pronto
networks

Enabling the Next Wave of Connectivity

Pronto Operations Support System (OSS)

An Architecture Overview

WHITE PAPER

Introduction

This document provides Pronto's service provider customers an overview of the architecture of the Hotspot OSS™ software (Pronto OSS). The target audience of this paper is the network operations, network planning, and IT personnel in a Wi-Fi service provider's organization. This reader is expected to be familiar with the terms and concepts commonly used in discussions of Operations Support Systems (OSS).

The purpose of the Pronto OSS is to enable wireless service providers to operate their business in an effective manner, and the structure of the OSS enables the organization of these service providers to perform their various functions. The OSS is designed to provide a complete Service Management solution for an independent Wi-Fi operator, while maintaining the scalability needed for large service providers. The architecture of the OSS allows large service providers to integrate the Pronto OSS with their existing back-office systems.

Pronto's Hotspot OSS is designed to enable wireless service providers to deploy Wi-Fi services in Hotspot locations for public W-LAN services, and enterprise markets. To accomplish this design goal, the Pronto OSS provides a complete, reliable, scalable, cost effective Wireless Internet Service Provider (WISP) business solution. It provides the order fulfillment, service assurance, and billing capabilities that wireless service providers need to operate the network efficiently, and allows them to provide differentiated service management through customized location branding and unique realm-based service authentication mechanisms.

This document contains a description of the modular and extensible design of the Pronto Hotspot Networking System OSS product suite. It provides architectural information about Pronto's feature-rich software platform and its use of open interfaces and methods and how they relate to industry standard specifications from such organizations as the IEEE, the TeleManagement Forum, the World Wide Web Consortium (W3C), the Engineering Task Force (IETF), the Wi-Fi Alliance, and the WISPr group.

Architecture Overview Description

This section shows how Pronto OSS supports those businesses deploying, provisioning, and managing services over 802.11x Wi-Fi networks.

Figure 1 illustrates the functional components and the interrelationships of these components that comprise the Pronto OSS.

Each layer or functional block provides the context for individual services. These components, when viewed as a system, provide the fault, configuration, accounting, performance, and security management (FCAPS) functions that all carrier-class networking communications software systems must provide. These FCAPS applications define the interaction between the Service Management Layer and Network Management Layer.

The network-centric FCAPS functions of managing the network include providing element management functions such as device configuration, for example - configuring DHCP parameters and other IP settings, SSID values, etc. It also includes remote monitoring capabilities that provide status to NOC administrators on the health of the Wi-Fi network, along with other performance metrics that enable delivery of Service Level Agreements to Wi-Fi customers.

Figure 1 also illustrates how wireless users would access the hotspot network when they acquire a signal from an Access Controller. In a typical scenario, the Access Controller provides a browser-based authentication portal, requesting users to choose a mode of authentication and request access to the network.

The Pronto OSS, along with the embedded software in the access controller, is also designed to serve third-party client applications, such as Boingo, iPass, and GRIC. Users with third-party client applications installed on their devices (laptops, PDAs, etc.) can use these applications to provide their authentication credentials. Regardless of how users access the network, the control plane components of the Pronto OSS provides the authentication services that allow each user to log in and access the Internet.

The control plane responds to login requests by routing the user's request to the appropriate authentication service (internal AAA, external servers such as other identity servers). Control plane functions also include communicating with roaming partners to authenticate roaming clients and customers that have credentials through inter-WISP roaming agreements. Once authenticated, the user session is configured and monitored by the services in the Network Management Layer that ensure the proper quality of service, performance, fault management, etc.

