



# Wireless ISP Roaming

*Copyright © 2002 Nomadix, Inc. All Rights Reserved.*

Tuesday, January 21, 2003

## White Paper

# Contents

Introduction .....	3
Wi-Fi HotSpot Roaming.....	3
Wi-Fi HotSpot Reference Architecture .....	5
Global Roaming Reference Architecture.....	6
User Experience .....	7
Welcome Page – Local Service Presentment .....	8
Login Using a Web Browser.....	9
Login Using a Smart Client.....	11
Login Using Windows XP or Other 802.1x-based Clients .....	12
Start Page .....	13
ServiceSelect Console (SSC).....	13
Remote Virtual Private Networking.....	14
Logout & Billing.....	14
RADIUS Client and AAA Support .....	15
New Subscriber Acquisition.....	15
User Authentication .....	15
User Authorization.....	16
Accounting .....	16
Integrating into a Roaming Intermediary .....	16
IP Address Management.....	17
Plug & Play Connectivity.....	17
Virtual Private Network Support.....	17
Transparent Proxy .....	17
Captive Portal.....	18
Home Page Redirect.....	18
Location Identification .....	18
IP Filtering and Access Control .....	18
Bandwidth Management.....	19
ServiceSelect Console .....	19
Optional Authentication and Billing Mechanisms.....	20
Property Management Systems (PMS) .....	20
Credit Card Authentication .....	20
XML (eXtensible Markup Language).....	20
Centralized Device Management.....	21
Web Management Interface .....	21
Command Line Interface.....	22
SNMP .....	23
User Authentication Test Facility.....	23
Summary .....	24

## Introduction

Enabling Wi-Fi™ Internet access everywhere means venue owners and their service provider partners need to provide any user access to the Public-access network, and then offer information and services tailored to that location. Once connected, customers need to retain the billing relationship with their chosen service provider, or retail provider in a wholesale provider model, enabling one bill to follow them wherever they travel.

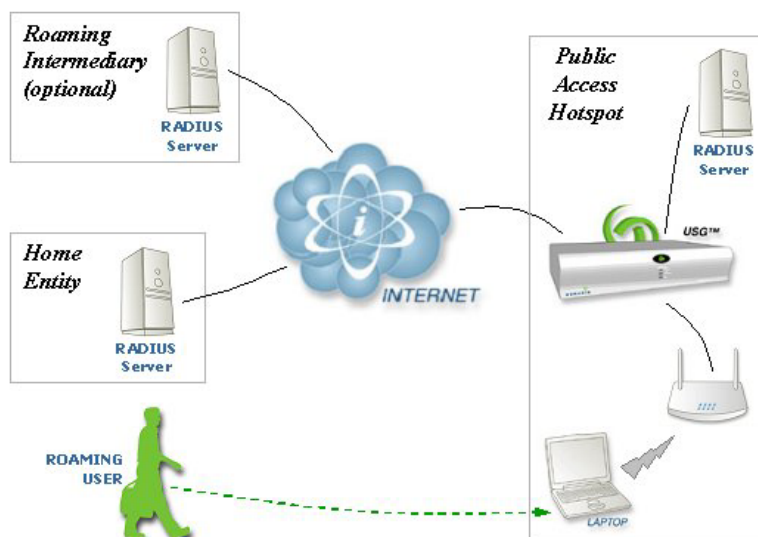
This document provides an overview of wireless ISP (WISP) roaming both locally and globally, including typical network architecture references and the solutions that Nomadix provides. The user HotSpot experience is explained in detail; along with an outline of the features and functionality the Nomadix family of Public-access Gateways provides for anyone designing and implementing Public-access Wi-Fi HotSpots.

Nomadix' solutions allow Public-access networks to instantly deliver “plug-and-play” broadband access to any customer—regardless of how their computer or device is configured—while passing the necessary parameters for billing and authentication to the service provider allowing settlement to occur; enabling **Global Roaming**.

## Wi-Fi HotSpot Roaming

The continued proliferation of wireless technologies, such as Wi-Fi compliant wireless LAN (WLAN) devices, has provided users with more desirable options for mobility and network connectivity. These technologies have also allowed high-speed Internet access providers to build WLAN HotSpots. However, it is difficult for a single service provider to build an infrastructure that offers access to its customers from any location, so roaming between service providers is essential for delivering universal customer access. Roaming allows enterprise companies and service providers to enhance employee connectivity and service offerings by enabling network access at Wi-Fi enabled HotSpots.

## White Paper



The figure above graphically depicts a generic model for Wi-Fi HotSpot roaming, including necessary functions and entities. This model demonstrates the scenario where a nomadic user travels outside of their Home Entity location/network and requires network access when roaming into another Public-access HotSpot. The user gains access to the HotSpot network by associating with the wireless network and then being authenticated by one of several methods, either locally within the HotSpot itself, remotely by their retail provider, or by an optional Roaming Intermediary. Further detail of this process is provided in the User Experience section.

The functional entities in the wireless HotSpot-roaming model include the Roaming User who is a mobile customer with a Wi-Fi enabled laptop or PDA. The roaming user frequents Public-access HotSpots and has a need to access the wireless HotSpot network.

The Public-access HotSpot can be any public location or venue that provides wireless access to the Internet for roaming users. The Public-access HotSpot is operated by the organization that enables user access to the Wi-Fi network and participates in the visitor authentication process. Examples of this type of HotSpot include hotel lobbies, coffee shops and airports.

The Home Entity (or retail provider) owns the account relationship with the roaming user. When roaming, the user must authenticate to the home entity in order to obtain roaming access at the Public-access HotSpot. Examples of home entities include WISPs, other service providers, and corporations.

