gateway” on page 26
- “Powering Up the System” on page 28
- “Logging In to the Command Line Interface” on page 29
- “Establishing the Start Up Configuration” on page 36
- “Logging Out and Powering Down the System” on page 44
- “Connecting the Access Gateway to the Customer’s Network” on page 44
- “Establishing the Basic Configuration for Subscribers” on page 45
- “Archiving Your Configuration Settings” on page 51
- “Installing the Nomadix Private MIB” on page 52

Once you have installed your Access Gateway and established the configuration settings, you should write the settings to an archive file. If you ever experience problems with the system, your archived settings can be restored at any time. See “Archiving Your Configuration Settings” on page 51.
Unpacking the Access Gateway

When you unpack the Access Gateway, you will find the following items in the carton:

<table>
<thead>
<tr>
<th>Item</th>
<th>Qty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Gateway module</td>
<td>1</td>
</tr>
<tr>
<td>Cable – power cord (US or European)</td>
<td>1</td>
</tr>
<tr>
<td>Cable – serial, DB9 female to DB9 female (6ft length) Null Modem (NM) or DB9 female to RJ45 (6ft length) Null Modem (NM)</td>
<td>1</td>
</tr>
<tr>
<td>Cable – CATS5, standard (7 ft. length)</td>
<td>1</td>
</tr>
<tr>
<td>Cable – CATS5, crossover (7 ft. length)</td>
<td>1</td>
</tr>
<tr>
<td>Screw 10-32 X 1/2 PH with internal washer</td>
<td>4</td>
</tr>
<tr>
<td>Screw 4-40 5/16” flathead 100 deg</td>
<td>8</td>
</tr>
<tr>
<td>Plastic bumper feet</td>
<td>4</td>
</tr>
<tr>
<td>Universal mounting bracket</td>
<td>2</td>
</tr>
<tr>
<td>Quick Start Guide</td>
<td>1</td>
</tr>
<tr>
<td>“Accessories” CD-ROM (containing this User Guide, README file, NOMADIX Enterprise MIB file, and any other useful accessories)</td>
<td>1</td>
</tr>
<tr>
<td>Customer letter</td>
<td>1</td>
</tr>
<tr>
<td>End User License Agreement (EULA)</td>
<td>1</td>
</tr>
<tr>
<td>Packing materials (polystyrene end caps)</td>
<td>2</td>
</tr>
</tbody>
</table>
Installation Workflow

The following flowchart illustrates the steps that are required to install and configure your Access Gateway successfully. Review the installation workflow before attempting to install the Access Gateway on the customer’s network.

1. Place the AG on a flat and stable work surface and connect the power cord.
2. Connect the AG to a “live” network. Use the DB9 serial cable (6 ft. length) between the AG’s serial port and your computer.
3. Power up your computer and turn on the AG.
4. Start a HyperTerminal session to communicate with the AG via the serial port.
5. Log in to the Command Line Interface.
6. When prompted, configure your AG’s IP, DNS, and Location settings. The AG will then prompt you to reboot the system.
7. When prompted, accept to the Nomadix End User License Agreement (EULA). You must accept the EULA before the AG can connect with the Nomadix License Key Server. When the key is successfully received from the server, your AG will reboot. You can now power down and connect the AG to the customer’s network.
8. Connect the AG to the customer’s network.
9. Power up the AG and log in via a Telnet session or the Web Management Interface.
10. Set the basic configuration parameters for subscribers.
11. The AG is now ready for administrators to add, delete, or change unique subscriber profiles.
12. Export your configuration settings to an archive file.

Network
Powering Up the System

Use this procedure to establish a direct cable connection between the Access Gateway and your laptop computer, and to power up the system.

1. Place the Access Gateway on a flat and stable work surface.
2. Connect the power cord.
3. Connect the DB9 serial cable between the Access Gateway’s “serial port” or “front Access RJ45 port” and your computer.
4. Turn on your computer and allow it to boot up.
5. Turn on the Access Gateway.
Logging In to the Command Line Interface

Use this procedure to initialize the system and log in to the Access Gateway’s Command Line Interface (CLI). The character-based CLI is used at initial start-up.

1. Start a HyperTerminal™ session to connect to the Access Gateway. Use the following HyperTerminal settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bits per second</td>
<td>9600</td>
</tr>
<tr>
<td>Data bits</td>
<td>8</td>
</tr>
<tr>
<td>Parity</td>
<td>None</td>
</tr>
<tr>
<td>Stop bits</td>
<td>1</td>
</tr>
<tr>
<td>Flow control</td>
<td>None</td>
</tr>
</tbody>
</table>

2. When connected to the Access Gateway, a login prompt appears on your screen. The default login user name is “admin.” The password is “admin.” Login names and passwords are case-sensitive.

3. Enter **admin** when prompted for a user name and password. The *Access Gateway Menu* appears when you have logged in to the Access Gateway’s management interface successfully. If this is an initial installation which requires the Access Gateway to receive...
a license key from the Nomadix License Key Server, you must accept the Nomadix End User License Agreement (EULA).
The Management Interfaces (CLI and Web)

The Access Gateway supports various methods for managing the system remotely. These include, an embedded graphical Web Management Interface (WMI), an SNMP client, or Telnet. However, until the unit is installed and running, system management is performed from the Access Gateway’s embedded CLI via a direct serial cable connection. The CLI can also be accessed remotely.

Until the unit is installed on the customer’s network and a remote connection is established, the CLI is the administrator’s window to the system. This is where you establish all the Access Gateway start-up configuration parameters, depending on the customer’s network architecture.

The Access Gateway Menu is your starting point. From here, you access all the system administration items from the 5 (five) primary menus available:

- Configuration
- Network Info
- Port-location
- Subscribers
- System

Although the basic functional elements are the same, the CLI and the WMI have some minor content and organizational differences. For example, in the WMI the “subscribers” menu is divided into “Subscriber Administration” and “Subscriber Interface.” See also, “Menu Organization (Web Management Interface)” on page 32.

Making Menu Selections and Inputting Data with the CLI

The CLI is character-based. It recognizes the fewest unique characters it needs to correctly identify an entry. For example, in the Access Gateway Menu you need only enter c to access the Configuration menu, but you must enter su to access the Subscribers menu and sy to access the System menu (because they both start with the letter “s”).

You may also do any of the following:

- Enter b (back) or press Esc (escape) to return to a previous menu.
- Press Esc to abort an action at any time.
- Press Enter to redisplay the current menu.
- Press ? at any time to access the CLI’s Help screen.
When using the CLI, if a procedure asks you to “enter sn,” this means you must type `sn` and press the `Enter` key. The system does not accept data or commands until you hit the `Enter` key.

**Menu Organization (Web Management Interface)**

When you have successfully installed and configured the Access Gateway from the CLI, you can then access the Access Gateway from its embedded Web Management Interface (WMI). The WMI is easier to use (point and click) and includes some items not found in the CLI. You can use either interface, depending on your preference.

For a complete description of all features available in the WMI, see “Using the Web Management Interface (WMI)” on page 54.

The following “composite” screen shows how the Access Gateway’s WMI menus (folders) are organized (shown here side-by-side for clarity and space). See also, About Your Product License.
Installing the Access Gateway

Note: Your browser preferences or Internet options should be set to compare loaded pages with cached pages.
**Inputting Data – Maximum Character Lengths**

The following table details the maximum allowable character lengths when inputting data:

<table>
<thead>
<tr>
<th>Data Field</th>
<th>Max. Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Messages (billing options)</td>
<td>72</td>
</tr>
<tr>
<td>All Messages (subscriber error messages)</td>
<td>72</td>
</tr>
<tr>
<td>All Messages (subscriber login UI)</td>
<td>72</td>
</tr>
<tr>
<td>All Messages (subscriber “other” messages)</td>
<td>72</td>
</tr>
<tr>
<td>Description of Service (billing options Plan)</td>
<td>140</td>
</tr>
<tr>
<td>Home Page URL</td>
<td>237</td>
</tr>
<tr>
<td>Host Name and Domain Name (DNS settings)</td>
<td>64</td>
</tr>
<tr>
<td>IP / DNS Name (passthrough addresses)</td>
<td>237</td>
</tr>
<tr>
<td>Label (billing options plan)</td>
<td>16</td>
</tr>
<tr>
<td>Location settings (all fields)</td>
<td>99</td>
</tr>
<tr>
<td>Partner Image File Name</td>
<td>12</td>
</tr>
<tr>
<td>Password (adding subscriber profiles)</td>
<td>128</td>
</tr>
<tr>
<td>Port Description (finding ports by description)</td>
<td>63</td>
</tr>
<tr>
<td>Redirection Frequency (in minutes)</td>
<td>2,147,483,647</td>
</tr>
<tr>
<td></td>
<td>(recommend 3600)</td>
</tr>
<tr>
<td>Reservation Number</td>
<td>24</td>
</tr>
<tr>
<td>Username (adding subscriber profiles)</td>
<td>96</td>
</tr>
<tr>
<td>Valid SSL Certificate DNS Name</td>
<td>64</td>
</tr>
</tbody>
</table>
Online Documentation and Help

The Web Management Interface (WMI) incorporates an online help system which is accessible from the main window.

Other online documentation resources, available from our corporate Web site (www.nomadix.com), include a full PDF version of this User Guide (viewable with Acrobat™ Reader), white papers, technical notes, and business cases. The PDF version of this User Guide and associated README files are also available on the “Accessories” CD-ROM supplied with your Access Gateway.
Quick Reference Guide

This manual contains a “Quick Reference Guide” on page 36 which provides information to help you navigate and use the management interfaces (CLI and Web) quickly and efficiently. It also contains the product specifications, a listing of the factory default settings, sample log reports, listings of commands (by menu and alphabetical), HyperTerminal settings, and some common keyboard shortcuts.

Establishing the Start Up Configuration

The CLI allows you to administer the Access Gateway’s start-up configuration settings.

When establishing the start-up configuration for a new installation, you are connected to the Access Gateway via a direct serial connection (you do not have remote access capability because the Access Gateway is not yet configured or connected to a network). Once the installation is complete (see “Installation Workflow” on page 27) and the system is successfully configured, you will have the additional options of managing the Access Gateway remotely from the system’s Web Management Interface, an SNMP client manager of your choice, or a simple Telnet interface.

The start up configuration must be established before connecting the Access Gateway to a customer’s network. The “start up” configuration settings include:

- **Assigning Login User Names and Passwords** – You must assign a unique login user name and password that enables you to administer and manage the Access Gateway securely.

  User names and passwords are case-sensitive.

- **Setting the SNMP Parameters (optional)** – The SNMP (Simple Network Management Protocol) parameters must be established before you can use an SNMP client (for example, HP OpenView) to manage and monitor the Access Gateway remotely.

- **Enabling the Logging Options (recommended)** – Servers must be assigned and set up if you want to create system and AAA (billing) log files, and retrieve error messages generated by the Access Gateway.
Assigning the Location Information and IP Addresses:

- **Assigning the Network Interface IP Address** - This is the public IP address that allows administrators and subscribers to see the Access Gateway on the network. Use this address when you need to make a network connection with the Access Gateway.

- **Assigning the Subnet Mask** – The subnet mask defines the number of IP addresses that are available on the routed subnet where the Access Gateway is located.

- **Assigning the Default Gateway IP Address** – This is the IP address of the router that the Access Gateway uses to transmit data to the Internet.

**Assigning Login User Names and Passwords**

When you initially powered up the Access Gateway and logged in to the Management Interface, the default login user name and password you used was “admin.” The Access Gateway allows you to define 2 concurrent access levels to differentiate between managers and operators, where managers are permitted read/write access and operators are restricted to read access only. Once the logins have been assigned, managers have the ability to perform all write commands (Submit, Reset, Reboot, Add, Delete, etc.), but operators cannot change any system settings. When Administration Concurrency is enabled, one manager and three operators can access the Access Gateway at any one time (the default setting for this feature is “disabled”).

1. Enter `sy` (system) at the Access Gateway Menu. The System menu appears.
2. Enter `lo` (login).

   The system prompts you for the current login. If this is the first time you are changing the login parameters since initializing the Access Gateway, the default login name and password is “admin.”

   - The system accepts up to 11 characters (any character type) for user names and passwords. All user names and passwords are case-sensitive.

3. When prompted, confirm the current login parameters and enter new ones.

   **Sample Screen Response:**
   ```
   System>lo
   Enable/Disable Administration Concurrency [disabled]: e
   Current login: admin
   Current password: *****
   Enter new manager login: newmgr
   Enter new password: *******
   Retype new password: *******
   ```
The administrative login and password were changed
Enter new operator login: newop
Enter new operator password: *****
Retype new operator password: *****
The operator login and password were changed

Enter RADIUS remote test login: rad
Enter new RADIUS remote test password: *****
Retype new RADIUS remote test password: *****
The RADIUS remote test login and password were changed

You must use the new login user name(s) and password(s) to access the system.

Setting the SNMP Parameters (optional)
You can address the Access Gateway using an SNMP client manager (for example, HP OpenView). SNMP is the standard protocol that regulates network management over the Internet. To do this, you must set up the SNMP communities and identifiers. For more information about SNMP, see “Using an SNMP Manager” on page 54.

If you want to use SNMP, you must manually turn on SNMP.

1. Enter c (configuration) at the Access Gateway Menu. The Configuration menu appears.
2. Enter sn (snmp).
3. Enable the SNMP daemon, as required. The system displays any existing SNMP contact information and prompts you to enter new information. If this is the first time you have initialized the SNMP command since removing the Access Gateway from its box, the system has no information to display (there are no defaults).
4. Enter the SNMP parameters (communities and identifiers). The SNMP parameters include your contact information, the get/set communities, and the IP address of the trap recipient. Your SNMP manager needs this information to enable network management over the Internet.
5. If you enabled the SNMP daemon, you must reboot the system for your changes to take effect. In this case, enter y (yes) to reboot your Access Gateway.

Sample Screen Response:
Configuration>sn
Enable the SNMP Daemon? [Yes]:
Enter new system contact: newname@domainname.com [Nomadix, Newbury Park, CA]
Enter new system location: Office, Newbury Park, CA
Enter read/get community [public]:
Enter write/set community [private]:
Enter IP of trap recipient [0.0.0.0]: 10.11.12.13

SNMP Daemon: Enabled
System contact: newname@domainname.com
System location: Office, Newbury Park, CA
Get (read) community: public
Set (write) community: private
Trap recipient: 10.11.12.13

Reboot to enable new changes? [yes/no] y
Rebooting...

You can now address the Access Gateway using an SNMP client manager.

**Enabling the Logging Options (recommended)**

System logging creates log files and error messages generated at the system level. AAA logging creates activity log files for the AAA (Authentication, Authorization, and Accounting) functions. You can enable either of these options.

> Although the AAA and billing logs can go to the same server, we recommend that they have their own unique server ID number assigned (between 0 and 7). When managing multiple properties, the properties are identified in the log files by their IP addresses.

When system logging is enabled, the standard SYSLOG protocol (UDP) is used to send all message logs generated by the Access Gateway to the specified server.

1. Enter **log** (logging) at the **Configuration** menu. The system displays the current logging status (enabled or disabled).
2. Enable or disable the system and/or AAA logging options, as required. If you enable either option, go to Step 3, otherwise logging is disabled and you can terminate this procedure.
3. Assign a valid ID number (0-7) to each server.
4. Enter the IP addresses to identify the location of the system and AAA SYSLOG servers on the network (the default for both is 0.0.0.0).

When logging is enabled, log files and error messages are sent to these servers for future retrieval. To see sample reports, go to “Sample SYSLOG Report” on page 278 and “Sample AAA Log” on page 277.
Sample Screen Response:

Configuration>log

Enable/disable System Log [disabled]: enable
Enter System Log Number (0-7) [0]: 2
Enter System Log Filter

0: Emergency
1: Alert
2: Critical
3: Error
4: Warning
5: Notice
6: Info
7: Debug

Select an option from above [7]: 7
Enter System Log Server IP [255.255.255.255]: 10.10.10.10
Enable/disable System Log Save to file [disabled]: enable

Enable/disable AAA Log [disabled]: enable
Enter AAA Log Number (0-7) [0]: 2
Enter AAA Log Filter

0: Emergency
1: Alert
2: Critical
3: Error
4: Warning
5: Notice
6: Info
7: Debug

Select an option from above [7]: 7
Enter AAA Log Server IP [255.255.255.255]: 10.10.10.10
Enable/disable AAA Log Save to file [disabled]: enable

Enable/disable RADIUS History Log [disabled]: enable
Enter RADIUS History Log Number (0-7) [0]: 2
Enter RADIUS History Log Filter

0: Emergency
1: Alert
2: Critical
3: Error
4: Warning
5: Notice
6: Info
7: Debug

Select an option from above    [6]: 7
Enter RADIUS History Log Server IP   [255.255.255.255]: 10.10.10.10
Enable/disable RADIUS History Log Save to file [disabled]: enable

Enable/disable System Report Log [disabled]: enable
Enter System Report Log Number (0-7) [0]: 2
Enter System Report Log Server IP   [255.255.255.255]: 10.10.10.10
Enter System Report Log interval (minutes) [0]: 5

Enable/disable Tracking Log [disabled]: enable
Enter Tracking Log Number (0-7) [0]: 2
Enter Tracking Log Server IP   [255.255.255.255]: 10.10.10.10
Enable/Disable Tracking Log Save to file [disabled]:
Enable/Disable Name Reporting [disabled]: enable
Enable/Disable Port Reporting [disabled]: enable
Enable/Disable Location Reporting [disabled]: enable
Enable/Disable 500th Packet Count Reporting [disabled]: enable

<table>
<thead>
<tr>
<th>System Log</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Log Number</td>
<td>2</td>
</tr>
<tr>
<td>System Log Filter</td>
<td>7</td>
</tr>
<tr>
<td>System Log Server IP</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>System Log Save to file</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AAA Log</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA Log Number</td>
<td>2</td>
</tr>
<tr>
<td>AAA Log Filter</td>
<td>7</td>
</tr>
<tr>
<td>AAA Log Server IP</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>AAA Log Save to file</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RADIUS History Log</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS History Log Number</td>
<td>2</td>
</tr>
<tr>
<td>RADIUS History Log Filter</td>
<td>7</td>
</tr>
<tr>
<td>RADIUS History Log Server IP</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>RADIUS History Log Save to file</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Report Log</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Report Log Number</td>
<td>2</td>
</tr>
<tr>
<td>System Report Log Server IP</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>System Report Log Interval (in minutes)</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tracking Log</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking Log Number</td>
<td>2</td>
</tr>
<tr>
<td>Tracking Log Server IP</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>Tracking Log Save to file</td>
<td>Disabled</td>
</tr>
<tr>
<td>Tracking Name Reporting</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
Assigning the Location Information and IP Addresses

The “location” command in the Configuration menu establishes the Access Gateway’s location settings, the network interface IP address, the subnet mask, and the default gateway IP address. All of these Access Gateway “location” parameters must be set up as part of the system’s start up configuration (otherwise the Access Gateway will not be “visible” on the network).

1. Enter c (configuration) at the Access Gateway Menu. The Configuration menu appears.
2. Enter loc (set Location options). The system displays the Company Name. If the name displayed is not correct (or no name is entered), enter it now.
3. When prompted, enter the company’s address (line by line - 6 lines).
4. When prompted, enter a valid email address for this company.

   The system now displays the current network interface IP address (the default address is 10.0.0.10) and prompts you for a valid address. The network interface IP address is the public IP address that allows administrators to see the Access Gateway on the network. Use this address when you need to make a network connection with the Access Gateway.

   The network interface address must be on the same subnet.

5. When prompted, enter a valid network interface IP address.
   The IP addresses from subscribers that are on a subnet different from the Access Gateway (for example, misconfigured) are translated by Nomadix’ Dynamic Address Translation (DAT).
6. Enter a valid subnet mask.
   After assigning the subnet mask, the system displays the current default gateway IP address (the factory default is 10.0.0.1). This is the IP address of the router that the Access Gateway uses to transmit data to the Internet.
7. Enter a valid default gateway IP address.
8. After establishing all “Location” settings, you must reboot the Access Gateway for your changes to take effect.
**Sample Screen Response:**

```
Configuration>loc
Please enter your company name [companyname]: newname
Please enter your site name [sitename]: Coffee House
Please enter your address <Line 1> [line1address]: newline1
   <Line 2> [line2address]: newline2
   <City> [city]: newcity
   <State> [state]: newstate
   <Zip/Postal Code> [zip]: newzip
   <Country> [country]: newcountry
Please enter your email address [em@em.com]: newmail@email.com
Please enter a number from the above list [  1]:
```

1. Apartment
2. Bar/Coffee/Restaurant
3. Convention Center
4. Corporate Guest Access
5. Education
6. Hospitality
7. Marina/Camp Ground
8. Public Space
9. Public Transport
10. Airport
11. Truckstop / Rest Area
12. Car Rental Facility
13. Club
14. Health Club
15. Bar
16. Retail Business
17. Marina
18. Arena
19. Theatre
20. Metro Area / HotZone
21. Indoor Public Space / Hospital / Museum / Library
22. Gas Station
23. Resort
24. Lab / Test
25. Other

Please enter a number from the above list [  1]:

Select Network Interface Configuration Mode:

0 - Static
1 - DHCP Client
2 - PPPoE Client

Select the Network Interface Configuration Mode [0]:

Enter network interface IP [ ]:
Enter subnet mask [ ]:
Enter default gateway IP [ ]:
Please enter your ISO country code [US]: US
Please enter your phone country code [1]: 1
Please enter your calling area code [818]: 818
Please enter your network SSID/Zone [ ]: samplezonename

The system must be reset to function properly. Reboot? [yes/no]: y

Your new settings are displayed and the Access Gateway reboots. When the system restarts, the Telnet interface is enabled (based on your new configuration settings which are saved to the Access Gateway’s on-board flash memory).

Start up configuration is now complete; however, before connecting the Access Gateway to the customer’s network, you must power down the system.

Go to “Logging Out and Powering Down the System” on page 44.

Logging Out and Powering Down the System

Use this procedure to log out and power down the Access Gateway.

1. Enter l (logout) at the Access Gateway Menu. Your serial session closes automatically.
2. Turn off the Access Gateway and disconnect the power cord.
3. Disconnect the serial cable between the Access Gateway and your computer.

Connecting the Access Gateway to the Customer’s Network

Use this procedure to connect the Access Gateway to the customer’s network (after the start up configuration parameters have been established).

1. Choose an appropriate physical location that allows a minimum clearance of 4cm either side of the unit (for adequate airflow).
2. Connect the Access Gateway to the router, then connect the Access Gateway to the customer’s subscriber port.
3. Connect the power cord and turn on the Access Gateway.
4. Go to “Establishing the Basic Configuration for Subscribers” on page 45.

Establishing the Basic Configuration for Subscribers

When you have successfully established the start up configuration and installed the unit onto the customer’s network, connect to the Access Gateway via Telnet. You must now set up the basic configuration parameters for subscribers, including:

- **Setting the DHCP Options** – DHCP (Dynamic Host Configuration Protocol) allows you to assign IP addresses automatically (to subscribers who are DHCP enabled). The Access Gateway can “relay” the service through an external DHCP server or it can be configured to act as its own DHCP server.

- **Setting the DNS Options** – DNS (Domain Name System) allows subscribers to enter meaningful URLs into their browsers (instead of complicated numeric IP addresses). DNS converts the URLs into the correct IP addresses automatically.

**Setting the DHCP Options**

When a device connects to the network, the DHCP server assigns it a “dynamic” IP address for the duration of the session. Most users have DHCP capability on their computer. To enable this service on the Access Gateway, you can either enable the DHCP relay (routed to an external DHCP server IP address), or you can enable the Access Gateway to act as its own DHCP server.
server. In both cases, DHCP functionality is necessary if you want to automatically assign IP addresses to subscribers.

The Access Gateway’s adaptive configuration technology provides Dynamic Address Translation (DAT) functionality. DAT is automatically configured to facilitate “plug-and-play” access to subscribers who are misconfigured with static (permanent) IP addresses, or subscribers that do not have DHCP capability on their computers. DAT allows all users to obtain network access, regardless of their computer’s network settings.

1. Enter c (configuration) at the Access Gateway Menu. The Configuration menu appears.
2. Enter dh (dhcp).

By default, the Access Gateway is configured to act as its own DHCP server and the relay feature is “disabled.” Please verify that your DHCP Server supports DHCP packets before enabling the relay. Not all devices containing DHCP servers (for example, routers) support DHCP Relay functionality.

When assigning a DHCP Relay Agent IP address for the DHCP Relay, ensure that the IP address you use does not conflict with devices on the network side of the Access Gateway.

Although you cannot enable the DHCP relay and the DHCP service at the same time, it is possible to “disable” both functions from the Command Line Interface. In this case, a warning message informs you that no DHCP services are available to subscribers.

3. Follow the on-screen instructions to set up your DHCP options. For example:

Sample Screen Response:

```
Configuration>dh
Enable/Disable IP Upsell   [disabled]:
Enable/Disable DHCP Relay  [disabled]:
Enable/Disable DHCP Server [enabled]:
Enable/Disable Subnet-based DHCP Service [disabled]
Enable/Disable Forwarded DHCP Clients [disabled]:
IP Upsell                Disabled
DHCP Relay               Disabled
External DHCP Server IP   0.0.0.0
DHCP Relay Agent IP      0.0.0.0
DHCP Server              Enabled
DHCP Server Subnet-based Disabled
Forwarded DHCP Clients   Disabled
```
DHCP Options from RFC 2132

You can configure DHCP options as defined in RFC 2132. The configured options are sent to subscribers who obtain their network configuration from the NSE via DHCP.

This capability only applies to the NSE’s DHCP Server function. There is no change to the NSE’s operation as a DHCP client.

The options are configurable on a per-pool basis. Different sets of options can be configured for different pools.

A given DHCP option consists of an option code and a value. RFC 2132 details the various available options, and the data type for each. The NSE will validate the data entered to ensure that it is type-correct for the option code in question. If it is incorrect, the option is not accepted.

Numerical integer values can be entered in decimal format, or hex format using a “0x” prefix.

The following DHCP option codes are supported:

<table>
<thead>
<tr>
<th>Option Description</th>
<th>Option Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single IP address</td>
<td>16, 28, 32</td>
</tr>
<tr>
<td>List of one or more IP addresses</td>
<td>3-5, 7-11, 41-42, 44-45, 48-49, 65, 69-76</td>
</tr>
<tr>
<td>List of zero or more IP addresses</td>
<td>68</td>
</tr>
<tr>
<td>List of one or more pairs of IP addresses (or address/mask pairs)</td>
<td>21, 33</td>
</tr>
</tbody>
</table>

After setting up your DHCP options, the system must be rebooted for your changes to take effect.
Disallowed options: Some option codes are not allowed, for one of the following reasons:

- Items that are already configured elsewhere as a separate DHCP pool or NSE configuration parameter, and/or are derived from one that is. Includes options 1 (subnet mask), 3 (router), 6 (domain name server), 15 (domain name), 51 (lease time), 54 (server identifier), 58 (renewal time), 59 (rebinding time).

- Items not valid in a DHCP offer or ACK message. Includes options 50 (requested IP address), 55 (parameter request list), 56 (error message), 57 (maximum message size), 60 (vendor class identifier), 61 (client identifier).

- Items generated automatically by the mechanism of DHCP message construction, which carry no application information. Includes options 0 (pad), 52 (option overload), 53 (DHCP message type), 255 (end).

Unrecognized options: Options 62-63, 77-254 are unrecognized. Some of these codes are legitimate and are defined in other RFCs, while others are not defined. These option codes are not explicitly disallowed on the NSE, but the NSE is “unaware” of them – that is, it will make no attempt to validate either the code or the data. It is the administrator’s responsibility to ensure that the option codes and data entered are legitimate.

The following screens illustrate adding additional DHCP options to a DHCP Pool.
Edit a DHCP Pool

- **DHCP Server IP**: 10.0.0.4
- **DHCP Server Netmask**: 255.255.255.0
- **DHCP Pool Start IP**: 10.0.0.11
- **DHCP Pool Stop IP**: 10.0.0.100
- **DHCP Lease Minutes**: 60
- **Router**: DHCP Server IP
- **Specify**: [ ]

Options:
- [ ] Public Pool
- [ ] Private Pool
- [ ] IP Upsell Pool
- [ ] Default Pool

**Note:** Please make sure pools do not overlap.

### Additional DHCP Options

**Add/Modify an option:**
(Data may be entered as ASCII text, or in hex format by prefixing with "0x". For hex data expressing 32-bit, 16-bit, or 8-bit integer values, an appropriate number of leading zeroes must be entered.)

- **Code**: 0
- **Data**: [ ]

**Existing additional options:**

<table>
<thead>
<tr>
<th>Code</th>
<th>Data</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>66</td>
<td>httpserver.xycgwpgw.com</td>
<td>Edit, Delete</td>
</tr>
<tr>
<td>24</td>
<td>10005675</td>
<td>Edit, Delete</td>
</tr>
</tbody>
</table>
Setting the DNS Options

DNS allows subscribers to enter meaningful URLs into their browsers (instead of complicated numeric IP addresses) by automatically converting the URLs into the correct IP addresses. You can assign a primary, secondary, or tertiary (third) DNS server. The Access Gateway utilizes whichever server is currently available.

You must configure DNS if you want to enter meaningful URLs instead of numeric IP addresses into any of the Access Gateway’s configuration screens.

Use the following procedure to set the DNS configuration options.

1. Enter c (configuration) at the Access Gateway Menu. The Configuration menu appears.
2. Enter dn (dns) at the Configuration menu. The system displays the current domain (the default is “nomadix”).
3. Enter a valid domain name (the Internet domain that DNS requests will utilize).
4. Enter the host name (the DNS name of the Access Gateway). The host name must not contain any spaces.

After assigning the host name, the system requests IP addresses for the primary, secondary, and tertiary DNS servers (the default for the DNS primary address is 0.0.0.2).

*The secondary and tertiary DNS servers are only utilized if the primary DNS server is unavailable.*

5. Enter the IP addresses for the DNS servers (located at the customer’s network operating center where DNS requests are sent).

6. You must now reboot the system for your settings to take effect. Enter `y` (yes) to reboot the Access Gateway.

**Sample Screen Response:**

```
Configuration>dns
```

NOTE: If DHCP Client or PPPoE Client is enabled, the Primary and Secondary DNS Server may not be configured, since the DHCP/PPPoE server may provide those items. Furthermore, if DHCP Client is configured, the Domain may not be configured.

```
Enter domain                       [nomadix.com ]:
Enter host name (no spaces)  [usg           ]:
Enter primary DNS            [0.0.0.2 ]: 4.2.2.2
Enter secondary DNS        [0.0.0.0 ]:
Enter tertiary DNS             [0.0.0.0      ]:
Enter DNS Redirection Port [1029         ]:
Enter Proxy DNS Port         [1028         ]:
```

The system must be rebooted to function properly.

The DNS options have been established. DNS will now convert subscriber browser URLs into the correct IP addresses automatically.

**Archiving Your Configuration Settings**

Once you have installed your Access Gateway and established the configuration settings, you should write the settings to an archive file. If you ever experience problems with the system, your archived settings can be restored at any time.

Refer to the following procedures:

- “Exporting Configuration Settings to the Archive File {Export}” on page 223.
- “Importing Configuration Settings from the Archive File {Import}” on page 228.
Installing the Nomadix Private MIB

The Nomadix Private MIB is supplied on the “Accessories” CD-ROM, delivered with your Access Gateway. After importing the *nomadix.mib* file from the CD-ROM you will be able to view and manage SNMP objects on your Access Gateway.

**Procedure**

1. Import the *nomadix.mib* file into your SNMP client manager.

2. Connect to the Access Gateway from a node on the network that is accessible via the Access Gateway’s network port (Internet, LAN, etc.). Be sure to enable the SNMP daemon on the Access Gateway (available on the Access Gateway’s CLI or Web Management Interface, under the *Configuration* menu – **snmp**).

3. All variables defined by Nomadix start with the following prefix:
   
   iso.org.dod.internet.private.enterprises.nomadix

4. You should now be able to define queries and set the SNMP values on your Access Gateway. If necessary, consult this User Guide or your SNMP client manager’s documentation for further details.

   *We recommend that you change the predefined community strings in order to maintain a secure environment for your Access Gateway.*
System Administration

This chapter provides all the instructions and procedures necessary for system administrators to manage the Access Gateway on the customer’s network (after a successful installation).

The system administration procedures in this section are organized as they are listed under their respective Web Management Interface (WMI) menus:

- “Configuration Menu” on page 56
- “Network Info Menu” on page 153
- “Port-Location Menu” on page 161
- “Subscriber Administration Menu” on page 173
- “Subscriber Interface Menu” on page 187
- “System Menu” on page 220

Now that the Access Gateway has been installed and configured successfully, this User Guide moves away from the Command Line Interface (CLI) and documents the Access Gateway from the Web Management Interface (WMI) viewpoint.

Choosing a Remote Connection

Once installed and configured for the customer’s network, the Access Gateway can be managed and administered remotely with any of the following interface options:

- **Using the Web Management Interface (WMI)** - Provides a powerful and flexible Web interface for network administrators.
- **Using an SNMP Manager** - Allows remote “Windows” management using an SNMP client manager (for example, HP OpenView). However, before you can use SNMP to access the Access Gateway, you must set up the appropriate SNMP communities. For more information, refer to “Managing the SNMP Communities {SNMP}” on page 140.
- **Using a Telnet Client**

To use any of the remote connections (Web, SNMP, or Telnet), the network interface IP address for the Access Gateway must be established (you did this during the installation process).

Choose an interface connection, based on your preference.
Using the Web Management Interface (WMI)

The Web Management Interface (WMI) is a “graphical” version of the Command Line Interface, comprised of HTML files. The HTML files are embedded in the Access Gateway and are dynamically linked to the system’s functional command sets. You can access the WMI from any Web browser.

To connect to the Web Management Interface, do the following:

1. Establish a connection to the Internet.
2. Open your Web browser.
3. Enter the network interface IP address of the Access Gateway (set up during the installation process).
4. Log in as usual (supplying your user name and password).

To access any menu item from the WMI, simply click on the item you want. The corresponding work screen then appears in the right side frame. From here you can control the features and settings related to your selection. Although the appearance is very different from the Command Line Interface, the information displayed to you is basically the same. The only difference between the two interfaces is in the method used for making selections and applying your changes (selections are checkable boxes, and applying your changes is achieved by pressing the Submit button). Pressing the Reset button resets the screen to its previous state (clearing all your changes without applying them).

Using an SNMP Manager

Once the SNMP communities are established, you can connect to the Access Gateway via the Internet using an SNMP client manager (for example, HP OpenView). SNMP is the standard protocol used in the Network Management (NM) system. This system contains two primary elements:

- **Manager** – The console (client) through which system administrators perform network management functions.
- **Agent** – An SNMP-compliant device which stores data about itself in a Management Information Base (MIB). The Access Gateway is an example of such a device.

The Access Gateway contains managed objects that directly relate to its current operational state. These objects include hardware configuration parameters and performance statistics.
Managed objects are arranged into a virtual information database, called a Management Information Base (MIB). SNMP enables managers and agents to communicate with each other for the purpose of accessing these MIBs and retrieving data. See also, “Installing the Nomadix Private MIB” on page 52.

The following example shows a (partial) SNMP screen response.

![SNMP Screen Response]

**Using a Telnet Client**

There are many Telnet clients that you can use to connect with the Access Gateway. Using Telnet provides a simple terminal emulation that allows you to see and interact with the Access Gateway’s Command Line Interface (as if you were connected via the serial interface). As with any remote connection, the network interface IP address for the Access Gateway must be established (you did this during the installation process).

**Logging In**

To access the Access Gateway’s Web Management Interface, use the Manager or Operator login user name and password you defined during the installation process (refer to Assigning Login User Names and Passwords).

*User names and passwords are case-sensitive.*

**About Your Product License**

Some features included in this section will not be available to you unless you have purchased the appropriate product license from Nomadix. In this case, the following statement will
Defining the AAA Services {AAA}

This procedure shows you how to set up the AAA (Authentication, Authorization, and Accounting) service options. AAA Services are used by the Access Gateway to authenticate, authorize, and subsequently bill subscribers for their use of the customer’s network. The Access Gateway currently supports several AAA models which are discussed in “Subscriber Management” on page 248.

1. From the Web Management Interface, click on Configuration, then AAA. The Authentication, Authorization, and Accounting Settings screen appears:

Your product license may not support this feature. You can upgrade your product license at any time.
## Authentication Authorization and Accounting Settings

**AAA Services**
- Enable

**Logout IP:**
- 1.1.1.1

**XML Interface**
- Enable
  - XML SERVER 1 IP
  - XML SERVER 2 IP
  - XML SERVER 3 IP
  - XML SERVER 4 IP

**Print Billing Command**
- Enable
  - Print Server URL

**AAA Passthrough Port**
- Enable
  - Port 443

**802.1X Authentication Support**
- Enable

**Notes:** 802.1x requires that both AAA and RADIUS Authentication be enabled.

**802.1X Reauth Period (secs):**
- 0

**Enable Origin Server (OS) parameter encoding for Portal Page and EWS**
- Enable

**Enable fallback to Internal Web Server Authentication if Portal Page/External Web Server is not reachable**
- Enable

**Port-based billing policies**
- Enable

**HTTP8 Redirection**
- Enable
Select one of the following:

**Internal Web Server**

- **SSL Support**
  - [ ] Enable

- **Encrypt only Sensitive Data**
  - [ ] Enable

*Note: To enable, make sure your license includes SSL support and you have all the certificate files in the flash.*

- **Certificate DNS Name**
  - [ ] certificate.com

- **Portal Page**
  - [ ] Enable

- **Portal Page URL**
  - 

- **Parameter Passing**
  - [ ] Enable

- **Parameter Signing**
  - Method:
    - None
    - HASH-CRC32
    - HMAC-MD5
  - [ ] UI
  - [ ] MA
  - [ ] RN
  - [ ] PORT
  - [ ] SIP
  - [ ] (write-only)

- **Manual Passsthrough Address**
  - [ ] Enable

- **Portal XML POST URL**
  - 

- **Portal XML Post Port**
  - 9000

- **Supports GIS Clients**
  - [ ] Yes

- **Enroll IWS Login Page**
  - [ ] Yes

- **Usernames**
  - [ ] Enable

*Note: Usernames option is enabled if any of the following are true: Relogin After Timeout, Relogin after Migration, Xover/Y billing, or Group Accounts.*

- **New Subscribers**
  - [ ] Enable

- **Credit Card Service**
  - [ ] Enable

- **Credit Card Server**
  - [ ] Enable

- **Credit Card Server URL**
  - [ ] Authorize.net

- **Merchant ID**
  - 

- **Use NBI's hostname and DNS domain name**
  - [ ] Enable

- **Authorize.net**
  - [ ] Enable

  - Change Transaction Key
    - [ ] Enable (write-only)

  - Set MD5 Hash Value (Shared Secret)
    - [ ] Enable (write-only)

- **Churn Reinit:**
  - Credit Card Transaction Time
    - [ ] 3 minutes

- **Smart Client Support**
  - [ ] Enable

*Note: To enable, make sure your license includes Smart Client support.*

**External Web Server**

- **Secret Key**
  - [ ] bigbrowndog

- **External login page URL**
  - [ ] http://usg.nomadic.com/usg/newuser/login.as

- **Parameter Signing**
  - Method:
    - None
    - HASH-CRC32
    - HMAC-MD5
  - [ ] UI
  - [ ] MA
  - [ ] RN
  - [ ] PORT
  - [ ] SIP
  - [ ] (write-only)

- **Restart after changes are saved?**
  - [ ] Yes

*Warning: Changing URLs on this page may result in removal of the hostname portion of the URL from the Passsthrough Addresses. Verification of Passsthrough Addresses configuration is recommended. This warning pertains to: 1) Portal Page URL, 2) Portal XML POST URL, 3) Credit Card Server URL, and 4) External login page URL.*
2. Enable or disable **AAA Services**. If you enable **AAA Services**, go to Step 3, otherwise this feature is disabled and you can exit the procedure.

3. Select a **Logout IP** address from the drop-down list. The list contains IP address that can be used as the logout IP address. The default IP address is 1.1.1.1.

4. Enable or disable the **XML Interface**, as required.

   XML (eXtensible Markup Language) is used by the Access Gateway’s subscriber management module for port location and user administration. Enabling the XML interface allows the Access Gateway to accept and process XML commands from an external source. XML commands are sent over the network to the Access Gateway. The Access Gateway parses the query string, executes the commands specified by the string, and returns data to the system that initiated the command request.

5. If you enabled the **XML Interface** feature, enter the **XML IP** (server) address.

6. Enable or disable **Print Billing Command**, as required. This feature enables NSE to support Driverless Print servers. If this feature is enabled, you must enable the XML interface and enter the IP address for the XML interface (Step 3 and Step 4). With Print Billing enabled, print servers can bill subscribers’ rooms for printing their documents without them having to install printers.

   The DNS name print.server.com will internally resolve to the Configured Print Server URL that is entered in the configuration. When subscribers are redirected to the Print Server the NSE adds Parameters to that request, so that the Server is able to charge the proper subscriber.

   With these variables sent to the server it can now send the XML command to bill the users properly.

   Print Server IP needs to be entered as one of the XML server IP for the command to successfully complete.

   The XML command is:

   ```
   <USG COMMAND="BILL_PRINT" IP_ADDR="">
     <ROOM_NUM></ROOM_NUM>
     <DOC_NAME></DOC_NAME>
     <NUM_COPIES></NUM_COPIES>
     <NUM_PAGES></NUM_PAGES>
     <COST></COST>
     <TIME_SUBMITTED></TIME_SUBMITTED>
   </USG>
   ```

   Subscribers could get to print.server.com by:

   - ICC button link
   - Printout in the hotel room
60 System Administration

- Link from the hotel’s HPR Page.

Your product license may not support this feature.

7. Enable or disable the **AAA Passthrough Port** feature, as required. System administrators can set the Access Gateway to pass-through HTTPS traffic, in addition to standard port 80 traffic, without being redirected. When access to a non-HTTPS address (for example, a Search Engine or News site) has been requested, the subscriber is then redirected as usual.

8. If AAA passthrough is enabled, enter the corresponding port number.

The port number must be different than 80, 2111, 1111, or 1112.

9. Enable or disable the **802.1x Authentication Support** feature, as required.

Both AAA and RADIUS Authentication must be enabled for 802.1x Authentication support.

10. Enable or disable the **Origin Server (OS) parameter encoding for Portal Page and EWS** feature, as required.

11. You can choose to **Enable failover to Internal Web Server Authentication if Portal Page/External Web Server is not reachable** by placing a check in that box.

12. Enable or disable **Port Based Billing Policies**.

   The Port Location capabilities on the NSE have been enhanced. It is now possible to define a policy on a port. The billing methods (RADIUS, Credit Card, PMS, L2TP Tunneling) and the billing plans available on each port can now be individually configured.

   This ability allows for having different billing methods and billing plans on different ports identified by VLANs or SNMP Port Query of the concentrator. A practical application of this feature is to have a normal hotel room with a plan A that is $9.99 for a day with PMS billing and have a meeting room with a plan of $14.99 an hour with Credit Card billing.

   In order for the port-based policies to work, you must enable Port Based Billing Policies. See also “Adding and Updating Port-Location Assignments {Add}” on page 162.

13. Enable or disable **HTTPS Redirection**.

   The NSE responds to regular HTTP requests from pending subscribers with a redirection to the login screen. The NSE does not respond to HTTPS requests from pending subscribers (HTTP requests with a destination port = 443) with a redirect; this will result in a timeout or invalid certificate warning.
Enabling **HTTPS Redirection** adds a security exception to the user’s browser to allow the certificate received from the NSE to be always “valid.”

14. Depending on which authorization mode you choose, go to the following sub-sections in this procedure:

- **Enabling AAA Services with the Internal Web Server** – The IWS is “flashed” into the system’s memory and the subscriber’s login page is served directly from the Access Gateway.

- **Enabling AAA Services with an External Web Server** – In the EWS mode, the Access Gateway redirects the subscriber’s login request to an external server (transparent to the subscriber). The login page served by the EWS reflects the “look and feel” of the solution provider’s network and presents more login options.

### Enabling AAA Services with the Internal Web Server

You are here because you want to enable the **AAA Services** with the Access Gateway’s **Internal Web Server**. The Access Gateway maintains an internal database of authorized subscribers, based on their MAC (hardware address) and user name (if enabled). By referring to its database record, also known as an authorization table, the Access Gateway instantly recognizes new subscribers on the network.

You can configure the Access Gateway to handle new subscribers in various ways (see the table on this page). With the IWS, you also have the option of enabling SSL support.