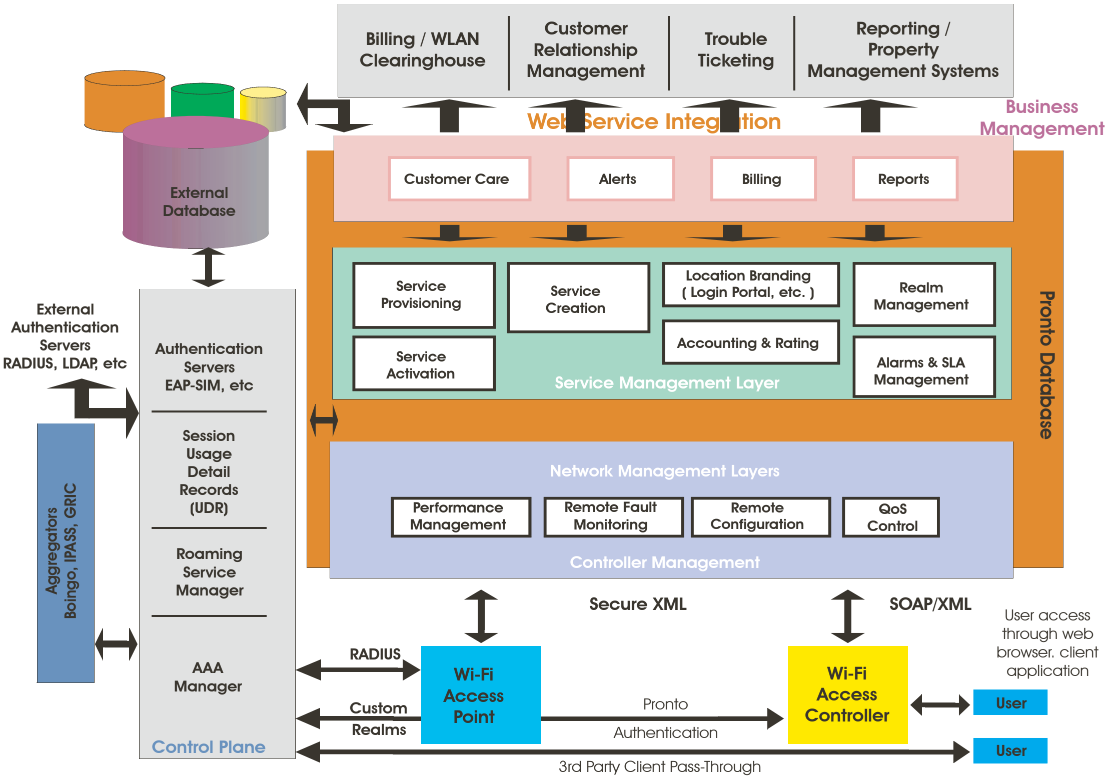

Figure 1: Software Architecture of Pronto's Hotspot OSS^{TM}

The Service Management Layer of the OSS provides capabilities for location branding and the customized login screens the users see when they launch their browser after acquiring a Wi-Fi signal. This layer then controls the network services required by a Network Operations Center (NOC) to support multiple WISPs that serve numerous franchises with far-flung locations. These unique service management capabilities assist Wi-Fi service providers in deploying hundreds of locations while providing an easy mechanism for managing the service offering. Customized location branding, and the ease of implementing a wide Hotspot deployment, fully branded for multiple WISPs, and locations, is one of the unique differentiators of the Pronto OSS and a key value-add for service providers.

Service management functionality also includes the creation of realms that facilitate differentiated modes of authentication. The Pronto OSS provides the means to combine various technologies, such as SMS messaging, RADIUS authentication, automated service registration, and account management capabilities to create unique service offerings. These capabilities allow service providers to offer differentiated Wi-Fi services. The Pronto OSS also allows for broadband wireless services to be integrated with narrowband authentication systems as well.

The Business Management layer of the OSS features applications that provide accounting, billing, alert processing, and other operations capabilities that complete the business aspects of the Wi-Fi service offering.

This layer also supports web service integration which allows internal business management applications to share information with external applications. This web service integration provides the flexibility to run internal applications or share network information with external applications. This includes capabilities such as importing authentication data records, providing access to usage records from external billing systems, etc. It also provides the framework to integrate with external SLA management and CRM systems, among others. This design allows Pronto OSS to quickly integrate with 3rd party applications.

The unique capabilities of the Pronto Hotspot Networking Solution are made possible by the embedded software capabilities in the Access Controller. Pronto Networks provides programs that allow these embedded software capabilities to be included in 3rd party access controllers. Hardware equipment manufacturers can partner with Pronto to include these capabilities to integrate the software on non-Pronto hardware platforms.

OSS Functionality

The traditional OSS model describes three layers of management: (i) the network management layer, which is responsible for network traffic management and network monitoring, (ii) the service management layer which focuses on service creation, service provisioning, service activation and other components of service fulfillment, trouble ticketing, etc. and (iii) the business management layer which provides the customer relationship capabilities that include billing, customer care, and service-level agreements. This section explores the functions that occur in each layer and describes the interfaces with other layers, the control plane, external authentication servers, and the central database.