The Roaming Intermediary is an optional entity that may facilitate AAA and financial settlement between one or more public access HotSpot operators and the home entity. Examples of AAA intermediaries include roaming brokers, roaming agents, aggregators, or clearinghouses such as Boingo Wireless or iPass.

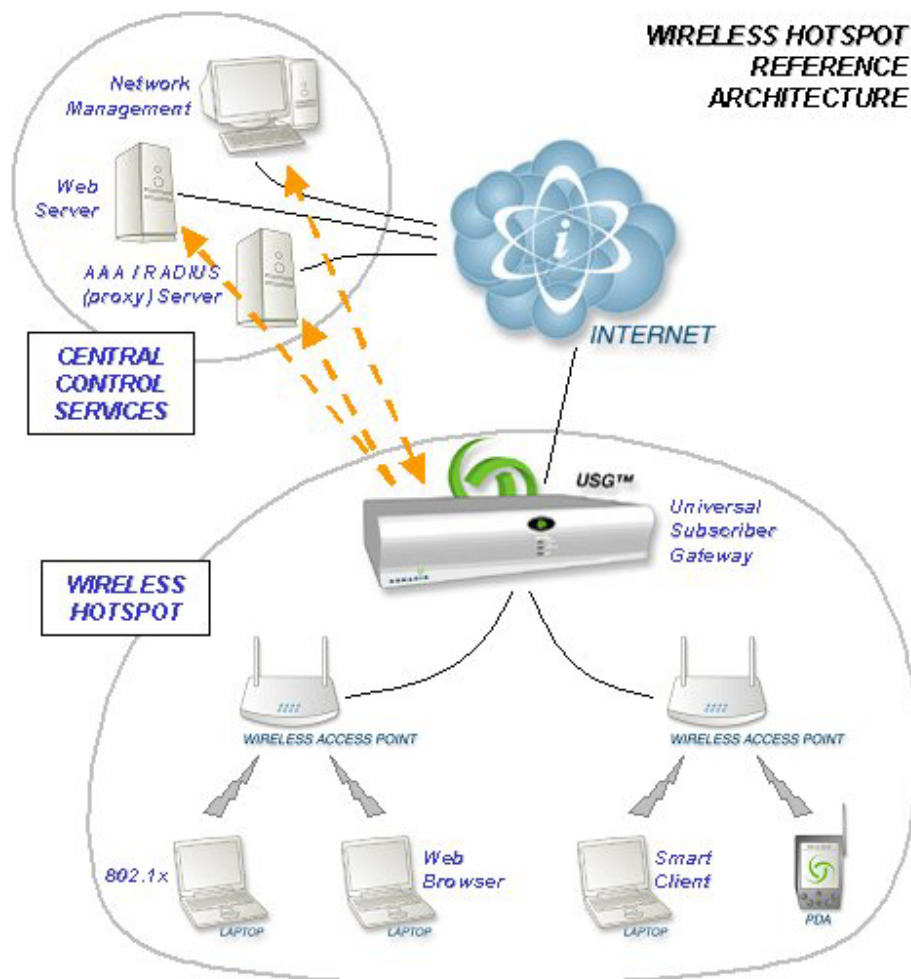
## Wi-Fi HotSpot Reference Architecture

The Nomadix family of Public-access Gateways, including the Universal Subscriber Gateway II™ (USG II) for large venues and the HotSpot Gateway™ (HSG-25) provide the core functionality that enables wireless HotSpot operators to offer local network access to roaming users. The Nomadix Gateways provide the HotSpot operator with the ability to specifically tailor local access and maintain full control over the user experience, as well as supplying the authentication and billing mechanisms that are critical to successful administration of these services.

The reference architecture below depicts a single Public-access wireless HotSpot containing a USG II, which enables any type of visitor to roam into the location and obtain access to the local network. Whether the roaming user has a laptop or a PDA, and no matter how they choose to access and authenticate to the network, the USG II makes it possible for the HotSpot operator to provide any services required.

Portal presentment, user authentication and billing is provided and maintained from a central control services location that is located remotely from the HotSpot. This architecture allows for multiple wireless HotSpots to be established and supported from a single central control center.