After selecting the **Internal Web Server** authorization mode, you have the option of enabling or disabling the **Usernames** and **New Subscribers** features. These features work in conjunction with each other to determine how new subscribers are handled. Refer to the following table:

<table>
<thead>
<tr>
<th>Usernames</th>
<th>New Subscribers</th>
<th>System Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Enabled</td>
<td>Allows new subscribers to enter the system without giving a user name and password.</td>
</tr>
<tr>
<td>Enabled (optional)</td>
<td>Enabled</td>
<td>Allows new subscribers or authentication by their user name and password.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Disabled</td>
<td>New subscribers are not allowed. Only existing subscribers are allowed after authenticating their user name and password.</td>
</tr>
<tr>
<td>Disabled</td>
<td>Disabled</td>
<td>You will not use this combination unless you want to lock out all subscribers.</td>
</tr>
</tbody>
</table>

1. Select the **Internal Web Server**.
2. Enable or disable the **SSL Support** feature, as required. If you enable SSL Support, you must provide a valid **Certificate DNS Name**.

For more information about setting up SSL, go to **Setting Up the SSL Feature**.

SSL support allows for the creation of an end-to-end encrypted link between the Access Gateway and its clients by enabling the Internal Web Server (IWS) to display pages under a secure link—important when transmitting AAA information in a network.

Adding SSL support to the Access Gateway requires service providers to obtain digital certificates from VeriSign™ to create HTTPS pages. Instructions for obtaining certificates are provided by Nomadix.

To enable SSL Support, your Access Gateway’s flash must include the `server.pem`, `cakey.pem`, and `cacert.pem` certificate files (the “cacert.pem” file is provided with your Access Gateway). For assistance, contact **Appendix A: Technical Support**.

You must reboot the Access Gateway every time you enable or disable SSL Support.

3. If you want to designate a portal page, you must enable the **Portal Page** feature, otherwise leave this feature disabled.

The Portal Page IP or DNS address are added to the IP passthrough list automatically.

4. If you enabled the Portal Page feature, provide the following supporting information:
   - Portal Page URL
   - Parameter Passing (enabled or disabled)
   - Parameter Signing (including Method, Parameters, and Shared Secret)

See **Redirection Parameter Signing** for more information about parameter signing.

   - Portal XML POST URL
   - Portal XML Post Port
● Support GIS Clients (enabled or disabled)


● Block IWS Login Page (enabled or disabled)

5. Enable or disable the Usernames feature, as required (refer to the table in “Enabling AAA Services with the Internal Web Server” on page 61).

Some subscribers may want additional account flexibility and security for their services (for example, if they use more than one computer and their MAC address changes, or if they move between port-locations). In this case, a subscriber can define a unique user name and password which they can use from any machine or location (without being re-charged). Subscribers who choose this option are prompted for their user name and password whenever they try to access the Internet. Solution providers can charge a fee for this service.

6. Enable or disable the New Subscribers feature (refer to the table in “Enabling AAA Services with the Internal Web Server” on page 61).

New Subscribers must be enabled before enabling the Credit Card and PMS options.

7. If you enabled New Subscribers, enable or disable the Relogin After Timeout option.

8. You can now enable or disable the Credit Card Service. When this feature is enabled, subscribers are prompted for their credit card information (for billing purposes). The Access Gateway is configured to use either Authorize.net or Chainfusion (selected from a pull-down menu). You will need to open a merchant account with Authorize.net, Chainfusion or Datacenter (Luxembourg) before this feature can be used.

Please contact Nomadix Technical Support for assistance. Refer to “Contact Information” on page 311.

All data communications between the Access Gateway and the credit card server are encrypted by the SSL (Secure Sockets Layer) protocol. The Access Gateway never “sees” subscriber credit card numbers.
9. If you enabled the Credit Card Service, define which service you require (Authorize.net or Chainfusion) from the pull-down menu.

   DNS must be configured if you want to enter meaningful URLs instead of numeric IP addresses into any of the Access Gateway’s configuration screens (for example, the Credit Card Server URL in the following step).

10. If the Credit Card Service is enabled, enter the information for the following fields:
    - Credit Card Server URL
    - Credit Card Server IP
    - Merchant ID (a valid ID issued by the credit card reconciliation service provider – Authorize.net or Chainfusion).

11. Check the Use NSE’s Hostname and DNS domain name box if you want the Hostname and domain name to be sent to the Credit Card server instead of the local NSE IP address.

12. Enable or disable the SIM Compliant feature, as required. With this feature enabled, you can change the transaction key at your discretion. To change the transaction key, simply enter the key in the Change Transaction Key box, then re-enter the key in the Verify Transaction Key box.

   The SIM Compliant option refers to Authorize.net's Simple Integration Method.

13. Enable or disable Smart Client Support, as required.

14. You can assign a session idle timeout parameter for subscribers (see following note). To assign an idle timeout, simply enter a numeric value (in seconds) in the Subscriber Idle Timeout box (the default is 1200).

   Subscriber Idle Timeout does not apply to RADIUS and Post Pay PMS subscribers.

15. If you enabled or disabled SSL Support on this screen, you must click the check box for Reboot after changes are saved? (the Access Gateway must be rebooted every time the SSL Support feature is enabled or disabled).

16. Click on the Submit button to save your changes, or click on the Reset button if you want to reset all the values to their previous state.

Enabling AAA Services with an External Web Server

You are here because you want to enable the AAA Services with an External Web Server (EWS). In the EWS mode, the Access Gateway redirects the subscriber’s login request to an external server.
1. Select the **External Web Server**.
   After enabling the External Web Server you must enter a Secret Key. The Secret Key ensures that the response the Access Gateway gets from the EWS is valid.

2. Enter the **Secret Key** (The Access Gateway and the external authorization server must use the same secret key).

   ![DNS must be configured if you want to enter meaningful URLs instead of numeric IP addresses into any of the Access Gateway's configuration screens (for example, the External login page URL in the following step).]

3. Enter a valid **External login page URL**.
4. Configure the **Parameter Signing** options.

   ![See Redirection Parameter Signing for more information about parameter signing.]

5. Click on the **Submit** button to save your changes, or click on the **Reset** button if you want to reset all the values to their previous state (making changes to the EWS settings does not require a system reboot).

**Redirection Parameter Signing**

External Web Server (EWS) and Internal Web Server (IWS) Portal Page Parameters can be digitally signed, preventing malicious subscribers from intercepting, forging and replaying URL redirection strings used by the NSE and EWS or IWS Portal Page to validate subscriber access. This capability eliminates a vulnerability that was previously exploited to gain unauthorized Internet access at charge-for-use sites.

The signing feature can create a cryptographically strong signature that protects the sensitive portions of a URL redirection string (i.e., NSE ID, MAC address of the subscriber, etc), while letting the EWS/Portal Page verify that the URL string has not been tampered or forged by the subscriber.
The feature is configured by selecting a signing method, the parameters to be signed, and assigning a secret key.

Two signature methods are supported:

- HASH-CRC32
- HMAC-MD5

Not all parameters that are part of the URL redirection string need to be included in the signature calculation. The following parameters are considered sensitive and can be selected:

- UI (the ID of the NSE)
- MA (the subscriber’s MAC address)
- RN (the Room Number)
- PORT (the port number the subscriber is connected to)
- SIP (the subscriber IP address)

The desired secret key simply needs to be entered in the field. Once entered, it is not visible to the user.

Information that indicates which parameters were signed, along with the resultant hash value, are then included in some additional parameters that are appended to the redirection string.
In order to utilize the parameter signing feature, the EWS or Portal Page Server used must be configured to correctly parse and verify the signing information. Documentation that includes guidelines for configuring a server to support signing can be obtained by contacting Nomadix Technical Support.

**Establishing Secure Administration {Access Control}**

The Access Gateway allows you to block administrator access to interfaces (Telnet, WMI and FTP, SSH and SFTP) and incorporates a master access control list that checks the source (IP address) of administrator logins. A login is permitted only to the interfaces that have not been blocked, and only if a match is made with the master “Source IP” list contained on the Access Gateway. If a match is not made with the “Source IP list,” the login is denied, even if a correct login name and password are supplied. The access control list for source IPs supports up to 50 (fifty) entries in the form of a specific IP address or range of IP addresses.

This procedure allows you to enable the “Access Control” feature and block administrator access to specific interfaces, and add or remove administrator “Source IP” addresses.

The NSE supports secure https connections to the Web Management Interface (WMI). Correct certificates must be installed on the NSE flash memory for these connections to function properly. The same certificate set that is used to support SSL connections for subscribers is used for this purpose. For documentation about configuring the system to support secure connections, contact technical support. See Appendix A: Technical Support.

In addition, corresponding options to block https connections (independent of http) are included in the NSE's Access Control functionality, for both the network and subscriber sides.

If the required certificates are not resident on the flash, an attempted https connection will generate an error syslog.
1. From the Web Management Interface, click on **Configuration**, then **Access Control**. The **Access Control** screen appears.

2. For **Configurable Ports**, enter a **Telnet Port** and an **HTTP Port**.

3. Enable or disable administrator access to any of the following interfaces:
ACCESS GATEWAY

- Telnet Access
- Web Management Access (HTTP)
- Web Management Access (HTTPS)
- FTP Access
- SFTP Access
- SSH Shell Access

*Blocking or unblocking interface access will terminate the current session.*

*Do not enable the blocking of all interfaces without setting up and enabling SNMP. Enabling the blocking of all interfaces and disabling SNMP will completely block access to the Access Gateway administration interface. For assistance, contact Nomadix Technical Support.*

4. Enable or disable subscriber-side interface blocking for any of the following interfaces
   - **Telnet Access**: enables/disables blocking of Telnet access from the subscriber-side to the NSE Telnet interface. Default setting is enabled.
   - **Web Management Access (HTTP)**: enables/disables blocking of Web Management access from the subscriber-side to the NSE WMI. Default setting is enabled.
   - **Web Management Access (HTTPS)**: enables/disables blocking of secure Web Management access from the subscriber-side to the NSE WMI. Default setting is enabled.
   - **FTP Access**: enables/disables blocking of FTP access from the subscriber-side to the NSE. Default setting is enabled.
   - **SFTP Access**: enables/disables blocking of SFTP access from the subscriber-side to the NSE. Default setting is enabled.
   - **SSH Shell Access**: enables/disables blocking of SSH shell access from the subscriber-side to the NSE CLI. Default setting is disabled.

5. Click the check box for **Access Control** if you want to enable this feature, then click on the **Submit** button to save your change.

If you enabled Access Control, administrator access is restricted only to the IP addresses shown under the “Currently Access is Permitted for IPs” listing. If you want to add to or remove IP addresses from the list, go to Step 6 through Step 8.

*The Access Control list can contain up to 50 (fifty) valid administrator IP addresses or ranges of IP addresses.*
6. To add an IP address (or range of IP addresses) to the list, enter the “starting” IP address in the Access Control Start IP field.

7. If you are adding a range of IP addresses to the access control list, you must now enter the “ending” IP address in the Access Control End IP field. If you are adding a single IP address, enter None in the Access Control End IP field.

8. Click on the Add button to add the IP address (or range of IP addresses) to the list.

9. To remove an IP address (or range of IP addresses) from the list, enter the “starting” IP address in the Access Control Start IP field.

   If you are removing a range of IP addresses from the access control list, you must now enter the “ending” IP address in the Access Control End IP field. If you are removing a single IP address, enter None in the Access Control End IP field.

10. Click on the Remove button to remove the IP address (or range of IP addresses) from the list.

    If you enabled Access Control and have “locked yourself out,” of the system (for example, because you’ve forgotten your password), you must establish a local serial connection with the CLI to disable the Access Control feature, or change the range of allowed IP addresses to access the management interfaces. If you have changed the serial port to act as a PMS interface, please contact Nomadix technical support. In this case, refer to “Contact Information” on page 311.

**Defining Automatic Configuration Settings {Auto Configuration}**

The Access Gateway allows you to define parameters to enable the automatic configuration of the system. See also, RADIUS-driven Auto Configuration.
1. From the Web Management Interface, click on **Configuration**, then **Auto Configuration**. The *Autoconfiguration Settings* screen appears:

![Autoconfiguration Settings](image)

- **Autoconfiguration**
  - Enable

  - **Radius Authentication Name**
  - **Radius Password**
  - **Confirm Password**

2. Enable or disable **Autoconfiguration**, as required.
3. If you enabled **Autoconfiguration**, you must enter the following information into the corresponding fields:
   - RADIUS Authentication Name
   - RADIUS Password
   - Confirm Password
4. Click on the check box for **Reboot after changes are saved?** to reboot the system when you submit your changes.
5. Click on the **Submit** button to save your changes, or click or the **Reset** button to reset all data to its previous state.

See **Enabling Auto Configuration**.

**Enabling Auto Configuration**

As shown in the diagram below, two subsequent events drive the automatic configuration of Nomadix devices:

1. A flow of RADIUS Authentication Request and Reply messages between the Nomadix gateway and the centralized RADIUS server that specifies the location of the meta
configuration file (containing a listing of the individual configuration files and their
download frequency status) are downloaded from an FTP server into the flash of the
Nomadix device.

2. Defines the automated login into the centralized FTP server and the actual download
process into the flash.

Step 1: RADIUS Authen Req/Response
message to determine location of meta
configuration file

Step 2: FTP download of configuration files
(secure)

The Auto-Configuration setup requires a few basic steps to be completed by both the field
engineer and the NOC administrator.

Administrative Steps to Enable Auto-Config
Typically, these tasks are performed either at a device pre-staging center or by the field
engineer.

1. Establish a WAN connection and electronically accept the EULA.
2. Setup RADIUS Server parameters (go to “Defining the Realm-Based Routing Settings
{Realm-Based Routing}” on page 130).

Administrative Steps to Enable Auto-Config for the NOC Administrator:
1. Add NAS IP address.
2. Add Nomadix Auto-Config VSA to the Nomadix dictionary file on the RADIUS server.
3. Create a RADIUS profile with the configuration VSA.
4. Create an FTP server with the configuration files.
5. The following diagram shows a sample RADIUS configuration file, meta file and illustration of the FTP server setup.

The Nomadix device will automatically initiate one reboot to enable the new settings. Configuration updates for network maintenance can be accomplished by simply enabling the Auto-Configuration option and rebooting the device (for example, using SNMP). See also, Defining Automatic Configuration Settings {Auto Configuration}.

**Setting Up Bandwidth Management {Bandwidth Management}**

The Access Gateway allows system administrators to manage the bandwidth for subscribers, defined in Kbps (Kilobits per seconds) for both upstream and downstream data transmissions. With the ICC feature enabled, subscribers can increase or decrease their own bandwidth dynamically, and also adjust the pricing plan for their service.
1. From the Web Management Interface, click on **Configuration**, then **Bandwidth Management**. The **Bandwidth Management** screen appears:

![Bandwidth Management Screen]

2. If required, click the check box for **Bandwidth Management Enabled** (this field is not available on the AG2300 platform because Bandwidth Management is always enabled).

3. If you enabled Bandwidth Management, enter the uplink and downlink speeds (in Kbps) in the appropriate fields.

   ![Setting the uplink or downlink speeds to anything greater than what your product supports is prevented by the NSE. Please refer to “Product Specifications” on page 266 for your product’s capabilities.]

4. If you made any changes to the settings on this screen, you must click the check box for **Reboot after changes are saved**? (the Access Gateway must be rebooted).

5. Click on the **Submit** button to save your changes and reboot the system, or click on the **Reset** button if you want to reset all the values to their previous state.

**Group Bandwidth Limit Policy**

The Group Bandwidth Limit Policy allows the you to assign a common bandwidth rate limiting policy to a group of subscriber devices. All devices within the group share the total bandwidth allocated to the policy.

The Group Bandwidth Limit Policy feature defines the following vendor-specific attributes (VSAs):
Group Bandwidth Limit Policy – Operation

The NSE maintains a collection of all installed group bandwidth policies. The collection is indexed by the bandwidth policy ID provided by the RADIUS server. The collection can store as many policy records as the number of licensed subscriber devices. All subscriber devices sharing the same group bandwidth policy ID belong to the same group. A subscriber device can participate in only one bandwidth-limiting group at a time.

When a login is performed to an account that returns a bandwidth policy ID that does not yet exist in the NSE, a new policy record is created and inserted into the aforementioned collection. The subscriber authorized by the Access-Accept is associated with the newly installed bandwidth policy ID, and the bandwidth limits returned are invoked.

When the Access-Accept for a subscriber contains a bandwidth policy ID already present on NSE, the subscriber is associated with the existing group policy. All subscribers that are now members of the group share the total bandwidth allocated to the policy.

If at some point a login is performed to an account that returns the policy ID for an existing policy, but also returns bandwidth values different than those currently allocated for that policy, the policy will be updated with the new values found in the Access-Accept. Thus, the latest Access-Accept determines the current rates for the entire group.

The lifetime of a group policy record in the collection is determined by the session time of the authorized (i.e. VALID) subscribers participating in the group. Group policy records are removed from the collection when the last subscriber device belonging to the group is logged out of the NSE regardless of the reason (e.g. session timeout, idle timeout, deletion of the subscriber by an administrator, etc).

The NSE does not support the ability to enforce both per-subscriber and group bandwidth rates simultaneously for the same subscribers. The RADIUS server must specify either per-
subscriber or group bandwidth attributes. However, in case a RADIUS Access-Accept contains both individual and group bandwidth attributes, the NSE will use the group attributes and ignore the per-subscriber attributes.

The NSE can concurrently support some subscribers as part of a group and some others with limits set on a per-subscriber basis. However, a single subscriber cannot be assigned group membership and individual limits at the same time.

**Group Bandwidth Limit Policy – Enable**

The Group Bandwidth feature is globally enabled via an option on the Bandwidth management page.

![Bandwidth Management](image)

<table>
<thead>
<tr>
<th>Bandwidth Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth Management Enabled: <strong>Enable</strong></td>
</tr>
<tr>
<td><strong>Group Bandwidth Policies</strong></td>
</tr>
<tr>
<td>Group Bandwidth Policies: <strong>Enable</strong></td>
</tr>
<tr>
<td>Bandwidth uplink (to network) speed 1000000 Kbps</td>
</tr>
<tr>
<td>Bandwidth downlink (to subscribers) speed 1000000 Kbps</td>
</tr>
</tbody>
</table>

NOTE: You must reboot for settings changes to take effect.

Reboot after changes are saved? □ Yes

Submit □ Reset
Group Bandwidth Limit Policy – Current Table

When the feature is enabled, a group bandwidth policy ID column is displayed in the current table. Once policies are instantiated, policy information can be viewed via XML.

<table>
<thead>
<tr>
<th>Current Subscribers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscriber Idle Timeout: 1200 s</td>
</tr>
<tr>
<td>Note: Doesn’t apply to Radius subscriptions. Factory default: 1200 s</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>Port</th>
<th>Room</th>
<th>UserName</th>
<th>Group Bw Policy</th>
<th>Bandwidth Up/Down</th>
<th>Throughput In-Out/In-Out/Down</th>
<th>AAA State</th>
<th>Expiration</th>
<th>Idle Timeout</th>
<th>Bytes Sent</th>
<th>Bytes Received</th>
<th>Total</th>
<th>Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>09.5A.B6.60.D8.08</td>
<td>10.149.67.11</td>
<td>1</td>
<td>1</td>
<td>group</td>
<td>1</td>
<td>1024/2048</td>
<td>12-12/513-513</td>
<td>Valid</td>
<td>Unlimited/Radius Unlimited</td>
<td>30 min : 0 sec</td>
<td>296066</td>
<td>15389610</td>
<td>15685171</td>
<td>OFF</td>
</tr>
<tr>
<td>09.12.B6.6E.4A.6E</td>
<td>10.149.67.13</td>
<td>0</td>
<td>1</td>
<td>group</td>
<td>1</td>
<td>1024/2048</td>
<td>12-12/423-423</td>
<td>Valid</td>
<td>Unlimited/Radius Unlimited</td>
<td>30 min : 0 sec</td>
<td>730974</td>
<td>4147935</td>
<td>42210509</td>
<td>OFF</td>
</tr>
<tr>
<td>09.12.C5.1C.9E.69</td>
<td>10.149.67.12</td>
<td>2</td>
<td>2</td>
<td>group</td>
<td>1</td>
<td>1024/2048</td>
<td>30-30/1106-1106</td>
<td>Valid</td>
<td>Unlimited/Radius Unlimited</td>
<td>30 min : 0 sec</td>
<td>881092</td>
<td>37050143</td>
<td>37851235</td>
<td>OFF</td>
</tr>
</tbody>
</table>

Establishing Billing Records “Mirroring” [Bill Record Mirroring]

The Access Gateway can send copies of credit card transaction and PMS billing records to external servers that have been previously defined by system administrators. The Access Gateway assumes control of billing transmissions and saving billing records. By “mirroring” the billing data, the Access Gateway can also send copies of billing records to predefined “carbon copy” servers. Additionally, if the primary and secondary servers are down, the Access Gateway can store up to 2,000 credit card transaction records. When a connection is re-established (with either server), the Access Gateway sends the stored information to the server—no records are lost!

For more information about the bill record mirroring feature, go to “Mirroring Billing Records” on page 300.

1. From the Web Management Interface, click on Configuration, then Bill Record Mirroring. The Credit Card/PMS Mirroring Settings screen appears:
2. If you want to enable the billing records “mirroring” functionality for credit card transactions, click on the check box for **Enable Bill Record Mirroring**.

3. Enter the property identification code in the **Property ID** field.

4. Enter the communication parameters for the primary server that is to be used for mirroring, including:
   - Primary IP
   - URL
   - Secret Key

   *The Access Gateway and the “mirror” servers must use the same secret key.*

5. Repeat Step 4 for the secondary server (if any) and all carbon copy servers.

6. Define the “fail-safe” provisions, including:
   - Retransmit Method – Alternate, or do not alternate.
● Number of Retransmit Attempts – This tells the system how many times it should attempt to retransmit billing records before suspending the task.
● Retransmit Delay – This specifies the time delay between each retransmission.

7. Click on the **Submit** button to save your changes, or click on the **Reset** button if you want to reset all the values to their previous state.

**Configuring Destination HTTP Redirect**

Destination HTTP Redirect provides DNS-triggered redirection of HTTP requests to one or more portal page URLs configured on the NSE. Portal pages could include account status, maps, local information, etc.

The NSE will intercept and respond to DNS queries containing configurable strings. Subscribers requesting a website at that DNS will obtain a DNS response that contains a “magic” IP address (which is the same value obtained when the subscriber queries the DNS string “logout.nomadix.com”).

The NSE will process HTTP requests for that “magic” IP address (configurable on the AAA page), and will reply with an HTTP redirection (which may include a number of signed redirection parameters) to a configured URL. By following the HTTP redirection, the subscriber will reach the target URL, and he/she will then be served a page containing whatever information is relevant (account and/or other specific information).
The figure above illustrates destination HTTP redirection, assuming a DNS query string for www.example.com, a magic IP address of 1.1.1.1, and a portal page URL of portal1.myhotel.com. Given this configuration, the following would apply:

- A DNS query for www.example.com is intercepted by the NSE, which responds with the magic IP address. Then, the subscriber’s browser sends an HTTP request to the magic IP and sets the Host header to www.example.com.

- The NSE will process the HTTP request and will analyze the Host header to find the redirection URL that corresponds to www.example.com, which is portal1.myhotel.com in this example. The NSE will then craft an HTTP redirection response that contains the portal page URL, followed by a query string. The string will include various redirection parameters, time-stamped and signed, if signing is enabled for that entry (which it is not in this example).

- The subscriber will follow the redirection string and will land on the portal page URL. The portal will verify and analyze the query string and then will return the relevant information (likely about the subscriber’s account status, depending on what the portal is configured to handle).
After successful redirection occurs the list of signed parameters and signature methods are passed to the portal page.

HTTP/1.0 302 RD

1. From the Web Management Interface, click on Configuration, then Destination HTTP Redirection. The Destination HTTP Redirection Settings screen appears:

   **Destination HTTP Redirection Settings**

   Destination HTTP Redirection   ☑ Enabled

   Submit

   **Portal Pages**

   Add a new Portal Page:
   Matching String: 
   URL: 

   Parameter Passing:
   ☐ Enable

   Parameter Signing:
   Method:
   ○ None  ○ HASH-CRC32  ○ HMAC-MD5

   Parameters:
   ☐ UI  ☐ MA  ☐ RN  ☐ PORT  ☐ SIP

   ☐ Set Shared Secret: [write-only]

   Add Portal Page  Reset

   **Existing Portal Page entries (up to 20 may be created):**

<table>
<thead>
<tr>
<th>Matching String</th>
<th>URL</th>
<th>Parameter Passing</th>
<th>Parameter Signing</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.example.com">www.example.com</a></td>
<td>portal1.myhotel.com</td>
<td>Disabled</td>
<td>None</td>
<td>Edit</td>
</tr>
</tbody>
</table>

1 Destination Portal Page(s) are defined

2. To enable Destination HTTP Redirection, click on the Enabled check box. The default setting is disabled.

   You may create up to 20 portal pages.

3. In the Portal Pages section, enter the matching string that will be directed to the portal page in the Matching String field.

4. Enter the portal page’s URL in the URL field.
5. To enable parameter passing, click on the Parameter Passing Enable check box.

6. Select the Parameter Signing:
   - **Method:** None, HASH-CRC32, or HMAC-MD5 (select one method).
   - **Parameters:** UI, MA, RN, PORT, and SIP (select all applicable parameters).

7. To enable Set Shared Secret, click on the Set Shared Secret check box. If you enable this feature, enter the shared secret text string in the Set Shared Secret field.

8. Click on the Submit button to save the redirection settings, or click on the Reset button if you want to reset all the values to their previous state.
   Portal page setting are saved to the table in Existing Portal Page entries section of the screen. From that table, you can edit or delete existing portal pages.

**Managing the DHCP service options {DHCP}**

When a device connects to the network, the DHCP server assigns it a “dynamic” IP address for the duration of the session. Most users have DHCP capability on their computer. To enable this service on the Access Gateway, you can either enable the DHCP relay (routed to an external DHCP server IP address), or you can enable the Access Gateway to act as its own DHCP server. In both cases, DHCP functionality is necessary if you want to automatically assign IP addresses to subscribers.
1. From the Web Management Interface, click on **Configuration**, then **DHCP**. The **DHCP Settings** screen appears:

![DHCP Settings Screen]

**Nomadix’ patented Dynamic Address Translation (DAT) functionality is automatically configured to facilitate “plug-and-play” access to subscribers who are misconfigured with static (permanent) IP addresses, or subscribers that do not have DHCP capability on their computers. DAT allows all users to obtain network access, regardless of their computer’s network settings.**

2. **DHCP Services** is enabled by default. Do not disable it unless you want to lose all your DHCP services.

   **By default, the Access Gateway is configured to act as its own DHCP server and the relay feature is disabled. If you want the Access Gateway to act as its own DHCP server, do not enable the relay. Go directly to Step 8.**
3. To route DHCP through an external server, enable the **DHCP Relay**.

4. If you enabled the DHCP Relay feature, you must assign a valid **DHCP Server IP** address (the default is 0.0.0.0) and a valid **DHCP Relay Agent IP** address.

   The DHCP Relay Agent allows the Access Gateway to request a specific range of IP addresses from different IP pools from the DHCP Server. Leaving these fields blank forces the system to use the IP pool that contains IP addresses that are on the same subnet as the Access Gateway.

   ![Warning icon] *You must disable the DHCP server before enabling the DHCP relay. Both features cannot be enabled concurrently.*

   **Warning:** *If the DHCP Relay Agent IP address is set for an address that is already used or the IP address of the server, the other system will get an IP conflict and will not have Internet access.*

5. If you want the Access Gateway to act as its own **DHCP Server** (you did not enable the **DHCP Relay**), enable it now.

6. If required, you can make the DHCP Server feature **Subnet-based** by checking the appropriate box.

7. If required, enable the **IP Upsell** feature.

   System administrators can set two different DHCP pools for the same physical LAN. When DHCP subscribers select a service plan with a public pool address, the Access Gateway associates their MAC address with their public IP address for the duration of the service level agreement. The opposite is true if they select a plan with a private pool address. This feature enables a competitive solution and is an instant revenue generator for ISPs. The IP Upsell functionality solves a number of connectivity problems, especially with regard to L2TP and certain video conferencing and online gaming applications.
8. If you want to add a new DHCP Pool, click on the Add button. The Add DHCP Pools screen appears:

9. Enter a valid DHCP Server IP address for the DHCP server.

10. Enter the DHCP Server Netmask.

11. Enter the starting and ending IP addresses for the DHCP address pool you want to use:
   - DHCP Pool Start IP
   - DHCP Pool Stop IP

12. Enter the DHCP Lease Minutes.

13. Select Public Pool or Private Pool, as required.

   A “public” IP address will not be translated by DAT.
14. If required, make this an IP Upsell Pool and/or the Default Pool by checking the appropriate boxes.

Do not allow pools to overlap.

15. Optional, if the gateway router for the DHCP Pool is other than that of the DHCP Server IP, select Specify and enter the IP address of the gateway router of choice.

16. When finished establishing your DHCP Pools, click on the Back to Main DHCP Configuration Page to return to the previous page.

17. You must now reboot the system for the new settings to take effect. Click the check box for Reboot after changes are saved? then click on the Submit button to save your changes and reboot the system, or click on the Reset button if you want to reset all the values to their previous state.

The existing lease pool and lease table are deleted and the Access Gateway reboots. The Access Gateway can issue IP addresses to any DHCP enabled subscriber who enters the network.

Enabling DNSSEC Support

DNSSEC support adds authentication and integrity capability to DNS systems. The DNSSEC feature in the NSE allows DNSSEC queries and responses to traverse the NSE between subscribers and the NSE’s configured DNS servers. The NSE itself does not participate in DNSSEC trust relationships with subscribers. Reboot is not required.

Use the following procedure to set the DNS configuration options.

1. From the Web Management Interface, click on Configuration, then DNS. The Domain Name System (DNS) Settings screen appears:
2. Check the **Enable** check box to enable DNSSEC Support functionality. The default setting is disabled.

3. Click on the **Submit** button to save your changes (reboot is not required), or click on the **Reset** button if you want to reset all the values to their previous state.

**Managing the DNS Options {DNS}**

DNS allows subscribers to enter meaningful URLs into their browsers (instead of complicated numeric IP addresses) by automatically converting the URLs into the correct IP addresses. You can assign a primary, secondary, or tertiary (third) DNS server. The Access Gateway utilizes whichever server is currently available.

Use the following procedure to set the DNS configuration options.

1. From the Web Management Interface, click on **Configuration**, then **DNS**. The *Domain Name System (DNS) Settings* screen appears:
2. Enter the **Host Name** (the DNS name of the Access Gateway).  

   *The host name must not contain any spaces.*

3. Enter a valid **Domain** name (the Internet domain that DNS requests will utilize).

4. Enter the IP addresses for the DNS servers (located at the customer’s network operating center where DNS requests are sent). Servers include:
   - Primary DNS Server
   - Secondary DNS Server
   - Tertiary DNS Server

   *The secondary and tertiary DNS servers are only utilized if the primary DNS server is unavailable.*

5. Enter a **DNS Redirection Port** and a **Proxy DNS Port**.

6. When finished, you must reboot the system for the new settings to take effect. Click on the check box for **Reboot after changes are saved?** to reboot the system after saving your changes.

7. Click on the **Submit** button to save your changes and reboot the system, or click on the **Reset** button if you want to reset all the values to their previous state.

**Managing the Dynamic DNS Options {Dynamic DNS}**

Use the following procedure to set the Dynamic DNS options.
1. From the Web Management Interface, click **Configuration**, then **Dynamic DNS**. The **Dynamic DNS Configuration** screen appears:

![Dynamic DNS Configuration Screen](image)

2. Check the **Enable** checkbox to enable Dynamic DNS (DDNS) functionality. The default setting is disabled.

3. Enter the **Provider Info**:
   - Select the provider protocol from the **Protocol** menu. Currently, only **dyndns.org** and **dyndns.org (secure)** are supported. The default setting is **dyndns.org (secure)**.
   - In the **Server** field, enter the server name to which the client sends updates to the DDNS server.
   - Select the port number for the server from the **Port** menu.

4. Enter the **Account Information**:
   - Enter the host name, which is the DDNS name that is mapped to the client IP address, in the **Hostname** field. DDNS mapping is configured on the DynDNS.org account.
   - Enter the user name for the DDNS server account in the **Username** field.
   - Enter the password name for the DDNS server account in the **Password** field.
5. In the **Force Update** field, click **Submit and Force Update** to force an immediate update to the DDNS.

Note that too many updates may be considered abuse by the DDNS vendor.

Alternatively, click **Submit** to save the settings or **Reset** to clear the changes and return the settings to the previous state.

**GRE Tunneling {Gre Tunneling}**

Use the following procedure to set the GRE Tunneling options.

1. From the Web Management Interface, click **Configuration**, then **Gre Tunneling**. The **GRE Tunneling** screen appears:

   ![GRE Tunneling Settings Table]

   **NOTE:** You must reboot for changes to take effect.

   Reboot after changes are saved?  Yes

   ![Submit and Reset Buttons]

2. Click the checkbox for **GRE Tunneling** to enable this feature.

3. Enter the **VPN Concentrator IP Address**. This is the IP address of the remote server.

4. Enter the **GRE Interface IP Address**. This is the IP of the local GRE interface on the Access Gateway.

5. Enter the **GRE Interface Subnet Mask**. This is the subnet mask for the GRE connection.

6. Enter the **GRE Interface Default Gateway**. This is the IP address of the GRE interface of the remote host.

7. When finished, you must reboot the system for the new settings to take effect. Click the check box for **Reboot after changes are saved?** to reboot the system after saving your changes.

8. Click **Submit** to save your changes and reboot the system, or click **Reset** to reset all the values to their previous state.
Setting the Home Page Redirection Options {Home Page Redirect}

This procedure shows you how to redirect the subscriber’s browser to a specified home page. Subscribers may also be redirected to a page specified by the solution provider, without any interaction with the authentication process.

You must configure DNS if you want to enter meaningful URLs instead of numeric IP addresses into any of the Access Gateway’s configuration screens.

1. From the Web Management Interface, click on Configuration, then Home Page Redirect. The Home Page Redirection Settings screen appears:

   ![Home Page Redirection Settings](image)

2. Click on the check box for Home Page Redirection to enable this feature. If you enable home page redirection, you must provide a URL for the redirected home page.

3. Enter the URL of the redirected home page in the Home Page URL field.

4. If required, click on the check box for Parameter Passing.

   Parameter passing allows the Access Gateway to track a subscriber’s initial Web request (usually their home page) and pass the information on to the solution provider. The solution provider uses this information to ensure that the subscriber can return to their home page easily.

5. In the Redirection Frequency field, specify the frequency (in minutes) for home page redirection. This is the interval at which the subscriber is redirected to the solution provider’s home page automatically.

6. Click on the Submit button to save your changes, or click on the Reset button if you want to reset all the values to their previous state.
Enabling Intelligent Address Translation (iNAT™)

Our patented iNAT™ feature contains an advanced, real-time translation engine that analyzes all data packets being communicated between the private and public address domains. The Nomadix iNAT™ engine performs a defined mode of network address translation based on packet type and protocol (for example, GRE, IKE etc…).

1. From the Web Management Interface, click on **Configuration**, then **iNAT**. The iNAT™ screen appears:

   ![INAT Screen](image)

2. Enable or disable the iNAT feature, as required.

3. If you enabled iNAT™, you have the option of enabling or disabling the following VPN protocols:
   - PPTP
   - PPTP CALL ID
   - IPSEC
   - SIP

4. Click on the **Submit** button to save your options.
   
   Use the **iNAT Start** and **iNAT End** fields to enter an IP address or range of IP addresses (up to 50), then click on the **Add** button to add the IP address(es), or click on the **Remove** button to delete the IP address(es) from the database.
Defining IPSec Tunnel Settings {IPSec}

1. From the Web Management Interface, click on Configuration, then IPSec. The IPSec Tunnel Settings screen appears:

   **IPSec Tunnel Settings**

   **Global Settings**
   Enable IPsec  
   NOTE: Enabling/disabling IPSec requires reboot to put into effect.

   ![IPSec Tunnel Peers](image)

   ![IPSec Security Policies](image)

2. Check the Enable IPsec checkbox to enable IPsec. Note that you will have to reboot for IPsec to take effect.

3. Click Submit to save the setting.

   To add or modify IPsec tunnel peers, see Managing IPSec Tunnel Peers. To add or modify IPsec security policies, see Managing IPSec Security Policies.
Managing IPSec Tunnel Peers

You can add a new IPSec tunnel peer or modify the settings of an existing IPSec tunnel peer from the IPSec Tunnel Settings screen.

Adding a new IPSec tunnel peer

1. Click the Add button in the IPSec Tunnel Peers table. The IPSec Tunnel Peer Settings screen opens.

2. Enter the IP address of the peer in the Tunnel Peer field.

3. In the Peer Authentication Method section, select one of the two peer authentication methods:
   - **Authenticate via pre-shared key** – Enter the pre-shared key in the Shared Key field.
   - **Authenticate via X.509 Certificate** –
     - Enter the filename of the private certificate in the Private Key Filename field.
     - Enter the filename of the public certificate in the Certificate Filename field.
Note that the files must exist on flash first.

4. In the **IKE Channel Security Parameters** section, select the following settings:
   - **Acceptable Encryption Algorithms** – Check the **DES** and/or **3DES** checkboxes (you must check at least one option).
   - **Acceptable Hash Algorithm** – Check the **MD5** and/or **SHA** checkboxes (you must check at least one option).
   - **Key Strength** (a.k.a. Diffie-Hellman) – Select either **768-bit** (Group 1) or **1024-bit** (Group 2).
   - **Lifetime** – Enter the value (in seconds) in the **Lifetime** field. Data life size is NOT supported.

5. Click **Add** to add the IPSec tunnel peer to the **IPSec Tunnel Peers** table on the **IPSec Tunnel Settings** screen.

6. Click the **Back to Main IPSec Tunneling Settings page** link to return to the **IPSec Tunnel Settings** screen.

**Modifying an Existing IPSec Tunnel Peer**

1. Click on the IPSec tunnel peer link that you wish to modify in the **IPSec Tunnel Peers** table. The **IPSec Tunnel Peer Settings** screen opens.

2. Modify the settings as desired.

3. Click:
   - **Modify** to save the changes to the peer.
   - **Remove** to remove the peer from the **IPSec Tunnel Peers** table.
   - **Reset** to undo any changes you made to the peer settings and return the peer to its original settings.

4. Click the **Back to Main IPSec Tunneling Settings page** link to return to the **IPSec Tunnel Settings** screen.

**Managing IPSec Security Policies**

You can add a new IPSec security policy or modify the settings of an existing IPSec security policy from the **IPSec Tunnel Settings** screen.
Adding a New IPSec Security Policy

1. In the **IPSec Security Policies** table, click the **Add** button to add an entry. The **IPsec Tunnel Security Policy Settings** screen opens.

2. Select the tunnel peer IP address for which you would like to add a security policy from the **Tunnel peer IP address** menu. You must select a peer if the policy is using ESP or AH; if the policy is a **Discard** or **Bypass** policy, select **none**.

3. In the **Traffic Selectors** section, define a specific protocol by one of the following methods:
   - Select a specific protocol from the **Protocol** menu.
   - Enter a specific protocol number in the **Protocol** field. Protocol numbers are available at [www.iana.org/assignments/protocol-numbers](http://www.iana.org/assignments/protocol-numbers).
Next you will define selectors of the Security Policy. All selectors must match for the policy to be applied.

4. Define the following selectors for the **Remote End**:
   - **Remote IP/Subnet** – Enter the IP address of the remote network secured by the IPSec tunnel. The address can specify a host.
   - **Subnet Mask** – Enter the subnet mask of the remote network secured by the IPSec tunnel.
   - **Remote UDP/TCP Port** – Enter the port number; 0 is for all ports (only if protocol is UDP or TCP).

5. Security Policy can derive the settings for the **Local End** from the current Network IP settings of the unit. Select one of the following network options for the **Local End**:
   - **Use current Network Interface IP Address** – Select this option if you would like to use the current network interface IP Address. Note that the network IP address is dynamic if DHCP or PPPoE client is enabled. This setting is the default setting.
   - **Use this static IP address/subnet** – If you select this option you must also enter the **Local IP/Subnet**, the **Subnet Mask**, and the **IP address of network interface for this policy**.
     - The **Local IP/Subnet** is the IP address of the local network secured by the IPSec tunnel. The address can specify a host.
     - The **Subnet Mask** is the subnet mask of the local network secured by the IPSec tunnel. The address can specify a host.
     - The **IP address of network interface for this policy** is the IP Address for the NSE inside an IPSec tunnel. The IP address must be within the Local LAN subnet or the same as the Local LAN IP address. IP address 0.0.0.0 disables the functionality. The default setting is 0.0.0.0.

6. Enter the port number in the **Local UDP/TCP Port** field; 0 is for all ports (only if protocol is UDP or TCP).

7. In the **Security Parameters** section, define the parameters of the security policy. The options are **Discard**, **Bypass**, **ESP**, and **AH**. **ESP** is the default setting.
   - **Discard**
   - **Bypass** – Select the direction of the discard/bypass; the options are: **In only**, **Out only**, or **In and Out. Out only** is the default setting.
   - **ESP** – Select all the acceptable encryption algorithms by putting a check in the checkbox of each option; the options are: **DES**, **3DES**, and **NULL**. **3DES** is the default setting. See **Setting joint ESP and AH parameters** to set parameters that pertain to both ESP and AH polices.
- **AH** – See **Setting joint ESP and AH parameters** to set parameters that pertain to both ESP and AH policies.

**Setting joint ESP and AH parameters**

These parameters affect both ESP and AH policies.

- Select all the **Acceptable authentication algorithms** by putting a check in the checkbox of each option; the options are: **MD5**, **SHA**, and **NULL**. The default settings are **MD5** and **SHA**.
- Select the **Perfect Forward Secrecy Strength** to enable PFS. PFS makes the keying material used in protecting the data independent of the keying material used for protecting the IKE exchanges. The options are **None**, **768-bit**, and **1024-bit**. The default setting is **None**.
- Enter the maximum lifetime (in seconds) in the **Maximum Lifetime** field. The default settings are **28800**.
- Enter the maximum life size (in kbytes) in the **Maximum Lifesize** field.
- Enable the automatic renewal option by putting a check in the **Automatic renewal** checkbox. The default setting is enabled.

8. Click **Add** to add the policy to the **IPSec Security Policy** table on the **IPSec Tunnel Settings** screen.

9. Click the **Back to Main IPSec Tunneling Settings page** link to return to the **IPSec Tunnel Settings** screen.

**Modifying an Existing IPSec Security Policy**

1. Click on the IPSec security policy link that you wish to modify in the **IPSec Security Policies** table. The **IPsec Tunnel Security Policy Settings** screen opens.

2. Modify the settings as desired.

3. Click:
   - **Modify** to save the changes to the policy.
   - **Remove** to remove the security policy from the **IPSec Security Policies** table.
   - **Reset** to undo any changes you made to the policy settings and return the policy to its original settings.

4. Click the **Back to Main IPSec Tunneling Settings page** link to return to the **IPSec Tunnel Settings** screen.
Establishing Your Location {Location}

This command sets up your location and the corresponding IP addresses for the network interface, subscriber interface, subnet, and default gateway. You *must* provide your full location information.

1. From the Web Management Interface, click on **Configuration**, then **Location**. The **Location Settings** screen appears:

![Location Settings Screen]

- **Company Name**
- **Site Name**
- **Address (Line 1)**
- **Address (Line 2)**
- **City**
- **State**
- **ZIP/Postal Code**
- **Country**
- **E-mail Address**

Please select the venue type that most reflects your location:

- [ ] Lab/Test
- [ ] Office

**ISO Country Code**
**Phone Country Code**
**Calling Area Code**
**Network SSID/ZONE**

- [ ] Enable WAN 802.1Q header for System Traffic:
  - **VLAN ID**

- [ ] Enable WAN 802.1Q header for Subscribers Traffic:
  - **Default VLAN ID**

**NOTE:** You must reboot for the following settings to take effect.

- **Network Interface Configuration Method**
  - [ ] DHCP Client
  - [ ] PPPoE Client
  - Static

![Static Configuration Parameters]

- **Network IP Address**
- **Gateway**
- **Default Gateway**

- [ ] Reboot after changes are saved?

* Required Field

**Note:** Changing these settings could result in loss of connectivity.
2. Enter your location information in the following fields:
   - Company Name
   - Site Name
   - Address (Line 1 and Line 2)
   - City, State, Zip, and Country
   - E-mail Address
   - ISO Country Code
   - Phone Country Code
   - Calling Area Code

3. Select the area type that most resembles your location from the drop down list.

4. Enter a Network SSID/Zone.

5. To enable the 802.1Q tag for:
   - **System traffic**, check the box **Enable WAN 802.1Q header for System Traffic**, and if necessary, enter the tag number.

   **Changing these settings could result in loss of connectivity.**

   - **Subscribers traffic**, check the box **Enable WAN 802.1Q header for Subscribers Traffic**, and if necessary, enter the tag number.

   **Changing these settings could result in loss of connectivity.**

You must reboot the system if you make changes to any of the following IP settings.