Network Management Layer (NML)

The Network Management Layer manages the connectivity between wireless user sessions and the Internet. The OSS communicates with the Access Controller at the Public Wireless Local Area Network (P-WLAN) via SOAP/XML over a secure SSL connection. Users connect through the 802.11x interface to the Access Controllers. Users connecting via a third-party access points embedded with a Pronto agent can also interface with the Network Management Layer over secure (SSL) XML connections.

All other users (for example, Boingo, iPass, or GRIC users) have their sessions managed and monitored through these NML features. Controller and network management services consists of the OSS connecting the user to their authenticated Internet or walled garden destination. Once the user connection is set up, the OSS relinquishes traffic management control to the local routers and servers while continuing to provide the variety of services inherent to an OSS. This is a key feature of the Pronto OSS, in that all user IP traffic is sent to the Internet without backhauling it to the NOC.

The following sections describe the controller manage-

Fault Management

The Pronto OSS has fault monitoring capabilities that are designed to support OSS requirements for carrier-class operations. The OSS monitors Access Controller heartbeats from each of the locations under its purview. The internal database support of the OSS allows for extensive data gathering and record keeping.

At a time interval defined at the NOC, each Access Controller periodically sends an autonomous message to the Access Controller. Because this message is sent through the SOAP/SSL protocol exchanged between the Access Controller and the OSS, it is impervious to firewalls and dynamically obtained IP addresses that can provide configuration and monitoring challenges for the NOC personnel. These periodic messages provide valuable information related to the health of the network element, and also provides performance and service assurance information related to users connected to the controller at the location. These remote monitoring capabilities are crucial for the management of a Wi-Fi network.

When a controller status degrades below acceptable levels, and an alert has been generated for the OSS, the

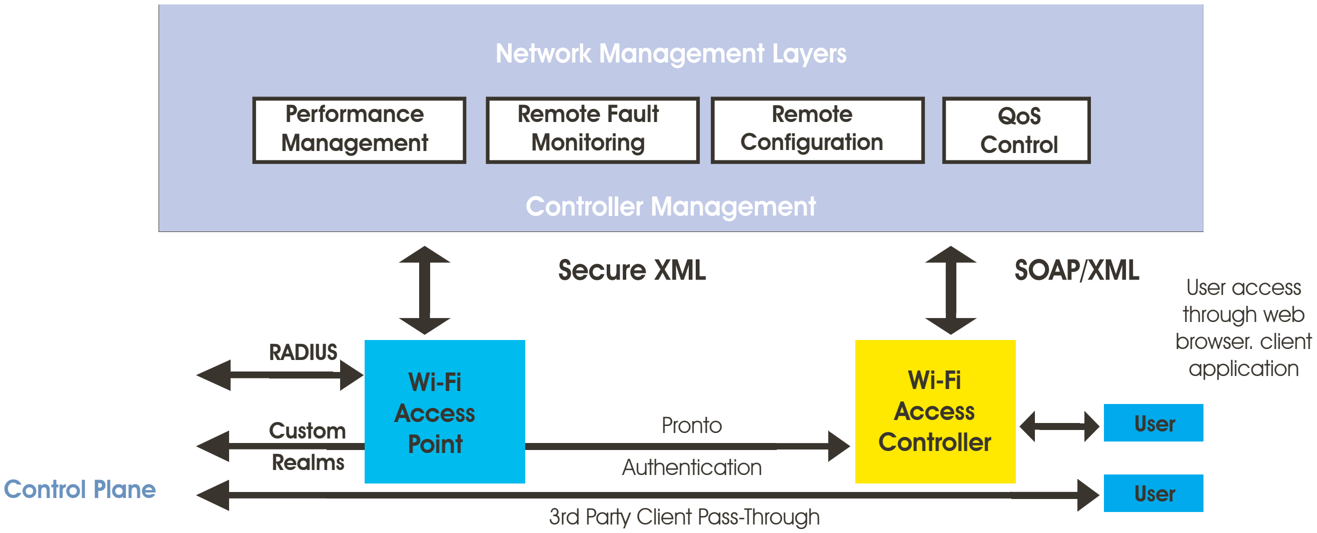

Figure 2: The Network Management Layer

OSS can respond with a message (payload) containing reboot instructions, user logoff commands, software upgrades, and the like. The OSS can also be configured to notify appropriate NOC personnel of the alert.