## White Paper



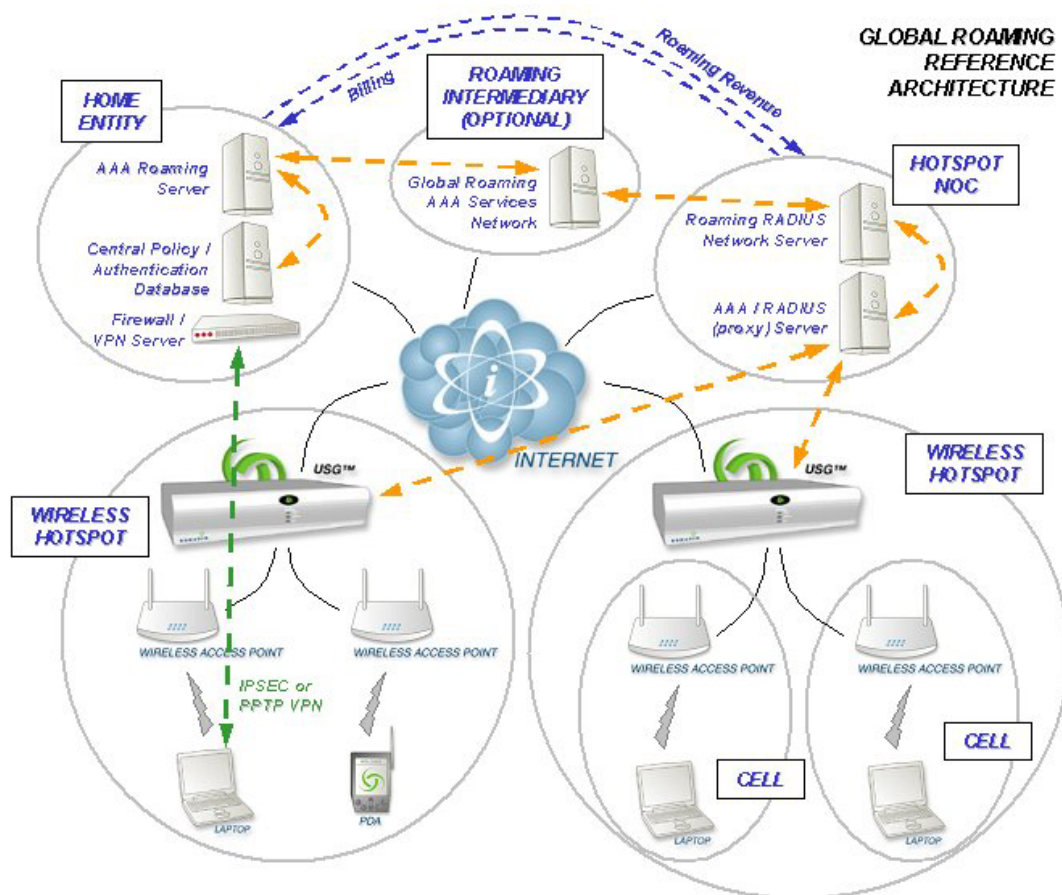
## Global Roaming Reference Architecture

Public-access HotSpots powered by a Nomadix Gateway enable roaming users to access Wi-Fi broadband networks globally while maintaining a single billing account worldwide.

The reference architecture below depicts multiple single- and multi-cell wireless HotSpots, each containing a local USG II (or HSG-25 for smaller venues), enabling visitors to roam into each location and obtain access to the local network. The USG II in each location presents the local roaming user with the service provider's customized portal page for local network access.

## White Paper

Authentication, authorization and accounting (AAA) for the billing details of the roaming user can be processed from one of several possible remote locations. The HotSpot central services can provide local AAA functions, as well as acting as a proxy to other AAA locations such as the user's home entity. As previously detailed, an optional roaming intermediary may also be used.



Once the roaming user has gained access to the HotSpot network, they may begin to utilize it for Internet access, or they may choose to establish a secure IPsec link or VPN tunnel back to the home entity in order to securely access those resources.

## User Experience

The following section provides an overview of the user's experience when visiting a Wi-Fi Public-access HotSpot and attempting to connect to the network. The process and requirements for user login, authentication, and access and are outlined below.

## White Paper

### Welcome Page – Local Service Presentment

Once associated to the network, the roaming user launches a Web browser and is presented with a Welcome Page from the local network. The Nomadix Gateway automatically loads this welcome page to any non-authenticated roaming user's browser. The welcome page is the first page that is presented to the user during URL redirection, instead of the user's default Home Page URL ([www.nomadix.com](http://www.nomadix.com), for example).

The user is able to view any local content and services provided by the HotSpot owner at no charge, such as information on local services, maps, restaurant menus, etc. The welcome page may also contain links to specific Web sites at no charge as part of the service.

The welcome page can contain various network access options at the discretion of the HotSpot operator, such as a link to a network login page, various billing options, and a choice of WISP access if available in a wholesale model. When multiple WISPs are available, the user will be able to select, login and gain access to the WISP of their choice.



### Selecting a Service Provider – Multiple WISP Support

It is likely that some Public-access Wi-Fi HotSpots will have multiple service providers available in a single location. This enables the roaming user to select a specific WISP with which they already have an established account, or if they prefer one WISP to another.