You may lose your connection if you change the IP settings incorrectly (using invalid IP addresses). If you “misconfigure” the Access Gateway and network connectivity is lost, you can still access the Access Gateway from the Command Line Interface (CLI) via a direct serial connection. In this case, refer to: Powering Up the System and “Logging In” on page 55.
6. Make a selection for **Network Configuration Method**. This determines how the Access Gateway receives its IP address to work on the network.
   - If the Access Gateway receives its IP address from a **DHCP Server**, select DHCP. Nothing else needs to be configured.
   - If the Access Gateway receives a **static IP address**, enter the static IP address, Subnet Mask, and Gateway in the **Static Configuration Parameters** box.
   - If the Access Gateway receives its IP address from a **PPPoE Server**, select the **Configure PPPoE Client** link and enter the following parameters:
     - **PPPoE Service Name** - This is the Service-Name TAG. The maximum allowed length is 31 characters.
     - **PPP Keep Alive**
       - **Echo Request Interval in seconds** - Setting this to 0 will disable echo requests from the NSE. The default value for this parameter is 30 seconds.
       - **Maximum Missed Responses allowed** - This is the number of echo-requests that can be allowed to go without a response before the NSE determines that the PPP link is down. This parameter can only set to whole number above 0.
     - **PPP Authentication**
       - **Username** - This is the username for PPP based authentication required by your service provider.
       - **Password** - This is the password for PPP based authentication required by your service provider. Max length for both username and password is 128 characters.
     - **IP Configuration Mode** - This defines the IP address configuration mode for the NSE. Setting this to **Dynamic** will obtain a dynamic IP address from PPPoE server similar to DHCP client. Setting this to static will require manually configuring IP address in the text box.
     - **Maximum TCP MSS** - Please note that this is the MSS not MTU. The maximum value suggested by the RFC is 1452.

7. Enter a valid subscriber IP address in the **Subscriber IP Address** field.
The IP addresses from subscribers that are on a subnet different from the Access Gateway (for example, misconfigured) are translated by Nomadix’ Dynamic Address Translation (DAT) patented technology to the **Subscriber IP Address**.

The subscriber interface acts as a multifunctional “translator.” For example, if a subscriber’s computer is setup statically for a network with a gateway address of 10.1.1.1, the Access Gateway emulates the gateway to accommodate this subscriber while emulating other gateways to accommodate other subscribers.

8. Enter a Valid Subnet Mask in the **Subnet Mask Field**.
   The subnet mask defines the number of IP addresses that are available on the routed subnet where the Access Gateway is located.

9. Enter a valid default gateway IP address in the **Default Gateway** field.
   The default gateway is the IP address of the router that the Access Gateway uses to transmit data to the Internet.

10. When finished, you must reboot the system for the new settings to take effect. Click on the check box for **Reboot after changes are saved?** to reboot the system after saving your changes.

11. Click on the **Submit** button to save your changes and reboot the system, or click on the **Reset** button if you want to reset all the values to their previous state.

### Managing the Log Options {Logging}

System logging creates log files and error messages generated at the system level. AAA logging creates activity log files for the AAA (Authorization, Authentication, and Accounting) functions. You can enable either of these options.

Although the AAA and billing logs can go to the same server, we recommend that they have their own unique server ID number assigned (between 0 and 7). When managing multiple properties, the properties are identified in the log files by their IP addresses.
1. From the Web Management Interface, click on Configuration, then Logging. The Log Settings screen appears:

<table>
<thead>
<tr>
<th>Log Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Log</td>
<td>Enable</td>
</tr>
<tr>
<td>System Log Number</td>
<td></td>
</tr>
<tr>
<td>System Log Filter</td>
<td>7 Debug</td>
</tr>
<tr>
<td>System Log Server IP</td>
<td>19.10.10.10</td>
</tr>
<tr>
<td>System Log save to file</td>
<td>Enable</td>
</tr>
<tr>
<td>AAA Log</td>
<td>Enable</td>
</tr>
<tr>
<td>AAA Log Number</td>
<td></td>
</tr>
<tr>
<td>AAA Log Filter</td>
<td>7 Debug</td>
</tr>
<tr>
<td>AAA Log Server IP</td>
<td>19.10.10.10</td>
</tr>
<tr>
<td>AAA Log save to file</td>
<td>Enable</td>
</tr>
<tr>
<td>RADIUS History Log</td>
<td>Enable</td>
</tr>
<tr>
<td>RADIUS History Log Number</td>
<td></td>
</tr>
<tr>
<td>RADIUS History Log Filter</td>
<td>7 Debug</td>
</tr>
<tr>
<td>RADIUS History Log Server IP</td>
<td>19.10.10.10</td>
</tr>
<tr>
<td>RADIUS History save to file</td>
<td>Enable</td>
</tr>
<tr>
<td>System Report Log</td>
<td>Enable</td>
</tr>
<tr>
<td>System Report Log Number</td>
<td></td>
</tr>
<tr>
<td>System Report Server IP</td>
<td>19.10.10.10</td>
</tr>
<tr>
<td>System Report Log Interval</td>
<td>5</td>
</tr>
<tr>
<td>Subscriber Tracking Log</td>
<td>Enable</td>
</tr>
<tr>
<td>Subscriber Tracking Log Number</td>
<td></td>
</tr>
<tr>
<td>Subscriber Tracking Log Server IP</td>
<td></td>
</tr>
<tr>
<td>Subscriber Tracking Log save to file</td>
<td>Enable</td>
</tr>
<tr>
<td>Include User Name reporting</td>
<td>Enable</td>
</tr>
<tr>
<td>Include Port reporting</td>
<td>Enable</td>
</tr>
<tr>
<td>Include Location reporting</td>
<td>Enable</td>
</tr>
<tr>
<td>Report every 500th packet</td>
<td>Enable</td>
</tr>
</tbody>
</table>

**NOTE:** To enable Subscriber Tracking the External Time Server must be enabled (see Configuration -> Time)

**WARNING:** Communication between the gateway and the syslog server may need to be secured to comply with local laws. Consider routing communication through an IPSec tunnel.
2. If required, click on the check box for **System Log** to enable system logging.

When system logging is enabled, the standard SYSLOG protocol (UDP) is used to send all message logs generated by the Access Gateway to the specified SYSLOG server.

3. Enter a unique number (between 0 and 7) in the **System Log Number** field. This ID number is assigned to the **System Log Server**.

4. Enter a valid IP address in the **System Log Server IP** field.

5. If required, repeat Steps 2 through 4 for the **AAA Log** feature.

6. **Setting a Log Filter**: The syslogs can be filtered at 7 levels as shown above. Setting the level to a number disables any syslogs above that filter setting. For e.g. setting the filter to 2:Critical only generates 0:Emergency, 1:Alert and 2:Critical level syslogs. All other syslogs are not generated.

7. **Log save to file Setting**: This setting enables/disables saving of syslogs generated by the system to a file named “syslog.txt” in the /flash directory of the NSE. This setting abides by the other settings set for the syslogs like filters, number and enable/disable.

   It is not required to input a server IP address if you intend to only store the syslogs locally. Please leave the IP address field blank for such cases.

The following Logs are available for configuration on the NSE:

**AAA Log**
These logs record events related to Authentication, Authorization, and Accounting on the NSE.

**RADIUS History Log**
These logs record RADIUS proxy accounting messages sent or received by the RADIUS proxy. Please refer to “Viewing RADIUS Proxy Accounting Logs {RADIUS Session History)” on page 186 for additional configuration information.

**System Logs**
These logs record events specific to the NSE system itself.

**System Report Log**
These are Periodic Syslogs that report the status of the NSE and carry information about the NSE ID, NSE IP Address and the current number of Subscribers on the NSE.

*Example:*

*Additional Configuration:*

**System Report Log Interval**
This is the time interval in minutes between the system report syslogs.
Subscriber Tracking Log

Enabling this checkbox enables the Subscriber Tracking log. Use this to track the network usage of specific Subscribers on the network by receiving a syslog of every Session that is opened by each subscriber. Each new DAT session that is created for subscribers is logged in these syslogs. Proxy state, type of access, and Username are included besides the source and destination information of each session. There are IN and OUT messages for the beginning and ending of each session.

Examples:


Field formats explained:

LI : IN-->: Day Month Date Time Year | NSE_Site_Name | S(Source_IP/Port), D(Destination_IP/Port), X(NSE_Translated_IP/Port), proxy_type , Subscriber_MAC, Billing_Type, UserName(first 12 char). LI : IN-->: THU JUN 23 11:43:58 2007 | testlab | S(192.168.2.4/3444), D(66.163.175.128/80), (67.130.149.4/5004), non-proxy , 00:90:27:78:81:00, RADIUS, IPASS/0U0000

Do not configure the Server IP as the Network side IP of the gateway Stored syslogs are viewable under System/Syslog menu. A total of 500 syslogs are stored locally.
Check the **Subscriber Tracking Log** option to enable or disable the Subscriber tracking log. *Note: NTP must be enabled on the NSE for Subscriber tracking log to be enabled.*

2. Enter the subscriber tracking log number in the **Subscriber Tracking Log Number** field. This is the syslog number to identify this syslog to your Server.

3. Enter the IP address of the Syslog server that is listening for the sylogs from your NSE in the **Subscriber Tracking Log Server IP** field.

Page Faults are stored in the file named “lograw.txt” in the /flash directory and is not viewable on the web management interface.
4. Check the **Subscriber Tracking Log save to file** option to save the syslogs locally to the NSE flash. *Note: Not recommended.*

5. Check the **Include User Name Reporting** option to include the first 25 characters of the username in the Syslog.

6. Check the **Port Location: Include Port Reporting** option and **Port Location: Include Location** option to include the port information from the port location table and the Port reported to the system by either VLAN or SNMP query. The Location information is limited to 25 characters.

7. Check the **Include every 500th Packet** option to follow the Danish law that requires the 500th packet for each subscriber to be logged. Enabling this will send the 500th packet for each subscriber to the syslog system.

Click on the **Submit** button to save your changes, or click on the **Reset** button if you want to reset all the values to their previous state.

When logging is enabled, log files and error messages are sent to these servers for future retrieval. To see sample reports, go to “Sample SYSLOG Report” on page 278 and “Sample AAA Log” on page 277.

**Enabling MAC Authentication {MAC Authentication}**

1. From the Web Management Interface, click on **Configuration**, then **MAC authentication**. The **MAC Authentication Settings** screen appears:

   ![MAC Authentication Settings](image)

2. Check the **MAC Authentication** checkbox to enable the MAC-based authentication functionality. The default setting is disabled.

3. Enter the retry frequency (in seconds) in the **Retry Frequency** field. This setting is the wait time, in seconds, before reattempting MAC authentication following a failed attempt. The minimum (and default) value is 10 seconds.

4. Select the **MAC Address Format**. This setting is the format in which the subscriber’s MAC address will be expressed in the RADIUS username and password attributes. The
RADIUS server must use the same format. The options are: **aa-bb-cc-dd-ee-ff**, **aa:bb:cc:dd:ee:ff**, or **aabbccddeeff**. The default setting is **aa-bb-cc-dd-ee-ff**.

5. Select the **Case of Hex-Alpha Characters**. This setting specifies, in the MAC addresses in RADIUS username and password attributes, whether the hex-alpha characters A-F will be uppercase or lowercase. The options are **Lower** or **Upper**. The default setting is **Lower**.

6. Select the **RADIUS Service Profile to use** from the **RADIUS Service Profile to use** menu. This setting specifies the RADIUS Service Profile (and therefore, which RADIUS servers) to use for MAC-based Authentication purposes.

7. Click **Submit** to save the settings or **Reset** to return the settings to the previous state.

---

### Assigning Passthrough Addresses (Passthrough Addresses)

The Access Gateway allows up to 300 IP passthrough addresses and DNS names. This feature allows users to “pass through” the Access Gateway and access predetermined services (for example, the redirected home page) at the solution provider’s discretion, even though they may not have subscribed to the broadband Internet service. This is useful if solution providers want to openly promote selected services to all users, even if they are not currently subscribing (paying) for access. Allowing up to 300 passthroughs (IP and DNS) offers customers greater promotional flexibility.

*The Access Gateway is supplied with “Hotmail®” as a default passthrough setting.*
1. From the Web Management Interface, click on **Configuration**, then **Passthrough Addresses**. The **Passthrough Address Settings** screen appears:

   ![Passthrough Address Settings](image)

   - **Passthrough Addresses** is checked to enable Passthrough Addresses.
   - Click **Submit** to apply the settings.

   Please enter either an IP address or a DNS name and click on one of the provided buttons. **Note**: DNS name should not contain protocol, port, or path information. Up to 300 Passthrough Addresses can be entered.

   **IP/DNS Name**: 

   - **Current Passthrough Address**
   - **DNS Name**: www.nomadix.com
   - **Email**: john.doe@nomadix.com
   - **IP Addresses**: 1.2.3.4, 2.3.4.5, 5.6.7.8, 6.7.8.9

   Number of Passthrough Addresses: 7

2. If required, enable **Passthrough Addresses**, then click on the **Submit** button.

3. In the **IP/DNS Name** field, enter the IP address or DNS name of the pass-through you want to add or remove from the system.

   *The system only accepts route DNS names (for example, www.nomadix.com). Do not include protocol, port, or path information.*

4. If adding this pass-through, click on the **Add** button, otherwise click on **Remove** to delete this pass-through from the list.

---

**Assigning a PMS Service {PMS}**

*Your product license may not support this feature.*

The Access Gateway can be integrated with existing Property Management Systems. For example, by integrating with a hotel’s PMS, the Access Gateway can post charges for Internet access directly to a guest’s hotel bill. In this case, the guest is billed only once. The Access Gateway outputs a call accounting record to the PMS system whenever a subscriber purchases Internet service and decides to post the charges to their room. The Access Gateway offers “post-paid” PMS billing functionality for all supported PMS interfaces, providing hotel guests...
with the option to terminate their connection (via the ICC) and be billed only for the actual time he/she was online. The Access Gateway is equipped with a serial port to facilitate connectivity with the system’s CLI or a customer’s Property Management System.

Some PMS vendors may require you to obtain a license before integrating the PMS with the Access Gateway. Check with the PMS vendor.

Some Property Management Systems may use interfaces that are incompatible with the Access Gateway. If your Access Gateway is having trouble communicating with a solution provider’s PMS, please contact technical support. Refer to “Contact Information” on page 311.

Before you can change the PMS settings, a PMS must be connected to the Access Gateway via the serial port on the rear panel. See also, “Connecting the Access Gateway to the Customer’s Network” on page 44.

The Access Gateway can query most popular Property Management Systems for confirmation of the “names” and “room numbers” of hotel guests—effectively becoming a “clone” of a popular Micros POS system. This functionality allows hotels to seamlessly deploy wireless networks (or alternatively use low-cost wired access concentration equipment) that either do not support port-ID or do so in a proprietary format that Nomadix does not currently support—and still be able to bill directly to the room.

Nomadix has certified interoperability with a variety of Property Management Systems:

- Encore
- FCS
- Galaxy (GEAC)
- GuestView
- Holodex (AutoClerk)
- Hilton 1
- Hilton 2
- Hotel Info Sys (HIS)
- Igets.net
- Innquest
- LanMark
- LIBICA
- Logistics
- Maestro
- Marriott
- Megasys Hospitality Systems
- Micros Fidelio FIAS (Serial, TCP/IP and Query/Post interface)
- MSI
- NH Hotels
- Protocol Technologies
- Ramesys ImagInn PMS
- OnQ (System 21)
- Xeta Virtual XL

Nomadix offers the following standards-based interfaces, generally used to establish an interface to any of the PMS systems that are not proprietary:

- HOBIC-RSI
- HOBIC-TSPS
- HOBIC-1BT2
- HOBIC-TEST
- HOBIC-OSPS
1. From the Web Management Interface, click on **Configuration**, then **PMS**. The **Property Management System Settings** screen appears:
2. You have the option of disabling PMS services by clicking on the **PMS services disabled** radio button, then clicking on the **Submit** button to save your choice. If you disable PMS services you can exit this procedure, otherwise go to Step 3.

3. Select the **Type of PMS (Pre-paid or Post-paid)** you require from the available list, or choose the **ASCII Serial Printer** option (when a serial printer is connected to the Access Gateway’s serial port)—you can choose only one of the listed options.

   The pre-paid option requires hotel guests to “pre-pay” for services. The post-paid option allows hotel guests to terminate their connection (via the ICC) and be billed only for the actual time they are online. The NH proprietary PMS is offered on a “post-paid” basis only.

   - If you choose HOBIC - RSI, you must select the **Type of Access**.
   - For Marriott, you can either choose Marriott or you can choose a type of WFB interface (Post Only, Query and Post, or Name and Room).
   - Click **Disable Registration Number** to suppress prompt for a registration number on guest login.
   - If you choose Micros Fidelio (Post Only with TCP/IP), you must provide the **Target IP Address** and the **Target Port Number**.
   - If you choose Micros (1700/2000/3700/4700/8700 emulation) you must provide the following additional information:
     - Communications System Unit Number (1 - 64)
     - Communications System Name
     - Store Revenue Center Number: Internet Access
     - Store Revenue Center Number: Other

   You also have the following check box options (see note):

   - **Match Last Name Only**
   - **Skip First Char in Last Name**
   - **OnQ Compliant** (Enable this option if you want to use Nomadix Micros POS emulation to query & post to Hilton Corporation's OnQ PMS system).
PMS solutions such as Galaxy require this option to be enabled to work with Nomadix Micros POS emulation in wireless hospitality networks. Some PMS systems send selection records as lastname, padded with white space (ascii 0x20) on the right, followed by a comma along with first name initial and some flags. Normally, the Access Gateway compares every character of the name as typed by the user to the contents of the selection record. If the “Match Last Name Only” feature is enabled, the Access Gateway compares only the user input with the part of selection record which comes before the comma (assumes that the user only enters a last name). If the “Skip First Char in Last Name” feature is enabled, the space is reserved for purposes other than the first character of the last name, so the Access Gateway will skip the first space in the last name field for name verification.

4. *Post-paid PMS only:* If you selected a Post-paid PMS option, you can define an **Idle Timeout** (in minutes) and an **Idle Data Threshold** (in bytes). These selections determine the thresholds when a “post-paid” hotel guest will be automatically disconnected from the service.

Property Management Systems generally operate at different baud rates. You must now select an appropriate baud rate for your chosen PMS.

5. Select the **Speed of PMS Interface** from the available list. If you are not sure which baud rate to choose, select **Not Sure** and the system will attempt to use the default.

6. You must now select the **Type of Service Post Mappings** you require relative to the billing plans you established in “Defining the Billing Options {Billing Options}” on page 187.

Because some Property Management Systems do not allow you to enter characters, you must enter these service descriptions as a numeric value only (no characters or delimiters). The numbers must be entered in the form of a “telephone number” which the selected PMS will interpret.

   *If the “phone number” field required by the PMS is shorter than 15 characters, only the first required number of characters will be supplied.*

7. Click on the **Submit** button to save your changes and restart the serial interface, or click on the **Reset** button if you want to reset all the values to their previous state.

   Based on the HOBIC interface standards, Nomadix, Inc. has also certified interoperability with a number of other PMS and call accounting solutions such as Ramesys’ ImagInn, Xeta Virtual XL, and Hilton’s proprietary standard OnQ. This development effort is on-going. For an up-to-date list of supported PMS systems, please contact our Technical Support team. Refer to “Appendix A: Technical Support” on page 311.
Setting Up Port Locations {Port-Location}

Port-Location allows you to establish the mode of operation for devices.

1. From the Web Management Interface, click on Configuration, then Port-Location. The Port-Location Settings screen appears:

   ![Port-Location Settings](image)

   - In Room Port Mapping
     - Enable
     - Username
     - Password

   Note: for security reasons this option should be disabled when In Room Port Mapping is done.

   - VLAN IDs
     - 802.1Q two-way

   - Access Concentrator Query
     - Tut Systems Expresso
     - Lucent DSL Terminator
     - Tut MDU Lite Systems
     - RFC1493 Compliant Systems
     - RiverDelta 1000B
     - Elastic Networks

   Note: when changing concentrator type, please remove old concentrators before entering new ones.

   - IP address:
   - SNMP community:
   - SNMP query interval: 5 (minutes) (Maximum time it takes to detect subscriber migration)

   Re-login after migration?

   [Submit] [Reset]
2. System administrators can set the properties for each room from the subscriber side of the Access Gateway. The system automatically detects which port number the administrator is using and allows them to enter the fields for the room corresponding to the port they are using.

If required, click on the check box for **In Room Port Mapping** to enable this feature.

3. If you enabled *In Room Port Mapping*, you must assign a **Username** and **Password**. You will need these when you perform port mapping from the subscriber side of the Access Gateway.

Go to “In Room Port Mapping” on page 118 to map rooms from the subscriber side of the Access Gateway.

*For security reasons, this feature should be disabled when in room port mapping (from the subscriber side of the Access Gateway) is completed.*

4. Select **No Port Location Mapping** if you are not using Port-based access.

5. If you are using an access concentration device that cannot handle VLAN IDs, select one of the available **Access Concentrator Query** options:

*The devices in the following list must be assigned an IP address on the same subnet as the Access Gateway. You must remove “old” concentrator types before entering new ones.*

- Tut Systems Expresso
- Lucent DSL Terminator
- Tut MDU Lite Systems
- RFC1493 Compliant Systems
- RiverDelta 1000B
- Elastic Networks
These options enable an SNMP query to “ask” the access concentration device which card, slot, or port the information is coming from. The information can then be “sent to” and “billed by” the PMS. You must enter the IP address (not name), SNMP community, and SNMP query duration (maximum time it takes to detect subscriber migration) of all access concentrators connected to the site. You can also opt to Relogin after migration by checking the “Relogin after migration” Enable box.

For “cascading” Tut and RFC1493 compliant systems, click on the associated Cascading button. The Cascading Support screen appears, allowing you to enter the IP address and SNMP community for the primary and all “cascading” devices connected to the site. For RFC1493 compliant systems, you have the additional option of defining the “Uplink port.”

From the Cascading Support screen, you can return to the main Port-Location Settings screen at any time by pressing the Back button.

6. Click on the Submit button to save your changes, or click on the Reset button if you want to reset all the values to their previous state.

See In Room Port Mapping.
In Room Port Mapping

This section shows In Room Port Mapping from the subscriber side, when the In Room Port Mapping feature is enabled.

Access Gateway multiple VLAN tagged systems can use the same tags and be placed on different Subscriber ports. Although it is technically possible to place two different VLAN tagged switches (one on each Subscriber side) that have the same VLAN tags designated, this configuration can cause problems. To avoid conflicts, you must ensure that the VLAN tags are different on the different devices.

1. Enable In Room Port Mapping and assign a user name and password (see previous section, Steps 2 and 3).

2. Enter the following URL target format:
   http://(Access Gateway IP address):1111/usg/roommapping
   For example:
   http://219.57.108.103:1111/usg/roommapping
   The Enter Network Password prompt appears:

   ![Enter Network Password dialog]

   Enter user name and password

   Click here if you want to save your user name and password

   OK

   Cancel
3. Enter your user name and password, then click on the **OK** button. The *In Room Port Mapping* screen appears:

4. Enter the room number and a description for this room.

5. Select the access mode you want to assign to this room:
   - Room Free Access
   - Room For Charge
   - Room Blocked

6. Click on the **Submit** button to save your changes.

7. Repeat Steps 4 through 6 for each room (see note).

*If you leave your browser open, the “cookie” that is placed on your system will allow you to go from room to room during the mapping process. However, if you close your browser, the cookie is deleted and you will need to login again.*
**Setting up Quality of Service {QoS}**

The Quality of Service feature allows subscriber traffic to be classified so that it can then be acted upon by devices that support QoS prioritization or other QoS capabilities. This requires the use of 802.1q-based VLANS on the network, as it is based on 802.1p Class of Service (CoS) marking. The QoS classification function supports both external and internal modes. In External mode, when the NSE received packets with 802.1p priority bits already set, it will pass the priority values through unaltered. In Internal mode, classification and resultant bit marking is performed via QoS policies that are defined within the NSE. The two modes can also be used in combination.

1. From the Web Management Interface, click on **Configuration**, then **QoS**. The **QoS Settings** screen appears:

   ![QoS Settings Screen](image)

2. Enable **QoS Mode** if you want to use QoS policies.

3. Enable **QoS Classification** to facilitate the classification mode desired. Classification can be based on internally defined policies, by incoming frames that are already classified, or both.

4. Enable **QoS Marking** to mark packets using 802.1p Class of Service values.
5. Select **Add Policy** to define a new QoS policy, or select a link to a policy that is already defined in order to modify it. The *Add QoS Policy for Subscribers* screen appears:

![Add QoS Policy for Subscribers](image)

6. Enter a name for the policy in the **QoS Policy** field.

7. Enter a brief summary about the policy **Description** field. The rule list displays a list of the rules that have been defined for this policy.

8. Click **Submit Policy** to accept the parameters and rules defined and add the policy to the policy list on the main page.

9. Select a traffic descriptor and a Class of Service for the rule, and then click **Add Rule**. Once added, rules will be displayed in the list above.

**Defining the RADIUS Client Settings {RADIUS Client}**

The Access Gateway supports Remote Authentication Dial-In User Service (RADIUS). RADIUS is an authentication and accounting system used by many Internet Service Providers.

```
The “Usernames” function must be enabled for a RADIUS login. See also, “Defining the AAA Services {AAA}” on page 56.
```

Nomadix offers an integrated RADIUS client, allowing service providers to track or bill users based on the number of connections, location of the connection, bytes sent and received, connect time, etc. The customer database can exist in a central RADIUS server, along with associated attributes for each user. When a customer connects into the network, the RADIUS...
client authenticates the customer with the RADIUS server, applies associated attributes stored in that customer's profile, and logs their activity (including bytes transferred, connect time, etc.).

The Access Gateway's RADIUS implementation also handles vendor specific attributes (VSAs), required by WISPs that want to enable more advanced services and billing schemes, such as a per device/per month connectivity fee.

All subscribers attempting to gain access to the network are validated by RADIUS.
For additional RADIUS information, see also:

- “Defining the RADIUS Proxy Settings {RADIUS Proxy}” on page 126
- “Defining the Realm-Based Routing Settings {Realm-Based Routing}” on page 130
- “RADIUS Attributes” on page 281

1. From the Web Management Interface, click on **Configuration**, then **RADIUS Client**. The **RADIUS Client Settings** screen appears:

   - **Server Selection and Communication**
     - Default RADIUS Mode: Disabled (to disable RADIUS authentication)
     - Realm-Based
     - Fixed

   - **Local Authentication Port**: 0 (0 means port number will be selected dynamically)
   - **Local Accounting Port**: 0 (0 means port number will be selected dynamically)

2. Under the **Server Selection and Communication** options, choose the **Default RADIUS Mode**:
   - **Disabled** (to disable RADIUS authentication)
   - **Realm-Based** (for Realm routing)
   - **Fixed** (for routing to predefined RADIUS servers)

3. Select the **Default RADIUS Service Profile** from the pull-down menu.

4. Enter a **Local Authentication Port** and a **Local Accounting Port**.
5. Select whether **Later Login Supersedes Previous**. This will allow a secondary form of authentication to override MAC authentication if necessary, and use the credentials of the last login to succeed.

See **Miscellaneous Options**.

**Miscellaneous Options**

1. In the “Miscellaneous Options” category, enter a value for the time (in seconds) in the **Default User Idle Timeout** field. This value determines how much “idle” time elapses before the subscriber’s session times out and they must log in again.

2. The Access Gateway can reauthenticate “repeat” subscribers who return to the system within 720 hours. To enable this feature, click on the check box for **Enable Automatic Subscriber Reauthentication**.

3. If you want to enable the URL redirection feature, click on the check box for **Enable URL Redirection**.

4. For a Network Access Server (NAS), if you want to send a NAS identifier with your account access request, click on the check box for **Send NAS identifier**, then define the NAS identifier in the **NAS identifier** field.

5. To send the NAS IP address with your account request, click on the check box for **Send NAS IP**.

6. To send a NAS port type with your account request, click on the check box for **Send NAS Port type**, then define the NAS port in the **NAS Port Type** field.

7. To send the Framed IP address with your account request, click on the check box for **Send Framed IP**.

8. To enable Radius termination action enhancement, click on the check box for **Enable Termination Action Radius Attribute**, then select the percentage (100% - 75%) of the maximum data volume threshold for which term-action will be enforced (volume-based sessions only).

   This option provides support for Radius Termination-Action for time- and volume-based subscribers working in conjunction with an external Radius server. Enforcement of this attribute will result in either:
   
   - logout of the subscriber
   - re-authentication of the subscriber through issuance of a new Radius Access-Request that contains a new Acct-Session ID.

   The Radius re-authentication that occurs due to term-action enforcement will be transparent to the subscriber. This is true for time based sessions that expire, as well. Radius accounting augmentation will take place as a result of a successful re-authentication.
The following VSAs are used for implementation of volume- and time-based Radius termination action:

<table>
<thead>
<tr>
<th>VSA Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Termination-Action</td>
<td>1</td>
</tr>
<tr>
<td>Session-Timeout</td>
<td>60</td>
</tr>
<tr>
<td>Nomadix-MaxBytesDown</td>
<td>3000000</td>
</tr>
<tr>
<td>Nomadix-MaxBytesUp</td>
<td>3000000</td>
</tr>
</tbody>
</table>

9. If required, check the box for **Enable Session-Terminate-End-Of-Day When Authorized** (to allow business policies that want to terminate the session at midnight of every day).

10. If required, check the box for **Enable Byte Count Reset On Account Start** (to reset the transmitted and received byte count for a subscriber once an “accounting start” is sent). This function prevents counting Walled Garden traffic if the billing plan is using bytes sent/received as a charge criterion.

11. If required, check the box for **Enable RADIUS Subnet Attribute** (if you want to allocate a specific subnet to a user).
12. If required, check the box for **Enable Goodbye URL** (if you want the system to display a post session “goodbye” page). The “goodbye” page can be defined as a RADIUS VSA or be driven by the Access Gateway’s Internal Web Server (IWS).

13. If required, check the box **Enable Forget your Password** to create a link that users can go to (and is added to the passthrough list) so they can run a page at their ISP to get their password.

14. If required, check the box **Enable RADIUS Based WAN VLAN** to allow the 802.1 q tag to be in the users profile and acted upon.

\[\text{Changing the default tag number may result in a loss of connectivity.}\]

15. Enable or disable the **User Session Time Adjustment** and credit functionality when the NSE is down.

16. **Enable charging for idle time** to count idle time in the session time of Radius accounting packets.

17. **Enable RADIUS QoS Policies** to assign a QoS policy to a user in their Radius Profile.

18. Click on the **Submit** button to save your changes, or click on the **Reset** button if you want to reset all the values to their previous state.

**Defining the RADIUS Proxy Settings {RADIUS Proxy}**

A RADIUS Proxy allows the NSE to relay authentication and accounting packets between the parties performing the authentication process. Different realms can be set up to directly channel RADIUS messages to the various RADIUS servers.

For additional RADIUS information, see also:

- “Setting up Quality of Service {QoS}” on page 120
- “Defining the Realm-Based Routing Settings {Realm-Based Routing}” on page 130
- “RADIUS Attributes” on page 281
1. From the Web Management Interface, click on **Configuration**, then **RADIUS Proxy**. The **RADIUS Proxy Settings** screen appears:

   ![RADIUS Proxy Settings](image)

   | RADIUS Proxy Services: Enable | 0 |
   | Authentication Server Port: | 0 |
   | Accounting Server Port: | 0 |
   | Local port for communicating with home servers: | 0 |

   ![Submit Reset](image)

   No upstream NASs are defined.
   - **Add**: Click here to add a new Upstream RADIUS NAS.

   Click here to see configured RADIUS service profiles and Realm Routing Policies.

2. Enable or disable **RADIUS Proxy Services**, as required, by clicking on the appropriate check box.

3. If you enabled RADIUS Proxy Services, you must provide the Authentication Server Port and the **Accounting Server Port** references.

4. Click on the **Submit** button to save your changes, or click on the **Reset** button if you want to reset all the values to their previous state.

See **Adding an Upstream RADIUS NAS**.
Adding an Upstream RADIUS NAS

1. If you want to add a new Upstream RADIUS NAS (for example, an 802.11 Access Point on the subscriber side of the Access Gateway), click on the Add button. The Add Upstream RADIUS NAS screen appears:

   
   ![Add Upstream RADIUS NAS screen](image)

   - Entry Active
   - IP Address: 
   - Authentication Secret Key: 
   - Accounting Secret Key: 

   **Note:** RADIUS requests originating from this Upstream NAS will be routed via the specified profile if it cannot be routed based on realm. Leave this field blank if default routing is not desired.

   - Default RADIUS Service Profile: (none)

   - Nomadix VSAs to be enforced by the Proxy for this entry
     - Enforce Bandwidth-Up VSA
     - Enforce Bandwidth-Down VSA
     - Enforce Redirect-URL VSA
     - Enforce Ip-Upsell VSA
     - Enforce Subnet VSA
     - Enforce QoS-Policy VSA

2. To make this entry the “active” NAS entry, click on the Entry Active check box.
3. Enter an IP Address for the Upstream NAS.
4. Enter a secret key in the Authentication Secret Key field. During the authentication process, the server and client exchange secret keys. The secret keys must match for communication between the server and the client to continue. The secret key is a valuable and necessary security measure.
5. Enter a secret key in the Accounting Secret Key field.
6. Select the Default RADIUS Service Profile from the pull-down menu (see note).

   **Note:** RADIUS requests originating from this Upstream NAS will be routed via the specified profile if it cannot be routed based on realm. Leave this field blank if default routing is not desired.
7. Place a check in the box of the **Nomadix VSAs to be enforced by the Proxy for this entry**:
   - **Enforce Bandwidth-Up VSA**: The Radius VSA for Bandwidth-Up will be passed on to the Upstream NAS when enabled.
   - **Enforce Bandwidth-Down VSA**: The Radius VSA for Bandwidth-Down will be passed on to the Upstream NAS when enabled.
   - **Enforce Redirect-URL VSA**: The Radius VSA for Redirect-URL will be passed on to the Upstream NAS when enabled.
   - **Enforce IP-Upsell VSA**: The Radius VSA for Ip-Upsell will be passed on to the Upstream NAS when enabled.
   - **Enforce Subnet VSA**: The Radius VSA for Subnet will be passed on to the Upstream NAS when enabled.
   - **Enforce QoS-Policy VSA**: The Radius VSA for QoS-Policy will be passed on to the Upstream NAS when enabled.

8. Click on the **Add** button to add this Upstream RADIUS NAS definition, then click on the **Back to Main RADIUS Proxy Settings page** link to return to the **RADIUS Proxy Settings** screen.
The Upstream RADIUS NAS definition you just added appears in the list. You can add up to 10 definitions.

**RADIUS Proxy Settings**

RADIUS Proxy Services: **Enable**

Authentication Server Port: 1812  
Accounting Server Port: 1813

[Submit]  [Reset]

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Default Service Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1</td>
<td>CWS</td>
</tr>
<tr>
<td>10.0.0.5</td>
<td>CWS</td>
</tr>
<tr>
<td>10.0.0.2</td>
<td>CWS</td>
</tr>
</tbody>
</table>

Click here to add a new Upstream RADIUS NAS.

9. Repeat Steps 5 through 11 to add more Upstream RADIUS NAS definitions, as required.

10. To view your configured RADIUS Service Profiles and Realm Routing Policies, click on the link: *Click here to see configured RADIUS service profiles and Realm Routing Policies* (this will take you to the *Realm-Based Routing Settings* screen).

See also, “Defining the Realm-Based Routing Settings {Realm-Based Routing}” on page 130.

**Defining the Realm-Based Routing Settings {Realm-Based Routing}**

Use this procedure when setting up RADIUS Service Profiles (up to 10) and Realm-based Routing Policies (up to 50).

For additional RADIUS information, see also:

- “Setting up Quality of Service {QoS}” on page 120.
- “Defining the RADIUS Proxy Settings {RADIUS Proxy}” on page 126.
“RADIUS Attributes” on page 281

From the Web Management Interface, click on Configuration, then Realm-Based Routing. The Realm-Based Routing Settings screen appears:

**Add Realm Routing Policy**

Entry Active

<table>
<thead>
<tr>
<th>Specific Realm</th>
<th>Realm name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wildcard match</td>
<td></td>
</tr>
</tbody>
</table>

Prefix match only (Match characters preceding "/")
Suffix match only (Match characters following ",", i.e., NAI realm)
Match either (Try prefix first, then try suffix if no prefix match)

**RADIUS Service Profile:**
Strip off routing information when sending to RADIUS server
Tunnel Profile

**Tunnel Parameters (for prefix-checked or RADIUS-tidigged tunnels):**
Strip off routing information when sending to tunnel server
Local hostname:

---

**Define RADIUS Service Profiles**

RADIUS service profiles are used to direct username access requests for both plain RADIUS users and users who supply realm/domain in their username. In response to a RADIUS access request, these RADIUS servers will return the L2TP tunnel parameters which the NSE will use to establish an L2TP tunnel.

Create a RADIUS service profile to a RADIUS server that will handle Prefix-based users. This is to handle users that will login with a username in the format type of “ISP/username”. In this case the delimiter is “/” and what appears before it, “ISP”, is the realm name.

Create a RADIUS service profile for a RADIUS server that will handle Suffix-based users. This is to handle users that will login with a username in the format type of “username@ISP.com”. In this case the delimiter is “@” and what appears after it, “ISP.com”, is the realm name.
To add a RADIUS Service Profile, click on the appropriate **Add** button. The *Add RADIUS Service Profile* screen appears:

![Add RADIUS Service Profile](image)

Enter a name of your choice for this service profile in the **Unique Name** field.

**Authentication**

This category requires input for enabling RADIUS authentication and requires you to define IP addresses, ports, and secret keys for the primary and secondary RADIUS servers (the secondary server is optional).

1. Enable or disable the RADIUS Authentication Service, as required, by clicking on the **Enable RADIUS Authentication Service** check box.

2. If you enabled the RADIUS Authentication Service, enter the *primary* RADIUS authentication server IP address in the **Primary IP** field. This field can also be populated by a DNS name to allow for changing the DNS resolution, instead of having to change settings in the NSE when the IP of the Radius server changes.

3. Enter the authorization port in the **Port** field for the *primary* RADIUS authentication server. This is the port the system uses when authorizing subscribers.

4. Enter a secret key in the **Secret Key** field for the *primary* RADIUS authentication server. During the authentication process, the server and client exchange secret keys. The secret...
keys must match for communication between the server and the client to continue. The secret key is a valuable and necessary security measure.

The Access Gateway and the RADIUS servers must use the same secret key.

5. Repeat Steps 2 through 4 for the secondary RADIUS authentication server (if used).

**Accounting**

This category requires input for enabling the RADIUS accounting service, and also requires the necessary IP addresses, ports and secret keys for the primary and secondary RADIUS accounting servers. The RADIUS accounting server is responsible for receiving accounting requests and returning a response to the client indicating that it has received the request.

1. To enable the accounting service for your RADIUS functionality, click on the check box for Enable RADIUS Accounting Service.
2. Enter the primary RADIUS accounting server IP address in the Primary IP field.
3. Enter the accounting port in the Port field for the primary RADIUS accounting server. This is the port the system uses when communicating accounting records.
4. Enter a secret key in the Secret Key field for the primary RADIUS accounting server.
5. Repeat Steps 1 through 4 for the secondary RADIUS accounting server (if used).

**Retransmission Options**

This category requires you to define the data retransmission method (failover or round-robin), the retransmission frequency, and how many retransmissions the system should attempt.

1. Select the Retransmission Method (Failover or Round Robin).
2. Enter a value for the time (in seconds) in the Retransmission Frequency field. This value determines how much time elapses between transmission attempts.
3. Enter a numeric value in the Retransmission Attempts (per server) field to define how many times the system attempts to transmit the data.
4. Click on the Add button to add this RADIUS Service Profile.
5. When you have completed the definition of your RADIUS Service Profile, you can return to the previous screen (Realm-Based Routing Settings) by clicking on the Back to Main Realm-Based Routing Settings page link.

The RADIUS Service Profile you just created is added to the list.
Define Tunnel Profiles

Tunnel profiles can be defined when L2TP tunnel parameters are known and it is not necessary to send an access request to a RADIUS server to obtain those parameters or for accounting purposes.

Create a tunnel profile for each L2TP tunnel whose parameters are known. The tunnel parameters that the profile contains are the IP address of the LNS and the tunnel password. See Figure 2 for an example of a tunnel profile. Where is Figure 2?

Define Realm Routing Policies

Realm routing policies are used to determine how supplied username/password input is used to authenticate users. Create a realm routing policy for each realm that will be handled. The realm routing policy will reference either a RADIUS service profile or a tunnel profile. Many different realm routing policies can reference the same RADIUS service or tunnel profile.

This policy references a RADIUS service profile so a realm match will result in an access request being sent to the RADIUS server(s) specified in the RADIUS service profile. In this case, the RADIUS service profile “RadiusPrefix” is referenced and so the RADIUS server(s) defined therein will receive RADIUS access requests.

Notice that the checkbox is unchecked for “Strip off routing information when sending to RADIUS server”. This box must always be unchecked in order to pass realm information to the RADIUS server(s) for matching of realm information to its defined tunnel profiles, which contain the needed tunnel parameters.

The checkbox “Strip off routing information when sending to tunnel server” may or may not be checked depending on the configuration of the tunnel server and how it will be authenticating subscribers. In this example, it is checked and so realm information will be stripped leaving only the simple username and password to be passed to the tunnel server.
The tunnel server in this case is configured to authenticate users via another RADIUS server that handles a single realm. Since it handles a single realm, no realm information is needed for users and so must be stripped. In this case, it is stripped by the NSE, but it could easily have been stripped by the tunnel server, or by the tunnel server’s RADIUS server. This is by design and for maximum flexibility.

Also note that the “Local hostname” field is blank which means that the NSE’s default local hostname of “usg_lac” will be used by the NSE. This allows for setting the local hostname to any desired value other than the default. The L2TP peers exchange their local hostnames during tunnel negotiation.

1. To add a RADIUS Service Profile, click on the appropriate **Add** button on the **Realm-Based Routing Settings** screen.

   The **Add Realm Routing Policy** screen appears:

2. To make this entry the “active” entry, click on the **Entry Active** check box.

3. To define a specific realm, choose the **Specific Realm** option and enter the destination in the **Realm Name** field. Alternatively, you can choose the **Wildcard match** option, then define your search options:
   - Prefix match only
   - Suffix match only
   - Match either

4. Select the required **RADIUS Service Profile** from the pull-down menu.

5. Click on the **Strip off routing information** check box if you want to remove the routing information.

6. Click on the **Add** button to add this Realm Routing Policy.

7. When you have completed the definition of your Realm Routing Policy, you can return to the previous screen (Realm-Based Routing Settings) by clicking on the **Back to Main Realm-Based Routing Settings page** link.

   The screen below shows a realm routing policy that handles prefix-based usernames using a RADIUS service profile. Notice that “Specific Realm” is clicked and the “Realm name” is “cisp”. Also notice that “Prefix match only” is clicked and that the delimiter is “/”. This means that this realm routing policy will match usernames that are of the format “cisp/username”.

   ![Realm Routing Policy Example](image-url)
Add Realm Routing Policy

Entry Active

Specific Realm
Realm name: cisp

Wildcard match

Prefix match only (Match characters preceding '/')
Suffix match only (Match characters following '@', i.e., NAI realm)
Match either (Try prefix first, then try suffix if no prefix match)

RADIUS Service Profile: RadiusPrefix
Strip off routing information when sending to RADIUS server

Tunnel Profile: (none)

Tunnel Parameters (for profile-triggered or RADIUS-triggered tunnels):
Strip off routing information when sending to tunnel server
Local hostname:

Add

Back to Main Realm-Based Routing Settings page
The following screen shows a realm routing policy that handles suffix-based usernames using a tunnel profile.

This differences in this example are that the realm name is “tcisp.com”, “Suffix match only” is enabled (the delimiter in this case is “@”), and a tunnel profile, “LNSOne”, is selected instead of a RADIUS service profile.

This means that this realm routing policy will match usernames that are of the format “username@tcisp.com”. Since this policy references a tunnel profile, no RADIUS access requests will be sent to any RADIUS server. In this case, the NSE will use the L2TP tunnel parameters specified in the tunnel profile to establish a tunnel and pass the username/password input to the tunnel server.

Again, as before, the username passed to the tunnel server will have realm information stripped since the checkbox for “Strip off routing information when sending to tunnel server” is checked. This checkbox may be unchecked if it is necessary for usernames to contain realm information for user authentication.
The “Local hostname” field is also blank in this example which means that the NSE will use the default value of “usg_lac” during tunnel negotiation.

**Configure RADIUS Client**

The NSE RADIUS client must be setup for realm-based routing mode since realm information will be used by the NSE’s L2TP tunnel feature to determine how to handle usernames that contain realm information. The screen below shows an example of setting the routing mode to handle realm-based usernames.