The design of the heartbeat/payload response cycle allows the OSS to maintain operational health for the controller regardless of the remoteness of the controller location or the local network security configuration (firewalls, etc). Finally, this mechanism also allows the Pronto OSS to monitor pure access points that may be subtending from the Access Controller at the location. Users' connectivity to these access points is also monitored at this layer of the software.

The OSS is also designed to support network management system extensions to support SNMP. This enables external management systems to perform typical enterprise management tasks on additional access points that may be subtending from the Wi-Fi Access Controller.

The NOC records heartbeats that report the status of each controller. These reports can be customized for NOC and WISP-level users with defined roles granting appropriate levels of access to view the usage levels and status of each controller over which they are responsible. Whenever a controller experiences an out-of-tolerance condition, the OSS responds by either correcting the condition directly or by notifying the appropriate technical support personnel who can respond to the condition.

Configuration Management

Network configuration management provides the flexibility to meet the varied needs of hotspot operators. The Pronto network is designed such that the only requirement for a controller to connect to the OSS is that it be able to obtain an IP address from the data network. For operators who need network devices to have static IP addresses, the controller can be configured with a static IP address. For operators relying on PPPoE, the controller can be configured to obtain its IP address using PPPoE. However, for the majority of hotspot operators, especially those with little or no network infrastructure at the hotspot location, the controller obtains its network access through DHCP, providing connectivity at a reduced cost. The common goal of this design is to achieve a high degree of reliability when the controller is connected and turned on by non-technical staff. This auto-configuration capability is essential to meeting the needs of the typical hotspot operation, and the flexibility it affords a service provider in the deployment of a Wi-Fi service makes the Pronto OSS solution unique in the marketplace.

Once the controller comes on line and connects to the OSS, the OSS downloads the appropriate configuration for that controller. This includes network settings and the service profile associated with the controller, which is centrally managed at the OSS. At this point, the controller, capable of supporting multiple SSIDs simultaneously, can start servicing the log on authentication requests from RADIUS, SIM, SMS, LDAP, MSN Passport, Boingo, iPass, and GRIC users.

In addition, during initialization, the service profiles including the location branding, white-listed sites, walled gardens, etc. are also downloaded to the controller. These service management features, allowing differentiated services, are thus provided during access controller initialization at the location.

The OSS creates a stateless network edge management environment wherein a variety of servers provides the appropriate services to edge devices (controllers). From the controller perspective, the connection is plug and play. This combination of ease of use and flexibility allows Wi-Fi deployment in environments that would otherwise not be possible or economically practical.

Performance Management

The Quality of Service (QoS) capabilities of the OSS allow WISPs to market and price bandwidth to support high-volume users, casual users, and everyone in between. Instead of being limited to a first come, first served design, hotspot operators can now manage and charge for available bandwidth.

While QoS gives the OSS a policy-based networking capability, the Pronto QoS implementation is easy to implement and simple to understand, thus providing service assurance capabilities.

Service Management Layer (SML)

This section describes the functions performed at the service management layer. These functions are defined in the context of the Telecommunication Management Forum telecommunications operation map (TMF/TOM) for each process from the network level up to the service layer. These dimensions are fulfillment, assurance, and billing (FAB). All of the