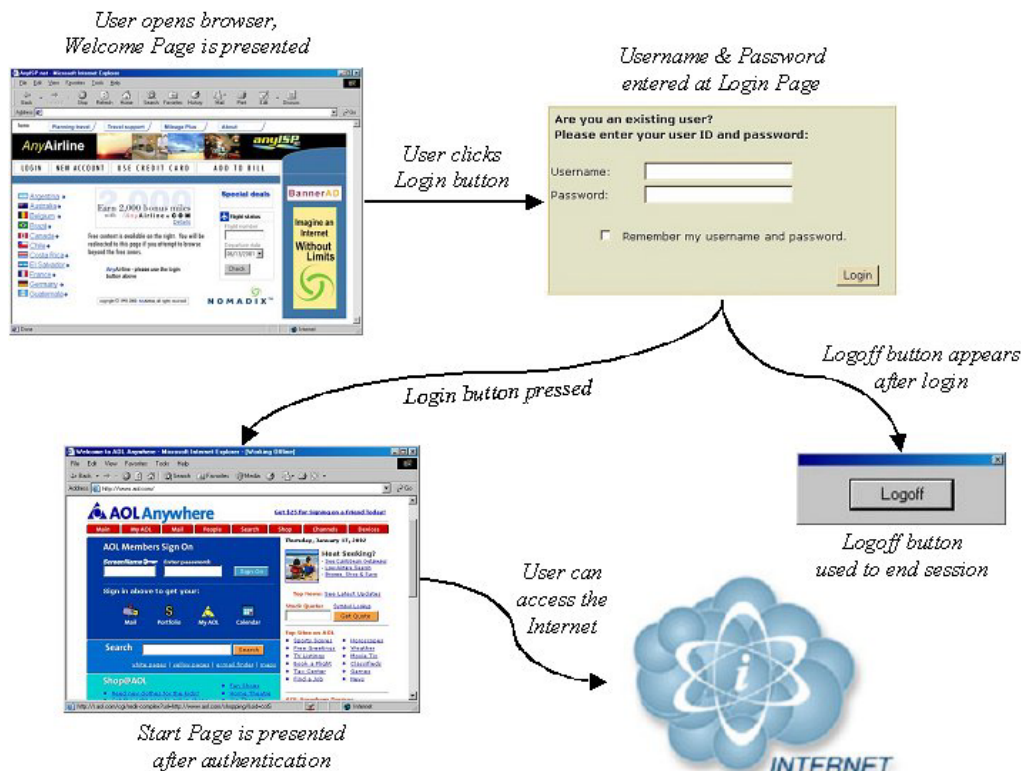
## White Paper

To facilitate this process, the HotSpot operator will present the multiple WISP options to the roaming user via the welcome page described above. Buttons or links will typically be provided on the welcome page to enable user access to the various service providers.

The Nomadix Gateway differentiates the login process for each WISP by appending a user ID prefix that associates the user to the WISP of their choice. To make this process as seamless as possible for the roaming user, the prefix is automatically appended to the user's login once they make their WISP selection. The WISP prefix is kept as a hidden variable for further simplicity for the user.

## Login Using a Web Browser

A HotSpot operator may choose to allow network access for the roaming user via a standard Web browser. With this method, any IP-based device with a web browser can login and be authenticated to the HotSpot network. The roaming user is not required to load additional client software or change the network configuration of their laptop. The process simply requires the user to launch a web browser and access is simply a few clicks away.



## White Paper

To obtain full access to the Wi-Fi HotSpot network beyond the welcome page, the roaming user must login to the network. The Login Page is delivered to the user when they click the login button on the welcome page. An example of the login page is shown below.

Are you a new user? Click this button:

New User


Are you an existing user?  
Please enter your user ID and password:

Username:

Password:

Remember my username and password.

Login

Please contact your Network Administrator in case of problems.  
[Help Message](#) 

The login page is made secure by the use of the SSL (Secure Sockets Layer) protocol, and contains fields to enter user credentials such as username and password, as well as a link to a help page hosted by the HotSpot operator.

### ***'Remember Me' Cookie Support***

Web browser cookies are a familiar part of web-based authentication methods that rely on it to provide all or part of the necessary AAA information. The use of cookies is particularly useful for the new set of Internet access-enabled PDAs (e.g. the Compaq iPAQ) since it prevents the user from having to re-enter the AAA information with a stylus every time they authenticate after the initial login. The Nomadix Gateway enables the roaming user to be remembered by the HotSpot network by placing an obfuscated cookie in the browser if the roaming user selects the feature at login.

### ***Protection of the User's Login Credentials***

When a wireless HotSpot operator provides support for login to the network via a standard web browser the roaming user's credentials must be kept secure and protected. Both the roaming user and service provider are protected from account "identity theft" and session-disconnect hijacking by enabling SSL protection for the username and password when the user requests login to the network. In addition, to protect the RADIUS messages from being intercepted for the username and password IPsec is used between RADIUS Servers.

## White Paper

### Login Using a Smart Client

Many roaming users utilize a Smart Client interface for network access, which enables global HotSpot roaming and network access via a trusted method and account that they have already established and are subscribed to. The user experience in the following section describes a typical user encounter at a Public-access HotSpot when using smart client software for access.

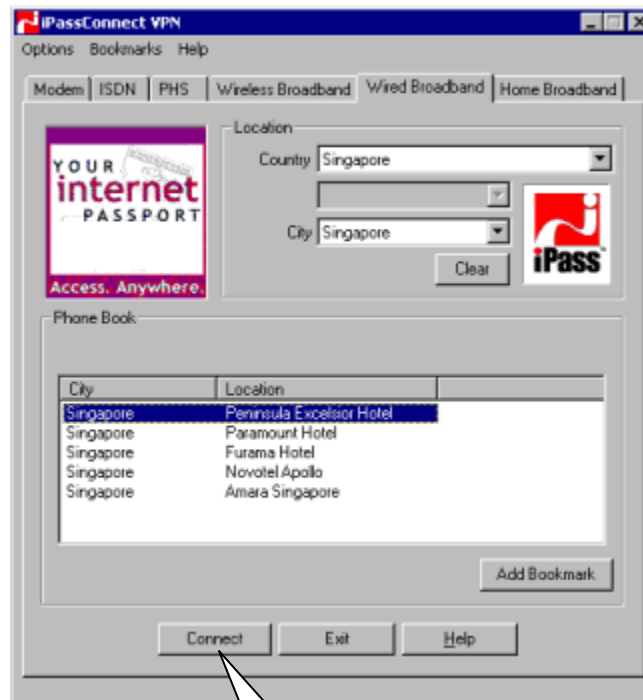
To access the local HotSpot network the roaming user launches their smart client software, selects the local network from the access list, and clicks the connect or login button. Depending on the smart client software used, the user may or may not be required to also enter their standard username and password credentials.

When the user no longer needs access to the Public-access network, they simply logout from within the smart client software.

### Smart Client Software

Boingo Wireless, GRIC Communications and iPass have developed Smart Client interfaces, all of which are supported by Nomadix.