The Realm Routing Policy you just created is added to the list. That covers the main steps for configuring an NSE to support L2TP tunneling.
Managing SMTP Redirection {SMTP}

When SMTP redirection is enabled (for misconfigured or properly configured subscribers), the Access Gateway redirects the subscriber’s E-mail through a dedicated SMTP server, including SMTP servers which support login authentication. To the subscriber, sending and receiving E-mail is as easy as it’s always been. This function is transparent to subscribers.

1. From the Web Management Interface, click on **Configuration**, then **SMTP**. The **SMTP Redirection Settings** screen appears:

   **SMTP Redirection Settings**

   - SMTP Redirection (Misconfigured) [ ] Enable
   - SMTP Redirection (Properly Configured) [ ] Enable
   - SMTP Server IP / DNS Name

   For SMTP servers which support login authentication, enter valid username and password for an account on that server.
   - SMTP Server Account Username
   - SMTP Server Account Password

   [Submit] [Reset]

2. Click on the check box for **SMTP Redirection (Misconfigured)** to enable this feature for “misconfigured” subscribers.

3. Click on the check box for **SMTP Redirection (Properly Configured)** to enable this feature for “properly configured” subscribers.

   If you enable SMTP redirection, you must provide the IP address of the SMTP server.

4. In the **SMTP Server IP/DNS** field, enter the address of the SMTP server you want to use.

5. For SMTP servers which support login authentication, enter a valid username in the **SMTP Server Account Username** field.

6. For SMTP servers which support login authentication, enter a valid password in the **SMTP Server Account Password** field.

7. Click on the **Submit** button to save your changes, or click on the **Reset** button if you want to reset all the values to their previous state.
Managing the SNMP Communities {SNMP}

You can address the Access Gateway using an SNMP client manager (for example, HP OpenView). SNMP is the standard protocol that regulates network management over the Internet. To do this, you must set up the SNMP communities and identifiers. For more information about SNMP, see “Using an SNMP Manager” on page 54.

If you want to use SNMP, you must manually turn on SNMP.

1. From the Web Management Interface, click on Configuration, then SNMP. The SNMP Settings screen appears:

2. Click on the check box for SNMP Daemon to enable this functionality.
3. Enter the SNMP parameters (communities and identifiers), including:
   - System Contact
   - System Location
   - Get (Read) Community
   - Set (Write) Community
   - Trap Community
   - Trap Recipient IP
   - Specify DAT Trap Interval (15-600) sec
   - check the box to enable Subscriber1 Link Traps
   - check the box to enable Subscriber2 Link Traps

   Your SNMP manager needs this information to enable network management over the Internet.

4. When finished, you must reboot the system for the new settings to take effect. Click on the check box for **Reboot after changes are saved?** to reboot the system after saving your changes.

5. Click on the **Submit** button to save your changes and reboot the system, or click on the **Reset** button if you want to reset all the values to their previous state.

   You can now use your SNMP client to manage the Access Gateway via the Internet.

---

**Enabling Dynamic Multiple Subnet Support (Subnets)**

Nomadix’ dynamic multiple subnet support allows you to create flexible and cost-effective IP pool solutions to meet the demands of complex networks in large residential and public access networks. For example:

- Establish a maximum of 15 different DHCP pools for routable IP addresses at the same time.
- Establish a maximum of 10 different public IP subnets that will not be address-translated by Nomadix’ market-leading Dynamic Address Translation (DAT) feature.
- Define the user's subnet via the management interfaces.
1. From the Web Management Interface, click on Configuration, then Subnets. The Public Subnets Settings screen appears:

   ![Public Subnets Settings](image)

   **Public Subnets Settings**

<table>
<thead>
<tr>
<th>Subnet</th>
<th>Netmask</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5.3.1</td>
<td>255.255.255.224</td>
</tr>
</tbody>
</table>

   Click here to add a new Public Subnet.

2. Click on the Add button to add a new public subnet. The Add Public Subnets screen appears:

   ![Add Public Subnets](image)

   **Add Public Subnets**

   ![Subnet field](image)
   ![Subnet Mask field](image)

   ![Add button](image)

3. Enter a valid IP address for this subnet in the Subnet field.
4. Enter the subnet mask for this subnet in the Subnet Mask field.
5. Click on the Back to Main Subnet Configuration Page link to return to the previous screen (Public Subnets Settings).
To edit the “Current Public DHCP Subnets” table, go to “Managing the DHCP service options {DHCP}” on page 82.

For additional information about the multiple subnet feature, go to “Contact Information” on page 311 for Nomadix Technical Support.

**Displaying Your Configuration Settings {Summary}**

You can display a summary listing of all your current Configuration settings.

To view the summary listing, go to the Web Management Interface, click on Configuration, then click on Summary.
The Summary of Configuration Settings screen appears (partial screen shown here):

### Summary of Configuration Settings

- **Current time:** TUE MAY 18 09:52:57 2010
- **Read-Only Values**
  - Operating System Version: AG 6000 v7.8.0.29
  - Operating System Installed: Fri Apr 24 09:42:24 2009
  - NSE ID: 
  - Network MAC Address: 00-50-65-01-63-3F
  - Subscribed MAC Address (Interface 1): 00-50-65-01-63-3E
  - Subscribed MAC Address (Interface 2): 00-50-65-01-63-3D
  - Dynamic Address Translation: Enabled
  - DNS Resolution: Enabled

### Authentication And Authorization Settings
- AAA Services: Enabled
- XML Interface: Enabled
- XML Server 1 IP: 07.130.149.167
- XML Server 2 IP: 07.131.213.194
- AAA Pass-through Port: Disabled
- AAA Pass-through Port: 0
- Print Billing Command: Disabled
- Print Server URL: Enabled
- 802.1X: Disabled
- 802.1X Re-auth period (sec): 0
- OS Encoding: Disabled
- Login Page/EWS Fallover: Disabled
- Port-based Billing Policies: Enabled
- Authorization Mode: Internal Web Server
- SSL: Disabled
- Only encrypt sensitive data: Enabled
- Certificate DNS Name: ssl.certdata.com
- Credit Card Service: Enabled
- Portal Pages: Enabled
- Portal Pages URL: http://87.130.149.167/content162.htm
- Parameter Passing: Disabled
- Manual Pass-through Address: Disabled

More listings ...

### Setting the System Date and Time {Time}

This procedure shows you how to set the system date and time.
1. From the Web Management Interface, click on **Configuration**, then **Time**. The *Set Date and Time* screen appears:

![Set Date and Time](image)

2. Select **Internal Time** to use the local hardware time or select **External Time Server** if you want to use NTP instead of the internal clock of the NSE.

   If you select **Internal Time**, enter the new date and time parameters in the relevant fields (if required):
   - Year (####)
   - Month (1-12)
   - Day (1-31)
   - Hour (0-23)
   - Minute (0-59)

   After entering new data for the final parameter (minutes), the system writes the information into its BIOS, then displays the new date and time.
If you select **External Time**:

- In the **Server Timeout** field, enter the number of seconds before the NSE gives up on receiving a time response from the NTP server.
- In the **Time Server 1-4** fields, enter up to 4 different NTP servers to query for the correct time.

3. The Access Gateway also allows you to enter a “Time offset from UTC.” This parameter is the Universal Coordinated Time, based on the ISO 8601 standard, and is used in conjunction with RADIUS servers (for example, if the RADIUS server is setup for a time zone that is different from the Access Gateway).

4. When finished, click on the **Submit** button to save your changes, or click on the **Reset** button if you want to reset all the values to their previous state.

**Setting up Traffic Descriptors**

Traffic Descriptors are a dependency of creating rules for a Quality of Service Policy. The Traffic Descriptors are how the Access Gateway identifies subscriber traffic. They are conditions or a group of conditions that are linked to a description.

1. From the Web Management Interface, click on **Configuration**, then **Traffic Descriptor**. The Traffic Descriptor Settings screen appears:
2. Select **Add** to create a new Traffic Descriptor, or select a link to an existing descriptor to modify it. The Add Traffic Descriptor screen appears.

3. Enter a name for the descriptor in the **Unique Name** field.

4. Enter a brief summary about the descriptor in the **Description** field.

5. Set condition matching to require a match to **All** conditions or **Any** one of the conditions. This condition list displays a list of the conditions that have been defined for this descriptor.

   Select a condition type from the **Add Condition** menu and define the matching parameters. Once added, conditions will be displayed in the condition list.

6. Select **Remove** to remove a condition from this descriptor.

7. Select **Add Descriptor** to accept the parameters and conditions defined and add the descriptor to the descriptor list on the main page.

### Setting Up URL Filtering {URL Filtering}

The Access Gateway can restrict access to specified Web sites based on URLs defined by the system administrator. URL filtering will block access to a list of sites and/or domains entered by the administrator using the following three methods:

- **Host IP address** (for example, 1.2.3.4)
- **Host DNS name** (for example, www.yahoo.com)
DNS domain name (for example, *.yahoo.com, meaning all sites under the yahoo.com hierarchy, such as finance.yahoo.com, sports.yahoo.com, etc.). The system administrator can dynamically add or remove specific IP addresses and domain names to be filtered for each property.

1. From the Web Management Interface, click on Configuration, then URL Filtering. The URL Filtering Address Settings screen appears:

![URL Filtering Address Settings](image)

Please enter either an IP address or a DNS name or a Domain name and click on one of the provided buttons.

**Note:** DNS name and Domain name should not contain protocol, port, or path information.

Up to 300 URL Filtering Addresses can be entered.

**IP/DNS Name:** [www.test.com]  
Add | Remove

2. If you want to enable this feature, click on the check box for URL Filtering.

3. Click on the **Submit** button to save your setting.

4. If URL Filtering is enabled, you can add (or remove) up to 300 addresses in the IP/DNS Name field. After entering the address you want to add, simply click on the Add button (the address will be added to the displayed list). Add or remove addresses, as required.

**Selecting User Agent Filtering Settings**

The Access Gateway can ignore traffic being generated by unsubscribed user devices that are not accessing walled garden sites or an unauthenticated users.
1. From the Web Management Interface, click on **Configuration**, then **User Agent Filtering**. The **User Agent Filtering Settings** screen appears:

![User-Agent Filtering Settings](image)

2. Enable **User-Agent Filtering** to use the filtering capabilities for the User-Agents.

3. Add the names of the different User-Agents that you want to filter to the **HTTP User-Agent name** field. Windows Update and Apple iTunes are default filtered Agents.

### Zone Migration

Zone migration is an expansion of the NSE’s “re-login after migration” capability, which currently allows the system to force a subscriber to log in again if the subscriber moves from one port location to another. Zone migration significantly expands this capability via the following means:

- It allows the creation of multiple zones, which are then constituted by groupings of multiple port locations. These groupings can be made up of any combination of desired ports (port values do not have to be sequential in order to be grouped within a given zone).
- The re-login requirement can then be configured so that subscribers can move from one port to another within a zone without being required to re-login. However, when moving between ports in different zones, the re-login requirement is enforced.
- It is also possible to configure a zone so that migration between ports within the zone requires the user to re-login.
- In addition, the re-login after migration function was previously limited to RADIUS and PMS users. This capability has now been extended to other subscriber login types.
1. From the Web Management Interface, click on Configuration, then Zone Migration. The Zone Migration Settings screen appears:

![Zone Migration Settings](image)

2. Select ReLogin after migration to enable the Zone Migration feature.

Add a new Zone

In the Zone-Based Migration section, new zones can be added and initially configured, using the following parameter fields:

- **Zone Name** – Allows entry of a name appropriate for the zone to be created. The name must be unique, cannot exceed 16 characters, and cannot contain characters that are not alphanumeric, dash, underscore, or space.

- **Port-Locations** – This is where the port configuration for the zone is entered. The data must be entered as a string between 1 and 128 characters in length. The string must contain either an individual numeric value ("211"), a comma-separated list of numeric values ("211, 212"), a range of numeric values with dash-separated delimiters ("211-899"), a list of ranges of numeric values ("211-300, 301-899"), or a comma-separated list of individual numeric values and ranges ("211, 212, 213-899").

- **Description** – Allows entry of a description for the zone. This must be a string between 0 and 128 characters in length, and cannot contain characters that are not alphanumeric, dash, underscore, or space.

In each of these fields, any leading or trailing spaces will be removed by the NSE when the page is submitted.
Relogin within Zone

This selection provides the option to require relogin after migration between ports that are within a given zone. The default is Disabled.

Existing Zones

Zones that have already been defined are listed here, and can be edited or deleted. (Note: The description field is not displayed in the list view).

Defining IPSec Tunnel Settings

There are many different ways to configure, manage and monitor the performance and up-time of network devices. SNMP, Telnet, HTTP and ICMP are all common protocols to accomplish network management objectives. And within those objectives is the requirement to provide the highest level of security possible.

While several network protocols have evolved that offer some level of security and data encryption, the preferred method for attaining maximum security across all network devices is to establish an IPSec tunnel between the NOC (Network Operations Center) and the edge device (early VPN protocols such as PPTP have been widely discredited as a secure tunneling method).

As part of Nomadix’ commitment to provide outstanding carrier-class network management capabilities to its family of public access gateways, we offer secure management through the NSE’s standards-driven, peer-to-peer IPSec tunneling with strong data encryption. Establishing the IPSec tunnel not only allows for the secure management of the Nomadix gateway using any preferred management protocol, but also the secure management of third party devices (for example, WLAN Access Points and 802.3 switches) on private subnets on the subscriber side of the Nomadix gateway.

The advantage of using IPSec is that all types of management traffic are supported, including the following typical examples:

- ICMP - PING from NOC to edge devices
- Telnet - Telnet from NOC to edge devices
- Web Management - HTTP access from NOC to edge devices
- SNMP
  - SNMP GET from NOC to subscriber-side device (for example, AP)
  - SNMP SET from NOC to subscriber-side device (for example, AP)
  - SNMP Trap from subscriber-side device (for example, AP) to NOC
Two subsequent events drive the secure management function of the Nomadix gateway and the devices behind it:

1. Establishing an IPSec tunnel to a centralized IPSec termination server (for example, Nortel Contivity). As part of the session establishment process, key tunnel parameters are exchanged (for example, Hash Algorithm, Security Association Lifetimes, etc.).

2. The exchange of management traffic, either originating at the NOC or from the edge device through the IPSec tunnel. Alternatively, AAA data such as RADIUS Authentication and Accounting traffic can be sent through the IPSec tunnel. See also, “Defining Automatic Configuration Settings {Auto Configuration}” on page 70.

This procedure allows system administrators to establish the peer-to-peer IPSec connection. Basic IPSec parameters must be entered by the system administrator to successfully establish the VPN session.

We recommend that you create different private subnets behind the VPN termination device and the Access Gateway.
Network Info Menu

**Displaying ARP Table Entries {ARP}**

You can display a table that shows the current status of the ARP (Address Resolution Protocol) assignments. ARP is used to dynamically bind a high level IP address to a low level physical hardware (MAC) address. ARP is limited to a single physical network that supports hardware broadcasting.

To view the *ARP Table*, go to the Web Management Interface, click on **Network Info**, then click on **ARP**.

The *ARP Table* screen appears:

<table>
<thead>
<tr>
<th>LINK LEVEL ARP TABLE</th>
<th>flags</th>
<th>Refcnt</th>
<th>Use</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.3.4</td>
<td>00:90:27:bd:2c:df</td>
<td>405</td>
<td>1</td>
<td>545</td>
</tr>
<tr>
<td>2.3.4.5</td>
<td>00:c0:7b:81:ac:b0</td>
<td>405</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Displaying DAT Sessions {DAT}**

Dynamic Address Translation (DAT) allows all users to obtain network access, regardless of their computer’s network settings.

To view the *DAT Session Table*, go to the Web Management Interface, click on **Network Info**, then click on **DAT**.
The **DAT Session Table** screen appears:

![DAT Session Table](image)

Click on the **Delete all sessions** button to clear all current subscriber sessions.

*Deleting DAT sessions will cause all misconfigured subscribers to lose their Internet connection for a short period of time.*

**Displaying the Host Table {Hosts}**

You can display a table which lists the hosts that are currently configured. This table includes the assigned host names, their corresponding IP addresses, and any aliases that may be assigned to each host. Hosts provide services to other computers that are linked to it by a network.

To view the **Host Table**, go to the Web Management Interface, click on **Network Info**, then click on **Hosts**.
The *Host Table* screen appears:

```
<table>
<thead>
<tr>
<th>hostname</th>
<th>inst address</th>
<th>aliases</th>
</tr>
</thead>
<tbody>
<tr>
<td>localhost</td>
<td>127.0.0.1</td>
<td></td>
</tr>
<tr>
<td>AG 5000</td>
<td>67.130.149.163</td>
<td></td>
</tr>
</tbody>
</table>
```

**Displaying ICMP Statistics {ICMP}**

You can display the current ICMP (Internet Control Message Protocol) statistics. ICMP is a standard Internet protocol that delivers error and control messages from hosts to message requestors. These statistics are presented as a listing which details the current status of each ICMP transmission element.

To view the *ICMP Statistics*, go to the Web Management Interface, click on **Network Info**, then click on **ICMP**.

The *ICMP Statistics* screen appears:

```
ICMP:
  0 call to icmp_error
  0 error not generated because old message was icmp
Output histogram:
  echo reply: 3
  0 message with bad code fields
  0 message < minimum length
  0 bad checksum
  0 message with bad length
Input histogram:
  routing redirect: 8
  echo: 3
  3 message responses generated
```

**Displaying the Network Interfaces {Interfaces}**

You can display the network interfaces which are presented as a detailed listing of all interface communication elements and their current status.

To view the *Network Interfaces*, go to the Web Management Interface, click on **Network Info**, then click on **Interfaces**.
The **Network Interfaces** screen appears:

### Network Interfaces

<table>
<thead>
<tr>
<th>Network Interface</th>
<th>Flags</th>
<th>Transmission Mode</th>
<th>Speed</th>
<th>MTU</th>
<th>Metric</th>
<th>Maximum Transfer Unit Size</th>
<th>Unit Size</th>
<th>Packets Received</th>
<th>Packets Sent</th>
<th>Errors</th>
<th>Discarded</th>
<th>Dropped</th>
<th>Queue Drops</th>
</tr>
</thead>
<tbody>
<tr>
<td>lo (unit number 0)</td>
<td>0x450A9</td>
<td>UP, MULTICAST, TRAILERS, ARP, RUNNING INET_UP</td>
<td>1500</td>
<td>65536</td>
<td>0</td>
<td>1500</td>
<td>65536</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>rtl (unit number 0)</td>
<td>0x888C</td>
<td>Link up, Auto-succeeded</td>
<td>100 Mbits</td>
<td>65536</td>
<td>0</td>
<td>1500</td>
<td>65536</td>
<td>16386</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5702033</td>
</tr>
<tr>
<td>rtl (unit number 1)</td>
<td>0x888C</td>
<td>Link up, Auto-succeeded</td>
<td>100 Mbits</td>
<td>65536</td>
<td>0</td>
<td>1500</td>
<td>65536</td>
<td>32912</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>238139037</td>
</tr>
</tbody>
</table>

**System Administration**
**Displaying the IP Statistics {IP}**

You can display the IP (Internet Protocol) statistics which are presented as a detailed listing of all IP elements and their current status. With IP transmissions, data is broken up into packets which are then sent over the network. By using IP addressing, Internet Protocol ensures that the data reaches its destination, even though different packets may “pass through” different networks to get to the same location.

To view the IP Statistics, go to the Web Management Interface, click on Network Info, then click on IP.

The IP Statistics screen appears:

```
<table>
<thead>
<tr>
<th>Statistics</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>total</td>
<td>3343</td>
</tr>
<tr>
<td>badsum</td>
<td>0</td>
</tr>
<tr>
<td>tooshort</td>
<td>0</td>
</tr>
<tr>
<td>tooosmall</td>
<td>0</td>
</tr>
<tr>
<td>badhlen</td>
<td>0</td>
</tr>
<tr>
<td>badlen</td>
<td>0</td>
</tr>
<tr>
<td>infragments</td>
<td>0</td>
</tr>
<tr>
<td>fragdropped</td>
<td>0</td>
</tr>
<tr>
<td>fragtimeout</td>
<td>0</td>
</tr>
<tr>
<td>forward</td>
<td>0</td>
</tr>
<tr>
<td>canforward</td>
<td>0</td>
</tr>
<tr>
<td>redirectsent</td>
<td>0</td>
</tr>
<tr>
<td>unknownprotocol</td>
<td>0</td>
</tr>
<tr>
<td>nobuffers</td>
<td>0</td>
</tr>
<tr>
<td>reassembled</td>
<td>0</td>
</tr>
<tr>
<td>outfragments</td>
<td>0</td>
</tr>
<tr>
<td>noroute</td>
<td>0</td>
</tr>
</tbody>
</table>
```

**Viewing IPSec Tunnel Status {IPSec}**

To view the current IPSec Tunnel Status, go to the Web Management Interface, click on Network Info, then click on IPSec.

**Displaying the Routing Tables {Routing}**

You can display the current Routing Tables, including any dynamically generated routes, unreachable routes, or wildcard routes.
To view the Routing Tables, go to the Web Management Interface, click on Network Info, then click on Routing.

The Routing Tables screen appears:

### Routing Tables

<table>
<thead>
<tr>
<th>DESTINATION</th>
<th>GATEWAY</th>
<th>FLAGS</th>
<th>REFCTR</th>
<th>USE</th>
<th>INTERFACE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>1.2.3.4</td>
<td>3</td>
<td>1</td>
<td>890</td>
<td>fei0</td>
</tr>
<tr>
<td>4.2.75.0</td>
<td>5.6.7.8</td>
<td>101</td>
<td>0</td>
<td>0</td>
<td>fei0</td>
</tr>
<tr>
<td>4.2.75.1</td>
<td>3.4.5.6</td>
<td>101</td>
<td>0</td>
<td>0</td>
<td>fei1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DESTINATION</th>
<th>GATEWAY</th>
<th>FLAGS</th>
<th>REFCTR</th>
<th>USE</th>
<th>INTERFACE</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.86</td>
<td>5.8.7.6</td>
<td>17</td>
<td>0</td>
<td>1448</td>
<td>fei0</td>
</tr>
<tr>
<td>10.1.1.109</td>
<td>6.7.6.5</td>
<td>17</td>
<td>0</td>
<td>301</td>
<td>fei0</td>
</tr>
<tr>
<td>10.1.1.205</td>
<td>7.6.5.4</td>
<td>17</td>
<td>0</td>
<td>6</td>
<td>fei0</td>
</tr>
<tr>
<td>10.1.1.225</td>
<td>4.3.2.1</td>
<td>17</td>
<td>1</td>
<td>1848</td>
<td>fei0</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>lo0</td>
</tr>
<tr>
<td>2.1.1.8</td>
<td>2.6.9.8</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>fei0</td>
</tr>
</tbody>
</table>

routing:
- 4 bad routing redirects
- 4 dynamically created routes
- 0 new gateway due to redirects
- 0 destination found unreachable
- 0 use of a wildcard route

### Displaying the Active IP Connections {Sockets}

You can display a table which provides a detailed listing of all currently active IP (Internet Protocol) connections.

To view the Socket Table, go to the Web Management Interface, click on Network Info, then click on Sockets.
The **Socket Table** screen appears:

### Socket Table

<table>
<thead>
<tr>
<th>PCB</th>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>3e6d2d8</td>
<td>TCP</td>
<td>0</td>
<td>742</td>
<td>8.6.1.7.80</td>
<td>3.2.8.1.18</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>3e6d1d0</td>
<td>TCP</td>
<td>0</td>
<td>C</td>
<td>8.6.1.7.80</td>
<td>3.2.8.1.18</td>
<td>TIME_WAIT</td>
</tr>
<tr>
<td>3e60c68</td>
<td>TCP</td>
<td>0</td>
<td>C</td>
<td>8.6.1.7.80</td>
<td>3.2.5.1.18</td>
<td>TIME_WAIT</td>
</tr>
<tr>
<td>3e6cd2e</td>
<td>TCP</td>
<td>0</td>
<td>C</td>
<td>8.6.1.7.21</td>
<td>0.4.5.1.24</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>3e66e6e</td>
<td>TCP</td>
<td>0</td>
<td>C</td>
<td>0.0.0.11.111</td>
<td>0.0.0.0.0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>3e6c678</td>
<td>TCP</td>
<td>0</td>
<td>C</td>
<td>0.0.0.30.0</td>
<td>0.0.0.0.0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>3e65f4a</td>
<td>TCP</td>
<td>0</td>
<td>C</td>
<td>0.0.0.23</td>
<td>0.0.0.0.0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>3e6c6ec</td>
<td>TCP</td>
<td>0</td>
<td>C</td>
<td>0.0.0.60</td>
<td>0.0.0.0.0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>3e6c660</td>
<td>TCP</td>
<td>0</td>
<td>C</td>
<td>0.0.0.21</td>
<td>0.0.0.0.0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>3e6c570</td>
<td>UDP</td>
<td>0</td>
<td>C</td>
<td>0.0.0.67</td>
<td>0.0.0.0.0</td>
<td>LISTEN</td>
</tr>
</tbody>
</table>

### Displaying the Static Port Mapping Table (Static Port-Mapping)

You can display a table which provides a detailed listing of the currently active static port mapping scheme.

To view the **Static Port-Mapping Table**, go to the Web Management Interface, click on **Network Info**, then click on **Static Port-Mapping**.

The **Static Port-Mapping Table** screen appears:

### Static Port-Mapping Table

**STATIC PORT-MAPPING TABLE**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) 6.2.7.1/80 (00:e0:f6:5b:7f:84)</td>
<td>2.5.3.1/8080</td>
<td>0.0.0.0/0 TCP</td>
</tr>
<tr>
<td>(2) 10.0.0.13/23 (00:00:47:15:5c:7)</td>
<td>2.5.3.1/9023</td>
<td>0.0.0.0/0 TCP</td>
</tr>
<tr>
<td>(3) 10.208.134.5/80 (00:60:1d:31:92:0)</td>
<td>2.5.3.1/8081</td>
<td>0.0.0.0/0 TCP</td>
</tr>
<tr>
<td>(4) 12.13.14.15/80 (00:00:23:45:67:80)</td>
<td>2.5.3.1/9000</td>
<td>0.0.0.0/0 TCP</td>
</tr>
<tr>
<td>(5) 10.208.134.6/6001 (00:20:a6:4c:42:ff)</td>
<td>2.5.3.1/6001</td>
<td>0.0.0.0/0 TCP</td>
</tr>
</tbody>
</table>
Displaying TCP Statistics {TCP}

You can display the TCP (Transmission Control Protocol) statistics which are presented as a detailed listing of all TCP elements and their current status. TCP is a standard protocol that manages data transmissions across networks.

To view the TCP Statistics, go to the Web Management Interface, click on Network Info, then click on TCP.

The TCP Statistics screen appears:

<table>
<thead>
<tr>
<th>TCP Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP:</td>
</tr>
<tr>
<td>1448 packets sent</td>
</tr>
<tr>
<td>511 data packets</td>
</tr>
<tr>
<td>1 data packet</td>
</tr>
<tr>
<td>480 ack-only packets</td>
</tr>
<tr>
<td>0 URG only packet</td>
</tr>
<tr>
<td>0 window probe packet</td>
</tr>
<tr>
<td>0 window update packet</td>
</tr>
<tr>
<td>156 control packets</td>
</tr>
<tr>
<td>1073 packets received</td>
</tr>
<tr>
<td>576 acks (for 371791 bytes)</td>
</tr>
<tr>
<td>136 duplicate acks</td>
</tr>
<tr>
<td>0 ack for unsent data</td>
</tr>
<tr>
<td>171 packets (49715 bytes) received in-sequence</td>
</tr>
<tr>
<td>32 completely duplicate packets (0 byte)</td>
</tr>
<tr>
<td>0 packet with some dup. data (0 byte duped)</td>
</tr>
<tr>
<td>136 out-of-order packets (0 byte)</td>
</tr>
<tr>
<td>0 packet (0 byte) of data after window</td>
</tr>
<tr>
<td>0 window probe</td>
</tr>
<tr>
<td>2 window update packets</td>
</tr>
<tr>
<td>0 packet received after close</td>
</tr>
<tr>
<td>0 discarded for bad checksum</td>
</tr>
<tr>
<td>0 discarded for bad header offset field</td>
</tr>
<tr>
<td>0 discarded because packet too short</td>
</tr>
<tr>
<td>7 connection requests</td>
</tr>
<tr>
<td>144 connection accepts</td>
</tr>
<tr>
<td>138 connections established (including accepts)</td>
</tr>
<tr>
<td>147 connections closed (including 13 drops)</td>
</tr>
<tr>
<td>0 embryonic connection dropped</td>
</tr>
<tr>
<td>474 segments updated rtt (of 469 attempts)</td>
</tr>
<tr>
<td>157 retransmit timeouts</td>
</tr>
<tr>
<td>13 connections dropped by retransmit timeout</td>
</tr>
<tr>
<td>0 persist timeout</td>
</tr>
<tr>
<td>0 keepalive timeout</td>
</tr>
<tr>
<td>0 keepalive probe sent</td>
</tr>
<tr>
<td>0 connection dropped by keepalive</td>
</tr>
<tr>
<td>0 pch cache lookup failed</td>
</tr>
</tbody>
</table>
Displaying UDP Statistics {UDP}

You can display the UDP (User Datagram Protocol) statistics which are presented as a detailed listing of all UDP elements and their current status. UDP is an Internet standard transport layer protocol. It is a connectionless protocol which adds a level of reliability and multiplexing to the Internet Protocol (IP).

To view the UDP Statistics, go to the Web Management Interface, click on Network Info, then click on UDP.

The UDP Statistics screen appears:

![UDP Statistics Screen]

Port-Location Menu

The Port Location capabilities on the NSE have been enhanced. It is now possible to define a policy on a port. The billing methods (RADIUS, Credit Card, PMS, L2TP Tunneling) and the billing plans available on each port can now be individually configured.

This ability allows for having different billing methods and billing plans on different ports of the NSE. A practical application of this feature is to have a normal hotel room with a plan A that is $9.99 for a day with PMS billing and have a meeting room with a plan of $14.99 an hour with Credit Card billing.

This new feature is called Port-based Policies. In order for the port-based policies to work it has to be enabled from the Configuration->AAA page.
Adding and Updating Port-Location Assignments {Add}

Port-locations can be assigned at any level (for example, a specific room in a hotel or apartment building, a floor number, wing, or building). There may even be multiple ports assigned to a single room or location. The Access Gateway uses a port-location authorization table to manage the assigned ports and ensure accurate billing for the services used by a particular port.

Adding a Port-Location Assignment

Updating a Port-Location Assignment
Adding a Port-Location Assignment

This procedure shows you how to add a port-location assignment. If you want to update an existing assignment, go to Updating a Port-Location Assignment.

1. From the Web Management Interface, click on Port-Location, then Add. The Add Port-Location Assignments screen appears:

![Add Port-Location Assignments](image)

**Add Port-Location Assignments**

<table>
<thead>
<tr>
<th>Location*</th>
<th>Port Location Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Subnet</td>
<td></td>
</tr>
</tbody>
</table>

**Default QoS Policy (no policy)**

**State**
- ☐ No Charge
- ☐ Blocked
- ☐ Charge for Use

**Note:** The following items have no effect unless the port-based billing policies feature is enabled. Also, each individual item has no effect unless the corresponding feature is enabled.

- ☐ Enable RADIUS Billing
- ☐ Enable Tunneling
- ☐ Enable PMS Billing
- ☐ Enable Credit Card Billing

**Billing plan(s) available on port**

![Billing plan(s) available on port](image)

**Note:** If you plan on using a PMS interface, please make sure that the Location field consists of numbers only.
2. Enter a location identifier in the Location field. Locations can be assigned as an alpha, numeric, or alpha-numeric value unless a PMS interface is used (see note).

If you are using a PMS interface, ensure that the "Location" field consists only of numbers (no alpha characters or symbols).

All alpha characters (used for locations and descriptions) are case-sensitive.

3. In the Port field, enter the port (the VLAN ID when using 802.1Q 2-way).
4. In the Description field, enter a meaningful description for this port-location assignment.
5. Enter a Subnet for the port assignment you are adding.
   You must now assign a State for this port-location. Possible states are, No Charge for using this port-location, Charge for Use, and Blocked. If you do not assign a conditional state, the state is registered as “No Charge” by default.
6. If applicable, select the Default QoS Policy for the port assignment you are adding.
7. Select the conditional state you want to assign to this port-location.
   - If you choose Charge for Use additional configurations are available. Refer to the Note. Port-based Policies should be enabled from the Configuration->AAA page for these settings to take effect.
   - Choose Enable RADIUS Billing if you want RADIUS billing to be enabled on this port.
   - Choose Enable Tunneling if you want L2TP Tunneling based billing to be enabled on this port.
   - Choose Enable PMS Billing if you want PMS based room billing to be enabled on this port.
   - Choose Enable Credit Card Billing if you want Credit Card based billing to be enabled on this port.

You can select any number of billing methods per port.

A specific billing plan can be assigned to a port or all the existing billing plans defined on the NSE can be enabled on the port. Please select the appropriate option from the dropdown list for Billing Plan(s) available on port.
Please note that while it is possible to set the value of a per-port configuration parameter independently of the value of the corresponding global parameter, the feature itself is disabled for a port unless both the per-port and global parameters are set to enabled. Thus:

- RADIUS authentication for a port is enabled only if the RADIUS Client is globally enabled AND the per-port enable RADIUS billing parameter is set.

- Credit card billing for a port is enabled only if Credit Card Services is globally enabled AND the per-port enable Credit Card billing parameter is set.

- PMS billing for a port is enabled only if PMS Services is globally enabled AND the per-port enable PMS billing parameter is set.

- Tunneling for a port is enabled only if Tunneling is globally enabled AND the per-port enable Tunneling parameter is set.

8. Click on the Add button to save your changes (the message: Entry added or updated in the location file appears), or click on the Reset button if you want to reset all the values to their previous state.

**Updating a Port-Location Assignment**

The procedure for updating a port-location assignment is similar to adding a port-location assignment. The difference between the two procedures is how they are presented to you. For example, if you already have port-locations assigned and you enter an existing “port” value, each data field that you go through (port, location, state, and description) displays the value currently assigned to the field.

To update a Port-Location assignment, simply update the fields with new values.

*If you have updated a port-location assignment, you may want to change its description to distinguish from the old assignment. Although the old assignment will no longer exist in the system, a meaningful description can often be a valuable quick reference guide.*

**Deleting All Port-Location Assignments {Delete All}**

This procedure shows you how to delete all port-location assignments. The Access Gateway displays a warning and prompts you to confirm this action before deleting all the port-locations currently assigned in the system.
1. From the Web Management Interface, click on Port-Location, then Delete All. The Delete All Port-Location Assignments screen appears:

   Delete All Port-Location Assignments

   Are you Sure?

   Delete All

2. Click on the Delete All button to delete all Port-Location assignments.

Deleting Port-Location Assignments by Location {Delete by Location}

This procedure shows you how to delete a port-location assignment, based on its location. The Access Gateway prompts you to confirm this action before deleting the requested port-location.

   If you are unsure which port-locations are currently mapped to the system, you can view a list at “Displaying the Port-Location Mappings {List}” on page 173.

1. From the Web Management Interface, click on Port-Location, then Delete by Location. The Delete Port-Location Assignments by Location screen appears:

   Delete Port-Location Assignments by Location

   Location

   Delete   Reset

2. In the Location field, enter the location of the port-location assignment you want to delete.

   Locations are case-sensitive.

3. Click on the Delete button to delete the specified port-location assignment, or click on the Reset button if you want to reset the “location” value to its blank state.
Deleting Port-Location Assignments by Port {Delete by Port}

This procedure shows you how to delete a port-location assignment, based on its port. The Access Gateway prompts you to confirm this action before deleting the requested port-location.

If you are unsure which port-locations are currently mapped to the system, you can view a list at “Displaying the Port-Location Mappings {List}” on page 173.

1. From the Web Management Interface, click on Port-Location, then Delete by Port. The Delete Port-Location Assignments by Port screen appears:

```
Delete Port-Location Assignments by Port

Port

Delete  Reset
```

2. In the Port field, enter the port of the assignment you want to delete.

The “port” is the VLAN ID (when using 802.1Q 2-way).

3. Click on the Delete button to delete the specified port-location assignment, or click on the Reset button if you want to reset the “port” value to its blank state.

Exporting Port-Location Assignments {Export}

This procedure shows you how to export your current port-location assignments to the “location.txt” file. The location.txt file is stored in: /flash/location.txt (resident in the Access Gateway’s flash memory).

Exporting your current port-location assignments to the Access Gateway’s flash memory will overwrite the existing location.txt file.
1. From the Web Management Interface, click on **Port-Location**, then **Export**. The *Export Port-Location Assignments* screen appears:

   ![Export Port-Location Assignments](image)

   Export Port-Location assignments to /flash/location.txt.

   ![Export](image)

2. Click on the **Export** button to export port-location assignment to the /flash/location.txt. file.

### Finding Port-Location Assignments by Description {Find by Description}

This procedure shows you how to find a port-location assignment, based on its description. This procedure is useful if you want to review the details of a specific port-location. You can also find port-locations based on their location or port.

1. From the Web Management Interface, click on **Port-Location**, then **Find by Description**. The *Find a Port-Location Assignment by Description* screen appears:

   ![Find a Port-Location Assignment by Description](image)

   Enter Description

   ![Show Reset](image)

2. In the **Enter Description** field, enter the description of the assignment you want to find.

   *The system ignores the case (upper or lower) of the characters you enter.*

3. Click on the **Show** button to view the specified port-location assignment, or click on the **Reset** button if you want to reset the “description” value to its blank state. The requested port-location is displayed:
Finding Port-Location Assignments by Location {Find by Location}

This procedure shows you how to find a port-location assignment, based on its location. This procedure is useful if you want to review the details of a specific port-location. You can also find port-locations based on their description or port.

1. From the Web Management Interface, click on Port-Location, then Find by Location. The Find a Port-Location Assignment by Location screen appears:

   Find a Port-Location Assignment by Location

   Enter Location | 123

   Show  Reset

2. In the Enter Location field, enter the location of the assignment you want to find.

   The system ignores the case (upper or lower) of the characters you enter.

3. Click on the Show button to view the specified port-location assignment, or click on the Reset button if you want to reset the “location” value to its blank state. The requested port-location is displayed:

   Find a Port-Location Assignment by Location

   Enter Location

   Show  Reset

   Location  Port  State  Description  Subnet
   1        1  No Charge  0.0.0.0

   Active link to “Port” processing screen
Finding Port-Location Assignments by Port {Find by Port}

This procedure shows you how to find a port-location assignment, based on its port. This procedure is useful if you want to review the details of a specific port-location. You can also find port-locations based on their description or location.

1. From the Web Management Interface, click on Port-Location, then Find by Port. The Find a Port-Location Assignment by Port screen appears:

   ![Find a Port-Location Assignment by Port]

   Enter Port 456

   Show Reset

2. In the Enter Port field, enter the port you want to find.

   The “port” is the VLAN ID (when using 802.1Q 2-way).

3. Click on the Show button to view the Process Port-Location Assignments screen, or click on the Reset button if you want to reset the “port” value to its blank state.

   From this screen you can add, update or delete port-location assignments.

   ![Process Port-Location Assignments]

   Location 123
   Port 4567
   Subnet 10.10.10.10
   Description bill test
   State
   - No Charge
   - Charge for Use
   - Blocked

   Add/Update Delete Reset
**Importing Port-Location Assignments {Import}**

This procedure shows you how to import port-location assignments from the “location.txt” file. The location.txt file is stored in: /flash/location.txt (resident in the Access Gateway’s flash memory).

*If you have never exported port-location assignments (since installing the Access Gateway at this site), the location.txt is empty. See also, “Exporting Port-Location Assignments {Export}” on page 167. You can create your own location.txt file, FTP to the Access Gateway’s flash directory (for example, [IP address]/flash/location.txt), and upload the file. See also, “Creating a “location.txt” File” on page 172.*

1. From the Web Management Interface, click on **Port-Location**, then **Import**. The *Import Port-Location Assignments* screen appears:

   ![Import Port-Location Assignments](image)

   **Import Port-Location Assignments**

   Import Port-Location assignments from flash/location.txt.

   ![Import button](image)

   ![View location.txt](image)

   ![Click here to view the “location.txt” file](image)

2. Click on the **Import** button to import port-location assignments from the /flash/location.txt file.

**Viewing the “location.txt” File**

You can click on the “View location.txt” link if you want to view the current contents of the file.
Creating a “location.txt” File

You can create your own “location.txt” file and upload the file to the Access Gateway’s flash memory at [IP address]/flash/location.txt.

Use the following format when creating the file:

“1”,1,00:00:00:00:00:00,0.0.0.0,0, “Room 101”

The 4 (four) fields used in the format represent the standard format for port-location assignments (location, port, modem MAC address for RiverDelta, subnet, state, description).

Characters (used for locations and descriptions) are case-sensitive.

- Location – Locations are assigned as an alpha, numeric, or alpha-numeric value (unless a PMS interface is used, in which case only numeric values can be used).
- Port – Any number between 1 and 65535.
- Modem MAC Address – MAC address of the modem being used.
- Subnet – Subscriber’s subnet address.
- State – Possible states are: (0) no charge for using this port-location, (1) charge for use, and (2) blocked. If you do not assign a conditional state, the state is registered as “No Charge” by default.
- Description – Use a meaningful description for the assignment.
Displaying the Port-Location Mappings {List}

You can display a listing of all port-locations assigned to this system.

To view the listing of port-location assignments, go to the Web Management Interface, click on Network Info, then click on List. The List Port-Location Assignments screen appears:

```
<table>
<thead>
<tr>
<th>Location</th>
<th>Port</th>
<th>Description</th>
<th>State</th>
<th>Billing Modes*</th>
<th>Billing Plan</th>
<th>Subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>1</td>
<td></td>
<td>No Charge</td>
<td>RAD,TUN,PMS,CC</td>
<td>All Plans</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>
```

* RAD=RADIUS, TUN=TUNNEL, PMS=PMS, CC=Credit Card

Subscriber Administration Menu

Adding Subscriber Profiles {Add}

This procedure shows you how to add subscriber profiles into a table of authorized users.

Three types of subscriber profiles are provided; see the following sections for configuration information for the different profile types:

- “Adding a Subscriber Type Profile” on page 174
- “Adding a Device Type Profile” on page 176
- “Adding a Group Type Profile” on page 177

For more information about subscriber access and billing options, see the following sections:

- “Authorization and Billing” on page 242
- “Subscriber Management” on page 248
- “Subscriber Management Models” on page 248
- “Configuring the Subscriber Management Models” on page 249
Adding a Subscriber Type Profile

1. From the Web Management Interface, click on **Subscriber Administration**, then **Add**. The *Add a Subscriber Profile to the Database* screen appears:

2. Choose the **Subscriber** account type.

3. Define the DHCP Address Type: **Public** or **Private** (only used when the IP Upsell feature is enabled, otherwise leave this set to “private”).

4. Enter a valid **MAC Address** for the subscriber.
   
   If you have chosen to manage this subscriber by user name only, you do not need to enter a MAC address (but you must enter a user name).

5. Enter the **IP Address** of the subscriber.

6. Enter a valid **Subnet** address for this subscriber.
7. In the **Username** field, enter a user name for this subscriber. If you entered a MAC address and you do not want to assign a user name, skip Step 9 (password).

   **User names and passwords are case-sensitive. Having a user name and password is an optional service that subscribers may request (for example, if they are using more than one machine, or moving between locations and they want an additional level of security). If they request this service, they are prompted at the login screen for the user name and password you assign here. Solution providers can charge a fee for this service, at their discretion.**

8. If you assigned a user name, you must now assign a **Password**.

9. In the **Expiration Time** field, define the duration (in hours and minutes) for the subscriber’s authorized access time. When the assigned time expires, the subscriber must “re-subscribe” to the service.

10. Enter an amount in the **Paid** field.

11. The next two fields (**User Definable 1** and **User Definable 2**) are optional. Use these fields for simple notations about the subscriber.

12. Define the **Max Upstream Bandwidth** and **Max Downstream Bandwidth** range for this subscriber (in Kbps).

13. Select a policy from the **QoS Policy** menu. See “**Setting up Quality of Service {QoS}**” on page 120 for more information.

14. Enable **Countdown after login** if you want the timeout amount to take effect after the user logins. If the option is not enabled, user timeouts take effect the moment the subscriber is added.

15. Enable **STMP Redirection** to allow the specified user to have their SMTP traffic redirected by the global SMTP redirect configuration.

