Nomadix Service Engine
Access in Large Public Venues

30851 Agoura Road
Suite 102
Agoura Hills CA 91301 USA
www.nomadix.com

White Paper 230-1026-001

Introduction

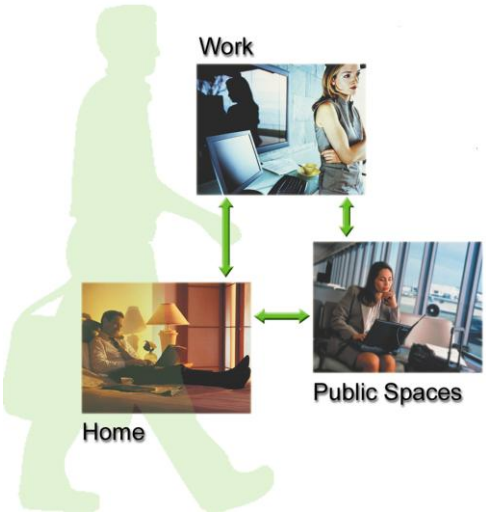
Providing cost-effective and profitable wired and wireless (Wi-Fi) public access means HotSpot owners and their Public Access Service Operators (PASOs) partners need to provide any user access to the service, and then offer information and services tailored to that location. Once connected, NSE roaming features enable these users to retain the billing relationship with their chosen (or home) service provider enabling one bill to follow them wherever they travel.

Nomadix offers its Nomadix Service Engine (NSE) software embedded on our family of Access Gateways. The NSE offers a full suite of functionality designed for deployment in public access networks allowing network operators to deploy a secure, revenue-producing service. The Nomadix solution resolves issues of connectivity, security, billing and roaming that are created when deploying these Wi-Fi networks.

Nomadix recommends the **AG 5600** running the NSE for deployment in large public access locations such as airports and convention centers. The **NSE** can also be used when deploying Wi-Fi service to mid-sized deployments. For single and dual cell deployments, the **AG 2300** is the ideal HotSpot in a box. In addition to the NSE Core features, Nomadix offers a series of Modules to further enhance the service offering:

- **NSE Hospitality Module**: This module provides the most extensive range of **CERTIFIED Property Management System (PMS) interfaces** to enable in-room guest billing for High-Speed Internet Access (HSIA).This module also includes one-way and two-way PMS interfaces for in-room billing in a WI-FI network.
- **High-Availability Module**: Provides enhanced network uptime and service availability when delivering high-quality Wi-Fi service by providing Fail-Over functionality allowing 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
- **NSE Routed Subscriber Module:** Provides additional flexibility in architecting your network by configuring an NSE enabled Access Gateway to support Layer 3, WLAN, MESH and other routed networks on the subscriber or network side of the Nomadix device.

How It Works



The Nomadix Service Engine running on an AG 5600 provides the essential components to deploying public access in a large venue.

1. Wireless/wired client enters a HotSpot
2. The user opens up their browser and is presented with a custom portal from the HotSpot owner or the PASO
    a. A new user can use this portal to sign up for service
    b. Existing customers supply their user name and password over a secure SSL link granting the client access to the Internet or they can be authenticated via 802.1x or via a Smart Client.
3. The AG 5600 passes necessary information for authentication, tracking and billing to the service provider
4. Customer obtains open access to the Internet, where he can VPN to his corporate network or obtains local information and services, etc.

Network Service Engine Overview

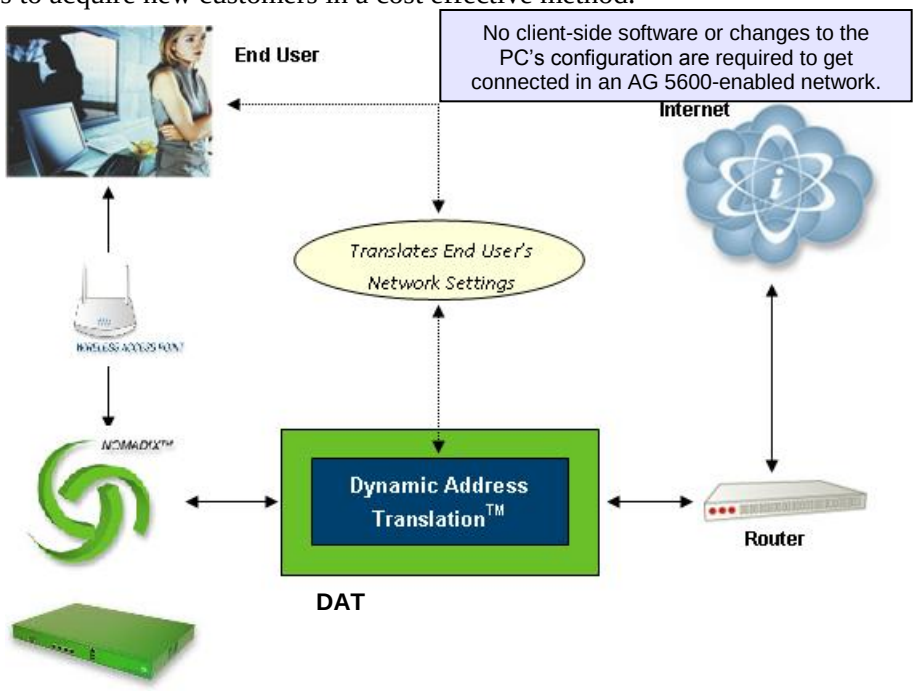
The NSE provides a range of features needed for the successful deployment of wired and Wi-Fi multi-use, multi-revenue public access service. The following key areas are addressed by the NSE deployed on a Nomadix Access Gateway:

- Customer Acquisition
- Service Provisioning
- Access Control and Multi-mode Authentication
- Billing Plan Enablement
- Policy-based Traffic Shaping
- Advanced Roaming

Customer Acquisition

Nomadix' Dynamic Address Translation

Nomadix' patented Dynamic Address Translation (DAT™) technology provides transparent broadband network connectivity as users travel between different locations—without requiring any changes to their computer's settings (Zero Configuration) or special client-side software—ensuring that everyone gets easy access to the network. A Nomadix-enabled network allows providers to acquire new customers in a cost effective method.



As mobility between locations (subnets) increases, wireless networks create an additional level of complexity. A DHCP lease from an Ethernet or wireless subnet is set by the DHCP Server and may last from several hours to several days, forcing a customer to either manually release and renew their DHCP lease at the new subnet or reboot their computer—increasing abandonment and decreasing the take rate of the service.

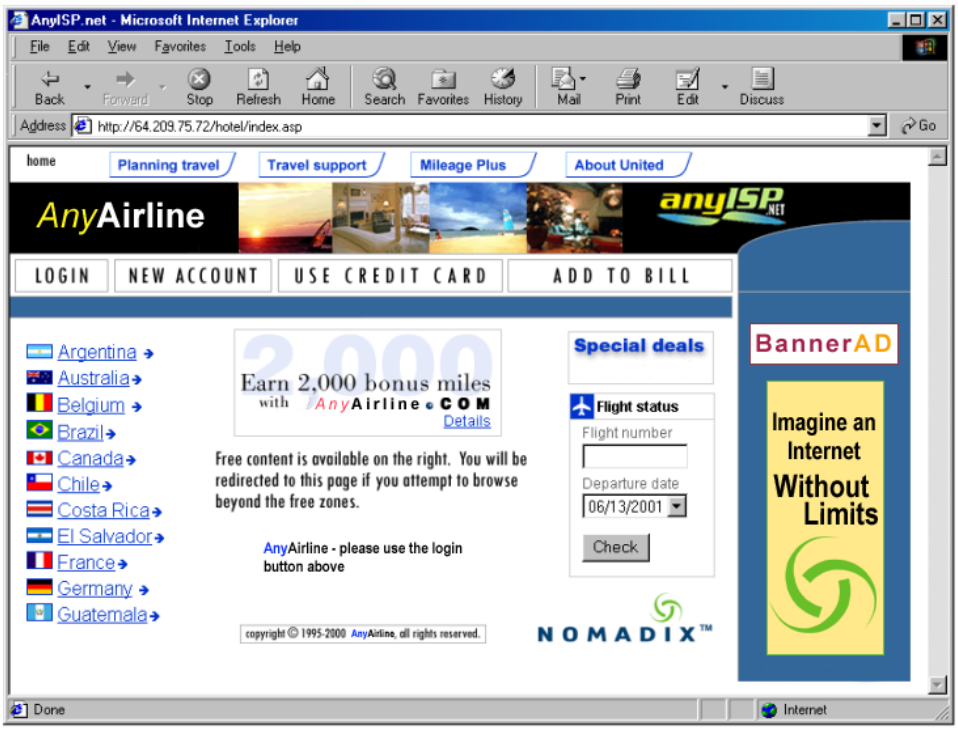
Nomadix developed DAT™ to actively monitor every packet transmitted from each device to ensure all packet are correctly configured for the network that computer is expecting. If necessary, DAT™ will perform standard Network and Port Address Translation and supports Application Level Gateways (ALGs) for 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.

DAT™ also ensures that a DNS server is always available to a user through the DNS redirection function. This function redirects a user's DNS requests to a local DNS server closer to the customer's location—improving the response time and enabling true plug-and-play access when the subscriber's configured DNS server is behind a firewall or located on a private Intranet.

Service Provisioning

Home Page Redirection

Once connected to the public access network, Nomadix' patented Home Page Redirection feature intercepts the user's browser settings and directs them to a web site to securely sign up for service or log in if they have a pre-existing account. Nomadix offers redirection opportunities pre and post authentication as well as at service disconnect for maximum service branding capability for both the service provider and the venue owner.