An example of the iPassConnect™ client from iPass Inc. is shown here, where the user selects the HotSpot location they want to connect to and is logged on by clicking the **Connect** button.



Click Here

## White Paper

The GRICdial™ client from GRIC Communications is shown below, where the user selects the HotSpot location they want to connect to and is logged on by clicking the **Login** button.



Click Here

### Login Using Windows XP or Other 802.1x-based Clients

IEEE 802.1x is a new standard for port-based authentication that is an integral part of the Microsoft Windows XP operating system. In addition, there are an increasing number of dedicated 802.1x-based clients for various common operating systems.

In a network where 802.1x support is required, the Nomadix Gateways provide all of the necessary functions to facilitate the authentication process between the 802.1x supplicant (roaming user) and 802.1x authentication server (RADIUS Server). Non-802.1x enabled roaming users are also simultaneously supported by the Nomadix Gateway.

Whether the roaming user is utilizing Windows XP or an 802.1x-based client for secure access to the network, the user will either be automatically presented with an 802.1x login screen or will be required to launch the 802.1x client software. The user is logged in to the network by entering username and password credentials.

When the user no longer needs access to the Public-access network, they simply logout of the network from within the 802.1x-based client software or by shutting down their laptop.

## White Paper

An example of the Microsoft Windows XP 802.1x login screen is shown below.



## Start Page

Once the roaming user has successfully logged in and been authenticated to the Wi-Fi HotSpot network, and then launches a Web browser they are presented with a Start Page hosted by the service provider. If the WISP does not provide a start page, the roaming user will be presented with either their default Home Page URL or a default Home Entity (retail) start page instead.

## ServiceSelect Console (SSC)

After they have authenticated, the roaming user can be presented with the ServiceSelect Console (SSC) via the Nomadix Gateway, which is a small pop-up window that provides information on the current session, links to other Web sites or services, and a button that allows the user to explicitly logoff from the network when they no longer need access to the Public-access network.



## White Paper

The SSC also allows the roaming user to change their service plan on the fly from within, a feature that is useful when more bandwidth is required dynamically. An example of how this can be used is when the user is downloading a large file at an airport HotSpot and their flight begins to board – instead to ending the session unsuccessfully, the user can dynamically increase the speed of their connection to complete the download without service interruption.



## Remote Virtual Private Networking

VPN tunneling (PPTP, IPsec) remains the recommended method for transmitting data across a wireless network for mobile workers wishing to connect back to their corporate resources. Nomadix' Gateways feature its patent-pending iNAT™ functionality that 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.

## Logout & Billing

Network access and billing requirements will differ from user to user, where one roaming user may be billed by the day and another billed by the minute. The Wi-Fi HotSpot operator will need to support the ability for the user to logout from the network even if they do not require it for their own billing purposes. In addition, the HotSpot operator should provide the capability for the user to specifically request to be logged out from the network or to automatically be logged out of the network when they stop using the network.

When the roaming user is successfully logged into the wireless HotSpot network, the ServiceSelect Console (SSC) is presented. The SSC includes a logout button that the user can utilize to explicitly logout from the HotSpot network at the end of their session, which provide an accounting record update that notifies the billing system to halt all charges.

If a roaming user inadvertently fails to request a logout, or they experience a failure that does not enable them to logout, the HotSpot operator will enforce an idle-timeout condition that will automatically cause a user to be logged out of the network after a pre-determined idle (lack of network activity) period. The roaming user will be implicitly logged out of the HotSpot network and accounting records will be issued as appropriate.

## RADIUS Client and AAA Support

The following section outlines the principal mechanisms available to public access wireless HotSpot service providers to authenticate, authorize and account (AAA) for the billing details of their subscriber base.

Wireless HotSpot networks include business models based on providing Internet access for short periods of time to temporary users as well as longer-term contracts for Internet access. In either case, Nomadix has placed particular emphasis on developing technology that allows for a zero-cost, self-provisioning method for visitors to purchase Internet connectivity. Currently, the Nomadix USG supports both Standard RADIUS and Enhanced RADIUS AAA mechanisms:

### New Subscriber Acquisition

The Nomadix Gateways support new user acquisition by interfacing with a provisioning web server to allow a new subscriber activation page to be presented to the user. A simple HTML web page can be designed by the service provider to allow for the self-provisioned purchase of broadband Internet access, enabling immediate new subscriber acquisition without support costs.

This purchase page could consist of multiple user-selectable service plans at different rates, fields to create a username and password, name and address billing credentials, contact information such as phone number and email address, and any other desired user information. Once the user submits their information a RADIUS profile is created for them and they are redirected to a login page where they can enter the new account information for access to the HotSpot network.

### User Authentication

Nomadix has developed a number of additional features based on the standard RADIUS protocol for two principal purposes:

- ❑ To dramatically increase the AAA flexibility inherent in the standard RADIUS protocol to allow for the creation of differentiated and profitable wireless broadband networks
- ❑ To ensure greater customer satisfaction for Internet access by allowing a choice of both access method and service provider

These additional features are Smart Client support, IEEE 802.1x support, and 'Remember Me' Cookie support, which were all previously described in the User Experience section.

## White Paper

### User Authorization

The Nomadix Gateways offer a set of RADIUS Vendor-Specific Attributes (VSAs) required by the emerging class of WISPs that want to enable more advanced services and billing schemes such as a per device per month connectivity fee. The VSAs currently include:

- ❑ Bandwidth Upstream (Kbps)
- ❑ Bandwidth Downstream (Kbps)
- ❑ IP address type (IP Upsell)
- ❑ Post-authorization Home Page Redirect (HPR)
- ❑ Expiration Time
- ❑ Volume-based Session Timeout
- ❑ End of Day Session Timeout

The HPR attribute allows the service provider or location owner to tailor the initial page after authorization to the individual user.