16. Click on the **Add** button to add this subscriber to the database, or click on the **Reset** button if you want to reset all the values to their previous state.
Adding a Device Type Profile

1. From the Web Management Interface, click on Subscriber Administration, then Add. The Add a Subscriber Profile to the Database screen appears:

2. Choose the Device account type for this profile.

3. If required, enable the Proxy Arp For Device feature.

4. Set the 802.1Q Device Port if the device is connected to a specific VLAN.

5. Enter a valid MAC Address for the device.

6. Enter the IP Address of the device.

7. Enter a valid Subnet address for this device.

8. In the Username field, enter a user name for this device.

9. The next two fields (User Definable 1 and User Definable 2) are optional. Use these fields for simple notations about the device.

10. Define the Min Upstream Bandwidth and Max Upstream Bandwidth range for this device (in Kbps).

11. Define the Min Downstream Bandwidth and Max Downstream Bandwidth range for this device (in Kbps).
12. Select a policy from the **QoS Policy** menu. See “Setting up Quality of Service {QoS}” on page 120 for more information.

13. Enable **STMP Redirection** to allow the specified user to have their SMTP traffic redirected by the global SMTP redirect configuration.

Click on the **Add** button to add this device to the database, or click on the **Reset** button if you want to reset all the values to their previous state.

**Adding a Group Type Profile**

Several changes have been made to improve the NSE's handling of group account administration.

- Group accounts can now be configured with a maximum user value, which limits the number of subscribers that can be logged in through the account at any given time.
- Group accounts can now be added via XML using the GROUP_ADD command.
- The overall layout and behavior of the WMI Subscriber Profile page has been modified to better reflect the configuration status of different account types, and to better support the Group Account changes:
  - The method of identifying an account as "group" has been modified. Instead of simply selecting a checkbox on the Subscriber page, group accounts now constitute a separate account “type” (along with Subscriber and Device). The Group Account checkbox has been removed from the bottom of the page, and replaced with a ‘Group Account’ button in the profile selection at the top.
  - A ‘Maximum Users per Group’ field has been added to allow setting the group user limit.
1. From the Web Management Interface, click on **Subscriber Administration**, then **Add**. The **Add a Subscriber Profile to the Database** screen appears:

<table>
<thead>
<tr>
<th>Add a Subscriber Profile to the Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Subscriber ☐ Device ☐ Group Account</td>
</tr>
<tr>
<td>DHCP Address Type: Private ○ Public ○ Only used if subscriber is configured for DHCP</td>
</tr>
<tr>
<td>Subnet</td>
</tr>
<tr>
<td>Username</td>
</tr>
<tr>
<td>Password</td>
</tr>
<tr>
<td>Expiration Time: 0 hrs 0 mins</td>
</tr>
<tr>
<td>Paid</td>
</tr>
<tr>
<td>User Definable 1</td>
</tr>
<tr>
<td>User Definable 2</td>
</tr>
<tr>
<td>Min Upstream Bandwidth: 0 Kbps</td>
</tr>
<tr>
<td>Max Upstream Bandwidth: 0 Kbps</td>
</tr>
<tr>
<td>Min Downstream Bandwidth: 0 Kbps</td>
</tr>
<tr>
<td>Max Downstream Bandwidth: 0 Kbps</td>
</tr>
<tr>
<td>QoS Policy: select policy/</td>
</tr>
<tr>
<td>Maximum users per group:</td>
</tr>
<tr>
<td>SMTP Redirection: Enable Note: Global SMTP Redirection must be enabled for subscriber SMTP Redirection to take effect, see SMTP page under Configuration options</td>
</tr>
</tbody>
</table>

2. Choose the **Group Account** type for this profile.
3. Define the DHCP Address Type: **Public** or **Private** (only used when the IP Upsell feature is enabled, otherwise leave this set to “private”).
4. Enter a valid **Subnet** address for this subscriber.
5. In the **Username** field, enter a user name for this subscriber.

**User names and passwords are required for Group Accounts.**

6. If you assigned a user name, you must now assign a **Password**.
7. In the **Expiration Time** field, define the duration (in hours and minutes) for the subscriber’s authorized access time. When the assigned time expires, the subscriber must “re-subscribe” to the service.
8. Enter an amount in the **Paid** field.
9. The next two fields (**User Definable 1** and **User Definable 2**) are optional. Use these fields for simple notations about the subscriber.
10. Define the **Min Upstream Bandwidth** and **Max Upstream Bandwidth** range for this subscriber (in Kbps).

11. Define the **Min Downstream Bandwidth** and **Max Downstream Bandwidth** range for this subscriber (in Kbps).

12. Enter the **Maximum users per group** for the subscriber account.

13. Select a policy from the **QoS Policy** menu. See “Setting up Quality of Service {QoS}” on page 120 for more information.

14. Enable **SMTP Redirection** to allow the specified user to have their SMTP traffic redirected by the global SMTP redirect configuration.

Click on the **Add** button to add this subscriber to the database, or click on the **Reset** button if you want to reset all the values to their previous state.

**Displaying Current Subscriber Connections {Current}**

You can display a listing of all the subscribers currently connected to the system. The list includes the MAC addresses of the subscribers, their active state, the individual expiration times, port numbers (if assigned), bandwidth limits, current bandwidth usage, and the number of bytes that have been passed from the subscriber to the Internet. This data can be used if a dispute arises between the subscriber and the solution provider (for example, if a subscriber claims that their connection to the Internet was not completed). By reviewing the “byte” statistics, you can clearly see if the subscriber made a successful connection.

To view the list of **Current Subscriber Connections**, go to the Web Management Interface, click on **Subscriber Administration**, then click on **Current**.
The **Subscriber Statistics** screen appears, showing the usage statistics for all subscribers currently connected to the system:

![Click on a link to view the associated subscriber]

<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>Port</th>
<th>Room</th>
<th>User Name</th>
<th>Bandwidth Up/Down</th>
<th>Throughout In-Out Up/In-Out Down</th>
<th>AAA State</th>
<th>Expiration</th>
<th>Idle Timeout</th>
<th>Bytes Sent</th>
<th>Bytes Received</th>
<th>Total</th>
<th>Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:01:22:1F:1B:2C</td>
<td>10.0.0.16</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>0-0/0-0</td>
<td>Valid</td>
<td>Unlimited</td>
<td>18 mins:58 sec</td>
<td>590469</td>
<td>1916633</td>
<td>2597102</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>00:09:04:29:17:56</td>
<td>10.0.0.14</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>0-0/0-0</td>
<td>Valid</td>
<td>Unlimited</td>
<td>15 mins:1 sec</td>
<td>11015</td>
<td>4462</td>
<td>15477</td>
<td>Off</td>
<td></td>
</tr>
</tbody>
</table>

*In the State field, “Valid” denotes that the subscriber has been authenticated. “Pending” indicates that the subscriber is still waiting for authentication.*

To view individual subscribers, simply click on the linked MAC address.

**Deleting Subscriber Profiles by MAC Address {Delete by MAC}**

This procedure shows you how to delete a subscriber profile from the Access Gateway’s database of authorized subscribers, based on the profile’s MAC address.

*To see a current listing of the subscriber database, sorted by MAC addresses, go to “Listing Subscriber Profiles by MAC Address {List by MAC}” on page 184.*
1. From the Web Management Interface, click on **Subscriber Administration**, then **Delete by MAC**. The *Delete a Subscriber Profile* (by MAC) screen appears:

```
Delete a Subscriber Profile

Enter MAC Address: 00

Delete  Reset
```

2. In the **Enter MAC Address** field, enter the MAC address of the profile you want to delete.

3. Click on the **Delete** button to delete this subscriber profile, or click on the **Reset** button if you want to reset the “MAC Address” value to the 00 state.

---

### Deleting Subscriber Profiles by User Name {Delete by User}

This procedure shows you how to delete a subscriber profile from the Access Gateway’s database of authorized subscribers, based on the profile’s user name.

*To see a current listing of the subscriber database, sorted by user name, go to “Listing Subscriber Profiles by User Name {List by User}” on page 185.*

1. From the Web Management Interface, click on **Subscriber Administration**, then **Delete by User**. The *Delete a Subscriber Profile* (by User) screen appears:

```
Delete a Subscriber Profile

Enter Username: ____________________________

Delete  Reset
```

2. In the **Username** field, enter the user name of the profile you want to delete.

3. Click on the **Delete** button to delete this subscriber profile, or click on the **Reset** button if you want to reset the “Username” value to its blank state.
Displaying the Currently Allocated DHCP Leases {DHCP Leases}

You can display a listing of the DHCP (Dynamic Host Configuration Protocol) leases that are currently active on the system’s DHCP server. DHCP is a standard method for assigning IP addresses automatically to network devices. DHCP leases define the amount of time that subscribers can utilize the system’s DHCP service.

To view the list of Currently Allocated DHCP Leases, go to the Web Management Interface, click on Subscriber Administration, then click on DHCP Leases.

To utilize this feature, your Access Gateway must be set to act as its own DHCP Server. The DHCP function cannot be set to DHCP Relay. Refer to “Managing the DHCP service options {DHCP}” on page 82.

The Currently Allocated DHCP Leases screen appears:

<table>
<thead>
<tr>
<th>Index</th>
<th>IP Address</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.0.0.32</td>
<td>00:50:DA:55:47:87</td>
</tr>
</tbody>
</table>

Deleting All Expired Subscriber Profiles {Expired}

This procedure shows you how to delete all expired subscriber profiles from the Access Gateway’s database of authorized subscribers. Use this procedure when you want to “clean up” the subscriber database.

1. From the Web Management Interface, click on Subscriber Administration, then Expired. The Remove Expired Profiles screen appears:

Remove expired subscriber profiles from the database.

Note: Your browser may be blocked for a few seconds after selecting this command.

OK
2. Click on the **OK** button to remove all expired profiles.

**Finding Subscriber Profiles by MAC Address {Find by MAC}**

This procedure shows you how to find a subscriber profile from the Access Gateway’s database of authorized subscribers, based on the profile’s MAC address. Use this procedure when you want to see the statistics corresponding to the MAC address. Statistics include user name and password (if any) and the access time remaining for this subscriber.

1. From the Web Management Interface, click on **Subscriber Administration**, then **Find by MAC**. The *Find a Subscriber Profile* screen appears:

   ![Find a Subscribers Profile](image)

2. In the **Enter MAC Address** field, enter the MAC address of the subscriber you want to find.

3. Click on the **Show** button to view this subscriber profile, or click on the **Reset** button if you want to reset the “MAC Address” value to the 00 state.

**Finding Subscriber Profiles by User Name {Find by User}**

This procedure shows you how to find a subscriber profile from the Access Gateway’s database of authorized subscribers, based on the profile’s user name. Use this procedure when you want to see the statistics corresponding to the user name. Statistics include the subscriber’s MAC address and the access time remaining for this subscriber.
1. From the Web Management Interface, click on **Subscriber Administration**, then **Find by User**. The *Find a Subscriber Profile* screen appears:

![Find a Subscribers Profile](image)

![Show](image)  ![Reset](image)

2. In the **Enter Username** field, enter the user name of the subscriber you want to find.

3. Click on the **Show** button to view this subscriber profile, or click on the **Reset** button if you want to reset the “Username” value to its blank state.

**Listing Subscriber Profiles by MAC Address {List by MAC}**

You can display the currently active database of authorized subscribers, based on MAC addresses.

To view the list of **Authorized Subscriber Profiles**, go to the Web Management Interface, click on **Subscriber Administration**, then click on **List by MAC**.

The **Authorized Subscriber Profiles** screen appears:

![Authorized Subscriber Profiles](image)

Click on a link to view the associated subscriber

*Note:*  
* indicates XoverY plan  
-1 indicates subscriber added by Admin or XML useradd or EWS with no associated plans
-1 indicates a subscriber added by Admin or XML useradd with no associated plans.

**Listing Subscriber Profiles by User Name {List by User}**

You can display the currently active database of authorized subscribers, based on user names. To view the list of *Authorized Subscriber Profiles*, go to the Web Management Interface, click on **Subscriber Administration**, then click on **List by User**.

The *Authorized Subscriber Profiles* screen appears:

Click on a link to view the associated subscriber

<table>
<thead>
<tr>
<th>Username</th>
<th>MAC Address</th>
<th>IP Address</th>
<th>Expiration</th>
<th>Paid</th>
<th>Amt Left</th>
<th>User1</th>
<th>User2</th>
<th>Current Plan</th>
<th>SMTP Redirection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>00:10:4F:95D</td>
<td>10.0.0.12</td>
<td>2 hrs 37 min</td>
<td>5.00</td>
<td>0.00</td>
<td></td>
<td></td>
<td>-1</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>61:50:99:1D:058</td>
<td>208.50.30.182</td>
<td>Unlimited</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
<td></td>
<td>-1</td>
<td>Disabled</td>
</tr>
<tr>
<td>john</td>
<td>00:00:00:00:00:00</td>
<td>0.0.0.0</td>
<td>Unlimited</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
<td></td>
<td>-1</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**Note:**
- * indicates XoverY plan
- -1 indicates subscriber added by Admin or XML useradd or EWS with no associated plans

-1 indicates a subscriber added by Admin or XML useradd with no associated plans.
Viewing RADIUS Proxy Accounting Logs {RADIUS Session History}

These settings are available under Subscriber Administration/RADIUS Session History menu.

**RADIUS Proxy Accounting Session History**

| RADIUS Proxy Accounting History Collection: | ☑ Enable logfile | ☑ Enable syslogs |

**Note:** Up to the 2000 most recent accounting messages will be displayed.

**Enable Logfile checkbox**

When this setting is enabled any RADIUS proxy accounting messages sent or received by the RADIUS proxy application are logged into a file named "RADHIST.RAD" in the /flash directory. This log contains accounting messages exchanged with downstream servers, and upstream NASs. The size of the log file is limited to 2000 records (accounting messages) or 320000 bytes -- when and if necessary the oldest records are purged to make room for new records.

If the logfile is disabled the current logfile is purged from the flash. If this is re-enabled again, only RADIUS accounting message sent/received from that point in time forward will be stored in the log.

**Enable Syslogs checkbox**

If enabled then the same information described above is sent to the configured Syslog server. The content of the syslogs is sent in human-readable format.

The configuration page of the syslog server to which these RADIUS proxy accounting messages are sent is available under the Configuration/Logging menu as described above. The third set of Syslog parameters on that page pertains to the RADIUS History Log.
Displaying Current Profiles and Connections {Statistics}

You can view the total number of profiles and connections currently stored in the Access Gateway’s database of authorized subscribers. The displayed list includes the number of subscribers currently in the database (Current Table) and a numerical breakdown of how the subscribers can utilize the system (for example, free access, credit card, etc.). The total number of user profiles stored in the Access Gateway’s internal database is also shown.

To view the Subscriber Statistics, go to the Web Management Interface, click on Subscriber Administration, then click on Statistics.

The Subscriber Statistics screen appears:

![Subscriber Statistics Table]

Subscriber Interface Menu

Defining the Billing Options {Billing Options}

- Duration-based Billing Plans
Setting Up a “Normal” Billing Plan, including pricing and bandwidth.

Setting Up an X over Y Billing Plan

Messages displayed to subscribers, including an Introduction Message, Offer Message and Policy Message.

Billing schemes (units of access).

Free billing options (free access).

Promotional code options (for example, when offering a percentage discount).

Duration-based Billing Plans

The purpose of this feature is to let hotels create billing plans that work in a similar fashion to pre-paid telephone cards. This means that an operator can set the Access Gateway’s Internal Web Server (IWS) to allow users online on a time “X” over period “Y” basis. Standard billing plans (where time “X” = period “Y”) can be used concurrently with “X” over “Y” plans. For example, multiple plans with flexible billing event options can be rolled out, such as:

- Plan A: 24 hours, 256kbit/s downstream, 128Kbit/s upstream, public IP address, $15 charge.
- Plan B: 8 hours to be used over 5 days, 512Kbit/s downstream, 256Kbit/s upstream, private IP address, $35 charge.
- Plan C: 1 week, 1Mbit/s downstream, 1Mbit/s upstream, public IP address, $99 charge.

In addition to credit card billing, Property Management Systems used by hotels are also supported along with the internal data base of the Access Gateway and billing via Nomadix' secure XML API.

See also, “Assigning a PMS Service {PMS}” on page 109 (see following note).

Your product license must support the PMS feature.
1. From the Web Management Interface, click on **Subscriber Interface**, then **Billing Options**. The *Internal Billing Options Setup* screen appears:

<table>
<thead>
<tr>
<th>Normal Plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>X over Y Plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
</tr>
<tr>
<td>5</td>
</tr>
</tbody>
</table>

**Introduction Message**: Please choose from the following plans.

**Offer Message**: How many days of Internet access would you like to purchase?

**Policy Message**: Contact your service provider with questions.

**Units of Access**

<table>
<thead>
<tr>
<th>Units of Access</th>
<th>Minimum</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minute</td>
<td>1</td>
<td>96700</td>
</tr>
<tr>
<td>Hour</td>
<td>1</td>
<td>16120</td>
</tr>
<tr>
<td>Day</td>
<td>1</td>
<td>672</td>
</tr>
<tr>
<td>Week</td>
<td>1</td>
<td>96</td>
</tr>
<tr>
<td>Month</td>
<td>1</td>
<td>24</td>
</tr>
</tbody>
</table>

**Free Billing Options**

**Default Free Access Time**: 7 Days

**Maximum Subcriber Lifetime**: 100 Days (Maximum 160 Days)

**Promotional Code Options**

<table>
<thead>
<tr>
<th>Code Definition</th>
<th>Percentage Discount</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>90</td>
</tr>
<tr>
<td>2</td>
<td>60</td>
</tr>
<tr>
<td>3</td>
<td>25</td>
</tr>
<tr>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>

2. Review the billing plans (normal plans and X over Y plans) that are currently active. To view or edit a billing plan, simply click on the **View/Edit/Delete** button opposite the corresponding plan.
The *Internal Billing Options Plan Setup* or *Internal Billing Options XoverY Plan Setup* screen appears for the billing plan (and type) you selected.

### Internal Billing Options Plan Setup

<table>
<thead>
<tr>
<th>Plan</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>☑</td>
</tr>
<tr>
<td>Label</td>
<td>Weekly</td>
</tr>
</tbody>
</table>

**Description of Service**: per week (maximum 3 weeks)

### Pricing

<table>
<thead>
<tr>
<th>Rate Per Minute</th>
<th>0.00</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Per Hour</td>
<td>0.00</td>
</tr>
<tr>
<td>Rate Per Day</td>
<td>17.33</td>
</tr>
<tr>
<td>Rate Per Week</td>
<td>92.40</td>
</tr>
<tr>
<td>Rate Per Month</td>
<td>346.50</td>
</tr>
</tbody>
</table>

### Time Unit

- Minute
- Hour
- Day
- Week
- Month

### Wired for Business

- ☐

### Maximum Bandwidth

- Up: 256
- Down: 512

**QoS Policy**: select a policy

### DHCP Pool

- Private
- Public

**NOTE**: Public option requires IP Upsell to be turned on. Otherwise, subscribers will receive private IP addresses.

Submit this Plan  | Delete this Plan  | Reset

Back
Sample of Internal Billing Options XoverY Plan Setup Screen

<table>
<thead>
<tr>
<th>Plan</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td>Prepaid Card 24h</td>
</tr>
<tr>
<td>Description of Service</td>
<td>Wireless Internet Access for 24 hour</td>
</tr>
</tbody>
</table>

**Plan Details**

<table>
<thead>
<tr>
<th>Plan Cost</th>
<th>17.33</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan Duration (X)</td>
<td>1</td>
</tr>
</tbody>
</table>

**Time Unit for Plan Duration**

- Minute
- Hour
- Day

**Plan Validity (Y) | 1**

**Time Unit for Plan Validity**

- Day
- Week
- Month

**Maximum Bandwidth**

- **Up**: 256
- **Down**: 512

**QoS Policy**: select a policy

**DHCP Pool**

- Private
- Public

*NOTE: Public option requires IP Upsell to be turned on. Otherwise, subscribers will receive private IP addresses.*

**Submit this Plan** | **Delete this Plan** | **Reset**

*NOTE: Usernames will be enabled if you submit an XoverY plan.*

Depending on the type of plan you want to set up, go to:

- “Setting Up a “Normal” Billing Plan” on page 192.
Setting Up a “Normal” Billing Plan

1. If required, click on the **Enable** check box to enable (make active) this billing plan.
2. Define a “label” for this billing plan in the **Label** field.

> Each plan must have a unique label, different from other plans.

3. Enter a description for this billing plan in the **Description of Service** field.
4. Define the **Pricing** schemes for this billing plan (rate per minute, per hour, per day, per week, and per month).
5. Define the **Time Unit** of the billable event (either Minute, Hour, Day, Week, or Month). One time unit is assigned to each billing plan.

> The Access Gateway allows you to define multiple billing plans with different time units at the same time. For example, you can define one billing plan that changes by the hour (e.g. $2.95 per hour) and a second plan that charges per day (e.g. $12.95 per day).

6. Define the **Up** (to network) and **Down** (to subscribers) bandwidth range for this billing plan.
7. Define the DHCP Pool (public or private) -- see following note.

> The “public” option requires IP Upsell to be turned on, otherwise subscribers will receive private IP addresses.

8. Click on the **Submit this Plan** button to save your changes and establish this billing plan. Alternatively, you can click on the **Delete this Plan** button if you want to delete this plan, or click on the **Reset** button if you want to reset all the values to their previous state.
9. Click on the **Back** button at any time to return to the **Internal Billing Options Setup** screen.
10. Repeat Steps 2 through 11 for each billing plan. You can enable (make active) any or all of the available billing plans.
11. Define the messages you want to present to subscribers, including:
   - Introduction Message
   - Offer Message
   - Policy Message

12. Define the Unit of Access (Minute, Hour, Day, Week, or Month) you want to make available to subscribers.

13. If you want to allow free access to subscribers, you can define the following free billing options:
   - Default Free Access Time (in days)
   - Maximum Subscriber Lifetime (in days)

14. Define any Promotional Code Options in the Code Definition and Percentage Discount fields, as required. You can define up to 5 Promotional Code Options.

   The “Percentage Discount” parameter must be between 1 and 100.

15. Click on the Submit button to save your changes, or click on the Reset button if you want to reset all the values to their previous state.

Setting Up an X over Y Billing Plan

1. If required, click on the Enable check box to enable (make active) this billing plan.

2. Define a “label” for this billing plan in the Label field.

   Each plan must have a unique label, different from other plans.

3. Enter a description for this billing plan in the Description of Service field.

4. Enter the cost the plan in the Plan Cost field.

5. Enter a duration value for this plan in the Plan Duration (X) field.

6. Define the “time unit” for the duration value you entered in Step 5. The time unit can be defined as either Minute, Hour, or Day.

7. Enter plan validity value for this plan in the Plan Validity (Y) field.

8. Define the “time unit” for the plan validity value you entered in Step 7. The time unit can be defined as either Day, Week, or Month.

9. Define the Up (to network) and Down (to subscribers) bandwidth range for this billing plan.
10. Define the DHCP Pool (public or private) -- see following note.

   The “public” option requires IP Upsell to be turned on, otherwise subscribers will receive private IP addresses.

11. Click on the Submit this Plan button to save your changes and establish this billing plan. Alternatively, you can click on the Delete this Plan button if you want to delete this plan, or click on the Reset button if you want to reset all the values to their previous state.

12. Click on the Back button at any time to return to the Internal Billing Options Setup (previous) screen.

Setting Up the Information and Control Console {ICC Setup}

The Nomadix ICC is a HTML pop-up window that is presented to subscribers, allowing them to select their bandwidth and billing plan options quickly and efficiently, and displays a dynamic “time” field to inform them of the time remaining on their account. The ICC also offers service providers an opportunity to display advertising banners and provide a choice of redirection options.

The Access Gateway also lets System Administrators define a simple HTML-based pop-up window for explicit Logout that can be used as an alternative to the more fully featured ICC
(described above). The pop-up Logout Console offers the opportunity to display the elapsed/count-down time and one logo for intra-session service branding.

This procedure allows you to set up how the ICC is displayed to subscribers. For more information about the ICC, go to “Information and Control Console (ICC)” on page 250.
1. From the Web Management Interface, click on **Subscriber Interface**, then **ICC Setup**. The **ICC Setup** screen appears:

### ICC Setup

- **Display ICC (Information and Control Console)**
  - Title: **Information and Control Console**

**Choice of ICC or Logout console:**
- ICC (Information and Control Console)
- Nomadix Logout Console

**Location of the Logout console:**
- Upper Left Corner
- Upper Right Corner
- Lower Left Corner
- Lower Right Corner

**How should the subscriber session time be displayed?**
- Elapsed Time
- Time Remaining

**What should the ICC do when a subscriber closes it?**
- Redisplay itself
- Logout (return the user to a “Pending” state - valid only with RADIUS)

<table>
<thead>
<tr>
<th>ISP Logo Button</th>
<th>Name/Text</th>
<th>Target URL</th>
<th>Image Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Button 1</td>
<td>Atyouroffice.com</td>
<td><a href="http://www.atyouroffice.com">http://www.atyouroffice.com</a></td>
<td>AOffice.jpg</td>
</tr>
<tr>
<td>Button 2</td>
<td>Altavista</td>
<td><a href="http://www.altavista.com">http://www.altavista.com</a></td>
<td>altavist.jpg</td>
</tr>
<tr>
<td>Button 3</td>
<td>Travelscape</td>
<td><a href="http://travelscape.com">http://travelscape.com</a></td>
<td>Travel.jpg</td>
</tr>
<tr>
<td>Button 4</td>
<td>BUY.COM</td>
<td><a href="http://www.buy.com">http://www.buy.com</a></td>
<td>Buy.jpg</td>
</tr>
<tr>
<td>Button 5</td>
<td>Food.com - order</td>
<td><a href="http://www.food.com">http://www.food.com</a></td>
<td>Food.jpg</td>
</tr>
<tr>
<td>Button 6</td>
<td>STORERUNNER.COM</td>
<td><a href="http://www.storunner.com">http://www.storunner.com</a></td>
<td>Store.jpg</td>
</tr>
<tr>
<td>Button 7</td>
<td>Amazon Books</td>
<td><a href="http://www.amazon.com">http://www.amazon.com</a></td>
<td>AMAZON.GIF</td>
</tr>
<tr>
<td>Button 8</td>
<td>UBID - where you</td>
<td><a href="http://www.ubid.com">http://www.ubid.com</a></td>
<td>Ubid.jpg</td>
</tr>
<tr>
<td>Button 9</td>
<td>Make the most of</td>
<td><a href="http://www.citysearch.com">http://www.citysearch.com</a></td>
<td>quokka.jpg</td>
</tr>
</tbody>
</table>

**Configure Banners**

**NOTE:** You must reboot for Banner Image or Button Image settings changes to take effect.

Reboot after changes are saved? □ Yes

[Submit][Reset]
2. If you want subscribers to see the ICC (pop-up window), click on the check box for **Display ICC (Information and Control Console)** to enable this feature.

3. Choose which ICC you want to be displayed (either the featured ICC or the simple Logout Console). Enable one of the following:
   - ICC (Information and Control Console)
   - Nomadix Logout Console

4. If you enabled either of the ICC pop-up options, you can choose a unique name for the console. Simply type a meaningful name in the **Title** field.

5. Define the physical location where you want the Nomadix Logout Console to appear on the subscriber’s screen.
   Choose one of the following options:
   - Upper Left Corner
   - Upper Right Corner
   - Lower Left Corner
   - Lower Right Corner

6. Define how you want to display the subscriber session time:
   - Elapsed Time (how much time has elapsed since the start of the session)
   - Time Remaining (how much time is remaining for the session)

7. You must now decide what you want the ICC to do if the subscriber closes it.
   Choose one of the following options:
   - Redisplay itself
   - Logout (return the subscriber to a “pending” state) – valid only with RADIUS and Post Paid PMS.

   You must now assign the buttons that you want to display to subscribers.

**Assigning Buttons**

When assigning the redirect buttons that will appear in the ICC, you can define one **ISP Logo Button** (large button) and up to 8 smaller buttons (**Button 2** through **Button 9**), with the following parameters:
**Name/Text** – The name of the button and the mouse-over text. The mouse-over text is the text that appears in the ICC’s Message Bar when your mouse pointer “rolls” over a button image.

![Message Bar](image)

**Target URL** – Where subscribers are sent when they click on the button.

**Image Name** – The representative image file you want to use for the button.

When assigning images for buttons, refer to: “Pixel Sizes” on page 200.

*If you assign (or change) button images or banner images, the Access Gateway must be rebooted for your changes to take effect.*

When you have completed assigning all your redirect buttons, click on the **Submit** button to save your changes, or click on the **Reset** button if you want to reset all the values to their previous state.

You can now assign the banners that you want to display to subscribers.
Assigning Banners

1. From the Subscriber Console (Information and Control Console - ICC) Setup screen, click on the Configure Banners link. The Subscriber Console (Information and Control Console - ICC) Banners Setup screen appears:

<table>
<thead>
<tr>
<th>Name/Text</th>
<th>Target URL</th>
<th>Image Name</th>
<th>Duration (sec)</th>
<th>Start Time (Optional)</th>
<th>Stop Time (Optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banner 1</td>
<td>Amazon.com</td>
<td>Amazon.gif</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Banner 2</td>
<td>Jobs Online at JCI.com</td>
<td>Jobs.jpg</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Banner 3</td>
<td>YellowPages.com</td>
<td>Yellow.jpg</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Banner 4</td>
<td>Education.com</td>
<td>Edu.jpg</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Banner 5</td>
<td>Priceline.com</td>
<td>Pricelin.jpg</td>
<td>10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NOTE: You must reboot for Banner Image or Button Image settings changes to take effect.

You can display up to 5 banners, but they must be defined here. Banners require all the same parameters that “buttons” use (see “Assigning Buttons” on page 197), with the addition of 3 (three) more. These are:

- **Duration** – Defines how long the banner is displayed in the ICC.
- **Start Time** – This is an optional parameter that you set if you want to assign a “start” time (for when the banner is displayed).
- **Stop Time** – This is an optional parameter that you set if you want to assign a “stop” time (for when the displayed banner closes).

When assigning images and times for banners, refer to: “Pixel Sizes” on page 200 and “Time Formats” on page 201.
2. Define the parameters for your banner(s):
   - Name/Text
   - Target URL
   - Image Name (see following note)
   - Duration (secs)
   - Start Time (Optional)
   - Stop Time (Optional)

   *If you assign (or change) button images or banner images, the Access Gateway must be rebooted for your changes to take effect.*

3. If you changed any of the Image Name definitions, click on the check box for **Reboot after changes are saved?** (to reboot the Access Gateway).

4. When finished, click on the **Submit** button to save your changes, or click on the **Reset** button if you want to reset all the values to their previous state.

5. To return to the previous screen, click on the **Configure ICC** link.

**Pixel Sizes**

Use the following parameters when defining images for buttons and banners:

- **Banners** – 373 pixels (width) x 32 pixels (height)
- **ISP Button** – 98 pixels (width) x 26 pixels (height)
- **Small buttons** – 45 pixels (width) x 26 pixels (height)
Time Formats

Use the following formats when defining times:

- Duration for Banners – 1 through 9999, or more
- Start or Stop times for Banners – hh:mm PM/AM (for example, 2:35 PM)

Defining Languages {Language Support}

The Access Gateway allows you to define the text displayed to your users by the Internal Web Server (IWS) without any HTML or ASP knowledge. The language you select here will determine the language encoding that the Access Gateway’s Internal Web Server instructs the browser to use.

The available language options are:

- English
- Chinese (Big 5)
1. From the Web Management Interface, click on **Subscriber Interface**, then **Language Support**. The **Language Support** screen appears:

![Language Support Screen](image)

**Language Support**

What language will your subscribers be using?

- English
- Chinese (Big5)
- French
- German
- Japanese (Shift_JIS)
- Spanish

*Other... Please choose a character set encoding:

- Submit
- Reset

2. Select the language you want to use (see notes).

*There are currently 6 (six) "pre-translated" language options. If you want to have the ICC pre-translated into Japanese and enter and display Japanese characters on the Web Management Interface and the subscriber’s portal page, choose the **Japanese (Shift_JIS)** option. If you want to have the ICC displayed in English but enter and display Japanese characters on the Web Management Interface and the subscriber’s portal page, choose the **Other** option, then choose one of the available Japanese character sets from the drop-down menu.*
If sufficient space is available, the Access Gateway’s Internal Web Server also supports multiple languages at the same time.

The following sample image shows the Web Management Interface (WMI) displayed with Asian language characters.

Enable Serving of Local Web Pages {Local Web Server}

Here are the quick setup instructions to enable serving of local web pages.

1. Upload the required pages and images to the /flash/web directory using FTP. Total file size of all pages and images cannot exceed 200 KB. File names should be labeled using the 8.3 format.

2. Go to WMI->Subscriber Interface->Local Web Server and add the names of the HTML or image files that were uploaded to the /flash/web directory.

3. Reboot the NSE.
4. The pages can now be served by referencing the URL http://nseip:1111/web/<filename> or at https://nseip:1112/web/<filename> for preauthenticated end users.

5. The post-authentication pages and images are available at http://nseip:3111/web/<filename>

These settings are available under Subscriber Interface/Local Web Server menu.

**Local Web Server Setup**

**Web Page File Name**

This text box lets you add or remove the names of the web pages that you intend to serve to the end users. Note: The name of the web page has to be added in order for it to be served to the end users. Uploading the web page to the /web directory is not sufficient.

**Image File Name**

This text box lets you add or remove the names of the image files that you intend to server to the end users. Note: The name of the image file has to be added in order for it to be served to the end users. Uploading the image file to the /web directory is not sufficient.

**Notes:**

1. Limit the total size of Web Pages and Images to 200 KB.
2. The Pre-Authentication Pages and Images are available at http://nseip:1111/web/<filename> or at https://nseip:1112/web/<filename>
3. The Post-Authentication Pages and Images are available at http://nseip:3111/web/<filename>
Defining the Subscriber’s Login UI {Login UI}

This procedure allows you to set up the presentation and content of the subscriber’s login User Interface (UI).
1. From the Web Management Interface, click on **Subscriber Interface**, then **Login UI**. The **Subscriber Login User Interface Settings** screen appears:

![Subscriber Login User Interface Settings](image)

2. Define the messages you want subscribers to see when they log in. Keep messages brief and to the point. Available message categories include:
   - **Service Selection Message**
ACCESS GATEWAY

- Existing Username Message
- New Username Message
- Contact Message
- PMS Username Message

3. If any of your devices do not support Java™ scripts, you have the option of disabling the Access Gateway’s JavaScript™ support (JavaScript support is enabled by default). If necessary (and if JavaScript support is already enabled), click on the check box for **Enable Javascript** to disable this feature.

4. Click on the check box for **Enable “Remember Me” option** if you want to enable (or disable) this feature. This option enables the Access Gateway to “remember” logins for a predetermined duration (see next step).

   The “Remember Me” option requires JavaScript to be enabled.

5. If you enabled the “Remember Me” option, define the duration (in days) in the **Remember for how many days** field.

6. If required, define a **Help Hyperlink Message** and a corresponding **Help Hyperlink URL**.

7. Define the location in the **Locale** field.

8. Define the currency labeling (for example, $) in the **Currency** field.

   The currency must be defined using an ISO 4217 currency code (for example, USD for US Dollars, GBP for Great British Pounds).

9. Enter a numeric value for the **Number of decimals for amount**. This field defines the number of decimal places that are shown for the displayed amounts.

10. Define the appearance of the internal login screen. Appearance settings include:
    - Image File Name (if you want to include a unique image)
    - Page Background Color
    - Table Background Color
    - Page Title Font
    - Line Item Font

Take care when mixing font and background colors. You may want to experiment before establishing these settings to ensure that your chosen color scheme is both presentable and readable to subscribers (see notes).

You must reboot the Access Gateway for the “Image File Name” or “Partner Image File Name” settings to take effect.

You can view a grid of acceptable screen colors. To view the grid, simply click on the “View Color Grid” link.

If you click on the “View Color Grid” link, the Browser Safe Background Colors by RGB screen appears (partial view only shown here):

---

<table>
<thead>
<tr>
<th>Color</th>
<th>Color</th>
<th>Color</th>
<th>Color</th>
<th>Color</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>#000000</td>
<td>#111111</td>
<td>#222222</td>
<td>#333333</td>
<td>#444444</td>
<td>#555555</td>
</tr>
<tr>
<td>#666666</td>
<td>#777777</td>
<td>#888888</td>
<td>#999999</td>
<td>#aaa999</td>
<td>#bbaa99</td>
</tr>
<tr>
<td>#cccccc</td>
<td>#ddcc99</td>
<td>#eee735</td>
<td>#ffe0a3</td>
<td>#ffec81</td>
<td>#ffff00</td>
</tr>
</tbody>
</table>

More colors ...

11. Click on the check box for Partner Image to enable this feature, then enter the name of the image file in the Partner Image File Name field. See “Subscriber Login Screen (Sample)” on page 209.

12. If you made changes to the Image File Name or Partner Image File Name fields, you must reboot the Access Gateway for your changes to take effect. In this case, click on the check box for Reboot after changes are saved?

The partner image (splash screen) is not the same screen that is defined by the Image File Name (IWS screen) field.

13. Click on the Submit button to save your changes, or click on the Reset button if you want to reset all the values to their previous state.
Subscriber Login Screen (Sample)

The following sample shows a subscriber login screen:

```
Are you a new user?
New Individual

You an existing user?
Please enter your login name

name: ______________________
Pass: ______________________

☐ Do you want the browser to store your current password

log

Please contact network administrator for help.
Click here if you need some help.
```

Defining the Post Session User Interface (Post Session UI)

The Post Session UI (Goodbye Page) can be defined either as a RADIUS VSA or be driven by the Access Gateway’s Internal Web Server (IWS). Using the IWS option means that this functionality is available for other post-paid billing mechanisms (for example, post-paid PMS—if your product license supports PMS). The IWS page displays the details of the user's connection, such as:

- IP address of the user.
- Type of AAA.
- Start/Stop time.
- Bytes sent/received.
- Freely configurable hypertext link (in case the ISP wants to link the user back to a sign-up/help page).

Sample of Post Session UI (Goodbye Page)
1. From the Web Management Interface, click on **Subscriber Interface**, then **Post Session UI**. The **Subscriber Post Session User Interface Settings** screen appears:

### Subscriber Post Session User Interface Settings

#### IWS Goodbye Page - Display Option

- Enable IWS Goodbye Page
- Display IP Address
- Display Authen Type
- Display Start Time
- Display Stop Time
- Display Byte Sent
- Display Byte Received
- Display Hypertext Link URL

#### Hyper Text Link URL

- [Hyper Text Link URL]

#### IWS Goodbye Page -- Field Label Definitions

- **Session Summary**
- **IP Address**
- **Authen Type**
- **Start Time**
- **Stop Time**
- **Byte Sent**
- **Byte Received**
- **Go To**

Revert  Revert all name fields to default values

Submit  Reset
2. Click on the **Enable IWS Goodbye Page** check box to enable (or disable) the IWS Goodbye Page, as required.

3. If you enabled the *IWS Goodbye Page*, select your preferred display options by checking the corresponding boxes:
   - Display IP Address
   - Display Authen Type
   - Display Start Time
   - Display Stop Time
   - Display Byte Sent
   - Display Byte Received
   - Display Hypertext Link URL

4. If you enabled the Hypertext Link URL feature, enter the URL for the link in the **Hyper Text Link URL** field.

5. Define the following *Field Label Definitions* for your Goodbye Page:
   - Session Summary
   - IP Address
   - Authen Type
   - Start Time
   - Stop Time
   - Byte Sent
   - Byte Received
   - Go To

   *If you enabled the Partner image for the Login UI, you will also see the same image in the IWS Post Session page.*

6. Click on the **Submit** button to save your changes. Alternatively, you can click on the **Reset** button to reset all values to their previous state, or click on the **Revert** button to revert all values to their default state.

---

### Defining Subscriber UI Buttons {Subscriber Buttons}

This procedure allows you to define how each of the control buttons are displayed to subscribers.
1. From the Web Management Interface, click on **Subscriber Interface**, then **Subscriber Buttons**. The **Subscriber Page -- Control Button Definitions** screen appears:

   **Subscriber Page -- Control Button Definitions**

<table>
<thead>
<tr>
<th>Control Buttons</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Back</td>
<td>Back</td>
</tr>
<tr>
<td>Login</td>
<td>Login</td>
</tr>
<tr>
<td>New User</td>
<td>New User</td>
</tr>
<tr>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>Purchase</td>
<td>Purchase</td>
</tr>
<tr>
<td>Submit</td>
<td>Submit</td>
</tr>
<tr>
<td>Try Again</td>
<td>Try Again</td>
</tr>
</tbody>
</table>

   - **Revert**  Revert all fields to default values
   - **Submit**  Submit
   - **Reset**   Reset

   See Caution

2. Enter the definitions you want for each control button in the corresponding fields.

   **Only the Login button should be named “Login.” Do not assign this name to any other button.**

3. Click on the **Submit** button to save your changes, or click on the **Reset** button if you want to reset all the values to their previous state.

   If you want to reset all field values to their default state, click on the **Revert** button.

**Defining Subscriber UI Labels {Subscriber Labels}**

This procedure allows you to define how the user interface (UI) field labels are displayed to subscribers.
1. From the Web Management Interface, click on **Subscriber Interface**, then **Subscriber Labels**. The **Subscriber Page -- Field Label Definitions** screen appears:

2. Enter the definitions you want for each label in the corresponding fields.

3. Click on the **Submit** button to save your changes, or click on the **Reset** button if you want to reset all the values to their previous state.
   
   If you want to reset all field values to their default state, click on the **Revert** button.
Defining Subscriber Error Messages {Subscriber Errors}

This procedure allows you to define how error messages are displayed to subscribers.

There are 2 (two) pages of error messages available.

1. From the Web Management Interface, click on Subscriber Interface, then Subscriber Errors, 1 of 2. The Subscriber Page -- Error Message Definitions, 1 of 2 screen appears:

2. Enter the definitions you want for each error message in the corresponding fields.

3. Click on the Submit button to save your changes, or click on the Reset button if you want to reset all the values to their previous state.
If you want to reset all field values to their default state, click on the **Revert** button.

4. Repeat Steps 1 – 3 for page 2 of 2 (see following screen):
Defining Subscriber Messages {Subscriber Messages}

This procedure allows you to define how “other” subscriber messages are displayed.

There are 3 (three) pages of subscriber messages available.

1. From the Web Management Interface, click on Subscriber Interface, then Subscriber Messages, 1 of 3. The Subscriber Page -- Other Message Definitions, 1 of 3 screen appears:
2. Enter the definitions you want for each subscriber message in the corresponding fields.

3. Click on the **Submit** button to save your changes, or click on the **Reset** button if you want to reset all the values to their previous state.

   If you want to reset all field values to their default state, click on the **Revert** button.

4. Repeat Steps 1 – 3 for page 2 of 3 (see following screen):
5. Repeat Steps 1 – 3 for page 3 of 3 (see following screen):
System Menu

Adding an ARP Table Entry {ARP Add}

ARP (Address Resolution Protocol) is used to dynamically bind a high level IP address to a low level physical hardware (MAC) address. ARP is limited to a single physical network that supports hardware broadcasting. This procedure shows you how to add an ARP table entry.

1. From the Web Management Interface, click on System, then ARP Add. The Add ARP Table Entries screen appears:

![Add ARP Table Entries screen]

1. Enter the IP Address of the entry you are adding.
2. Enter the MAC Address of the entry you are adding.
3. Define whether this entry is:
   - Static – Will only last until the next reboot
   - Persistent – Will be written to the current.txt file and loaded on each boot of the NSE
4. Define whether the interface that the device the ARP entry is connected to is:
   - Network – WAN Interface
   - Subscriber 1 – LAN 1 Interface
   - Subscriber 2 – LAN 2 Interface
5. Click on the Add button to add your entry, or click on the Reset button if you want to reset all the values to their previous state.
Deleting an ARP Table Entry \{ARP Delete\}

ARP (Address Resolution Protocol) is used to dynamically bind a high level IP address to a low level physical hardware (MAC) address. ARP is limited to a single physical network that supports hardware broadcasting. This procedure shows you how to delete an ARP table entry.

1. From the Web Management Interface, click on System, then ARP Delete. The Delete ARP Table Entries screen appears:

```
<table>
<thead>
<tr>
<th>Internet Address</th>
<th>Physical Address</th>
<th>Flags</th>
<th>Use</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>00:0c:29:7f:e1:0c</td>
<td></td>
<td></td>
<td>Network</td>
</tr>
<tr>
<td>192.168.1.2</td>
<td>00:0c:29:7f:e1:0c</td>
<td></td>
<td></td>
<td>Network</td>
</tr>
</tbody>
</table>
```

Enter IP Address [ ]

Delete  Reset

2. Enter the IP address of the entry you want to delete.

3. Click on the Delete button to delete this entry, or click on the Reset button if you want to reset the “IP Address” value to its blank state.

Configurable Gateway ARP Refresh Interval

The NSE will periodically refresh its ARP cache entry for the gateway IP. When gateway redundancy is implemented via the use of multiple gateway devices with the same IP address, the periodic refresh enables the NSE to quickly discover the new MAC address of the gateway.