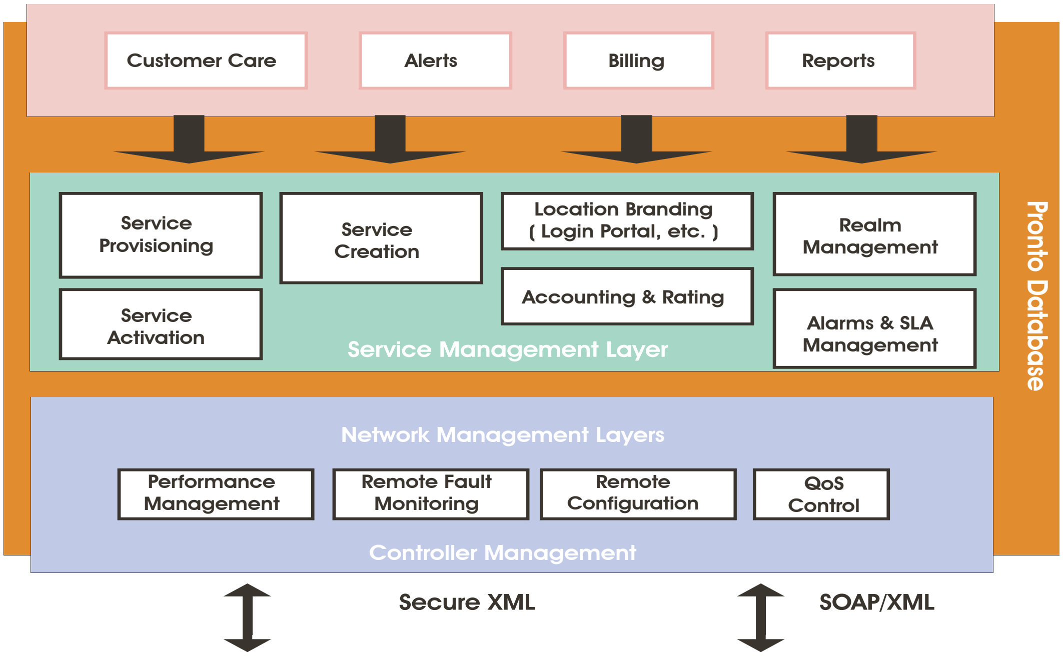

Figure 3: The Service Management Layer

interactions of the Network Management Layer to the Service Management and Business Management Layer can be categorized in terms of how they perform fulfillment, assurance, or billing functions.

The Interfaces

The service functions of the OSS map either to internal business management applications, or they can be exported via web services to external business management applications. This flexibility allows existing NOCs and WISPs to integrate applications already in place and working. It also gives emerging Wi-Fi players the opportunity to be in business without already having to own the network and necessary applications. The OSS is also designed to allow NOCs and WISPs to chose any combination of internal/external business management applications that suit their present or future needs.

The implied interface for this layer is the integration of all traffic to the internal database, which provides the ability to implement all the services available at this level.

Service Creation, Provisioning, and Activation

The Service Management Layer defines the price plans and service packages, allows users to register to use these packages, and to configure and administer services in real-time using a simple, web-based GUI.

At this level, Service Level Agreements and bandwidth throttling allow the operator to control available bandwidth in real time, adjusting to changing needs and demands for access.

SLAs can be implemented strictly or flexibly to allow users to log on even when the bandwidth they have contracted for is not available. The system allows users to logon when the full amount of bandwidth they should have is not available. The user is advised of the out-of-agreement condition and can choose to proceed based on their current needs as opposed to only being able to access the system under ideal conditions. The benefit of this flexibility serves those users who pay for service that allows them large amounts of bandwidth when they need it, but allows them to connect at other times to use the system for less bandwidth-intensive purposes. Otherwise, these users might only be able to connect under low usage conditions.

The service creation, activation, and provisioning of Wi-Fi services and the location branding services perform the fulfillment function for the service management layer.

Location Branding - Location-specific Login Portals, Walled Gardens etc.

The login portal and branding functions allows the OSS to provide unique profiles for WISPs, their franchises, and the franchises locations (and sub locations). These profiles allow for localization (specific templates and logo files) for each controller.

White listing/walled garden sites are also supported at all levels which allows the service provider to control where unauthenticated user go when they connect. This feature allows operators to provide information and advertising to casual users who might otherwise not pursue the connection.

The branding function not only allows hotspot operators to identify each controller, but to update the login page with timely content. For example, a restaurant hotspot operator can use this feature to post the menu of the day. Because each controller is brandable, a hotspot operator with multiple controllers at one location can download different screens to each controller. For example, a hotel with a controller in the registration desk area can download daily information relevant to hotel operations, while a controller adjacent to the lounge can download entertainment, menu, and other information on a daily basis.

Rating

Rating provides time-based, flat rate or volume-based rating, specification of peak and off-peak billing time, location-specific billing, and pre-paid card generation. The goal of the OSS is to enable wireless users to connect in whatever fashion meets their needs.

The rating service provides some of the billing capabilities at the service management layer.

Alarm Management

The alarm management function of the service management layer, part of the service assurance aspects of the Pronto OSS, defines classes of alarms, severity levels, required responses, and the like.

Alerts notify responsible parties of events. Alerts are generated by the system for a variety of conditions for which admins need to track or respond to. These include unresponsive controllers, log files being overwritten, and warnings of low levels of free memory or disk space. It can also include notifications of the status of the WLAN interface. OSS users can manage alerts by creating rules, which define who handles each type of alert. OSS users can manage alerts by type, severity, or by controller for equipment-based alerts.