### Accounting

The Nomadix Gateways have an integrated RADIUS Client allowing the service provider to track or bill based upon several factors, including number of connections, location of connections, 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 roaming user connects to the wireless HotSpot network, the RADIUS Client in the Nomadix Gateway authenticates the customer with the RADIUS Server, applies associated attributes stored in that customer's profile, and logs their details of their network activity.

### Integrating into a Roaming Intermediary

There are times when a roaming user requires access to a wireless HotSpot and needs to be billed via a roaming intermediary, which could be a roaming broker, roaming agent, aggregator, or clearinghouse such as Boingo Wireless, iPass or GRIC Communications.

In order to support this requirement, the service provider or HotSpot operator must configure their RADIUS Server to act as a proxy to the roaming intermediary's RADIUS Server. This action enables the roaming user to access the HotSpot network and be billed via the roaming intermediary to an account that they have already established.



## IP Address Management

### Plug & Play Connectivity

Nomadix' patented Dynamic Address Translation™ (DAT™) function offers a true “plug-and-play” solution that provides transparent broadband network connectivity ensuring everyone gets access to the Public-access HotSpot.

Nomadix developed DAT to actively monitor every packet transmitted from each device to ensure the packet is correctly configured for the network that computer is expecting. If necessary, DAT will perform standard Network and Port Address Translation and supports Application Level Gateways (ALGs) for protocols such as FTP, H.323, PPTP, etc., to ensure the customer gains network access without having to reconfigure their PC or load client-side software.

By supporting clients configured for DHCP or that have statically assigned or incorrectly configured IP Addresses, the wireless HotSpot operator can natively offer services to the broadest range of heterogeneous devices and IP settings.

### Virtual Private Network Support

Nomadix supports Virtual Private Network (VPN) sessions, allowing a user to establish a VPN tunnel to a home entity. Once the user has logged on to the network and is successfully authenticated, their VPN client is launched and they are able to establish the tunnel in the normal manner. Nomadix' products feature its patent-pending iNAT functionality that 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.

### Transparent Proxy

The Nomadix Gateways direct all HTTP and HTTPS proxy requests through an internal proxy, which is transparent to the user so that reconfiguration within their browser is not necessary. The proxy also facilitates DNS caching. When the cached DNS files are requested again, the proxy returns the data from the cache source. This feature resolves configuration problems for the subscribers with proxy settings preset to their corporate network.

## Captive Portal

### Home Page Redirect

The Home Page Redirect (HPR) feature of the Nomadix Gateways enable the network to intercept the browser's home page setting and redirect it to a new portal page determined by the service provider or premise owner. When redirecting the customer to a new home page, the original home page (Origin Server) is passed as a parameter to the new home page so the customer can still access their default home page after the local or personalized page has been presented.

HPR allows redirects of the user's homepage to either the internal web server of the Nomadix Gateway or to an external web server and allows the HPR setting to be unique per user via a RADIUS attribute stored in that customer's account. The Nomadix Gateways allow redirects pre and post authentication for maximum brand exposure for the service or the venue.

### Location Identification

Dependent upon the network architecture, the Nomadix Gateway can determine the physical location of the user in order to personalize the service presentation. This is achieved by using aggregation equipment that supports port based IEEE 802.1q VLANs or using the integrated SNMP Manager to query the Bridge MIB (RFC 1493 or certain proprietary MIBs) to determine the physical port associated with the user's MAC address and each packet it came through.

An example of this is that a user visiting an airport can receive a Web page that contains flight schedules specific to that terminal based upon the port they are connecting into. The end user doesn't need to know where they are physically located to receive services and since identification is performed within the network.

### IP Filtering and Access Control

The Nomadix Gateway can be used to create a "walled garden," allowing roaming users to access predetermined Web sites, services or applications on the network even though they may not have subscribed to the wireless HotSpot broadband service. Nomadix provides up to 300 IP pass-through addresses and allows the service provider to enforce security based upon whether or not the customer has been authenticated. The "walled garden" can be used to push local content and services providing a custom experience dependent upon the HotSpot operator.

## Bandwidth Management

The Bandwidth Management feature of the Nomadix Gateways enable service providers to limit bandwidth usage on a per device (MAC Address/User) basis. This ensures 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.

The bandwidth for each device can be defined asymmetrically for both upstream and downstream data transmissions. The service provider can also allow the individual user to dynamically increase or decrease their bandwidth without having to disconnect or re-establish a new session.

The Nomadix Gateway can also manage the WAN Link traffic providing complete bandwidth management through the public access HotSpot. Bandwidth Management performs traffic shaping on the WAN link interface to prevent over-utilization. Nomadix' products queue traffic from overly busy instances in time, and send the packets over the WAN Link when a lull in traffic occurs.

## ServiceSelect Console

The ServiceSelect Console (SSC) that is presented by the Nomadix Gateway is a JAVA-based applet that is driven to each customer's browser post-authorization providing them with the ability to self-select services and upgrade their bandwidth and billing options in a real-time fashion.



The SSC also allows the venue owner or service provider to send custom messages and advertising directly to the screen of the customer. For credit card usage, the SSC displays a dynamic "time" field to inform customers of the time remaining on their account.