You can set the refresh frequency on the Location page. The frequency must be between 30 and 600 seconds. 600 seconds is half of the ARP cache refresh interval, so the ARP entry can never expire.
Enabling the Bridge Mode Option {Bridge Mode}

*Bridge Mode* allows complete and unconditional access to devices on the subscriber side of the Access Gateway. When the *Bridge Mode* option is enabled, the Access Gateway is effectively transparent to the network in which it is located, allowing clusters of switches (especially Cisco Systems switch clusters) to be managed using the STP (Spanning Tree Protocol), or any other algorithm/protocol. The Access Gateway forwards any and all packets (except those addressed to the Access Gateway network interface). The packets are unmodified and can be forwarded in both directions. This is a very useful feature when troubleshooting your entire network as it allows administrators to effectively “remove” the Access Gateway from the network without physically disconnecting the unit.

You can still manage the Access Gateway when *Bridge Mode* is enabled, but you have no other functionality. If you enable the *Bridge Mode* option and then plug the Access Gateway into a network, all you need to do is assign it routable IP addresses. You can then set up all other features and disable the *Bridge Mode* option whenever you want to start using the Access Gateway in that network.

This procedure shows you how to enable the *Bridge Mode* option.
1. From the Web Management Interface, click on System, then Bridge Mode. The Bridge Mode (Passthrough) Settings screen appears:

   ![Bridge Mode (Pass through) Settings](image)

   Bridge Mode
   
   Enable

   NOTE: You must reboot for setting changes to take effect.

   Reboot immediately after changes are saved? Yes

   Submit  Reset

2. Click on the check box for Bridge Mode to enable this feature.

   The Access Gateway should be rebooted if this setting is changed.

3. If you want the changes to take effect immediately, Select Yes to "Reboot immediately after changes are saved".

4. Click on the Submit button to save your changes, or click on the Reset button if you want to reset the “Enable” option to its previous state.

**Exporting Configuration Settings to the Archive File {Export}**

This procedure shows you how to export the current system authentication settings to an archive file for future retrieval. This function is useful if you want to change the configuration settings and you are unsure of the effect that the changes will have. You can restore the archived system configuration settings at any time with the import function.
1. From the Web Management Interface, click on **System**, then **Export**. The *Export Configuration* screen appears:

   ![Export Configuration Screen]

   The current settings are exported to the **archive.txt** file.

   ![Click to View archive.txt]

   ![Click to View current.txt]

   ![Click here to view the “archive.txt” file]

   ![Click here to view the “current.txt” file]

2. Click on the **OK** button to export the current authentication settings to the **archive.txt** file.

**Importing the Factory Defaults {Factory}**

This procedure shows you how to replace the current authentication settings with the settings that were established at the factory.

You will need to reboot the system for some of the imported default settings to take effect.
1. From the Web Management Interface, click on **System**, then **Factory**. The **Factory Configuration** screen appears:

   **Factory Configuration**

   Load the original factory configuration settings and save them as the current settings.

   **NOTE**: Will reboot automatically after the factory settings are restored.

   **WARNING**: The factory configuration does not include network settings. The network connection will be service interruption, perform this import in the command line interface via the serial port.

   ![Submit and Reboot button](button.png)

   ![View factory.txt](view_factory.png)

   ![View current.txt](view_current.png)

   ![Click here to view the “factory.txt” file](click_factory.png)

   ![Click here to view the “current.txt” file](click_current.png)

2. Click on the **Submit and Reboot** button to replace the current system configuration settings with the factory default settings and reboot the Access Gateway.

**Defining the Fail Over Options {Fail Over}**

Your product license may not support this feature.

Many large scale networks require fail-over support for all devices in the public access network. The Fail Over Options feature allows two Nomadix Gateways to act as siblings, where one device will take up the users should the other device become disconnected from the network. As part of this functionality, the settings (except IP addresses) between the two devices will be synchronized automatically.
1. From the Web Management Interface, click on **System**, then **Fail Over**. The **Fail Over** screen appears:

<table>
<thead>
<tr>
<th>Fail Over</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSE Status</td>
<td>Primary</td>
</tr>
<tr>
<td>Sibling IP address</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>Fail Over Port</td>
<td>8888</td>
</tr>
<tr>
<td>Secondary To Primary Fail Over Time</td>
<td>5 Mins</td>
</tr>
</tbody>
</table>

**NOTE:** Failover may not work with dynamically assigned IP addresses (DHCP or PPPoE client).

**NOTE:** You must reboot for configuration changes to take effect.

**Reboot after changes are saved?**

**Submit** | **Reset**

2. Enable or disable the **Fail Over** feature, as required.

3. If you enabled Fail Over, define the **Sibling Status** (Primary or Secondary).

4. Enter an IP address in the **Sibling IP Address** field.

5. Define the port in the **Fail Over Port** field.

6. Select the **Secondary To Primary Fail Over Time**. The time set here is how long the Secondary will wait while not receiving messages from the Primary before it takes over.

7. Click on the check box for **Reboot after changes are saved?**

   *If you are using RADIUS, it is recommended to add both Nomadix gateways to the RADIUS server.*

8. Click on the **Submit** button to save your changes, or click on the **Reset** button to reset all values to their previous state.

### Viewing the History Log {History}

You can view a history log of the system’s **Access**, **Reboot**, and **Uptime** activities. The history log contains up to 500 entries. Over 500 entries and each new log item removes the oldest entry in the list. The latest entry is always at the top of the list.
To view the history log, go to the Web Management Interface and click on **System**, then **History**. The **Uptime and Access/Reboot History** screen appears:

The “Uptime” field displays the time (in days, hours, minutes, and seconds) that the system has been up and running.

The “Access and reboot History” log fields include:
- **Message** – Administrator / Operator action.
- **Login** – User name of the Administrator / Operator.
- **IP** – Source IP address (see note).

**Establishing ICMP Blocking Parameters {ICMP}**

The Access Gateway includes the option to block all ICMP traffic from “pending” or “non authenticated” users that are destined to addresses other than those defined in the pass-through
(walled garden) list. The default setting for this option is “disabled” because ICMP pass-through is a useful end-user troubleshooting feature and is also required by certain smart clients (for example, GRIC).

1. From the Web Management Interface, click on System, then ICMP. The ICMP screen appears:

![ICMP Screen](image)

2. Click on the check box for **Block ICMP from pending users** to enable (or disable) this feature, as required.

3. You can **Ping a host via the network port** by entering either an IP address or DNS name of host. This is the site that you want the ping to be sent to from the NSE.

4. Click on the **Submit** button to save your changes, or click on the **Reset** button to reset all values to their previous state.

**Importing Configuration Settings from the Archive File {Import}**

This procedure shows you how to restore the system configuration settings from an archive file (previously created with the *export* function).

*You will need to reboot the system for some of the imported default settings to take effect (especially DHCP).*
1. From the Web Management Interface, click on System, then Import. The Import Configuration screen appears:

**Import Configuration**

Import configuration settings from the archive file and save them as the current settings.

**NOTE:** A reboot may be required for some imported settings to take effect, particularly DHCP.

**WARNING:** The network connection may be lost when the import is performed if the network settings in the archive are different from those currently in use.

[View archive.txt] [View current.txt]

2. Click on the OK button to replace the current system configuration settings with the settings contained in the archive.txt file (see notes above).

**Establishing Login Access Levels {Login}**

This procedure shows you how to assign differentiated access levels for operators and managers at login.

The Access Gateway allows you to define 2 concurrent access levels to differentiate between managers and operators, where managers are permitted read/write access and operators are restricted to read access only. Once the logins have been assigned, managers have the ability to perform all write commands (Submit, Reset, Reboot, Add, Delete, etc.), but operators cannot change any system settings. Administrative Concurrency may be enabled to further restrict the amount of management sessions allowed at one time. When this feature is enabled, one manager and three operators can access the Access Gateway at any one time (the default is “disabled”).

This feature supports the following interfaces:
- Telnet
- Command Line Interface (CLI) – serial
- Web Management Interface (WMI)
- FTP and SFTP (no operator access allowed)
- SSH Shell Access
- SSL

Only managers can assign a username and password for the remote RADIUS testing login option.

1. From the Web Management Interface, click on System, then Login. The Login Name and Password screen appears:

   ![Login Name and Password Screen]

2. Click on the check box for Administration Concurrency if you want to assign concurrent Manager and Operator logins.
3. In the **Manager Login** field, enter a login name for this manager.

   *Login names and passwords are case-sensitive. Use login names and passwords that are easy to remember (up to 11 characters, any character type).*

4. In the **Manager Password** field, enter a password for this manager.

5. In the **Confirm Password** field, enter the password again to confirm it.

   *If you forget your password, you will need to contact technical support. See also, “Appendix A: Technical Support” on page 311.*

6. If you enabled **Administration Concurrency**, repeat steps 3 to 5 for an operator login.

   As part of its Smart Client feature, the Access Gateway offers a remote RADIUS testing feature (enabled by default). With this feature, the Access Gateway provides a password-protected Web page. From this Web page, technical support can type a username and password and instruct the Access Gateway to send a RADIUS access request to the RADIUS server—following the same basic rules as if the request was from a user. The URL for the test page is `http://<Nomadix Access Gateway IP>/radtest/testradius.htm` and can be accessed from the network side of the Access Gateway. You must open a separate browser to utilize this feature. The “Framed IP” field is configurable by the user and can be set to any IP address.

7. Click on the check box for **Radius Authentication Enable** to enable the Centralized Authentication mechanism. If chosen, the system will first try to authenticate against the local database and then will check against the RADIUS Service Profiles that are configured.

8. Select the RADIUS Service Profile from the pop-up list. The list of available profiles is defined in Realm-Based Routing.

9. Enter a Session Timeout value in minutes. This defines the time of validity period of the cookie passed to the Web browser from the WMI Session and RADIUS session.
10. *Managers Only*: If RADIUS is enabled, you can enter a login name in the RADIUS Remote Test Login field.

   ![Remote RADIUS Authentication Test Page](image)

   For RADIUS logins, the maximum number of characters for usernames is 96. The maximum number of characters for passwords is 128.

11. *Managers Only*: If you entered a login name in Step 7, enter a password in the RADIUS Remote Test Password field.

12. *Managers Only*: Click on the Submit button to save the login and password parameters, or click on the Reset button if you want to reset all the values to their previous state.

**Defining the MAC Filtering Options {Mac Filtering}**

MAC Address filtering enhances Nomadix’ access control technology by allowing System Administrators to block malicious users based on their MAC address. Up to 600 MAC addresses can be blocked at any one time (see caution).

*MAC addresses that you enter here will cause the subscribers at these addresses to be blocked from service. Please make sure that you enter the correct addresses before submitting the data.*
1. From the Web Management Interface, click on **System**, then **MAC Filtering**. The **MAC Filtering** screen appears:

   ![MAC Filtering Screen]

   - Click on the check box for **MAC Filtering** to enable (or disable) this feature, as required.
   - Enter a MAC address in the **MAC** field, then click on the **Add** button to add this address to the “blocked” list, or click on the **Remove** button to remove this address from the list.

   For advanced security, see also, “Establishing Session Rate Limiting {Session Limit}” on page 235.

### Rebooting the System {Reboot}

This procedure shows you how to reboot the Access Gateway.

**The “reboot” procedure outlined on this page allows you to decide when to reboot (if you are making multiple changes to different menu functions and you want to reboot just one time after completing all your changes).**
1. From the Web Management Interface, click on System, then Reboot. The Reboot Device screen appears:

```
Reboot Device
```

Reboot operating system.

```
OK
```

2. Click on OK to reboot the operating system.

**Adding a Route {Route Add}**

This procedure shows you how to add a route into the Access Gateway’s routing table. This is accomplished by establishing the route’s destination IP address, and by setting the gateway or router IP address by which the route’s destination can be reached.

1. From the Web Management Interface, click on System, then Route Add. The Add Static Routes screen appears:

```
Add Static Routes
```

<table>
<thead>
<tr>
<th>Destination/Prefix</th>
<th>Gateway</th>
<th>Flags</th>
<th>Use</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>67.130.149.190</td>
<td>0x3</td>
<td>502</td>
<td>Network (WAN)</td>
</tr>
<tr>
<td>67.130.149.160/27</td>
<td>67.130.149.163</td>
<td>0x101</td>
<td>0</td>
<td>Network (WAN)</td>
</tr>
<tr>
<td>172.30.30.0/24</td>
<td>172.30.30.172</td>
<td>0x101</td>
<td>0</td>
<td>Network (WAN)</td>
</tr>
</tbody>
</table>

```
Destination IP/Prefix Length
```

```
Gateway IP
```

2. Enter the Destination IP/Prefix Length address of the route you want to add to the routing table. This is the Destination IP or Subnet that the Route is trying to reach included with the /prefix length to determine how large the subnet might be.

3. Enter the Gateway IP address for the Route being added so that the NSE knows what to use to try to reach the destination IP/Subnet.
4. Click on the **Add** button to add this route to the routing table, or click on the **Reset** button if you want to reset all the values to their previous state.

**Deleting a Route {Route Delete}**

This procedure shows you how to delete a route to a specific IP destination.

1. From the Web Management Interface, click on **System**, then **Route Delete**. The *Delete Static Routes* screen appears:

   **Delete Static Routes**

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Flags</th>
<th>Use</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>8.46.5.2</td>
<td>3</td>
<td>955</td>
<td>Network</td>
</tr>
<tr>
<td>10.0.0.0</td>
<td>10.0.0.254</td>
<td>3</td>
<td>186</td>
<td>Network</td>
</tr>
<tr>
<td>8.46.1.0</td>
<td>8.46.16.1</td>
<td>101</td>
<td>0</td>
<td>Network</td>
</tr>
<tr>
<td>8.46.5.1</td>
<td>8.46.16.5</td>
<td>101</td>
<td>0</td>
<td>Subscriber</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>5</td>
<td>0</td>
<td>Loopback</td>
</tr>
</tbody>
</table>

   Destination IP

   ![Delete, Reset buttons]

2. Enter the **Destination IP** address of the route you want to delete from the routing table.
3. Click on the **Delete** button to delete this route from the routing table, or click on the **Reset** button if you want to reset the “Destination IP” value to its blank state.

**Establishing Session Rate Limiting {Session Limit}**

Session Rate Limiting (SRL) significantly reduces the risk of “Denial of Service” attacks by allowing administrators to limit the number of DAT sessions any one user can take over a given time period and, if necessary, then block malicious users.
1. From the Web Management Interface, click on **System**, then **Session Limit**. The Session Rate Limiting screen appears:

```
<table>
<thead>
<tr>
<th>Session Rate Limiting</th>
<th>Enable</th>
<th>Sessions per Time Interval defined below, Default: 200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean Rate</td>
<td>200</td>
<td>Sessions per Time Interval defined below, Default: 400</td>
</tr>
<tr>
<td>Burst Size</td>
<td>400</td>
<td>Seconds, Default: 60</td>
</tr>
<tr>
<td>Time Interval</td>
<td>60</td>
<td>Note: MAC filtering must be enabled</td>
</tr>
<tr>
<td>Add offenders to MAC filtering</td>
<td>Enable</td>
<td></td>
</tr>
</tbody>
</table>
```

2. Click on the check box for **Session Rate Limiting** to enable (or disable) this feature, as required.

3. Enter values for the following session “limiting” parameters:
   - Mean Rate
   - Burst Size
   - Time Interval (in seconds)

4. Click on the **Submit** button to save your changes.

For advanced security, see also “Defining the MAC Filtering Options {Mac Filtering}” on page 232.

**Adding Static Ports {Static Port-Mapping Add}**

Static Port-Mapping allows the network administrator to setup a port mapping scheme that forwards packets received on a specific port to a particular static IP (typically private and mis-configured) and port number on the subscriber side of the Access Gateway. The advantage for the network administrator is that free private IP addresses can be used to manage devices (such as Access Points) on the subscriber side of the Access Gateway without setting them up with public IP addresses.

This procedure shows you how to add static ports.
1. From the Web Management Interface, click on System, then Static Port-Mapping Add. The Add Static Port-Mapping Entries screen appears:

2. Enter the Internal IP Address.

   Ensure that the device with the Internal IP Address has been added to the subscriber’s table.

3. Enter the Internal Port reference.

4. Enter a valid MAC Address.

5. Enter the External IP Address.

   The External IP address field will default to the IP address of the Access Gateway.

6. Enter the External Port reference.

7. Optional: Enter the Remote IP Address. Leave this field set to zero if you want to connect to the internal device from any network-side workstation.

8. Optional: Enable the Protect with Source IP-based Access Control option. Enabling this will only allow address in the source-based access control list to connect on this port mapping. Source-based access control needs to be enabled for this to be in effect.

9. Optional: Enter the Remote Port reference. Leave this field set to zero if you want to connect to the device from any TCP/UDP port of a network-side workstation.
10. Select the protocol (TCP or UDP) from the pull-down menu.

11. Click on the Add button to add this static port, or click on the Reset button to reset all values to their previous state.

For more information about Static Port-Mapping, see also:
- “Displaying the Static Port Mapping Table {Static Port-Mapping}” on page 159.
- “Deleting Static Ports {Static Port-Mapping Delete}” on page 238.

**Deleting Static Ports {Static Port-Mapping Delete}**

Static Port-Mapping allows the network administrator to setup a port mapping scheme that forwards packets received on a specific port to a particular static IP (typically private and misconfigured) and port number on the subscriber side of the Access Gateway. The advantage for the network administrator is that free private IP addresses can be used to manage devices (such as Access Points) on the subscriber side of the Access Gateway without setting them up with public IP addresses.

This procedure shows you how to add static ports.

**1.** From the Web Management Interface, click on System, then Static Port-Mapping Delete. The Delete Static Port-Mapping Entries screen appears:

**Delete Static Port-Mapping Entries**

<table>
<thead>
<tr>
<th>Internal Address/Internal Port (MAC Address)</th>
<th>External Address/External Port</th>
<th>Remote Address/Remote Port Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 4.2.7.1/80</td>
<td>10.0.0.123:4567</td>
<td>0.0.0.0/0 TCP</td>
</tr>
<tr>
<td>2. 10.0.0.123/23</td>
<td>4.2.7.1/8025</td>
<td>0.0.0.0/0 TCP</td>
</tr>
<tr>
<td>3. 9.2.1.1</td>
<td>2.0.0.1:4321</td>
<td>0.0.0.0/0 TCP</td>
</tr>
<tr>
<td>4. 2.1.4.15/80</td>
<td>0.0.0.0:7456</td>
<td>0.0.0.0/0 TCP</td>
</tr>
<tr>
<td>5. 10.20.1.34/6001</td>
<td>0.0.0.0:4321</td>
<td>0.0.0.0/0 TCP</td>
</tr>
</tbody>
</table>

**2.** Enter the External IP Address and/or the External Port of the item you want to delete.

**3.** Click on the Delete button to delete the static port, or click on the Reset button to reset your changes to their previous state.

For more information about Static Port-Mapping, see also:
Blocking a Subscriber Interface {Subscriber Interfaces}

The Access Gateway allows System Administrators to block subscriber interfaces.

1. From the Web Management Interface, click on **System**, then **Subscriber Interfaces**. The **Subscriber Interfaces** screen appears:

2. Enable or disable the following items by clicking on the corresponding check box:
   - Block Subscriber Interface 1
   - Block Subscriber Interface 2

3. Click on the **Submit** button to save your changes, or click on the **Reset** button to reset all values to their previous state.

Updating the Access Gateway Firmware {Upgrade}

Upgrading the Access Gateway firmware is performed from the Access Gateway’s Command Line Interface (CLI) only. Refer to the Firmware Upgrade Procedure (separate document available from Nomadix Technical Support).
The Subscriber Interface

This chapter provides an overview of the Access Gateway’s Subscriber Interface and sections outlining the authorization and billing processes, subscriber management models, and the ICC.

Overview

The Subscriber Interface is the window to the solution provider’s Web site, and much more than that. When a subscriber accesses the solution provider’s high speed network, the Access Gateway points their browser to a sign-in page. The Access Gateway then creates a database entry that automatically records the subscriber’s Media Access Control (MAC) address and integrates this address with a PMS interface for secure billing. Like a router, the Access Gateway continuously tracks subscriber IP and MAC settings, eliminating the need for further sign-ins and ensuring that subscriber usage and billing is recorded accurately. The Access Gateway also eliminates configuration issues between the subscriber’s computer and the network.

The Subscriber Interface is the portal Web site of the solution provider’s broadband network, and as such, its appearance and functionality reflect the needs of the solution provider. The Access Gateway is a gateway to this network, providing connection services that enable and automate an effective Enterprise relationship between a supplier (the solution provider) and its customer (the subscriber). The Access Gateway’s role in this customer/supplier relationship is effectively “invisible” to subscribers.
Authorization and Billing

As a gateway device, the Access Gateway enables plug-and-play access to broadband networks. Broadband network solution providers can now offer their subscribers a wide range of high speed services, including access to the Internet. Of course, a high speed Internet connection is not free – subscribers pay an access fee, based on the duration of their connection. Additionally, subscribers may want to take advantage of the solution provider’s local network services (for example, purchasing goods and local services). In either case, the subscriber is required to pay. Naturally, subscribers expect to pay only for the services rendered to them.

In any environment, billing is a complex process. It requires accurate data collection and reconciliation, a means to validate and protect the data, and an efficient method for collecting payments.

The Access Gateway offers powerful billing support functionality called “Authentication, Authorization, and Accounting.” This feature (also known as AAA) employs a combination of command routines designed to create a flexible, efficient, and secure billing environment. For example, when a subscriber logs into the system, their unique MAC address is placed into an authorization table. The system then authenticates the subscriber’s MAC address and billing information before allowing them to access the Internet and make online purchases.
The Subscriber Interface

The AAA Structure

The Access Gateway’s Authentication, Authorization, and Accounting (AAA) module enables the solution provider to provision, track, and bill new or returning subscribers. This includes:

- Allowing the solution provider (for example, a hotel) to bill its guests for the high speed network services it provides, track usage on the network, and deny service to those guests who have not paid.
- Allowing the solution provider to bill subscribers for services rendered, either directly on their hotel bill (in the hotel scenario), via a mailed invoice, or directly to the subscriber’s credit card account.

The following illustration shows the functional relationship between the Access Gateway’s internal modules and the external support systems.
The Authentication module is responsible for ensuring that when subscribers log in to the system they are correctly identified. It can identify subscribers in many different ways. For example:

- Based on their hardware (MAC) address.
- By validating their user name and password.
- By looking up subscribers on a local (flash) database.
- By looking up subscribers on a remote database.

*The Authentication module can support user name and MAC address authentication simultaneously.*
The initial login page can be presented in various ways, depending on the system’s configuration. The Access Gateway supports any of the following methods and tools:

- Internal and external Web pages.
- External “portal” page for redirection.
- User name and MAC-based logins (simultaneous or stand-alone).
- User-selectable options and parameters (for example, defining the time purchased).
- Interaction with a Property Management System (PMS) and Web interfaces enabling administrators to edit the subscriber’s input.

Only subscribers that are correctly identified and authenticated are authorized to access the system. Once authorized, the subscriber’s activity is logged and billed through the Access Gateway’s Accounting module.

The Accounting module fully supports the following functions:

- Credit card billing (for example, interaction with AuthorizeNet).
- User name and password verification.
- Billing verification.
- Per port-location (for example, room or unit) billing.
**Process Flow (AAA)**

The following flowchart outlines the AAA and billing process. All actions depicted in the chart are administered and tracked by the Access Gateway.

AG detects connection and verifies user against authorization table

New User

Login Page

Specify lease time required, and choose a user ID and password

Provide credit card details

PMS System

Reject

Accept

Bill for goods and services, and credit provider’s bank account

Billing Mirror Server

Lease time has expired

Yes

Purchase more time

No

Existing Subscriber

Internal or External Web Server

Solution Provider’s Portal Page

Internet and local online services

Browsing

Online purchases

Reject

Bill for goods and services, and credit provider’s bank account

Accept

Billing Mirror Server
**Internal and External Web Servers**

The Access Gateway supports both internal and external Web servers which act as a login interface between subscribers and the solution provider’s network, including the Internet. The internal Web server is “flashed” into the system’s memory and the login page is served directly from the Access Gateway. In the external Web server model, the Access Gateway redirects the subscriber’s login request to an external server. Either method is transparent to the subscriber; however, the advantage of using the internal Web server is obvious – no login redirection tasks and a faster response time for the subscriber.

**Language Support**

The Access Gateway’s subscriber interface supports many Asian and European languages, including: English, Chinese, French, German, Japanese, and Spanish.

**Home Page Redirection**

The Access Gateway can be configured to redirect all valid subscribers to a Web portal or home page determined by the solution provider. After a specified time, from the first home page redirection (determined by the system administrator), subscribers are redirected again to the portal at the next Web page request.
Subscriber Management

The Access Gateway provides several subscriber management models, including:

- Free access (for example, no AAA functionality)
- MAC address
- Port-Location ID (for example, by room or unit number)
- User name and password
- Credit card

Combinations of two or more subscriber management models can be used. When a subscriber connects to the network and attempts to access the Internet, the Access Gateway looks for each model in the given order above.

Subscriber Management Models

The system administrator establishes the subscriber management model via the Command Line Interface (CLI) or the Web Management Interface. These models can be changed while the Access Gateway is running (without rebooting or interrupting the service).

- **Free Access** – If the Access Gateway is configured to disable AAA services, all subscribers will have free access to the Internet.

- **MAC Address** – Each computer with an Ethernet interface card has a unique MAC (hardware) address. The Access Gateway can be configured to allow access for specified MAC addresses. In this model, when a subscriber attempts to access the Internet, the Access Gateway validates the subscriber’s MAC address against a MAC authorization table. If the MAC address is verified, the Access Gateway authorizes access to the Internet. A possible scenario for using this model is to allow Internet access to administrative personnel in all locations.

- **User Name and Password** – Each subscriber can choose a unique user name and password (and be charged for it). In this model, when a subscriber attempts to access the Internet, they are prompted for the user name and password before access is authorized. Possible scenarios in which this model is appropriate include allowing subscribers to use more than one computer or when subscribers want to move between locations.

- **Credit Card** – In this model, when subscribers connect to the network and attempt to access the Internet, they are prompted for their credit card information. The Access Gateway is pre-configured to use the Authorize.Net service and you will need to open a merchant trading account with them before using this subscriber management model.
# Configuring the Subscriber Management Models

<table>
<thead>
<tr>
<th>Model</th>
<th>What You Need To Do</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free access</td>
<td>Disable the AAA services.</td>
</tr>
<tr>
<td>MAC address</td>
<td>Enable the AAA services and add a subscriber profile to the database for each MAC address you want to enable.</td>
</tr>
<tr>
<td>User Name and Password</td>
<td>Enable the AAA services and Usernames. Add a subscriber profile to the database for each user name and password you want to enable. You will need to request a unique user name and password when they pay for the service. The user name and password are optional (the MAC address will be substituted), but in this event the service is not transferable between computers.</td>
</tr>
<tr>
<td>Credit card</td>
<td>Enable the AAA services. You have the choice of enabling the Access Gateway’s internal authorization module or using an external credit card authorization server. Internal Authorization Enabled Enter the credit card server’s URL and IP address, then enter the merchant ID you obtain from Authorize.Net. If you have NOT enabled Internal Authorization Set up your own external authorization server with your merchant ID. Enter the secret key (the default is <code>bigbrowndog</code>). Enter the external authorization server’s URL, then enter its IP address as a pass-through IP address.</td>
</tr>
</tbody>
</table>
Information and Control Console (ICC)

The ICC is a HTML pop-up window that is presented to subscribers, allowing them to select their bandwidth and billing options quickly and efficiently, and displays a dynamic “time” field to inform them of the time remaining on their account. The ICC also offers service providers an opportunity to display advertising banners and provide a choice of redirection options.

For information about configuring the ICC, refer to “Defining Languages {Language Support}” on page 201.

**ICC Pop-Up Window**

The ICC displays a HTML-based applet in the form of a pop-up window from which subscribers can dynamically control their billing options and bandwidth, and which allows service providers to display advertising banners and redirect their subscribers to predetermined Web sites.

The pop-up window automatically displays at Home Page Redirection (HPR) or whenever the subscriber brings up a new browser window.
**Logout Console**

The Access Gateway allows System Administrators to define a simple HTML-based pop-up window for explicit logout that can be used as an alternative to the more fully featured ICC. The pop-up Logout Console can display the elapsed/count-down time and one logo for intra-session service branding.
Quick Reference Guide

This chapter contains product reference information, organized by topic. Use this chapter to locate the information you need quickly and efficiently.

Web Management Interface (WMI) Menus

The following tables contain a listing and brief explanation of all menus and menu items contained in the Access Gateway’s Web Management Interface (WMI), listed as they appear on screen.

<table>
<thead>
<tr>
<th>Menus</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Menu</td>
<td>Displays the Configuration menu. Items in this menu let you establish IP parameters, set DHCP options, set DNS and home page redirection options, set MAC-based authentication, display configuration settings, and set the system date and time, SNMP and SYSLOG parameters.</td>
</tr>
<tr>
<td>Network Info Menu</td>
<td>Displays the Network Info menu. The items in this menu are used to monitor and review network connections, routings, protocols, and network session statistics.</td>
</tr>
<tr>
<td>Port-Location Menu</td>
<td>Displays the Port-Location menu. Items in this menu let you find, add, remove, and update the Port-Location Assignments (for example, VLAN tags).</td>
</tr>
<tr>
<td>Subscriber Administration Menu</td>
<td>Displays the Subscriber Administration menu. The items in this menu allow you to add, remove, and monitor subscriber profiles, display the current DHCP leases, and monitor the subscribers currently connected to the network.</td>
</tr>
<tr>
<td>Subscriber Interface Menu</td>
<td>Displays the Subscriber Interface menu. The items in this menu allow you to define how the subscriber interface is displayed to users and what information it contains.</td>
</tr>
<tr>
<td>System Menu</td>
<td>Displays the System menu. Items in this menu let you manage login names and passwords, configuration settings, and routings.</td>
</tr>
</tbody>
</table>
## Configuration Menu Items

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Establishes the AAA service options.</td>
</tr>
<tr>
<td>Access Control</td>
<td>To enable secure administration of the product, the Nomadix Access Gateway incorporates a master access control list that checks the source (IP address) of administrator logins. A login is permitted only if a match is made with the master list contained on the Nomadix Access Gateway. If a match is not made, the login is denied, even if a correct login name and password are supplied. The access control list supports up to 50 (fifty) entries in the form of a specific IP address or range of IP addresses. Additionally, the Nomadix Access Gateway offers access control based on the type of Interface being used. This feature allows administrators to block access from Telnet, Web Management, and FTP sources.</td>
</tr>
<tr>
<td>Auto Configuration</td>
<td>Provides an effortless and rapid method for configuring devices for fast network roll-outs.</td>
</tr>
<tr>
<td>Bandwidth Management</td>
<td>Manages the bandwidth for subscribers, defined in Kbps (Kilobits per seconds) for both upstream and downstream data transmissions.</td>
</tr>
<tr>
<td>Bill Record Mirroring</td>
<td>Configures the Nomadix Access Gateway to send copies of billing records to external servers.</td>
</tr>
<tr>
<td>DHCP</td>
<td>Assigns the Nomadix Access Gateway as its own DHCP server, or enables the DHCP relay for an external server.</td>
</tr>
<tr>
<td>DNS</td>
<td>Sets up the DNS parameters, including the host name, domain, and the primary and secondary DNS servers.</td>
</tr>
<tr>
<td>Dynamic DNS</td>
<td>Sets parameters for Dynamic DNS.</td>
</tr>
<tr>
<td>GRE Tunneling</td>
<td>Sets GRE Tunneling parameters.</td>
</tr>
<tr>
<td>Home Page Redirect</td>
<td>Redirects the subscriber’s browser to a specified home page.</td>
</tr>
<tr>
<td>iNAT™</td>
<td>Enables Intelligent Address Translation for Transparent VPN Access.</td>
</tr>
<tr>
<td>IPSec</td>
<td></td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Location</td>
<td>Sets up your location and IP addresses for the network, subscriber, subnet mask, and default gateway.</td>
</tr>
<tr>
<td>Logging</td>
<td>Enables logging options for the system and AAA functions.</td>
</tr>
<tr>
<td>MAC Authentication</td>
<td>Enables MAC authentication, retry frequency, MAC address format, MAC address hex-alpha case, and RADIUS service profile.</td>
</tr>
<tr>
<td>Passthrough Addresses</td>
<td>Establishes IP pass-through addresses (up to 300).</td>
</tr>
<tr>
<td>PMS</td>
<td>Enables one of the listed PMS options, or allows you to disable the PMS feature.</td>
</tr>
<tr>
<td>Port-Location</td>
<td>Establishes the Access Concentrator settings.</td>
</tr>
<tr>
<td>RADIUS Client</td>
<td>This procedure sets up the RADIUS client.</td>
</tr>
<tr>
<td>RADIUS Proxy</td>
<td>Establishes RADIUS proxies, where different realms can be set up to directly channel RADIUS messages to the various RADIUS servers.</td>
</tr>
<tr>
<td>RADIUS Routing</td>
<td>Sets up RADIUS Service Profiles (up to 10) and Realm-based Routing Policies (up to 50).</td>
</tr>
<tr>
<td>SMTP</td>
<td>Enables the SMTP (E-mail) redirection functions.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Establishes the SNMP parameters.</td>
</tr>
<tr>
<td>Subnets</td>
<td>Enables dynamic multiple subnet support.</td>
</tr>
<tr>
<td>Summary</td>
<td>Displays a summary listing of all configuration settings.</td>
</tr>
<tr>
<td>Time</td>
<td>Sets the system date and time.</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>Dynamically adds or removes up to 300 specific IP addresses and domain names to be filtered for each property.</td>
</tr>
</tbody>
</table>
## Network Info Menu Items

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>Displays the ARP table, including the destination IP address and the gateway MAC address.</td>
</tr>
<tr>
<td>DAT</td>
<td>Displays the DAT session table.</td>
</tr>
<tr>
<td>Hosts</td>
<td>Displays the host table, including host names, associated IP addresses and any assigned aliases.</td>
</tr>
<tr>
<td>ICMP</td>
<td>Displays the ICMP (Internet Control Message Protocol) performance statistics.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Displays statistics for the interfaces.</td>
</tr>
<tr>
<td>IP</td>
<td>Displays the IP performance statistics.</td>
</tr>
<tr>
<td>Routing</td>
<td>Displays the routing tables and performance statistics.</td>
</tr>
<tr>
<td>Sockets</td>
<td>Displays the active Internet connections.</td>
</tr>
<tr>
<td>Static Port-Mapping</td>
<td>Displays the currently active static port-mapping scheme.</td>
</tr>
<tr>
<td>TCP</td>
<td>Displays the TCP performance statistics.</td>
</tr>
<tr>
<td>UDP</td>
<td>Displays the UDP performance statistics.</td>
</tr>
</tbody>
</table>

## Port-Location Menu Items

<table>
<thead>
<tr>
<th>Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Adds or updates port-location assignments.</td>
</tr>
<tr>
<td>Delete All</td>
<td>Deletes all port-location assignments. Use this command with caution.</td>
</tr>
<tr>
<td>Delete by Location</td>
<td>Deletes port-location assignments, based on a specified location.</td>
</tr>
<tr>
<td>Delete by Port</td>
<td>Deletes port-location assignments, based on a specified port (VLAN tag).</td>
</tr>
<tr>
<td>Items</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Export</td>
<td>Exports specified port-location assignments to the <code>location.txt</code> file.</td>
</tr>
<tr>
<td>Find by Description</td>
<td>Finds a port-location assignment, based on a unique description.</td>
</tr>
<tr>
<td>Find by Location</td>
<td>Finds a port-location assignment, based on a specified location.</td>
</tr>
<tr>
<td>Find by Port</td>
<td>Finds a port-location assignment, based on a specified port.</td>
</tr>
<tr>
<td>Import</td>
<td>Imports specified port-location assignments from the <code>location.txt</code> file.</td>
</tr>
<tr>
<td>List</td>
<td>Displays the port-location file, listing all port-location assignments.</td>
</tr>
</tbody>
</table>
## Subscriber Administration Menu Items

<table>
<thead>
<tr>
<th>Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Adds subscriber profiles to the database.</td>
</tr>
<tr>
<td>Current</td>
<td>Displays a list of all currently connected subscribers.</td>
</tr>
<tr>
<td>Delete by MAC</td>
<td>Deletes a subscriber, based on a specific MAC address.</td>
</tr>
<tr>
<td>Delete by User</td>
<td>Deletes a subscriber, based on a specific user name.</td>
</tr>
<tr>
<td>DHCP Leases</td>
<td>Sets up the current subscriber DHCP leases.</td>
</tr>
<tr>
<td>Expired</td>
<td>Removes expired profiles.</td>
</tr>
<tr>
<td>Find by MAC</td>
<td>Finds a subscriber profile, based on a specified MAC address.</td>
</tr>
<tr>
<td>Find by User</td>
<td>Finds a subscriber profile, based on a specified user name.</td>
</tr>
<tr>
<td>List by MAC</td>
<td>Displays a list of authorized subscriber profiles, sorted by MAC address.</td>
</tr>
<tr>
<td>List by User</td>
<td>Displays a list of authorized subscriber profiles, sorted by user name.</td>
</tr>
<tr>
<td>Statistics</td>
<td>Displays the current subscriber profile statistics (for example, how many profiles are currently in the database).</td>
</tr>
</tbody>
</table>

## Subscriber Interface Menu Items

<table>
<thead>
<tr>
<th>Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Billing Options</td>
<td>Establishes the various billing plans and rates (schemes), including messages and appearance.</td>
</tr>
<tr>
<td>ICC Setup</td>
<td>Sets up the Information and Control Console (ICC) for subscribers.</td>
</tr>
<tr>
<td>Language Support</td>
<td>Defines the language to be displayed on the Web Management Interface and the subscriber's portal page.</td>
</tr>
<tr>
<td>Login UI</td>
<td>Defines the appearance of the internal subscriber login user interface, including all the login messages and fonts, etc., and establishes the currency.</td>
</tr>
</tbody>
</table>
### System Menu Items

<table>
<thead>
<tr>
<th>Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP Add</td>
<td>Adds an Address Resolution Protocol (ARP) table entry.</td>
</tr>
<tr>
<td>ARP Delete</td>
<td>Deletes an ARP table entry.</td>
</tr>
<tr>
<td>Bridge Mode</td>
<td>Enables the Bridge Mode option.</td>
</tr>
<tr>
<td>Export</td>
<td>Exports the system’s configuration settings to an archive file.</td>
</tr>
<tr>
<td>Factory</td>
<td>Imports the factory default settings.</td>
</tr>
<tr>
<td>FailOver</td>
<td>Sets up a “sibling” Nomadix Gateway, allowing one device to take up the</td>
</tr>
<tr>
<td></td>
<td>users should the other device become disconnected from the network.</td>
</tr>
<tr>
<td>History</td>
<td>Displays a history log of the system’s activity, including Access, Reboot</td>
</tr>
<tr>
<td></td>
<td>and Uptime.</td>
</tr>
</tbody>
</table>

### System Menu Items

<table>
<thead>
<tr>
<th>Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post Session UI</td>
<td>Defines the post session “Goodbye” page.</td>
</tr>
<tr>
<td>Subscriber Buttons</td>
<td>Defines how each of the subscriber’s user interface control buttons are</td>
</tr>
<tr>
<td></td>
<td>displayed.</td>
</tr>
<tr>
<td>Subscriber Labels</td>
<td>Defines how the subscriber’s user interface field labels are displayed.</td>
</tr>
<tr>
<td>Subscriber Errors, 1 of 2</td>
<td>Defines how error messages are displayed to subscribers (page 1 of 2).</td>
</tr>
<tr>
<td>Subscriber Errors, 2 of 2</td>
<td>Defines how error messages are displayed to subscribers (page 2 of 2).</td>
</tr>
<tr>
<td>Subscriber Messages, 1 of 3</td>
<td>Defines how “other” general messages are displayed to subscribers (page 1 of 3).</td>
</tr>
<tr>
<td>Subscriber Messages, 2 of 3</td>
<td>Defines how “other” general messages are displayed to subscribers (page 2 of 3).</td>
</tr>
<tr>
<td>Subscriber Messages, 3 of 3</td>
<td>Defines how “other” general messages are displayed to subscribers (page 3 of 3).</td>
</tr>
</tbody>
</table>
## Items

<table>
<thead>
<tr>
<th>Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP</td>
<td>Sets up ICMP blocking for traffic from “pending” or “non authenticated” users that are destined to addresses other than those defined in the pass-through (walled garden) list.</td>
</tr>
<tr>
<td>Import</td>
<td>Imports previously exported system configuration settings from an archive file.</td>
</tr>
<tr>
<td>Login</td>
<td>Sets up the login name and password.</td>
</tr>
<tr>
<td>Mac Filtering</td>
<td>Blocks malicious users based on their MAC address. Up to 50 MAC addresses can be blocked at any one time.</td>
</tr>
<tr>
<td>Reboot</td>
<td>Reboots the Nomadix Access Gateway.</td>
</tr>
<tr>
<td>Route Add</td>
<td>Adds a route into the Nomadix Access Gateway’s routing table.</td>
</tr>
<tr>
<td>Route Delete</td>
<td>Deletes a route to a specific IP destination.</td>
</tr>
<tr>
<td>Session Limit</td>
<td>Limits the number sessions any one user can take over a given time period and, if necessary, then blocks malicious users.</td>
</tr>
<tr>
<td>Static Port-Mapping Add</td>
<td>Sets up static port-mapping schemes.</td>
</tr>
<tr>
<td>Static Port-Mapping Delete</td>
<td>Deletes static port-mapping schemes.</td>
</tr>
<tr>
<td>Subscriber Interfaces</td>
<td>Blocks subscriber interfaces.</td>
</tr>
<tr>
<td>Upgrade</td>
<td>Obtain the latest Firmware Upgrade Procedure from Nomadix Technical Support.</td>
</tr>
</tbody>
</table>

## Items

<table>
<thead>
<tr>
<th>Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP Add</td>
<td>Adds an Address Resolution Protocol (ARP) table entry.</td>
</tr>
<tr>
<td>ARP Delete</td>
<td>Deletes an ARP table entry.</td>
</tr>
<tr>
<td>Bridge Mode</td>
<td>Enables the Bridge Mode option.</td>
</tr>
<tr>
<td>Export</td>
<td>Exports the system’s configuration settings to an archive file.</td>
</tr>
<tr>
<td>Factory</td>
<td>Imports the factory default settings.</td>
</tr>
<tr>
<td>Items</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>FailOver</td>
<td>Sets up a “sibling” Nomadix Gateway, allowing one device to take up the users should the other device become disconnected from the network.</td>
</tr>
<tr>
<td>History</td>
<td>Displays a history log of the system’s activity, including Access, Reboot and Uptime.</td>
</tr>
<tr>
<td>ICMP</td>
<td>Sets up ICMP blocking for traffic from “pending” or “non authenticated” users that are destined to addresses other than those defined in the pass-through (walled garden) list.</td>
</tr>
<tr>
<td>Import</td>
<td>Imports previously exported system configuration settings from an archive file.</td>
</tr>
<tr>
<td>Login</td>
<td>Sets up the login name and password.</td>
</tr>
<tr>
<td>Mac Filtering</td>
<td>Blocks malicious users based on their MAC address. Up to 50 MAC addresses can be blocked at any one time.</td>
</tr>
<tr>
<td>Reboot</td>
<td>Reboots the Access Gateway.</td>
</tr>
<tr>
<td>Route Add</td>
<td>Adds a route into the Access Gateway’s routing table.</td>
</tr>
<tr>
<td>Route Delete</td>
<td>Deletes a route to a specific IP destination.</td>
</tr>
<tr>
<td>Session Limit</td>
<td>Limits the number sessions any one user can take over a given time period and, if necessary, then blocks malicious users.</td>
</tr>
<tr>
<td>Static Port-Mapping Add</td>
<td>Sets up static port-mapping schemes.</td>
</tr>
<tr>
<td>Static Port-Mapping Delete</td>
<td>Deletes static port-mapping schemes.</td>
</tr>
<tr>
<td>Subscriber Interfaces</td>
<td>Blocks subscriber interfaces.</td>
</tr>
<tr>
<td>Syslog</td>
<td>Displays syslog history.</td>
</tr>
<tr>
<td>System Utilization</td>
<td>Displays system utilization information.</td>
</tr>
<tr>
<td>Upgrade</td>
<td>Obtain the latest Firmware Upgrade Procedure from Nomadix Technical Support.</td>
</tr>
<tr>
<td>User Settings</td>
<td>Blocks IPPROTO traffic from misconfigured subscribers.</td>
</tr>
</tbody>
</table>
Alphabetical Listing of Menu Items (WMI)