Realm Management

The OSS provides authenticated access to the Internet (except for walled garden sites which do not require authentication). This is a fundamental service of the system which is key to network security and account management. The OSS is designed to support an ever-expanding methodology of authentication technologies including RADIUS, SMS, prepaid cards, and aggregators such as Boingo, iPass, and GRIC. As new authentication methods become available, the OSS will expand to support them. Realms reflect the numerous methods available for the creation of unique service offerings. Through this architecture, Pronto enables the creation of

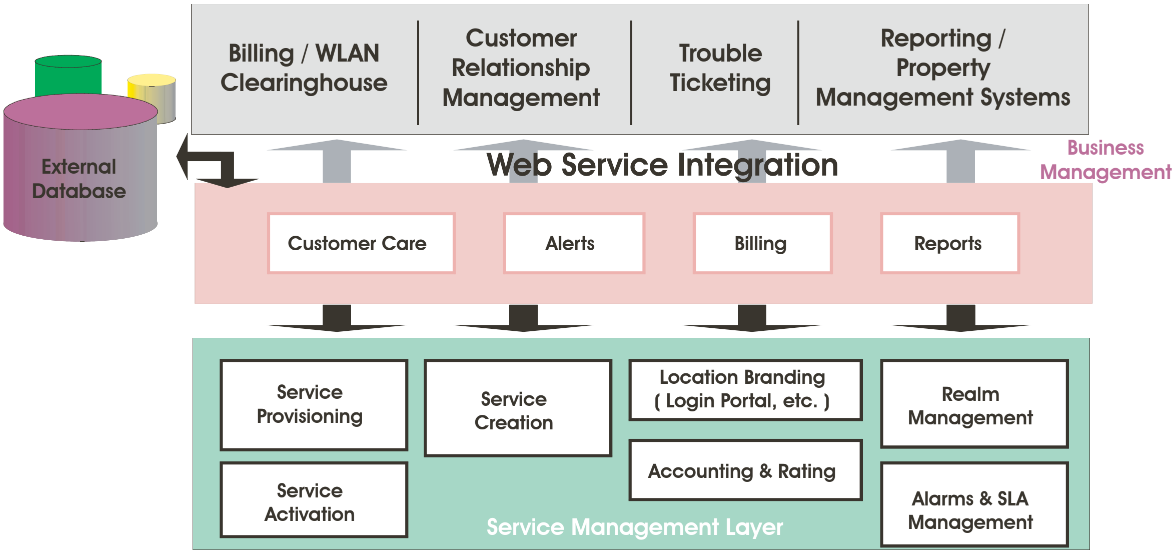

Figure 4: The internal and external business management interfaces

custom services which combine two or more authentication mechanisms, for example, a RADIUS authentication request validated with an SMS message, etc.

Business Management Layer

The Business Management Layer provides the business logic for the services generated in OSS. This layer also provides the interfaces to external applications and databases that process OSS data. This external connectivity is valuable for those OSS users who want to integrate the OSS with their own proprietary or legacy systems.

Customer Care

The customer portal is accessible by the user from the login screen. This service allows the user to perform self-provisioning, account management, and other service fulfillment tasks.

Billing

OSS includes account management tools which allow the NOC (only) to set up guest accounts, track incidents, manage and modify existing accounts, etc.

OSS accounting allows account managers to adjust account balances and even write off uncollectable accounts.

Alerts

Business management alerts deal with managing account credit limits, incident tracking and the like.

Reports

The OSS is an end-to-end system that generates logs of all transaction data and stores this in the database. This data can be used to create a wide variety of reports for the NOC, WISPs, and license usage.

Reporting allows custom billing and payment reports and roaming reports. The OSS can also process recurring as well as ad hoc fees to be charge to each WISP by the NOC and reports this information in the monthly WISP settlement statement.

The alerts and reports services perform the assurance function for the internal business management layer.

Database

The OSS database function integrates all Network, Service, and Business Management functions. Through the control plane, it also connects to external databases.

Because the database is central to all OSS activity, the potential exists for performance degradation to increase as WISP activity increases. To allow for expansion and scalability, the Pronto OSS solution incorporates load balancers to deal with uneven traffic loads. These load balancers, coupled with the integrated Oracle database, provides the architecture to support large Hotspot deployments.