## Optional Authentication and Billing Mechanisms

### Property Management Systems (PMS)

When a HotSpot operator deploys a network in a hotel environment, certain Nomadix Gateways also contain functionality to directly interface to the hotel's Property Management System (PMS). A HotSpot operator is able to offer this payment method as another convenient choice for the roaming user. The Nomadix Gateway also contains unique technology developed specifically for Wi-Fi networks that allows the real-time querying of the PMS to authenticate a guest against the hotel's PMS database.

### Credit Card Authentication

Casual or one time users who do not have an existing relationship with a wireless HotSpot operator must be able to purchase Internet access via credit cards on an ad-hoc basis. Advanced functionality, such as integration with on-line secure credit card based self-provisioning, allows the customer to setup a credit account. Similar to a standard eCommerce transaction, the credit card authentication authorizes the MAC address of the individual user to gain access to the HotSpot network for a specified time and a specific service plan.

In addition, in order to support a revenue-splitting business model between the property management company and the service provider, an integrated Billing Mirror capability is provided in the Nomadix Gateways that performs the logging of customer's billing activities using credit cards and PMS to more than one server.

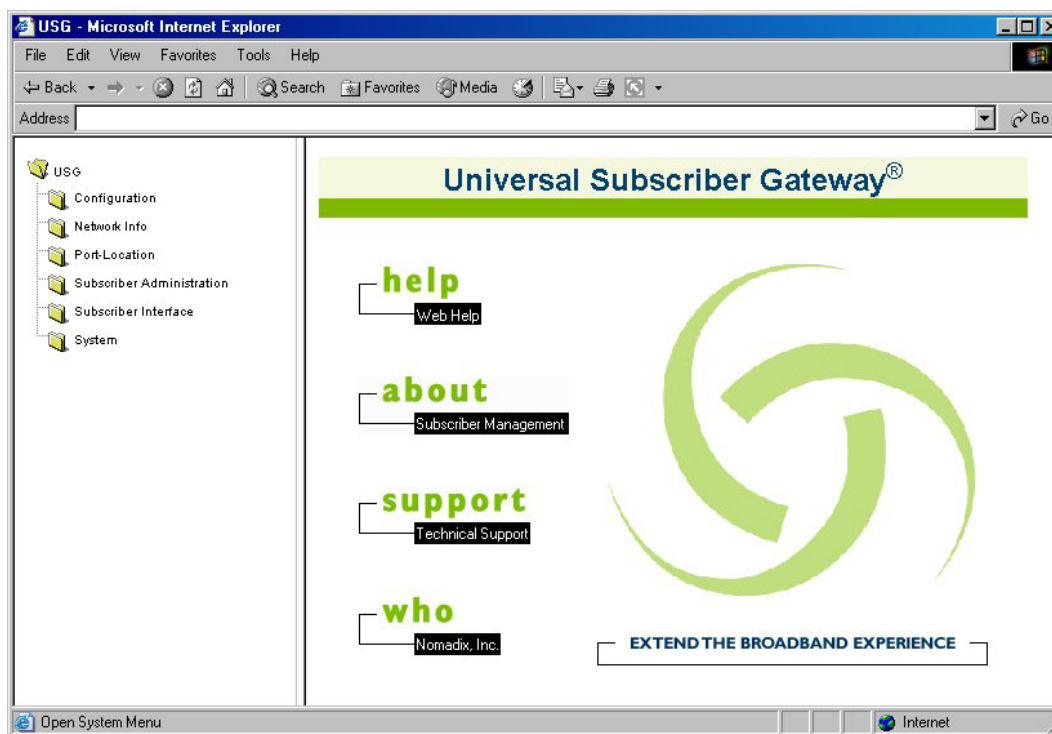
### XML (eXtensible Markup Language)

The XML Application Programmer's Interface (API) allows the Nomadix Gateways to accept and process XML commands from an external source for integration with OSS, provisioning, and other network management elements for subscriber management and location/port management. XML commands are sent over the network in the form of an encoded query string. The XML interface enables solution providers and integrators to customize and enhance the installations with a range of value-added capabilities and services.

## Centralized Device Management

### Web Management Interface

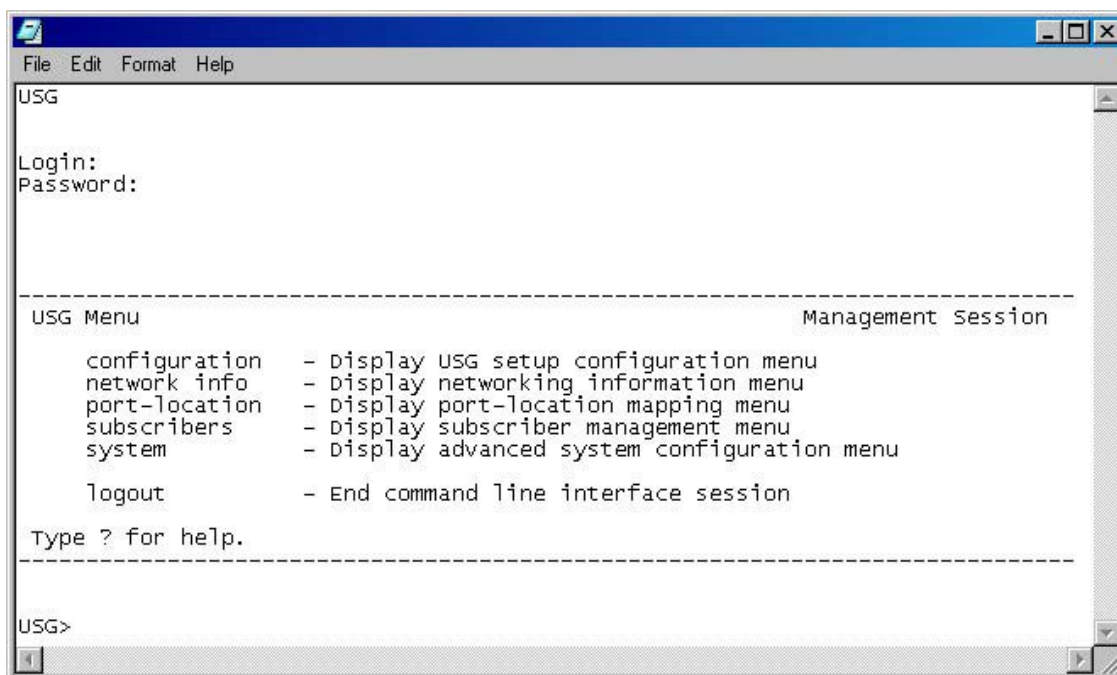
All of the Nomadix Gateways can be managed via its embedded Web Management Interface (WMI) from any standard Web Browser application. The WMI is a graphical menu-driven interface that provides the administrator with full configuration control and access to the platform via the point-and-click of a mouse.