The menu items listed here are for a fully featured Nomadix Access Gateway (with all optional modules included). Refer to “About Your Product License” on page 55.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Set AAA options</td>
</tr>
<tr>
<td>Access Control</td>
<td>Enables secure administration of the Access Gateway</td>
</tr>
<tr>
<td>Add</td>
<td>Add or update port-location assignments</td>
</tr>
<tr>
<td>Add</td>
<td>Add subscriber profiles to the database</td>
</tr>
<tr>
<td>ARP</td>
<td>Display the ARP table</td>
</tr>
<tr>
<td>ARP Add</td>
<td>Add an ARP table entry</td>
</tr>
<tr>
<td>ARP Delete</td>
<td>Delete an ARP table entry</td>
</tr>
<tr>
<td>Bandwidth Management</td>
<td>Define upstream and downstream bandwidth</td>
</tr>
<tr>
<td>Billing Options</td>
<td>Establish the billing options</td>
</tr>
<tr>
<td>Bill Record Mirroring</td>
<td>Enable bill record copying to external servers</td>
</tr>
<tr>
<td>Bridge Mode</td>
<td>Enable the Bridge Mode option</td>
</tr>
<tr>
<td>Current Address</td>
<td>Display currently connected subscribers</td>
</tr>
<tr>
<td>DAT</td>
<td>Display the DAT session table</td>
</tr>
<tr>
<td>Delete All</td>
<td>Delete all port-location assignments</td>
</tr>
<tr>
<td>Delete by Location</td>
<td>Delete port-location assignments by location</td>
</tr>
<tr>
<td>Delete by MAC</td>
<td>Delete subscriber profiles by MAC address</td>
</tr>
<tr>
<td>Delete by Port</td>
<td>Delete port-location assignments by port</td>
</tr>
<tr>
<td>Delete by User</td>
<td>Delete subscriber profiles by user</td>
</tr>
<tr>
<td>DHCP</td>
<td>Set the DHCP service options</td>
</tr>
<tr>
<td>DHCP Leases</td>
<td>Set the current subscriber DHCP leases</td>
</tr>
<tr>
<td>DNS</td>
<td>Set the DNS parameters</td>
</tr>
<tr>
<td>Export</td>
<td>Export configuration settings to the archive file</td>
</tr>
<tr>
<td>Export</td>
<td>Export port-location assignments to file</td>
</tr>
<tr>
<td>Factory</td>
<td>Import the factory default configuration settings</td>
</tr>
<tr>
<td>FailOver</td>
<td>Sets up a “sibling” Nomadix Gateway</td>
</tr>
<tr>
<td>Find by Description</td>
<td>Find port-location assignments by description</td>
</tr>
<tr>
<td>Find by Location</td>
<td>Find port-location assignments by location</td>
</tr>
<tr>
<td>Find by MAC</td>
<td>Find a subscriber profile by MAC address</td>
</tr>
<tr>
<td>Find by Port</td>
<td>Find port-location assignments by port</td>
</tr>
<tr>
<td>Find by User</td>
<td>Find a subscriber profile by user name</td>
</tr>
<tr>
<td>History</td>
<td>Display the system’s history log</td>
</tr>
<tr>
<td>Home Page Redirect</td>
<td>Redirect the subscriber’s browser</td>
</tr>
<tr>
<td>Hosts</td>
<td>Display the host table</td>
</tr>
<tr>
<td>ICC Setup</td>
<td>Sets up the Information and Control Console</td>
</tr>
<tr>
<td>ICMP</td>
<td>Display ICMP performance statistics</td>
</tr>
<tr>
<td>Import</td>
<td>Import configuration settings from the archive file</td>
</tr>
<tr>
<td>Import</td>
<td>Import port-location assignments from file</td>
</tr>
<tr>
<td>iNAT</td>
<td>Enable translation for transparent VPN access</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Display performance statistics for interfaces</td>
</tr>
<tr>
<td>IP</td>
<td>Display IP performance statistics</td>
</tr>
<tr>
<td>Language Support</td>
<td>Define different languages</td>
</tr>
<tr>
<td>List</td>
<td>Display the room file</td>
</tr>
<tr>
<td>List by MAC</td>
<td>List the subscriber database, sorted by MAC address</td>
</tr>
<tr>
<td>List by User</td>
<td>List the subscriber database, sorted by user name</td>
</tr>
<tr>
<td>Location</td>
<td>Establish your location and network IP parameters</td>
</tr>
<tr>
<td>Logging</td>
<td>Enable system and AAA logging options</td>
</tr>
<tr>
<td>Login</td>
<td>Establish access for managers and operators</td>
</tr>
<tr>
<td>Login U1</td>
<td>Establish the internal login screen settings</td>
</tr>
<tr>
<td>Mac Filtering</td>
<td>Blocks traffic based on MAC address</td>
</tr>
<tr>
<td>Pass through Addresses</td>
<td>Establish up to 100 IP pass-through addresses</td>
</tr>
<tr>
<td>Port-Location</td>
<td>Establish the access concentrator settings</td>
</tr>
<tr>
<td>Post Session U1</td>
<td>Sets up the post session “Goodbye” page</td>
</tr>
<tr>
<td>RADIUS Client</td>
<td>Sets up RADIUS client options</td>
</tr>
<tr>
<td>RADIUS Proxy</td>
<td>Establishes RADIUS proxies</td>
</tr>
<tr>
<td>RADIUS Routing</td>
<td>Sets up service profiles and realm-based routing policies</td>
</tr>
<tr>
<td>Reboot</td>
<td>Reboot the operating system</td>
</tr>
</tbody>
</table>
Route Add............................. Add a route to the routing table ............................................. System
Route Delete......................... Delete a route from the routing table ............................................. System
Routing ................................. Display routing performance statistics and tables .......... Network Info
Session Limit........................ Limits subscriber sessions...................................................... System
SMTP ................................... Set the SMTP redirection options .......................................... Configuration
SNMP ................................... Establish the SNMP parameters............................................. Configuration
Sockets.................................. Display the active IP connections ........................................ Network Info
Static Port-Mapping ............. Displays currently active static port-mapping schemes .......... Network Info
Static Port-Mapping Add...... Adds a static port-mapping scheme ....................................... System
Static Port-Mapping Delete .. Deletes a static port-mapping scheme.................................... System
Statistics.............................. Display the subscriber profile statistics ................................. Subscriber Admin
Subnets ................................. Enable dynamic multiple subnet support ......................... Configuration
Subscriber Buttons ............... Define how control buttons are displayed to subscribers ...... Subscriber I’face
Subscriber Interfaces ............ Blocks subscriber interfaces .................................................. System
Subscriber Labels ................. Define how field labels are displayed.......................... Subscriber I’face
Subscriber Errors.................. Define how error messages are displayed....................... Subscriber I’face
Subscriber Messages .......... Define how “other” general messages are displayed .......... Subscriber I’face
Summary .............................. Display a summary of the configuration settings .......... Configuration
TCP....................................... Display the TCP performance statistics ................................. Network Info
UDP....................................... Display the UDP performance statistics ................................ Network Info
Upgrade ................................ Upgrade the Access Gateway system firmware..................... System
URL Filtering....................... Define URLs for filtering....................................................... Configuration
**Default (Factory) Configuration Settings**

The following table shows a partial listing of the Access Gateway’s primary default configuration settings (the settings established at manufacturing). For a complete listing of the factory default settings, refer to the factory.txt file. For more information, go to “Importing the Factory Defaults {Factory}” on page 224.

<table>
<thead>
<tr>
<th>Function</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version</strong></td>
<td>Nomadix Access Gateway v5.4.xxx (depends on firmware version)</td>
</tr>
<tr>
<td>Nomadix Access Gateway ID</td>
<td>AG3100</td>
</tr>
<tr>
<td>Network Interface MAC</td>
<td>MAC address is unique for each product</td>
</tr>
<tr>
<td>Subscriber Interface MAC</td>
<td>MAC address is unique for each product</td>
</tr>
<tr>
<td><strong>Network Interface IP</strong></td>
<td>10.0.0.10</td>
</tr>
<tr>
<td>Subscriber IP</td>
<td>10.0.0.11</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway IP</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td>DHCP Client</td>
<td>Enabled</td>
</tr>
<tr>
<td>Admin IP</td>
<td>172.30.30.172</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>nomadix.</td>
</tr>
<tr>
<td>Host Name</td>
<td>AG3100</td>
</tr>
<tr>
<td>Primary DNS</td>
<td>0.0.0.2</td>
</tr>
<tr>
<td>Secondary DNS</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Tertiary DNS</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td><strong>DHCP Relay</strong></td>
<td>Disabled</td>
</tr>
<tr>
<td>External DHCP Server IP</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>DHCP Relay Agent IP</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>Enabled</td>
</tr>
<tr>
<td>DHCP Server IP</td>
<td>10.0.0.4</td>
</tr>
<tr>
<td>DHCP Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>DHCP Pool Start IP</td>
<td>10.0.0.12</td>
</tr>
<tr>
<td>DHCP Pool End IP</td>
<td>10.0.0.250</td>
</tr>
<tr>
<td>Lease Duration Minutes</td>
<td>1440</td>
</tr>
<tr>
<td><strong>Home Page Redirection</strong></td>
<td>Disabled</td>
</tr>
<tr>
<td>Parameter Passing</td>
<td>Disabled</td>
</tr>
<tr>
<td>Redirection Frequency Minutes</td>
<td>3600</td>
</tr>
<tr>
<td><strong>Dynamic Address Translation (DAT)</strong></td>
<td>Enabled (cannot be changed)</td>
</tr>
<tr>
<td>Function</td>
<td>Default Setting</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>AAA Logging</td>
<td>Disabled</td>
</tr>
<tr>
<td>AAA Log Server Number</td>
<td>3</td>
</tr>
<tr>
<td>AAA Log Server IP</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>SYSLOG (System Logging)</td>
<td>Disabled</td>
</tr>
<tr>
<td>SYSLOG Server Number</td>
<td>2</td>
</tr>
<tr>
<td>SYSLOG Server IP</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>AAA Services</td>
<td>Disabled</td>
</tr>
<tr>
<td>Internal Authorization</td>
<td>Enabled</td>
</tr>
<tr>
<td>New Subscribers</td>
<td>Enabled</td>
</tr>
<tr>
<td>Credit Card Service</td>
<td>Enabled</td>
</tr>
<tr>
<td>Parameter Passing</td>
<td>Disabled</td>
</tr>
<tr>
<td>Usernames</td>
<td>Enabled</td>
</tr>
<tr>
<td>XML</td>
<td>Disabled</td>
</tr>
<tr>
<td>DNS Redirection</td>
<td>Enabled</td>
</tr>
<tr>
<td>SMTP Redirection</td>
<td>Disabled</td>
</tr>
<tr>
<td>SMTP Server IP</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>SNMP</td>
<td>Disabled</td>
</tr>
<tr>
<td>SNMP Get Community</td>
<td>public</td>
</tr>
<tr>
<td>SNMP Set Community</td>
<td>private</td>
</tr>
<tr>
<td>SNMP Trap IP</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>System Administration Login User Name</td>
<td>admin</td>
</tr>
<tr>
<td>System Administration Password</td>
<td>admin</td>
</tr>
</tbody>
</table>
## Product Specifications

### AG2300 Specifications

<table>
<thead>
<tr>
<th><strong>AVAILABLE NSE MODULES</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>High Availability - Fail Over</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>PERFORMANCE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>User Support: Up to 50 users concurrently</td>
</tr>
<tr>
<td>Throughput: up to 20Mbits/s*</td>
</tr>
<tr>
<td>*As defined by RFC1242, Section 3.17</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>PHYSICAL</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1U rack space in a 19” rack</td>
</tr>
<tr>
<td>10.00”(L) x 10.00”(D) x 1.73”(H)</td>
</tr>
<tr>
<td>254mm(L) x 254mm(D) x 44mm(H)</td>
</tr>
<tr>
<td>Weight: 5.0 lbs.</td>
</tr>
<tr>
<td>Weight: 2.27 Kg</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>OPERATING VOLTAGE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>100 – 240 VAC, 50/60Hz, Auto Sensing</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>POWER CONSUMPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>44 watts</td>
</tr>
</tbody>
</table>

---
<table>
<thead>
<tr>
<th><strong>AG2300 Specifications</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ENVIRONMENTAL</strong></td>
</tr>
<tr>
<td>Operating temperature: 5°C to 40° C</td>
</tr>
<tr>
<td>Storage temperature: 0°C to 70° C</td>
</tr>
<tr>
<td>Operating humidity: 20 - 90% RH non-condensing</td>
</tr>
<tr>
<td>Storage humidity: 5 - 95% RH</td>
</tr>
<tr>
<td>Altitude: Up to 15,000ft</td>
</tr>
<tr>
<td><strong>COMPLIANCE</strong></td>
</tr>
<tr>
<td>FCC Class A, Part 15</td>
</tr>
<tr>
<td>CE Mark</td>
</tr>
<tr>
<td>CENELEC EN 61000-3-2:2000</td>
</tr>
<tr>
<td>UL Std. 1950</td>
</tr>
<tr>
<td>CSA22.2 No. 950</td>
</tr>
<tr>
<td><strong>INTERFACES</strong></td>
</tr>
<tr>
<td>3 x 10/100 Mbps Ethernet (RJ-45)</td>
</tr>
<tr>
<td>1 x DB9 serial (for serial management and PMS interface)</td>
</tr>
<tr>
<td><strong>LED INDICATORS</strong></td>
</tr>
<tr>
<td>ACT/LINK and 10/100 for each Ethernet port</td>
</tr>
<tr>
<td>Power</td>
</tr>
<tr>
<td><strong>NETWORK MANAGEMENT</strong></td>
</tr>
<tr>
<td>Multi-Level Administration Controls</td>
</tr>
<tr>
<td>Integrated VPN Client (IPSec) for secure connection to an NOC</td>
</tr>
<tr>
<td>Access Control Lists</td>
</tr>
<tr>
<td>Web Administration UI</td>
</tr>
<tr>
<td>CLI via Telnet and Serial Port</td>
</tr>
<tr>
<td>SNMPv2c</td>
</tr>
<tr>
<td>Secure XML API</td>
</tr>
<tr>
<td>Auto Configuration and Upgrades</td>
</tr>
<tr>
<td>Syslog/AAA log</td>
</tr>
<tr>
<td>NETWORKING</td>
</tr>
<tr>
<td>----------------------------</td>
</tr>
<tr>
<td>IEEE 802.3 / 3u</td>
</tr>
<tr>
<td>IEEE 802.1d</td>
</tr>
<tr>
<td>DHCP Server</td>
</tr>
<tr>
<td>DHCP Relay</td>
</tr>
<tr>
<td>RADIUS Client (MD-5, PAP, CHAP, MS-CHAPv1, v2)</td>
</tr>
</tbody>
</table>
## AG3100 Specifications

### AVAILABLE NSE MODULES
- High Availability - Fail Over
- Hospitality Module - Property Management Interface (PMS)

### PERFORMANCE
- **User Support**: Up to 200 users concurrently
- **Throughput**: up to 85Mbits/s*

*As defined by RFC1242, Section 3.17

### PHYSICAL
- 1U rack space in a 19" rack
- 10.00"(L) x 10.00"(D) x 1.73"(H)
- 254mm(L) x 254mm(D) x 44mm(H)
- Weight: 5.0 lbs.
- Weight: 2.27 Kg

### OPERATING VOLTAGE
- 100 – 240 VAC, 50/60Hz, Auto Sensing

### POWER CONSUMPTION
- 44 watts
### AG3100 Specifications

#### Environmental
- Operating temperature: 5°C to 40°C
- Storage temperature: 0°C to 70°C
- Operating humidity: 20 - 90% RH non-condensing
- Storage humidity: 5 - 95% RH
- Altitude: Up to 15,000ft

#### Compliance
- FCC Class A, Part 15
- CE Mark
- CENELEC EN 61000-3-2:2000
- UL Std. 1950
- CSA22.2 No. 950

#### Interfaces
- 3 x 10/100 Mbps Ethernet (RJ-45)
- 1 x DB9 serial (for serial management and PMS interface)

#### LED Indicators
- ACT/LINK and 10/100 for each Ethernet port
- Power

#### Network Management
- Multi-Level Administration Controls
- Integrated VPN Client (IPSec) for secure connection to an NOC
- Access Control Lists
- Web Administration UI
- CLI via Telnet and Serial Port
- SNMPv2c
- Secure XML API
- Auto Configuration and Upgrades
- Syslog/AAA log

#### Networking
- IEEE 802.3 / 3u
- IEEE 802.1d
- DHCP Server
- DHCP Relay
- RADIUS Client (MD-5, PAP, CHAP, MS-CHAPv1, v2)
**AG5500 Specifications**

**AVAILABLE NSE MODULES**
- High Availability - Fail Over
- Hospitality Module - Property Management Interface (PMS)

**PERFORMANCE**
- *User Support*: Up to 2000 users concurrently
- *Throughput*: up to 100Mbits/s*
  
  *As defined by RFC1242, Section 3.17

**PHYSICAL**
- 1U rack space in a 19” rack
- 16.85”(L) x 10.04”(W) x 1.73”(H)
- 428mm(L) x 255mm(W) x 44mm(H)
- Weight: 6.61 lbs
- Weight: 3.00Kg

**OPERATING VOLTAGE**
- 100 – 240 VAC, 50/60Hz, Auto Sensing

**POWER CONSUMPTION**
- 64 watts
# AG5500 Specifications

## Environmental
- Operating temperature: 5°C to 40°C
- Storage temperature: 0°C to 70°C
- Operating humidity: 20 - 90% RH non-condensing
- Storage humidity: 5 - 95% RH
- Altitude: Up to 15,000ft

## Compliance
- FCC Class A, Part 15
- CE Mark
- CENELEC EN 61000-3-2:2000
- UL Std 1950
- CSA22.2 No. 950

## Interfaces
- 3 x 10/100 Mbps Ethernet (RJ-45)
- 1 x DB9 serial (for serial management and PMS interface)

## LED Indicators
- ACT/LINK and 10/100 for each Ethernet port
- Power

## Network Management
- Multi-Level Administration Controls
- Integrated VPN Client (IPSec) for secure connection to an NOC
- Access Control Lists
- Web Administration UI
- CLI via Telnet and Serial Port
- SNMPv2c
- Secure XML API
- Auto Configuration and Upgrades
- Syslog/AAA log
<table>
<thead>
<tr>
<th>AG5500 Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NETWORKING</strong></td>
</tr>
<tr>
<td>IEEE 802.3 / 3u</td>
</tr>
<tr>
<td>IEEE 802.1d</td>
</tr>
<tr>
<td>DHCP Server</td>
</tr>
<tr>
<td>DHCP Relay</td>
</tr>
<tr>
<td>RADIUS Client (MD-5, PAP, CHAP, MS-CHAPv1, v2)</td>
</tr>
</tbody>
</table>
### AG5600 Specifications

#### AVAILABLE NSE MODULES
- High Availability - Fail Over
- Hospitality Module - Property Management Interface (PMS)

#### PERFORMANCE
- **User Support:** Up to 2000 users concurrently
- **Throughput:** up to 750Mbits/s*

*As defined by RFC1242, Section 3.18

#### PHYSICAL
- 1U rack space in a 19" rack
- 17.24"(L) x 11.53"(W) x 1.73"(H)
- 438mm (L) x 292.0mm (W) x 44mm (H)
- Weight: 8.8 lbs.
- Weight: 4.00 Kg

#### OPERATING VOLTAGE
- 100 – 240 VAC, 50/60Hz, Auto Sensing

#### POWER CONSUMPTION
- 65 watts

#### ENVIRONMENTAL
- Operating temperature: 0°C to 40° C
- Storage temperature: 10°C to 70° C
- Operating humidity: 20 - 90% RH non-condensing
- Storage humidity: 5 - 95% RH
- Altitude: Up to 15,000ft
<table>
<thead>
<tr>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>UL (US and Canada)</td>
</tr>
<tr>
<td>FCC Class A</td>
</tr>
<tr>
<td>CE:</td>
</tr>
<tr>
<td>IEC 61000-4-3: 2006</td>
</tr>
<tr>
<td>IEC 61000-4-4: 2004</td>
</tr>
<tr>
<td>IEC 61000-4-5: 2005</td>
</tr>
<tr>
<td>IEC 61000-4-6: 2007</td>
</tr>
<tr>
<td>IEC 61000-4-11: 2004</td>
</tr>
<tr>
<td>Low Voltage Directive:</td>
</tr>
<tr>
<td>IEC 60950-1: 2005 (2nd Edition)</td>
</tr>
<tr>
<td>EN60950-1:2006 + A11: 2009</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 x 10/100/1000 Mbps GigE (RJ-45) LAN</td>
</tr>
<tr>
<td>1 x 10/100/1000 Mbps GigE (RJ-45) WAN</td>
</tr>
<tr>
<td>1 x DB9 serial (PMS Interface)</td>
</tr>
<tr>
<td>1 x Front Access RJ-45 serial system console</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LED Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACT/LINK and 10/100/1000 for each Ethernet port</td>
</tr>
<tr>
<td>Power</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Level Administration Controls</td>
</tr>
<tr>
<td>Integrated VPN Client (IPSec) for secure connection to an NOC</td>
</tr>
<tr>
<td>Access Control Lists</td>
</tr>
<tr>
<td>Web Administration UI</td>
</tr>
<tr>
<td>CLI via Telnet and Serial Port</td>
</tr>
<tr>
<td>SNMPv2c</td>
</tr>
<tr>
<td>Secure XML API</td>
</tr>
<tr>
<td>Auto Configuration and Upgrades</td>
</tr>
<tr>
<td>Syslog/AAA log</td>
</tr>
</tbody>
</table>
AG5600 Specifications

**NETWORKING**

- IEEE 802.3/ 3u/ 3ab
- IEEE 802.1d
- DHCP Server
- DHCP Relay
- RADIUS Client (MD-5, PAP, CHAP, MS-CHAPv1, v2)
Sample AAA Log

The following table shows a sample AAA log. This log is generated by the Access Gateway and sent to the SYSLOG server that is assigned to AAA logging.

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Access Gateway Name</th>
<th>Type of Data</th>
<th>Log Code</th>
<th>Log Message</th>
<th>Subscriber MAC Address</th>
<th>Expiration Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 31</td>
<td>18:23:10</td>
<td>nomad237.nomadix.com</td>
<td>INFO</td>
<td>AAA:4207</td>
<td>AAA_Authentication Successful</td>
<td>00:00:0E:32:2C:BC</td>
<td>2 hrs 1 min</td>
</tr>
<tr>
<td>Mar 31</td>
<td>18:23:26</td>
<td>nomad237.nomadix.com</td>
<td>INFO</td>
<td>AAA:4207</td>
<td>AAA_Authentication Successful</td>
<td>00:10:5A:61:40:FF</td>
<td>12 hrs 0 min</td>
</tr>
<tr>
<td>Mar 31</td>
<td>18:21:53</td>
<td>nomad237.nomadix.com</td>
<td>INFO</td>
<td>AAA:4106</td>
<td>AAA_lookup Added_in_memory_table_pending</td>
<td>00:00:0E:32:2C:BC</td>
<td></td>
</tr>
<tr>
<td>Mar 31</td>
<td>18:43:54</td>
<td>nomad237.nomadix.com</td>
<td>INFO</td>
<td>AAA:4208</td>
<td>AAA_Authentication Unsuccessful_Error</td>
<td>00:00:0E:32:2C:BC</td>
<td></td>
</tr>
<tr>
<td>Mar 31</td>
<td>21:34:21</td>
<td>nomad237.nomadix.com</td>
<td>INFO</td>
<td>AAA:4007</td>
<td>AAA_Interface Added_by_administrator</td>
<td>00:00:0:12:34:56</td>
<td>20 hrs 34 min</td>
</tr>
<tr>
<td>Mar 31</td>
<td>21:35:15</td>
<td>nomad237.nomadix.com</td>
<td>INFO</td>
<td>AAA:4009</td>
<td>AAA_Interface Updated_by_administrator</td>
<td>00:00:0:12:34:56</td>
<td>2 hrs 34 min</td>
</tr>
<tr>
<td>Mar 31</td>
<td>21:36:05</td>
<td>nomad237.nomadix.com</td>
<td>INFO</td>
<td>AAA:4006</td>
<td>AAA_Interface Removed_by_administrator</td>
<td>00:00:0:12:34:56</td>
<td></td>
</tr>
</tbody>
</table>

**Message Definitions (AAA Log)**

The six basic messages are defined as follows:

<table>
<thead>
<tr>
<th>Message</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA_Authentication Successful</td>
<td>Subscriber profile was successfully added to the Access Gateway authorization table after being authenticated by the credit card server.</td>
</tr>
</tbody>
</table>
Sample SYSLOG Report

Syslog reports are generated by the Access Gateway and sent to the syslog server that is assigned to general error detection and reporting.

2003-02-10 11:25:53 Local2.Info 1.2.3.4 INFO [Access Gateway v51.4.126]
DHCP: ndxDHCPInit: 0021 DHCP initialized
2003-02-10 11:25:53 Local2.Info 1.2.3.4 INFO [Access Gateway v51.4.126]
CLISRD: 0206 Setting COM1 to 9600 baud
2003-02-10 11:25:53 Local2.Info 1.2.3.4 INFO [Access Gateway v51.4.126]
CLISRD: Starting CLI on the serial port
2003-02-10 11:25:53 Local2.Info 1.2.3.4 INFO [Access Gateway v51.4.126]
INIT: Access Gateway v51.4.126 with ID 010384 Initialized
Sample History Log

A history log is generated by the Access Gateway which includes the system’s activity (Access, Reboot and Uptime).

<table>
<thead>
<tr>
<th>No.</th>
<th>Timestamp</th>
<th>Login</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC1</td>
<td>MON APR 29 17:34:45</td>
<td>admin</td>
<td>10.1.1.184</td>
</tr>
<tr>
<td></td>
<td>WMI: Getting index.htm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CC2</td>
<td>MON APR 29 17:34:42</td>
<td>admin</td>
<td>10.1.1.184</td>
</tr>
<tr>
<td></td>
<td>WMI: Getting intro.htm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CC3</td>
<td>MON APR 29 17:34:41</td>
<td>admin</td>
<td>10.1.1.184</td>
</tr>
<tr>
<td></td>
<td>WMI: Getting index.htm</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

More listings...
Keyboard Shortcuts

The following table shows the most common keyboard shortcuts.

<table>
<thead>
<tr>
<th>Action</th>
<th>Keyboard Shortcut</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cut selected data and place it on the clipboard.</td>
<td>Ctrl + X</td>
</tr>
<tr>
<td>Copy selected data to the clipboard.</td>
<td>Ctrl + C</td>
</tr>
<tr>
<td>Paste data from the clipboard into a document (at the insertion point).</td>
<td>Ctrl + V</td>
</tr>
<tr>
<td>Copy the active window to the clipboard.</td>
<td>Alt + Print Screen</td>
</tr>
<tr>
<td>Copy the entire desktop image to the clipboard.</td>
<td>Print Screen</td>
</tr>
<tr>
<td>Abort an action at any time.</td>
<td>Esc</td>
</tr>
<tr>
<td>Go back to the previous screen.</td>
<td>b</td>
</tr>
<tr>
<td>Access the Help screen.</td>
<td>?</td>
</tr>
</tbody>
</table>

HyperTerminal Settings

Use the following settings when establishing a HyperTerminal session.

<table>
<thead>
<tr>
<th>Item</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bits per second</td>
<td>9600</td>
</tr>
<tr>
<td>Data bits</td>
<td>8</td>
</tr>
<tr>
<td>Parity</td>
<td>None</td>
</tr>
<tr>
<td>Stop bits</td>
<td>1</td>
</tr>
<tr>
<td>Flow control</td>
<td>None</td>
</tr>
</tbody>
</table>
RADIUS Attributes

RADIUS (Remote Authentication Dial-In User Service) was originally created to allow remote authentication to the dial-in networks of corporations and dial-up ISPs. It is defined and standardized by the IETF (Internet Engineering Task Force) and several RADIUS server packages exist in both the public domain and for commercial sale.

RADIUS software stores a database of attributes about their valid subscriber base. For example, usernames, passwords, access privileges, account limits and subscriber attributes can all be stored in a RADIUS database. RADIUS works in conjunctions with NAS (Network Access Server) devices to determine if access to the service network should be granted, and if so, with what privileges.

All subscribers attempting to gain access to the network are validated by RADIUS.

When a subscriber attempts to access the service provider's network, the Access Gateway delivers a Web page to the subscriber asking for a login name and password. This information (password) is encrypted and sent across the network to the ISP's RADIUS server. The RADIUS server decrypts the information and compares it against its list of valid users. If the subscriber can be authenticated, the RADIUS server replies to the Access Gateway with a message instructing it to grant access to the subscriber. Optionally, the RADIUS server can instruct the NAS to perform other functions; for example, the RADIUS server can tell the Access Gateway what upstream and downstream bandwidth the subscriber should receive. If RADIUS cannot authenticate the subscriber, it will instruct the NAS to deny access to the network.
The Nomadix Access Gateway RADIUS functionality can be broken down into the following categories:

- Authentication-Request
- Authentication-Reply (Accept)
- Accounting-Request
- Selected Detailed Descriptions
- Nomadix Vendor Specific Attributes

**Authentication-Request**

- Username
- Password
- Service-Type
- NAS-Port (port number)
- NAS-Identifier
- Framed-IP Address
- NAS-IP Address
- NAS-Port-Type
- Acct-Session-ID
- Log-Off-URL
- EAP-Packet (used for 802.1x)
- Message-Authenticator (used for 802.1x)
- State (used/tested for 802.1x)
- Called-Station-ID
- Calling-Station-ID

**Authentication-Reply (Accept)**

- Reply-Message
- Reject-Message
- State (used/tested for 802.1x)
- Class
- Session-Timeout
- Idle-Timeout
- EAP-Packet (used for 802.1x)
- Message-Authenticator (used for 802.1x)
- Acct-Interim-Interval
- Nomadix VSAs:
  - Nomadix-Bw-Up
  - Nomadix-Bw-Down
  - Nomadix-URL-Redirection
  - Nomadix-IP-Upsell
  - Nomadix-MaxBytesUp
  - Nomadix-MaxBytesDown
  - Nomadix-Net-VLAN
  - Nomadix-Session-Terminate-End-Of-Day
  - Nomadix-Subnet
  - Nomadix-Expiration

**Accounting-Request**

- Username
- Acct-Status-Type (Start/Stop/Update)
- Acct-Session-ID
- Acct-Output-Octets
- Acct-Input-Octets
- Acct-Output-Packets
- Acct-Input-Packets
- Class
- Nomadix VSAs:
  - Nomadix-Subnet
  - Nomadix-URL-Redirection
  - Nomadix-IP-Upsell
• Acct-Session-Time (Stop)
• Terminate-Cause (Stop)
• NAS ID
• NAS-IP Address
• NAS-Port-Type
• NAS-Port
• Framed-IP Address
• Acct-Delay-Time
• Called-Station-ID
• Calling-Station-ID

Selected Detailed Descriptions

Acct-Session-ID
The Acct-Session-ID is created when the RADIUS authentication request is built. It is transmitted in both the Access-Request and the Accounting-Request.

Session Timeout
There is currently no default session timeout that you can set in the Access Gateway Web Management Interface (WMI). If the Radius server does not send a Session-Timeout, the Access Gateway will set the subscriber expiration time to 0, which means access forever.

Log-Off-URL
Allows for the placement of a log off URL (for example, 1.1.1.1) on an external portal page.

Idle Timeout
The WMI allows the setting of a default timeout. If the Radius server does not send an Idle-Timeout in the Radius Access-Accept, the Access Gateway will use the default one to disconnect subscribers. “0” means forever.

Timeout Detection
If a subscriber is sending traffic through the Access Gateway, the Access Gateway will immediately detect a Session-Timeout. However in the case of an Idle-Timeout or an inactive subscriber Session-Timeout, the Access Gateway detects it via a clean-up function that is currently called every 2 minutes. Thus the current precision for sending the Acct-Stop is about 2 minutes.
**Subscriber Session Duration**
Acct-Session-Time is calculated the following way (for each transmitted/retransmitted Acct-Stop):

\[ \text{Acct-Session-Time} = \text{time of last sent packet} - \text{subscriber login time}. \]

Another attribute, Acct-Delay-Time, will take into consideration the time spent in retransmissions.

**Interim Accounting Updates**
The Access Gateway parses the attribute Acct-Interim-Interval in an Access-Accept. If this attribute is present the Access Gateway tries every \([\text{Acct-Interim-Interval}]\) seconds to send a Radius Accounting Interim message for the specific subscriber. If this attribute is not present or equal to 0, no Interim message is sent.

The precision is 2 minutes. The Access Gateway will not send Interim messages more frequently than every 2 minutes.

**Called-Station-ID**
This is the Media Access Control (MAC) address of the Access Gateway.

**Calling-Station-ID**
This is the Media Access Control (MAC) address of the client's computer.

**New Attributes in Acct-Request**
The Access Gateway has to send the following attributes in an Accounting-Stop:

- Acct-Output-Packets: number of packets sent by subscriber.
- Acct-Input-Packets: number of packets received by subscriber.

Upon a reboot, these 2 attributes are saved in `currfile.dat` the same way as for Acct-Input-Octets and Acct-Input-Octets.

*If you plan to implement RADIUS, go to “Contact Information” on page 311 for Nomadix Technical Support.*

**Nomadix Vendor Specific Attributes**

**Nomadix-Bw-Up**
This attribute value (in Kbps) restricts the speed at which uploads are performed.
**Nomadix-Bw-Down**
This attribute value (in Kbps) restricts the speed at which downloads are performed.

**Nomadix-URL-Redirection**
This attribute allows the administrator to redirect the user to a page of the administrators choice each time the user logs in.

**Nomadix-IP-Upsell**
This attribute allows the user to receive a public address from a DHCP pool when the Access Gateway has the IP-Upsell feature enabled.

**Nomadix-Volume-Based-Session-Timeout**
This attribute allows you to terminate a session once a specified data volume has been reached.

**Nomadix-Session-Terminate-End-Of-Day**
This attribute allows business policies to terminate the session at midnight of every day.

**Nomadix-Subnet**
This attribute allows you to allocate a specific subnet to a user.

**Nomadix-Expiration**
This attribute defines a fixed time and date at which a session will be terminated. This feature can be used to cut off access to a certain profile for a defined user group at a specified time.
Setting Up the SSL Feature

This section describes how to set up the Access Gateway’s SSL feature.

**Prerequisites**

- You should be a business that is qualified to obtain an SSL secure server ID from different Certificate Authorities (CAs), such as VeriSign. The Certificate Authority sets this qualification criterion.
- You will need to generate your own Private Key and Certificate Signing Request (these instructions are provided below).
- You must obtain your own Signed Public Key from the Certificate Authority. The selected Certificate Authority should be commonly supported in the subscribers’ browser. We recommend that you use VeriSign (all instructions in this document are based on obtaining a key from VeriSign). Please contact Nomadix Technical Support if you want to use a different Certificate Authority.

For Nomadix technical support, go to “Contact Information” on page 311.

**Obtain a Private Key File (cakey.pem)**

To create a Private Key File, you must install OpenSSL on your Windows 9x or NT operating system on a PC with Internet access.

**Requirements for Certificate Signing Request (CSR) and Key Generation**

- Cygwin and OpenSSL application installed on Windows 9x or NT.
- 5 large random files residing on the workstation (large compressed log files recommended by VeriSign). These files are put in as file1:file2:file3:file4:file5 in the key generation command.

**Downloading Cygwin**

There are several sources for obtaining “Cygwin” to install OpenSSL. One popular source is: http://sources.redhat.com/cygwin/.

Nomadix used Cygwin version 1.3.2 for generating this section of the User Guide.
Installing Cygwin and OpenSSL on a PC

The example in this document is based on downloading the software with Netscape 4.75.

The procedure starts from the Cygwin Net Release Setup Program screen:

Click on the Next button.

The following screen appears:

Click on the Next button to display the next setup screen.
Click on the **Next** button to display the next setup screen.

Click on the **Next** button to display the next setup screen.

Click on the **Next** button to display the next setup screen.
Select a location and click on the **Next** button.

*For the purposes of this document, Nomadix used: ftp://planetmirror.com.*

In the following screens, please skip all packages except “cygwin” and “openssl,” then click on the Next when you are done.

*At the time of this writing, there are more than 70 packages to install. Please ensure that you “skip” all of them except the two packages mentioned above.*
Click on the **Next** button to start the “download” process. Wait for the download process to complete.

![Cygwin Setup](cygwin_setup_download.png)

Click on the **Next** button to start the “install” process. Wait for the install process to complete.

![Cygwin Setup](cygwin_setup_install.png)

There will be a pop-up dialog to inform you that the installation process is completed. At the pop-up dialog, click on the **OK** button.

**Private Key Generation**

Create a directory from Root and put 5 random files, `a.dat`, `b.dat`, `c.dat`, `d.dat`, and `e.dat` (see note) into the `C:\cygwin\bin\` directory (or the directory where you installed openssl.exe).

*These random files can be any file type, such as Word, Excel, etc. Change the files to .dat files (shown above). All files must follow the DOS naming format (maximum 8 characters).
Run the “command” prompt from Windows, then click on the OK button.

Go to the c:\cygwin\bin\ directory and run the following command:

```
```

The following table provides an explanation of the command elements:
Because there is a parameter buffer size limitation of the “openssl” command, the argument length should not have more than 80 characters.

If you are creating multiple keys, please output them into different directories and save them as different names. However, if you are saving them as different names, you must change the names back to “cakey.pem” when trying to FTP to the Access Gateway.

*Do not include “-des3” option to keep the private key in an unencrypted form.*
Create a Certificate Signing Request (CSR) File

Run the following command to generate the certificate signing request:

```
> openssl req -new -key cakey.pem > server.csr
```
The following table provides an explanation of the command elements:

<table>
<thead>
<tr>
<th>openssl</th>
<th>“openssl” command</th>
</tr>
</thead>
<tbody>
<tr>
<td>req</td>
<td>A parameter for creating a request</td>
</tr>
<tr>
<td>new</td>
<td>Defining a “new” request</td>
</tr>
<tr>
<td>key</td>
<td>… from private key</td>
</tr>
<tr>
<td>&gt;</td>
<td>Output to …</td>
</tr>
<tr>
<td>server.csr</td>
<td>… the output file</td>
</tr>
</tbody>
</table>

Fill in your company information. If “States” or “Province” names do not exist in your country, please repeat the “Locality Name.”

The “Common Name” is the name used in the Access Gateway->AAA->SSL Certificate Domain Name. The Common Name in the Public Key must match the SSL Certificate Domain Name in the Web Management Interface of the Access Gateway (refer to the Access Gateway setup information later in this document).