The Pronto OSS database function, internal and external is integrated into every aspect of OSS activity to provide centralized data management. The database function also allows for database management services such as data mining, account management, and revenue share processing between WISPs and Managed Service Partners (MSPs) for every transaction.

The database, based on Oracle's 9i, can also be analyzed using business intelligence data-mining applications to provide useful reports to NOC administrators and network analysts.

Control Plane - The Captive Portal/Customer Portal

The Pronto OSS control plane supports user access to the system. Because Pronto allows a wide variety of user authentication methods, the control plane has to be robust enough and flexible enough to process all requests quickly and accurately. Figure 5 illustrates the interface-intense design of the control plane.

For users connecting through Pronto controllers or access points with embedded Pronto agents, the control plane performs the authentication chores and maintains the user data records for each session.

For roaming network operators, such as Boingo, iPass, etc. the control plane allows users to pass through the Pronto network infrastructure and directly obtain their aggregator-supplied applications, bypassing the Pronto web-browser based authentication process.

Roaming services allows inter-WISP roaming, and roaming support for iPass, GRIC, and Boingo as aggregators.

The control plane provides the embedded RADIUS client for access points and controllers authenticating with an external RADIUS server.

The control plane also provides 802.1X support (EAP or extensible authentication protocol, etc) for robust standards-based authentication (EAP-TLS or transparent layer security, EAP-TTLS or tunneled TLS, PEAP or protected EAP, SMS, SIM, LDAP, etc.).

Once an authentication portal is presented to the client, and the user's credentials obtained, these credentials (username / password) are verified against the appropriate database. These could be Pronto's own database, or external RADIUS, or other authentication servers defined as part of the realm chosen by the user. The AAA management components perform these functions. Session information is maintained in the database, and when the user session is terminated, a session detail record is created and maintained in the database. Depending on the service offering, a session message may be forwarded to external systems.

Web Services and APIs

The Pronto OSS supports a number of internal applications that perform customer care, billing, alert processing, and the like. There are also a number of external applications (perhaps already in use by a wireless service provider) that perform the same functions. Therefore, it is important that the OSS be able to import or export data to these external applications.

The interface between internal business management applications and external applications is made possible by a standard created by the W3C called web services. Web services are defined as programmatic interfaces made available over the World Wide Web. The interface is described using Web Services Definition Language (WSDL), the traffic is encapsulated as SOAP/XML-based messages, and the transport medium is HTTP or HTTPS.

Keep in mind that these applications interfaced through web services can use different operating systems and in fact use different programming languages. This ability to share data allows applications to be loosely coupled to achieve complex operations that individual applications could not perform. Thus relatively simple programs interacting with each other can create new and powerful services.

Figure 6 illustrates connections to various third party billing, CRM, PMS, and trouble ticketing applications that reside outside of the Pronto OSS, which has its own internal systems capable of performing these functions for some service provider deployments.

Consider what is involved in exporting internal customer records to an external billing system: The Pronto OSS creates a WSDL description of the customer record (in the database). This WSDL information is shared with