## White Paper

### Command Line Interface

The Nomadix Gateways contain an embedded Command Line Interface (CLI) for management purposes, which is accessible locally via a direct serial cable connection or remotely via a network Telnet session. The CLI is a character-based interface and acts as the administrator's window to the configuration of the product.



```
File Edit Format Help
USG

Login:
Password:

-----
USG Menu                                     Management Session
-----
configuration - Display USG setup configuration menu
network info  - Display networking information menu
port-location - Display port-location mapping menu
subscribers   - Display subscriber management menu
system        - Display advanced system configuration menu

logout        - End command line interface session

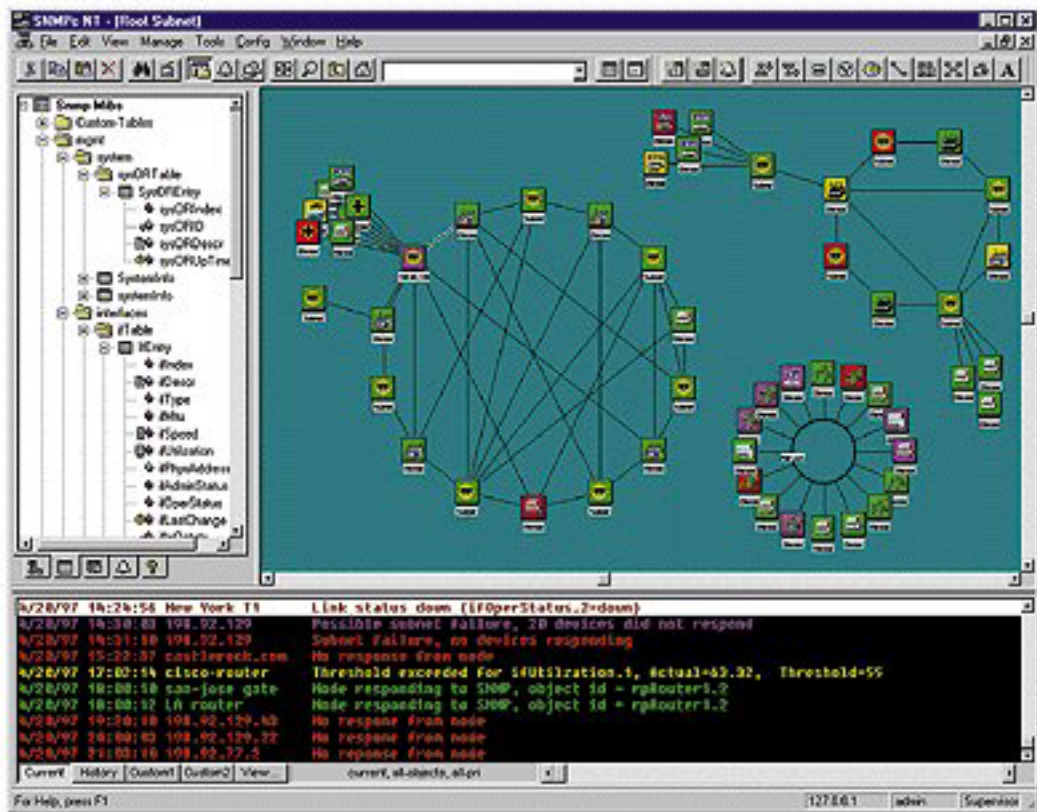
Type ? for help.

-----
USG>
```

## White Paper

### SNMP

The Nomadix Gateways can also be managed over the network or via the Internet with an SNMP client manager (such as HP OpenView or Castle Rock SNMPc) by importing the Nomadix MIB into the client manager.



### User Authentication Test Facility

Nomadix provides a test facility that allows a system administrator to remotely test the end-to-end user authentication process within the network. Using this test facility the administrator can remotely login to the wireless HotSpot network and can enter a username and password that will be authenticated without any accounting records being generated or access to the network being granted.

## Summary

Nomadix offers a full family of Public-access Gateways that allow roaming users to receive broadband connectivity when entering a Public-access Wi-Fi HotSpot, allowing them to self-provision services and gain access to local content and services. These products enable the service provider to offer a broad array of services by supporting the widest range of existing back-end systems for billing and authentication.

Nomadix was founded with one objective in mind – to enable the broad-based deployment of high-speed Internet access, allowing users to transparently roam within diverse networks creating an Internet everywhere. This is true Nomadic computing.