Here is the output of server.csr:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB7DCCAVUCAAQAwgaxCzAJBgNVBAgTAlVTMRMwEQYDVQQIIwDPYWxp2m9ybmlh
MRkwFwYDVQQHEBZIXNUbGFrZSBWamXwYWI5MRAwDgYDVQQKEwOb21hZG14MRQw
EgYDVQQLEwFbmdpbmVlcmluZzEcMBoGA1UEAxMTdGVzZHJpZ2h0c2Vhbi5j
bTEmMCQGCqGCSqIBIb3QJARYXdvGvjaHh1cHBvcnQAbmStYWPrerC5jb20wZgQYb
Ko2IhvaNAQEBQQAgY0AMIGJaoGfABJ/+hFc22G9GGECL2j88U0d2DqFt4g929Rn
25fog0CCFVb8VhRNe6nM+jgHA0CDMhNCmzNWPbFR2USvq0iB3bNbhJTyipUaOqi
12+DRxXrGh/oYw8BoM12F13zHVUubId5iS33wUJK/zIPBwuf0R9Ex5iBHGSnWcUt
y1vFH4b/AqMBAAGqADANBgkqhkiG9w0BQQA0BggQA2Sey18i01d40POzY6LBE
CqRldvZ12c2B6BkfyFya/cvRReAS0QFMR3mRHFv1Eb39Q9GFf22N0z62m
RASQCIYgdJbVS8uqQs/hUNP/cLy5eL3d0ndF30w75BL8cJip6nt/YtK4fnUUt
n7zDKp2Chyl9G/zYMF4NQ==
-----END CERTIFICATE REQUEST-----
```

**Create a Public Key File (server.pem)**

VeriSign Purchasing Process

The signing process varies by Certificate Authority. Generally, you will need to send a Certificate Signing Request to the Certificate Authority (CA) and the CA will create a public key base on the certificate request.
This is the procedure to get a 40-bit encryption or 128-bit Public Key from VeriSign.

With IE or Netscape, go to www.verisign.com/products/site/index.html.

Select **Buy** for Secure Site Service.
Select **Buy Now** for 40-bit SSL (Secure Server) ID or 128-bit SSL (Global Server) ID.

*Some older versions of popular browsers only support 40-bit or 56-bit encryption. Since it impossible to forecast the browsers that may be used in a visitor-based network, Nomadix recommends implementing a 40-bit Public Key.*

During the process, VeriSign will ask for your business information and verification. There are several ways to proof the existence of your business. Please follow the instruction from VeriSign carefully. In addition, there is one section about generating a CSR; however, since you have already created the CSR in step 2 with OpenSSL, you can skip the instructions.

**CSR Submission to VeriSign:**

Please select “Apache Freeware” to submit the CSR to VeriSign. The Certificate Signing Request is in the server.csr (created in the previous step). Open server.csr and copy and paste all data into the edit box.

Select the purchase method and summit the required contact information.

*For Expedited Service, you will typically be able to get the Public Key by email within two days. For Regular Service, you will typically be able to obtain the key within seven days.*

When you receive an email from VeriSign with “Secure Server ID” (Global Server ID if you create a 128-bit key) that contains the Public Key information, cut and paste the key to paste it into a new file, named server.pem.
The file, “server.pem” will look like this:

![Certificate Image]

You have now finished the process of obtaining a public key.

**Setting Up Access Gateway for SSL Secure Login**

FTP the “cakey.pem” and “server.pem” files into the Access Gateway platform's flash directory.


Drag and drop the “cakey.pem” and “server.pem” files into the directory.

**Changing Settings in the WMI**

To change settings in the Web Management Interface (WMI), go to “Defining the AAA Services {AAA}” on page 56.
Setting Up the Portal Page

System administrators can create login button(s) on the Portal Page, and can setup “http” links for regular logins, secure logins, or both. When subscribers enter the Portal Page, they can then choose either a regular login or a secure login. To setup the Portal Page, add the following:

**For Regular Logins:**


**For Secure Logins:**

Mirroring Billing Records

Multiple Access Gateway units can send copies of credit card billing records to a number of external servers that have been previously defined by system administrators. The Access Gateway assumes control of billing transmissions and saving billing records. By effectively “mirroring” the billing data, the Access Gateway can send copies of billing records to predefined “carbon copy” servers.

Additionally, if the primary and secondary servers are down, the Access Gateway can store up to 2,000 credit card transaction records. The Access Gateway regularly attempts to connect with the primary and secondary servers. When a connection is re-established (with either server), the Access Gateway sends the cached information to the server. Customers can be confident that their billing information is secure and that no transaction records are lost.

This document describes the process used by the Access Gateway for mirroring billing records, and is organized into the following sections:

- “Sending Billing Records” on page 300
- “XML Interface” on page 301
- Establishing Billing Records “Mirroring” {Bill Record Mirroring}

**Sending Billing Records**

When there is a message (billing record) in the message queue, the system “wakes up” and performs the following tasks:

1. Stores the billing record in the flash
2. Create an XML packet, based on the new billing record
3. Send the billing record to the carbon copy server(s)
4. Transmit the data currently stored in the flash, based on the specified retransmission method (round-robin: A-B-A-B, or fail-over: A-A-B-B)

The system stores the billing record in the flash so that the record will not be lost (for example, if the Access Gateway is powered down during transmission attempts.

*Billing records are sent to the carbon copy server(s) only after the records are placed in the message queue. Carbon copy servers will not receive the records again if a task for retransmitting to the primary or secondary server needs to be performed.*
**XML Interface**

**XML for the External Server**

The Access Gateway sends a string of XML commands according to specifications. HTTP headers are added to the XML packets that are built, as the billing “mirroring” information is sent to the external server in HTTP compliant XML format. Content-length has also been added to the HTTP post.

The XML string built from the billing mirror record is in the following format:

**Access Gateway to External Server:**

```xml
<USG RMTLOG_COMMAND="ADD_REC">
  <REC_NUM>max 4 characters</REC_NUM>
  <USG_ID>max 6 characters</USG_ID>
  <PROPERTY_ID>max 64 characters</PROPERTY_ID>
  <DATE>max 10 characters</DATE>
  <TIME>max 8 characters</TIME>
  <ROOM_NUM>max 20 characters</ROOM_NUM>
  <AMOUNT>max 10 characters</AMOUNT>
  <TRANS_TYPE>max 5 characters</TRANS_TYPE>
</USG>
```

**Format for each field:**

- REC_NUM: 00923 (numbers only, no alpha characters)
- Access Gateway_ID: 00020b
- PROPERTY_ID: Any regular string
- DATE: 03/30/2001 (mm/dd/yyyy)
- TIME: 23:41:38 (24 hour format)
- ROOM_NUM: Any regular string
- AMOUNT: 234.34
- TRANS_TYPE: CC
- RESULT_VALUE: OK or ERROR
- IP: Standard IP address format (123.123.123.123)
The packet after the HTTP headers added looks like this:

```xml
POST http://testing.com/brm HTTP/1.0
Content-Type: text/xml
Content-Length: 249
Host: 172.168.0.4

<USG COMMAND="ADD_REC">
  <REC_NUM>0000</REC_NUM>
  <USG_ID>012345</USG_ID>
  <PROPERTY_ID>USGI</PROPERTY_ID>
</USG>

<DATE>03/19/2004</DATE>
<TIME>10:12:56</TIME>
<ROOM_NUM>5</ROOM_NUM>
<AMOUNT>1800.00</AMOUNT>
<TRANS_TYPE>2</TRANS_TYPE>
</USG>
```

**XML to Access Gateway**

The Access Gateway accepts a single line of XML text in the specified format. The XML string is a command sent by the External Server to the Access Gateway product. In this case, the acknowledgement received from the External Server forms the command. The Access Gateway expects the acknowledgement in the following format:

**External Server to Access Gateway:**

```xml
<USG COMMAND="RMTLOG_ACK">
  <ACK_VALUE>RESULT_VALUE</ACK_VALUE>
  <IP_ADDR>Server IP</IP_ADDR>
  <ERROR_CODE>ERROR_CODE</ERROR_CODE>
</USG>
```
Example of a Positive Acknowledgement:

```xml
<USG COMMAND="RMTLOG_ACK">
  <ACK_VALUE>OK</ACK_VALUE>
  <IP_ADDR>11.22.33.44</IP_ADDR>
  <ERROR_CODE>1</ERROR_CODE>
</USG>
```

Example of a Negative Acknowledgement:

```xml
<USG COMMAND="RMTLOG_ACK">
  <ACK_VALUE>ERROR</ACK_VALUE>
  <IP_ADDR>11.22.33.44</IP_ADDR>
  <ERROR_CODE>5</ERROR_CODE>
</USG>
```

Format for each Field:
RESULT_VALUE: OK or ERROR
IP: Standard IP format (123.123.123.123)
ERROR_CODE: 1 for OK, or any other number

Please contact Nomadix Technical Support for the complete XML DTD. Refer to “Contact Information” on page 311.

For more information about Billing Records Mirroring, see also:
- “Billing Records Mirroring” on page 9
- “Establishing Billing Records “Mirroring” {Bill Record Mirroring}” on page 77
Troubleshooting

This chapter provides information to help you resolve common hardware and software problems. It also contains a list of known error messages associated with the Management Interface.

- General Hints and Tips
- Management Interface Error Messages
- Common Problems

General Hints and Tips

The Access Gateway is both a hardware device and a powerful software utility. As a hardware computing device, the Access Gateway requires careful handling. It should be positioned in a dust-free and temperature-controlled environment. Never block the unit’s ventilation holes, and do not stack with other equipment (unless correctly mounted in a rack). If you suspect the unit is overheating, check that the internal cooling fan is operating correctly. The fan should run freely and silently at all times. The power cord and the UTP patch cables must have an unrestricted path between the unit and their destinations. Ensure that the RJ45 connectors are firmly located in their receptacles. Applying these guidelines should ensure trouble-free operation.
The following table contains the error messages associated with the Management Interface (CLI and Web). All messages are listed alphabetically.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA must be enabled before adding a subscriber to the profile database.</td>
<td>You are attempting to add a subscriber profile while AAA is disabled.</td>
</tr>
<tr>
<td>Command not available “xx”</td>
<td>The system does not recognize your command (“xx” denotes your input).</td>
</tr>
<tr>
<td>Current settings were not archived.</td>
<td>This message is displayed if you answer “no” when prompted to overwrite the configuration archive file with new settings.</td>
</tr>
<tr>
<td>Current settings were not changed.</td>
<td>This is either a response to your decision not to change settings, or the message is generated by the system when it fails to locate the data it needs.</td>
</tr>
<tr>
<td>Error loading factory settings.</td>
<td>The system cannot find the default configuration file when attempting to restore the factory settings.</td>
</tr>
<tr>
<td>Error occurred, ARP entry not added.</td>
<td>The IP or MAC address is invalid. Ensure that you input the correct format for these fields.</td>
</tr>
<tr>
<td>NFS client support not included.</td>
<td>This message is displayed when the system reboots and NFS clients are not supported.</td>
</tr>
<tr>
<td>No matching MAC address found in profile database.</td>
<td>The system could not match the MAC address you defined while attempting to remove a subscriber profile.</td>
</tr>
<tr>
<td>[not defined]</td>
<td>This is the factory default for some system parameters.</td>
</tr>
<tr>
<td>The system must be reset to function properly.</td>
<td>You have made changes to the system’s configuration that requires you to reboot before your changes become effective.</td>
</tr>
<tr>
<td>The system must be rebooted to function properly!</td>
<td></td>
</tr>
<tr>
<td>Error Message</td>
<td>Cause</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Warning: before using this command you must FTP a valid boot image to the flash.</td>
<td>When upgrading the software, the system needs the new boot image file. You must FTP the file from NOMADIX™ to your local hard drive.</td>
</tr>
<tr>
<td>Warning: no DHCP services are available to subscribers.</td>
<td>This message is displayed because you have disabled both the external DHCP relay and the system’s DHCP service. To make DHCP available to subscribers, at least one of these functions must be enabled.</td>
</tr>
<tr>
<td>“x” is ambiguous.</td>
<td>The system has more than one option it can display. You must provide additional characters to narrow the system’s choices down to just one.</td>
</tr>
<tr>
<td>“xxx” is invalid, enter ...</td>
<td>Your input is not recognized by the system.</td>
</tr>
</tbody>
</table>
## Common Problems

If you are having problems, you may find the answers here.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>When using the internal AAA login Web server, you cannot communicate with Authorize.Net.</td>
<td>The internal AAA login server communicates with Authorize.Net on a specified port which is not enabled within the company’s firewall.</td>
<td>Enable communications with Authorize.Net on port 1111.</td>
</tr>
<tr>
<td>When a subscriber who is enabled with DHCP logs onto the system, they are not assigned an IP address.</td>
<td>The DHCP relay is enabled with an incorrect IP address for the external DHCP server.</td>
<td>Check the IP address for the external DHCP server. If necessary, test the communication with the “ping” command.</td>
</tr>
<tr>
<td></td>
<td>The DHCP relay is enabled with the correct IP address for the external DHCP server, but the DHCP server is misconfigured.</td>
<td>Check the external DHCP server settings (for example, is it configured to a routable class of IP addresses? Are there enough IP address specified? If you specified a subnet, is it correct?). If you suspect the subnet, try using 255.255.255.0.</td>
</tr>
<tr>
<td></td>
<td>The DHCP relay is disabled and the DHCP service settings in the Access Gateway are misconfigured.</td>
<td>Check the internal DHCP service settings.</td>
</tr>
<tr>
<td>Subscribers are unable to route to a domain name, but they can route to an IP address.</td>
<td>The DNS server settings are misconfigured.</td>
<td>Check the DNS settings (host, domain, and the primary, secondary, and tertiary DNS).</td>
</tr>
<tr>
<td></td>
<td>The DNS server is down.</td>
<td>Check with the service provider. Is the DNS server down?</td>
</tr>
</tbody>
</table>
When a subscriber logs in for the first time, their browser is not redirected to the specified home page.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home page redirection is not enabled in the Access Gateway.</td>
<td>Re-enter the correct URL.</td>
<td></td>
</tr>
<tr>
<td>The home page URL was entered into the Access Gateway incorrectly.</td>
<td>Re-enter the correct URL.</td>
<td></td>
</tr>
<tr>
<td>The server that hosts the home page is down, or the service provider (if different from the host) is not able to route to your page.</td>
<td>Check that the server is operational and that the home page can be accessed through your service provider (if different).</td>
<td></td>
</tr>
<tr>
<td>DNS is misconfigured in the Access Gateway.</td>
<td>Check the DNS settings (host, domain, and the primary, secondary, and tertiary DNS).</td>
<td></td>
</tr>
</tbody>
</table>
This page intentionally left blank.
Appendix A: Technical Support

We have tried to ensure that you get the most up-to-date information available about the Access Gateway, and we hope this User Guide has met all your operational and performance needs. However, we understand that occasionally you may run into problems that require additional technical support.

“Troubleshooting” on page 305 provides some basic troubleshooting information and procedures that will help you to diagnose and solve your problem (if the problem is related to the Access Gateway). Additionally, you should check with your network documentation to verify that the network components are functioning correctly.

If you cannot resolve the problem with your documentation resources, try connecting to our corporate Web site. We may have new information posted here that addresses your issues.

If you are still having problems, our friendly and experienced technical support team is always ready to assist you.

When contacting technical support, please have your Access Gateway’s serial number available. The serial number is located on the bottom panel of your Access Gateway.

Contact Information

You can contact us by Email, fax, telephone, or regular mail.

Telephone
++1.818.575.2590

E-mail
support@nomadix.com

Fax
++1.818.597.1502

Address
Nomadix, Inc.
30851 Agoura Rd, Suite 102
Agoura Hills, CA 91301
USA
Attn: Technical Support
This page intentionally left blank.
**Glossary of Terms**

**802.11x**
Refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station, or between two wireless clients. The IEEE accepted the specification in 1997. There are several specifications in the 802.11 family:

**802.11**
Applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS).

**802.11a**
An extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band. 802.11a uses an Orthogonal Frequency Division Multiplexing (OFDM) encoding scheme rather than FHSS or DSSS.

**802.11b**
(also referred to as 802.11 High Rate or Wi-Fi™) An extension to 802.11 that applies to wireless LANs and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.

**802.11g**
Applies to wireless LANs and provides 20+ Mbps in the 2.4 GHz band.

**802.1Q**
An IEEE standard for providing a virtual LAN capability within a campus network. 802.1Q establishes a standard format for frame tagging (Layer 2 VLAN markings), enabling the creation of VLANs that use equipment from multiple vendors.

**10/100 Ethernet**
See Ethernet.

**AAA**
(Authentication, Authorization, and Accounting) A combination of commands used by Nomadix Gateways to authenticate, authorize, and subsequently bill subscribers for their use of the customer’s network. When a subscriber logs into the system, their unique MAC address is placed into an authorization table. The system then authenticates the subscriber’s MAC address and billing information before allowing them to access the Internet and make online purchases. See also, MAC Address.

**Access Concentrator**
A type of multiplexor that combines multiple channels onto a single transmission medium in such a way that all the individual channels can be simultaneously active. For example, ISPs use concentrators to combine their dial-up modem connections onto faster T-1 lines that connect to the Internet. Concentrators are also used in Local Area Networks (LANs) to combine transmissions from a cluster of nodes. In this case, the concentrator is often called a hub.

**Access Router**
A router at a customer site, which connects to the network service provider. Also known as a Customer Premises Equipment (CPE) router. See also, Router.
ACK
(ACKnowledgment) If all the transmitted data is present and correct, the receiving device sends an ACK signal, which acts as a request for the next data packet.

Adaptive Configuration Technology
A Nomadix, Inc. patented technology that enables Dynamic Address Translation. See also, DAT.

ad-hoc mode
An 802.11x networking framework in which devices or stations communicate directly with each other, without the use of an Access Point (AP). Ad-hoc mode is also referred to as peer-to-peer mode, or an Independent Basic Service Set (IBSS). Ad-hoc mode is useful for establishing a network where wireless infrastructure does not exist or where services are not required.

ADSL
(Asynchronous Digital Subscriber Line) A method for moving data at high speed over regular phone lines.

AP
(Access Point) A hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN. APs are important for providing heightened wireless security and for extending the physical range of service a wireless user has access to.

ARP
(Address Resolution Protocol) Used to dynamically bind a high level IP address to a low level physical hardware address. ARP is limited to a single physical network that supports hardware broadcasting.

ATM
(Asynchronous Transfer Mode) A network technology based on transferring data in “cells” or packets of a fixed size (53 bytes each). The cell used with ATM is relatively small compared to units used with older technologies. The small, constant cell size allows ATM equipment to transmit video, audio, and computer data over the same network, and assures that no single type of data monopolizes the line. ATM can offer multi-gigabit bandwidth. See also, Bandwidth and Packet.

Bandwidth
The maximum speed at which data can be transmitted between computers across a network, usually measured in bits per second (bps). If you think of the communication path as a water pipe, the bandwidth represents the width of the pipe which consequently determines how many gallons of water can flow through it at any given time. See also, Broadband.

Beacon Interval
The frequency interval of the beacon, which is a packet broadcast by a router to synchronize a wireless network.

Broadband
A high speed data transmission medium capable of supporting a wide range of varying frequencies. Broadband can carry multiple signals at fast rates of speed by dividing the total capacity of the medium into multiple, independent bandwidth channels, where each channel operates only on a specific range of frequencies. See also, Bandwidth.

BSS
(Basic Service Set) See infrastructure mode.

Carrier frequency
A frequency in a communications channel modulated to carry analog or digital signal information. For example, an FM radio transmitter modulates the frequency of a carrier signal and the receiver processes the carrier signal to extract the analog information. An AM radio transmitter modulates the amplitude of a carrier signal.
**CoS**
(Class of Service) A category based on the type of user, type of application, or some other criteria that QoS systems can use to provide differentiated classes of service. The characteristics of the CoS may be appropriate for high throughput traffic, for traffic with a requirement for low latency, or simply for best effort. The QoS experienced by a particular flow of traffic will be dependent on the number and type of other traffic flows admitted to its class. See also, QoS.

**Daemon**
A program that runs continuously in the background, or is activated by a particular event (for example, an error may trigger Syslog). The word daemon is Greek for “spirit” or “soul.” See also, SYSLOG.

**DAT**
(Dynamic Address Translation) Nomadix Gateways provide “plug-and-play” access to subscribers who are misconfigured with static (permanent) IP addresses, or subscribers that do not have DHCP functionality on their computers. DAT is a Nomadix, Inc. patented technology that allows all users to obtain network access, regardless of their computer’s network settings. See also, DHCP.

**DHCP**
(Dynamic Host Configuration Protocol) A standard method for assigning IP addresses automatically to devices connected on a TCP/IP network. When a new device connects to the network, the DHCP server assigns an IP address from a list of its available addresses. The device retains this IP address for the duration of the session. When the device disconnects from the network, the IP address becomes available for reassignment to another device. See also, Dynamic IP Address, IP Address, Static IP Address, and TCP/IP.

**DNS**
(Domain Name System) A system that maps meaningful domain names with complex numeric IP addresses. See also, Domain Name and IP Address.

**Domain Name**
A unique and meaningful name representing each addressable computing device on a dynamic network (for example, the Internet). Some devices have more than one domain name. When a user types a domain name, requesting a connection to the device, DNS converts the domain name into a numeric IP address. The location of the device on the network is known by its IP address. WWW.YAHOO.COM is an example of a commercial domain name on the World Wide Web. See also, DNS, Internet, and IP Address.

**Driverless Print Servers**
Servers that can bill subscribers’ rooms for printing their documents without them having to install printers. See also, Print Billing Command.

**DSSS**
(Direct Sequence Spread Spectrum) One of two types of spread spectrum radio—the other being Frequency Hopping Spread Spectrum (FHSS). DSSS is a transmission technology used in WLAN transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or “chipping” code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission.

**DTIM**
(Delivery Traffic Indication Message) A message included in data packets that can increase wireless efficiency.
Dynamic IP Address
A temporary IP address that is assigned by the DHCP server to a device. Devices retain dynamic IP addresses only for the duration of their networking session. When a device disconnects from the network, the IP address is recaptured by the DHCP server and becomes available for reassignment to another device. See also, DHCP, IP Address, IP Address Translation, Static IP Address, and Translation.

EAP
(Extensible Authentication Protocol) An extension to PPP. EAP is a general protocol for authentication that also supports multiple authentication methods (for example, public key authentication and smart cards). IEEE 802.1x specifies how EAP should be encapsulated in LAN frames. In wireless communications using EAP, a user requests connection to a WLAN through an AP, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the AP for proof of identity, which the AP gets from the user and then sends back to the server to complete the authentication.

ECommerce
A business venture between a supplier and its customers using online services (for example, the Internet). Both parties use online services to conduct business transactions. Transactions may include generating orders, invoices, and payments, and submitting inquiries. Also known as Enterprise.

ESS
(Extended Service Set) See infrastructure mode.

Ethernet
A Local Area Network (LAN) protocol developed by Xerox Corporation in cooperation with DEC and Intel in 1976. Ethernet uses a bus or star topology and supports data transfer rates of 10 Mbps. The Ethernet specification served as the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers. Ethernet is one of the most widely implemented LAN standards. A newer version of Ethernet, called 100Base-T (or Fast Ethernet), supports data transfer rates of 100 Mbps. The latest version, Gigabit Ethernet, supports data rates of 1 Gigabit (1,000 Mbps) per second. See also, Mbps.

Fast Ethernet
See Ethernet.

FCC
(Federal Communications Commission) US wireless regulatory authority. The FCC was established by the Communications Act of 1934 and is charged with regulating Interstate and International communications by radio, television, wire, satellite and cable.

FDM
(Frequency Division Multiplexing) A multiplexing technique that uses different frequencies to combine multiple streams of data for transmission over a communications medium. FDM assigns a discrete Carrier frequency to each data stream and then combines many modulated carrier frequencies for transmission. For example, television transmitters use FDM to broadcast several channels at once.

FHSS
(Frequency Hopping Spread Spectrum) One of two types of spread spectrum radio—the other being Direct-Sequence Spread Spectrum (DSSS). FHSS is a transmission technology used in WLAN transmissions where the data signal is modulated with a narrowband carrier signal that "hops" in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. The signal energy is spread in time domain rather than chopping each bit into small pieces in the frequency domain. This technique reduces interference because a signal from a narrowband system will only affect the spread spectrum signal if both are transmitting at the same frequency at the
same time. If synchronized properly, a single logical channel is maintained. The transmission frequencies are
determined by a “spreading” or “hopping” code. The receiver must be set to the same hopping code and must listen to
the incoming signal at the right time and correct frequency in order to properly receive the signal. Current FCC
regulations require manufacturers to use 75 or more frequencies per transmission channel with a maximum dwell time
(the time spent at a particular frequency during any single hop) of 400 ms.

**Flash Memory**
A special type of EEPROM (Electrically Erasable Programmable Read Only Memory) that can be erased and
reprogrammed in blocks instead of one byte at a time. Many modern PCs have their BIOS stored on a flash memory
chip so that it can easily be updated. Such a BIOS is sometimes called a flash BIOS. Flash memory is also popular in
modems because it enables the modem manufacturer to support new protocols as they become standardized.

**Forwarding Rate**
The maximum rate at which 64K packets can be delivered to their destination. See also, Packet, Packet Switching
Network, pps, and Throughput.

**Fragment Length (Fragmentation)**
Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of
the packet. The fragment length value should remain at its default setting unless you experience a high packet error
rate. Setting the fragment length too low may result in poor performance.

**FTP**
(File Transfer Protocol) A standard protocol used for copying and moving files quickly, efficiently, and securely across
public and private networks. An FTP site is one where files are available for downloading and uploading. FTP sites
usually require a secure login (name and password) to gain access.

**Gateway**
Any device that provides a seamless connection between otherwise incompatible systems.

**Gopher**
A computer program, and an accompanying data transfer protocol, for reading information that has been made
available to the public on the Internet. Gopher is gradually being superseded by HTML.

**Home Page**
Usually the first page users see when they visit a Web site (if they address the home page’s URL). A well constructed
Web site will normally consist of a home page that provides a clear and concise overview of the entire Web site,
together with the tools for accessing other pages and topics quickly and efficiently. In this case, the home page is the
“portal” to the Web site. See also, Portal and URL.

**Host**
Any computer that provides services to other computers that are linked to it by a network. Generally, the host is the
more remote of the computers. For example, if a user in California accesses a computer in New York, the computer in
New York is considered the host.

**HPR**
(Home Page Redirection) Nomadix Gateways enable solution providers to redirect subscribers to a “portal” home page
of their choice. This allows the solution provider to generate online advertising revenues and increase business
exposure. See also, Home Page.

**HTML**
(HyperText Markup Language) The programming language used to create hypertext documents for use on the Internet.
See also, HTTP, Hypertext, and Internet.
HTTP
(HyperText Transfer Protocol) The standard method used for publishing hypertext documents in HTML format on the Internet. See also, HTML, Hypertext and Internet.

Hypertext
Electronic documents that are structured to enable readers to go directly to the source of the information they need by following directional links (unlike books which are generally read sequentially). Help files and CD-ROM encyclopedias are examples of hypertext documents.

ICMP
(Internet Control Message Protocol) A standard Internet protocol that delivers error and control messages from hosts to message requestors. An ICMP echo test can determine whether a target destination is reachable. An ICMP echo test is also called a ping. See also, Ping.

IEEE
(Institute of Electrical and Electronics Engineers) Founded in 1884, the IEEE is an organization composed of engineers, scientists, and students. The IEEE is best known for developing standards for the computer and electronics industry. In particular, the IEEE 802 standards for Local Area Networks are widely followed.

iNAT™
(Intelligent Network Address Translation) Nomadix’ iNAT™ feature creates an intelligent mapping of IP addresses and their associated VPN tunnels allowing multiple tunnels to be established to the same VPN server—creating a seamless connection for all the users at the public-access location.

infrastructure mode
An 802.11x networking framework in which devices communicate with each other by first going through an Access Point (AP). In infrastructure mode, wireless devices can communicate with each other or can communicate with a wired network. When one AP is connected to a wired network and a set of wireless stations it is referred to as a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs that form a single subnetwork. Most corporate wireless LANs operate in infrastructure mode because they require access to the wired LAN in order to use services such as file servers or printers. See also, ad-hoc mode.

Internet
Originally developed by the U.S. Defense Department, the Internet is now a global collection of networks that transfer information between each other using the Internet Protocol (IP). Additionally, the Internet carries the hypertext system commonly known as the World Wide Web. See also, Hypertext and Internet Protocol.

Internet Protocol
The global standard used to regulate data transmissions between computers and the Internet. Data is broken up into packets which are then sent over the network. By using IP addressing, Internet Protocol ensures that the data reaches its destination, even though different packets may pass through different networks to get to the same location. See also, Internet and IP Address.

Internet Service Provider
The agency that provides you with access to the Internet. Your Internet Service Provider (ISP) may be a large commercial organization (for example, America Online) or, if you access the Internet via your employer, then your employer is your Internet Service Provider. See also, Internet.

Intranet
A network confined to a single organization (but not necessarily a single site). Usually thought of as a corporate mini Internet.

IP
See Internet Protocol.
IP Address
The numeric address of a device, in the format used on the Internet. The actual numeric value takes the form of a 32-bit binary number broken up into four 8-bit groups, with each group separated by a period (for example, 198.43.7.85). To make it easier for the user, the IP address is mapped to a meaningful domain name. IP addresses can be static (permanent) or dynamic (assigned each time you connect). See also, Domain Name, Dynamic IP Address, Internet Protocol, and Static IP Address.

IP Address Translation
Nomadix Gateways use adaptive configuration technology which can accommodate all network configurations, including dynamic and static IP address assignments. This enables it to solve IP addressing problems in environments where the service provider does not have control over the subscriber’s network settings. Whenever a subscriber logs on, your Nomadix Gateway automatically translates their computer’s network settings to provide them with seamless access to the broadband network. Subscribers no longer need to alter their computer’s settings. See also, Dynamic IP Address, IP Address, and Static IP Address.

ISDN
(Integrated Services Digital Network) An international communications standard for sending voice, video, and data over digital telephone lines or normal telephone wires. ISDN supports data transfer rates of 64 Kbps (64,000 bits per second).

ISP
See Internet Service Provider.

LAWN
(Local Area Wireless Network) A type of Local Area Network that uses high-frequency radio waves rather than wires to communicate between nodes. Also referred to as WLAN. See also, Node.

LDAP
(Lightweight Directory Access Protocol) Directories containing information such as names, phone numbers, and addresses are often stored on a variety of incompatible systems. LDAP provides a simple protocol that allows you to access and search these disparate directories over the Internet. LDAP is commonly used for online billing applications.

MAC Address
(Media Access Control) The hardware address that uniquely identifies each node of a network. In IEEE 802 networks, the Data Link Control (DLC) layer of the OSI Reference Model is divided into two sub layers – the Logical Link Control (LLC) layer and the Media Access Control (MAC) layer. The MAC layer interfaces directly with the network media. Consequently, each type of network media requires a different MAC layer. On networks that do not conform to the IEEE 802 standards but do conform to the OSI Reference Model, the node address is called the Data Link Control (DLC) address.

Mbps
(Megabits per second) A standard measure for data transmission speeds (for example, the rate at which information travels over the Internet). 1 Mbps denotes one million bits per second. Several factors can influence how quickly data travels, including modem speed, bandwidth capacity, and Internet traffic levels at the time of transmission. Not to be confused with MegaBytes per second (MBps). See also, Throughput.

MIB
(Management Information Base) A set of parameters an SNMP management station can query or establish in the SNMP agent of a network device (for example, a router). Standard minimal MIBs have been defined, and vendors often have their own private enterprise MIBs. In theory, any SNMP manager can talk to any SNMP agent with a properly defined MIB. See also, SNMP.
**Misconfigured User**
A Nomadix, Inc. term used to describe users who have IP address configurations that are different from the current network. For example, if the current network is 123.45.67.89 but the user’s IP address is 10.10.10.15, then this user is considered to be “misconfigured.”

**NAT**
(Network Address Translation) An Internet standard that enables a Local Area Network (LAN) to use one set of IP addresses for internal traffic and a second set of IP addresses for external traffic. A NAT box located where the LAN meets the Internet performs all the necessary IP address translations. NAT provides a type of firewall by hiding its internal IP addresses. Additionally, NAT enables companies to use more internal IP addresses (because the addresses are only used internally and there’s no possibility of conflicting with IP addresses used by other companies). NAT also allows companies to combine multiple ISDN connections into a single Internet connection. See also, [ISDN](#).

**Node**
An addressable point on a network. A node can connect a computer system, a terminal, or various peripheral devices to the network. Each node on a network has a distinct name. On the Internet, a node is a host computer with a unique domain name and IP address. See also, [Domain Name](#) and [IP Address](#).

**NTP**
(Network Time Protocol) An Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization (to the millisecond) of computer clock times in a network of computers. Based on [UTC](#), NTP synchronizes client workstation clocks to the U.S. Naval Observatory master clocks. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client’s clock.

**OFDM**
(Orthogonal Frequency Division Multiplexing) An FDM modulation technique for transmitting large amounts of digital data over a radio wave. OFDM works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. OFDM reduces the amount of crosstalk in signal transmissions. 802.11a WLAN technology uses OFDM.

**OSPF**
(Open Shortest Path First) This routing protocol was developed for IP networks based on the shortest path first or link-state algorithm. Routers use link-state algorithms to send routing information to all nodes on a network by calculating the shortest path to each node based on a topography of the Internet constructed by each node. Routers send that portion of the routing table (keeping track of routes to particular network destinations) that describes the state of its own links, and it also sends the complete routing structure (topography). The advantage of shortest path first algorithms is that they result in smaller more frequent updates everywhere. They converge quickly, thus preventing such problems as routing loops and count-to-infinity (when routers continuously increment the hop count to a particular network). This makes for a stable network. OSPF (version 2) is defined in RFC 1583 and is rapidly replacing RIP on the Internet as the preferred routing protocol. See also, [RFC](#) and [Router](#).

**Packet**
How data is distributed over the Internet. A packet contains the source and destination addresses, as well as the data. An ethernet packet is normally 1,518 bytes. In IP networks, packets are often called datagrams. See also, [Forwarding Rate](#), [Packet Switching Network](#), [pps](#), and [Throughput](#).
Packet Switching Network
Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at its destination, they are recompiled into the original message. Most modern Wide Area Network (WAN) protocols, including TCP/IP, X.25, and Frame Relay, are based on packet-switching technologies. By contrast, normal telephone services use a circuit-switching technology in which a dedicated line is allocated for transmission between two parties. Circuit-switching is ideal for fast data transmissions where the data must arrive in the same order in which it is sent. This is the case with most real-time data, such as live audio and video. Packet switching is more efficient and robust for data that can withstand some delays in transmission, such as e-mail messages and Web pages. See also, Forwarding Rate, Packet, pps, and Throughput.

PDF
(Portable Document Format) A type of file format developed by Adobe Systems© that displays documents identically on any computer system. PDF files retain their original formatted design, unlike HTML documents which adjust the format depending on the users viewing medium (for example, monitor size).

Ping
(Packet INternet Groper) A program that transmits a signal to a host and expects a response within a predetermined time. This is useful when troubleshooting network transmission problems. See also, ICMP.

Portal
A portal is a Web site. The portal consists of a collection of links to the most popular Web services on the Internet. Generally speaking, a portal is a door to the Internet. See also, Internet.

PPP
(Point-to-Point Protocol) PPP has superseded SLIP as the standard protocol for serial data communications over the Internet. See also, SLIP.

pps
(packets per second) The rate at which packets are delivered to their destination. See also, Forwarding Rate, Packet, and Packet Switching Network.

PPTP
(Point-to-Point Tunneling Protocol) Developed jointly by Microsoft Corporation, U.S. Robotics, and several remote access vendor companies, known collectively as the PPTP Forum, PPTP is a new technology used for creating Virtual Private Networks (VPNs). Because the Internet is essentially an open network, PPTP is used to ensure that messages transmitted from one VPN node to another are secure. PPTP allows users to dial in to their corporate networks via the Internet. See also, Internet, Tunneling, and VPN.

Preamble
In wireless networks, part of the wireless signal that synchronizes network traffic.

Print Billing Command
Authentication, Authorization and Accounting configuration that allows the NSE to support Driverless Print servers that can bill subscribers’ rooms for printing their documents without them having to install printers.

Profile
An electronic file that defines how subscribers normally interact with the service provider’s network.
Protocol
A standard process consisting of a set of rules and conditions that regulates data transmissions between computing devices. Some examples of protocols include HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol), TCP/IP (Transmission Control Protocol/Internet Protocol), and POP (Post Office Protocol). All these protocols are responsible for regulating the transmission of their specific data file types.

QoS
(Quality of Service) A collective measure of the level of service delivered to the customer. QoS can be characterized by several basic performance criteria, including availability (low downtime), error performance, response time and throughput, lost calls or transmissions due to network congestion, connection set-up time, and the speed of fault detection and correction. Service providers may guarantee a particular level of QoS (defined by a service level agreement) to their subscribers. QoS-enabled hardware and software solutions sort and classify IP packet requests into different traffic classes and allocate the proper resources to direct traffic based on various criteria, including application type, user or application ID, source or destination IP address, time of day, and other user-specified variables. See also, CoS and ToS.

RADIUS
(Remote Authentication Dial-In User Service) An authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server which checks that the information is correct and then authorizes access to the ISP system.

RFC
(Request for Comments) A series of notes about the Internet, started in 1969 (when the Internet was the ARPANET). An RFC note can be submitted by anyone. Each RFC is designated by an RFC number. Once published, an RFC never changes. Any modifications to an original RFC are assigned a new RFC number.

Roaming
In wireless networking, roaming refers to the ability to move from one AP coverage area to another without interruption in service or loss in connectivity.

Round Robin Queuing
An algorithm that services each queue in a predefined sequence. For example, it might empty 1,500 bytes apiece from queue 1 (high priority), queue 2 (medium priority), and queue 3 (low priority), servicing each in turn.

Router
A hardware device that connects two or more networks and routes the incoming data packets to the appropriate network.

RTS (Length)
(Request to Send) A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data. The RTS Length value should remain at its default setting unless you encounter inconsistent data flow. Only minor modifications to this value are recommended.

SLIP
(Serial Line Internet Protocol) SLIP is a standard protocol for connecting to the Internet with a modem over a phone line. It has trouble with noisy dial-up lines and other error-prone connections, so look to higher-level protocols like PPP for error correction.

SMTP
(Simple Mail Transfer Protocol) A standard protocol that regulates how e-mail is distributed over the Internet. See also, Protocol.
SNMP
(Simple Network Management Protocol) A standard protocol that regulates network management over the Internet. SNMP uses TCP/IP to communicate with a management platform, and offers a standard set of commands that make multi-vendor operability possible. SNMP uses a standard set of definitions, known as a MIB (Management Information Base), which can be supplemented with enterprise-specific extensions. See also, TCP/IP and MIB.

Socket
A communication path between two computer programs, not necessarily running on the same machine. Sockets are managed by a “socket device driver” that establishes network connections, as needed. Programs that communicate through sockets need not know anything about how the network functions.

Solution Provider
Vendors are considered to be solution providers when they provide products and/or services that meet their customer’s specific needs. Normally, a solution provider is offering a solution that isn’t readily available on the open market. For example, NOMADIX™ is a solution provider to its customers (broadband network service providers), and those customers are solution providers to their end users (network subscribers).

SSID
(Service Set Identifier) A 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be “sniffed” in plain text from a packet it does not supply any security to the network. An SSID is also referred to as a “network name” because essentially it is a name that identifies a wireless network.

SSL
(Secure Sockets Layer) A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that is transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. See also, Protocol.

Static IP Address
An IP address that is assigned to a computing device permanently (or until the user changes it manually), unlike a dynamic IP address which is assigned to a device temporarily by the DHCP server. See also, DHCP, IP Address and Dynamic IP Address.

STP
(Spanning Tree Protocol) A link management protocol that is part of the IEEE 802.1 standard for media access control bridges. Using the spanning tree algorithm, STP provides path redundancy while preventing undesirable loops in a network that are created by multiple active paths between stations. Loops occur when there are alternate routes between hosts. To establish path redundancy, STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby (or blocked) state. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and reestablishes the link by activating the standby path. Without spanning tree in place, it is possible that both connections may be simultaneously “live,” which could result in an endless loop of traffic on the LAN.

Subnet
A portion of a network, which may be a physically independent network segment, which shares a network address with other portions of the network and is distinguished by a unique subnet address. In general, a subnet is to a network what a network is to the Internet.
Subnet Address
The subnet portion of an IP address that is dedicated to the subnet. In a subnetted network, the host portion of an IP address is split into a subnet portion and a host portion using an address (subnet) mask. See also, IP Address and Subnet.

Subnet Mask
See Subnet Address.

Subscriber
Any person or organization that pays a period fee for services.

SYSLOG
(SYstem LOGging) Syslog is the standard event logging subsystem for Unix and consists of a server daemon, a client function library, and a client command line utility. You can log to files, terminal devices, logged on users, or even forward to other syslog systems. See also, Daemon.

TCP
(Transmission Control Protocol) Manages data into small packets and ensures that the data is transmitted correctly over a network. If an error is detected, the data is transmitted again in its original form. See also, TCP/IP.

TCP/IP
(Transmission Control Protocol/Internet Protocol). A suite of protocols that regulates data communications for the Internet. See also, Internet Protocol, Protocol, and TCP.

Telnet
A software program and command utility used to connect between remote locations and services. Telnet connects you to the login prompt of another host (that you have access rights to). See also, Host.

Throughput
The net data transfer rate between an information source and its destination, using the maximum packet size without loss. Throughput is expressed as Megabits per second (Mbps), defined by RFC1242, Section 3.17. See also, Forwarding Rate, Mbps, Packet, Packet Switching Network, pps, and RFC.

TLS
(Transport Layer Security) A protocol that guarantees privacy and data integrity between client/server applications communicating over the Internet. The TLS protocol is made up of two layers:

TLS Record Protocol
Layered on top of a reliable transport protocol, such as TCP, it ensures that the connection is private by using symmetric data encryption and ensures that the connection is reliable. The TLS Record Protocol also is used for encapsulation of higher-level protocols, such as the TLS Handshake Protocol.

TLS Handshake Protocol
Allows authentication between the server and client and the negotiation of an encryption algorithm and cryptographic keys before the application protocol transmits or receives any data.

TLS is application protocol-independent. Higher-level protocols can layer on top of the TLS protocol transparently. Based on Netscape’s SSL 3.0, TLS supercedes and is an extension of SSL. TLS and SSL are not interoperable. See also, Protocol and SSL.

Translation
See IP Address Translation.
**Tunneling**
A technology that enables one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network. For example, Microsoft's PPTP technology enables organizations to use the Internet to transmit data across a Virtual Private Network (VPN). It does this by embedding its own network protocol within the TCP/IP packets carried by the Internet. See also, TCP/IP and VPN.

**ToS**
(Type of Service) A field within an IP header which can be used by the device originating the packet, or by an intermediate networking device, to signal a request for a specific QoS level. ToS uses three bits to tell a router how to prioritize a packet and one bit apiece to signal requirements for delay, throughput, and reliability. See also, Packet, QoS, Router, and Throughput.

**URL**
(Uniform Resource Locator) The standard method used for identifying the location of information available to the Internet. This is effectively the “address” of a document or file, expressed in the form: protocol://domain.filename/path.type (for example, http://www.myfile.com/nextpage.html).

**UTC**
(Coordinated Universal Time) A time scale that couples Greenwich Mean Time (GMT), which is based solely on the Earth's inconsistent rotation rate, with highly accurate atomic time. When atomic time and Earth time approach a one second difference, a leap second is calculated into UTC. UTC was devised on January 1, 1972 and is coordinated in Paris by the International Bureau of Weights and Measures. UTC, like GMT, is set at 0 degrees longitude on the prime meridian.

**VoIP**
(Voice over IP) An emerging technology for transporting integrated digital voice, video, and data over IP networks. A major advantage of VoIP and Internet telephony is that it avoids the tolls charged by ordinary telephone services. See also, Internet and IP.

**VPN**
(Virtual Private Network) A network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

**VxWorks®**
A real-time operating system, manufactured and sold by Wind River Systems of California, USA. VxWorks program development requires a host machine running Unix or Windows.

**W3C**
(World Wide Web Consortium) An international consortium of companies involved with the Internet and the Web. The organization's purpose is to develop open standards so that the Web evolves in a single direction rather than being splintered among competing factions. The W3C is the chief standards body for HTTP and HTML. See also, HTML and HTTP.

**WAN**
(Wide Area Network) Take two local area networks, hook them together, and you've got a WAN. Wide area networks can be made up of interconnected smaller networks spread throughout a building, a state, a country, or the entire globe.
WEP
(Wired Equivalent Privacy) A security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. LANs are inherently more secure than WLANs because LANs are somewhat protected by the physicalities of their structure, having some or all of the network inside a building that can be protected from unauthorized access. WLANs, which are over radio waves, do not have the same physical structure and therefore are more vulnerable to tampering. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.

Wi-Fi™
(Wireless Fidelity) Used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance. Any products tested and approved as "Wi-Fi Certified" (a registered trademark) by the Wi-Fi Alliance are certified as interoperable with each other, even if they are from different manufacturers. A user with a "Wi-Fi Certified" product can use any brand of access point with any other brand of client hardware that also is certified. Typically, however, any Wi-Fi product using the same radio frequency (for example, 2.4GHz for 802.11b or 802.11g, or 5GHz for 802.11a) will work with any other product, even if that product is not "Wi-Fi Certified."

WLAN
(Wireless Local Area Network) Also referred to as LAWN. A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes. See also, Node.

WMI
(Web Management Interface) The browser-based system administrators interface for all Nomadix Gateways.

WPA
(Wi-Fi™ Protected Access) A Wi-Fi™ standard that was designed to improve upon the security features of WEP. The technology is designed to work with existing Wi-Fi products that have been enabled with WEP (as a software upgrade to existing hardware), but the technology includes two improvements over WEP:

- Improved data encryption through the temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven’t been tampered with.
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer’s hardware-specific MAC address, which is relatively simple to be “sniffed out” and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

It should be noted that WPA is an interim standard that will be replaced with the IEEE’s 802.11i standard upon its completion.

XML
(eXtensible Markup Language) A specification developed by the W3C. XML is a pared down version of SGML, designed especially for Web documents. It enables designers to create their own customized tags to provide functionality not available with HTML. For example, XML supports links that point to multiple documents, as opposed to HTML links, which can reference just one destination each. For all Nomadix Gateways, XML is used by the subscriber management module for port location and user administration. Enabling the XML interface allows your Nomadix Gateway to accept and process XML commands from an external source. XML commands are appended to a URL in the form of an encoded query string. Nomadix Gateways parse the query string, executes the commands specified by the string, and return data to the system that initiated the command request. See also, HTML, TCP, and W3C.
Index

A
AAA log 104
AAA services 56
   External Web Server 64
   Internal Web Server 61
log
   message definitions 277
log sample 277
   process flow 246
access control 5, 8, 67
access levels 229
accounting 56
archiving 51
ARP tables 153
   adding entries 220
   deleting entries 221
authentication 5, 56
authorization 56, 242
   and billing 242
auto configuration 16

B
bandwidth management 8, 73
basic configuration 45
billing 242
   process
      overview 242
billing enablement 5
billing log options 102
billing options 187
billing records mirroring 9, 77, 300
blocking subscriber interfaces 239
branding 5
bridge mode 9, 222

C
cautions 24, 214
Certificate Signing Request 294
character lengths 34
CLI 10

Command Line Interface 10
   inputting data 31
   logging in 29
common problems 308
concurrent login 229
Configurable Gateway ARP Refresh Interval 221
configurable ports 68
Configuration menu 56
configuration settings 143
   archiving 51
   exporting 223
   importing from archive 228
connecting to network 44
connections
   choosing 53
   types of 53
connectivity 4
contacting NOMADIX 311
Copyright ii
Credit Card 10
CSR 294

D
DAT 4, 10
DAT sessions 153
data 34
   inputting 34
date and time 144
default
   gateway 42
DHCP leases 182
DHCP options 45
DHCP Options from RFC 2132 47
DHCP service options 82
DNS options 50, 51, 87, 88
DNS Redirection Port 88
domain name 50, 88
Driverless print servers 59
   see Print billing command 59
ACCESS GATEWAY

location information 42, 44
locations 99
Log Filter 104
Log settings
  AAA log 104
  RADIUS history log 104
  Subscriber tracking log 105
  System report log 104
  System report log interval 104
logging
  in 55
  out 44
logging in 29, 37, 55
logging options 39, 102
login
  screen
    subscriber
      sample 209
login access levels 229
Login UI 205
Logout Console 194, 251
logout console 14
logout IP address 59

M
MAC Authentication 107
MAC filtering 15, 232
Management Information Base
  installing 52
management interfaces
  CLI 31
  WMI 31
menu organization 32
menus
  alphabetical listing 262
messages 217
MIB
  installing 52
Mirroring billing records 300
multi-level administration 15, 229
multiple subnets 141

N
NAI 17
Network Access Identifier 17
network architecture (sample) 23
network connections 44
Network Info menu 153
network interfaces 155
notes 24, 214
NSE core functionality 7
NTP support 15

O
optional NSE modules 22
  High Availability Module 22
  Hospitality Module 22

P
PageFaults 106
passthrough addresses 108
PMS 109
PMS integration 22
pop-up window 14
port assignments 163, 165
  adding 163
  deleting all 165
  deleting by location 166
  deleting by port 167
  exporting 167
  finding by description 168
  finding by location 169
  finding by port 170
  importing 171
  mapping 173
  updating 165
port locations 115
port mapping 20, 118, 159
  in-room port mapping 116
Portal Page 299
portal page redirect 15
Port-based billing policies 60, 161
  enabling 161
Port-Location menu 161
post session user interface 209
powering down 44
powering up the Access Gateway 28
PPP
  Authentication 101
  Echo Request 101
subscriber interfaces
  blocking 239
Subscriber Login 205
Subscriber Management 248
  configuration 249
  models 248
subscriber messages 217
subscriber profiles
  adding 173
  deleting all expired 182
  deleting by MAC 180
  deleting by user 181
  displaying 186, 187
  finding by MAC 183
  finding by user 183
  listing by MAC 184
  listing by user 185
Subscriber tracking log 105
  Log settings
    Subscriber tracking log 105
Subscriber UI buttons 212
Subscriber UI error messages 215
Subscriber UI labels 213
subscribers
  current connections 179
subscriber-side management 69
summary report 143
support
  administration 311
  technical 311
  user 311
Syslog
  History 105, 106
  Log Filter 104
  Save file 104
SYSLOG report 278
System Administration menu 53
System menu 220
System report log 104
System report log interval 104

T
TCP statistics 160
  technical support 311
    contact information 311
Telnet client 55
time 144
 Trademarks iii
transparent connectivity 4
transparent proxy 10
Tri-Mode 20
troubleshooting 305
  common problems 308
  error messages 306
  hints and tips 305

U
UDP statistics 161
UI buttons 212
UI labels 213
updating firmware 239
URL filtering 147
user session time adjustment 126

V
vendor-specific attributes (VSAs) 74
VPN tunneling 151

W
warnings 24, 214
Web Management Interface 54
  menu organization 32
Wholesale Roaming Module 17
workflow 27

X
XML API 18
XML interface 301