The Home Page Redirect (HPR) feature of the NSE enables the network to intercept the Internet browser's home page setting and redirect it to a new portal page determined by the service provider or HotSpot 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 also allows unique redirects on a per subscriber basis per a RADIUS attribute stored in that customer's account.

Location-based Identification

Depending on the network architecture and vendor, the NSE can determine the physical location of the user to personalize the service presentation and perform security or billing functions. 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.

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 in the network, it is secure and can be used for a billing function based upon the port they have plugged into.

Access Control and Authentication

The NSE running on the AG 5600 provides an additional layer of security for the public access network by blocking access to the Internet or allowing access to a pre determined "Walled Garden" area of the web until the user has been authenticated. The NSE also provides protection of the network against DoS attacks through its Session Rate Limiting and MAC address filtering capabilities complimenting a centralized provisioning system.

In addition to supporting the secure Browser-based Universal Access Method, Nomadix simultaneously supports Port-based Authentication using IEEE 802.1x and authentication mechanisms used by Smart Clients by companies such as Boingo Wireless, and iPass. Nomadix products enable 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.

By allowing selective access control to the network before the customer authenticates themselves, service selection and Web based self-provisioning can be provided in a standard, efficient, low cost and convenient way that doesn't depend on the transport technology (wireless or wired). This also overcomes the limitation of not having an authentication method standardized across multiple vendors.

Billing Plan Enablement

A Nomadix-enabled network can automatically authenticate, authorize, track, and bill users for access. Users can be identified and billed according to their Media Access Control (MAC) address, username/password, and/or port identification number.

The NSE supports a wide variety of billing models enabling the deployment of profitable public access networks. Our solutions allow providers or venue owners to create billing plans using credit cards, scratch cards or that enable monthly subscriptions—then bill by a host of different parameters including time, volume, or bandwidth. Users can also be billed directly to their room bill through a Property Management Interface (PMS) in a hotel setting.

RADIUS

Nomadix offers an integrated RADIUS client with the NSE allowing the service provider to track or bill based upon 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.). Our 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.

Credit Card Billing

As an added module to the NSE, integration with on-line secure credit card based self-provisioning services are offered, allows the user to set up a credit or time based dynamic account. Also, in order to support a revenue splitting business model between access providers and service providers, an integrated Billing Mirror capability is provided that performs logging of customer's billing activities to more than one server. This allows the service provider to perform ad-hoc, pay-per-use service creation—a critical function to grow their customer bases.

XML Interface

Nomadix provides a secure XML Application Programmer's Interface (API) with the NSE allowing the AG 5600 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 via an SSL tunnel in the form of an encoded query string. The XML interface enables solution providers and integrators to customize and enhance the installations with value added capabilities and services.

Service Awareness

The NSE can drive a HTML-based window down to each customer's Internet browser providing them with the ability to self-select services and upgrade their bandwidth and billing options in real-time.

Nomadix' patented Information and Control Console (ICC) also allows the premise owner or service operator to send custom messages and advertising directly to the screen of the customer. For credit card usage, the ICC displays a dynamic "time" field to inform customers of the time remaining or expired on their account.

Advanced Security

The NSE enhances today's standards, enabling the secure deployment of large-scale public access networks, regardless of the standards supported at the client, enabling a solution that covers the wide variety of clients that will roam into the location.

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' products feature its patented 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. Additionally, the NSE allows tracking logs to support Lawful Intercept initiatives.

Policy-based Traffic Shaping

The Bandwidth Management feature is part of the NSE Core and enables 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 increase or decrease

their bandwidth by the minute—or on an hourly, daily, weekly, or monthly basis—without having to disconnect or re-establish a new session.

The AG 5600 can also manage the WAN Link traffic providing complete bandwidth management through the public access location. Bandwidth Management shapes traffic going over the WAN Link to prevent its over-utilization. The AG 5600 queues traffic from overly busy instances in time and sends the packets over the WAN Link when a lull in traffic occurs.

Advanced Roaming

Public access locations and networks powered by the NSE enable roaming users to access wireless broadband networks globally while maintaining a single billing account worldwide. The NSE allows the "network" to make an intelligent decision on how a user is authenticated and billed for access by directing them to the entity they have a pre-existing relationship through advanced NAI routing capabilities. This also allows multiple providers to service one location, further enabling the development of the Wholesale public access model.

AG 5600

The AG 5600 is a stand-alone, high performance dedicated network appliance placed at the edge of the network providing transparent connectivity, advanced security and billing enablement in large scale wired or wireless public access networks. The AG 5600 running the NSE provides the functionality needed to create an intelligent public access network supporting up to 2,000 simultaneous users allowing them to have a transparent, secure experience while enabling the provider or venue owner to extract revenue from providing the service.

AG-5600

Summary

The NSE running on the AG 5600 is specifically designed for large scale public access venues such as airports, convention centers and large hotels creating an intelligent network that allows users to receive broadband connectivity that requires no client-side software or configuration changes, then allows them to self-provision services and gain access to local content and services while integrating into the widest range of existing back-end systems for billing and authentication.