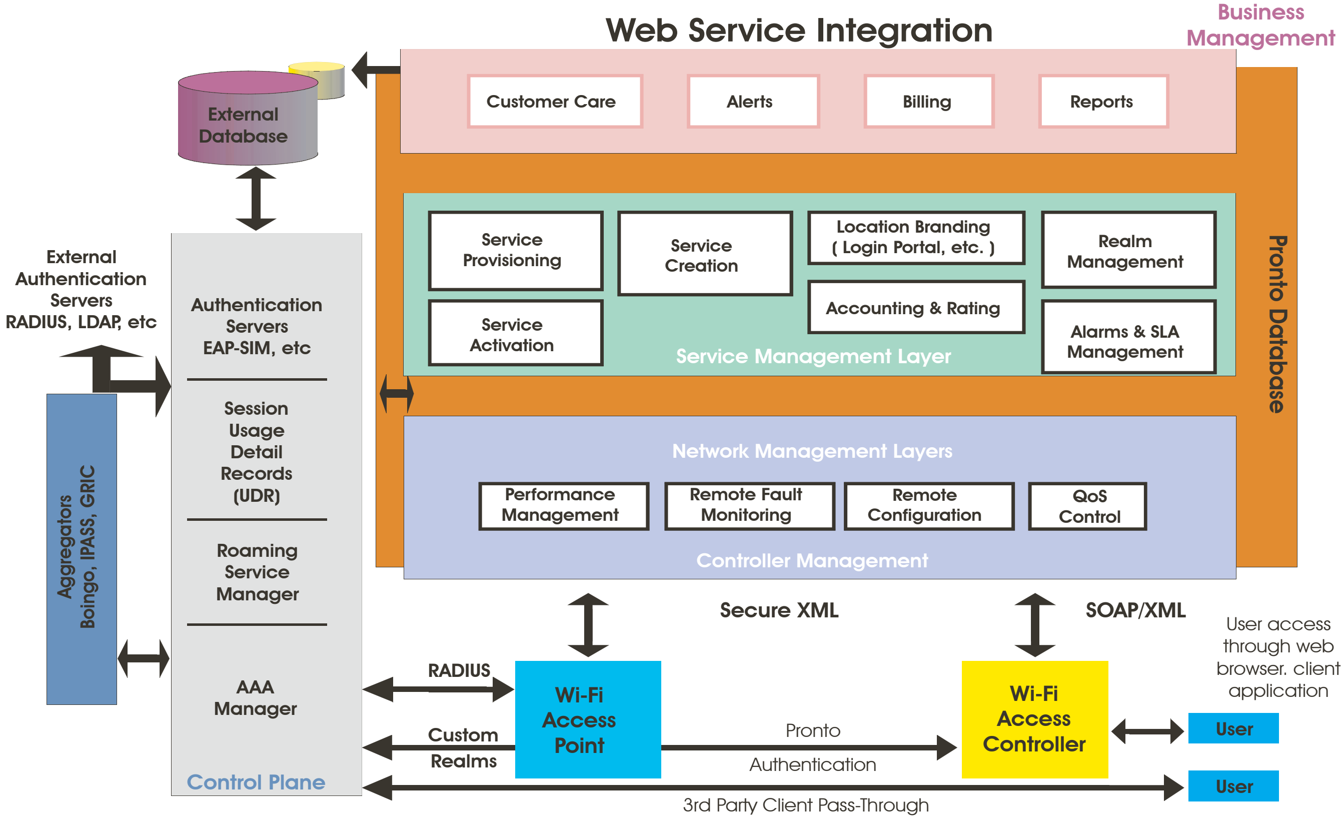

Figure 5: The control plane functionality

the external application so both applications understand how the data is structured. Acting as the web services client, the OSS responds to a request from the external application by sending these records encapsulated in SOAP/XML messages over HTTP or HTTPS.

Pronto OSS can also act as a web service server to import external information from a web service client into internal applications.

In cases involving the need to share information with external applications that do not support web services, Pronto OSS relies on application program interfaces (APIs) to exchange information.

The OSS design thus allows WISPs to import or export data with virtually any application they need.

Reporting

The reporting function allows NOCs and WISPs to gather information on usage details including service plan activity (prepaid sales and refunds), customer activity (subscription, cancellations), invoicing (details, payments, refunds), roaming settlements, etc.

Reports are structured such that NOC level reports show all the WISPs, WISP level reports only show their franchises and their locations.

The OSS supports a wide variety of reports which include:

- All details of activity from which prepaid cards have been used, to who bought them.
- Prepaid card sales (on and offline), and subscrip tion sales reports.
- Service reports show online refunds, account (new, closed, suspended, and romotional) reports.
- Revenue, billing, and payment reports show sales, refunds, generated bills, credit card actity, accounts receivable, write off, and miscellneous information.
- Settlement reports show monthly settlements, roaming usage, roaming settlement, and cost/ margin reports.
- WISP reports are a WISP-specific subset of these NOC reports, but also include a customer usage history report which shows connection details like time and amount of data sent and received.

OSS users can output reports online, print a hard copy, or export to a Excel (CSV) or PDF format.

Roaming

Roaming allows users to move from hotspot to hotspot while retaining their WISP profile (with its plans, etc.). The Pronto OSS roaming implementation integrates the interaction of a roaming settlement manager, a roaming policy manager, a roaming aggregator support manager, a roaming access manager, and a roaming server working together to provide the end user with seamless access to the Internet independent of which WISP provides the connection.

The OSS administers roaming contracts with WISPs and Managed Service Partners. Inter-WISP roaming rates can be applied on a time or data usage basis.

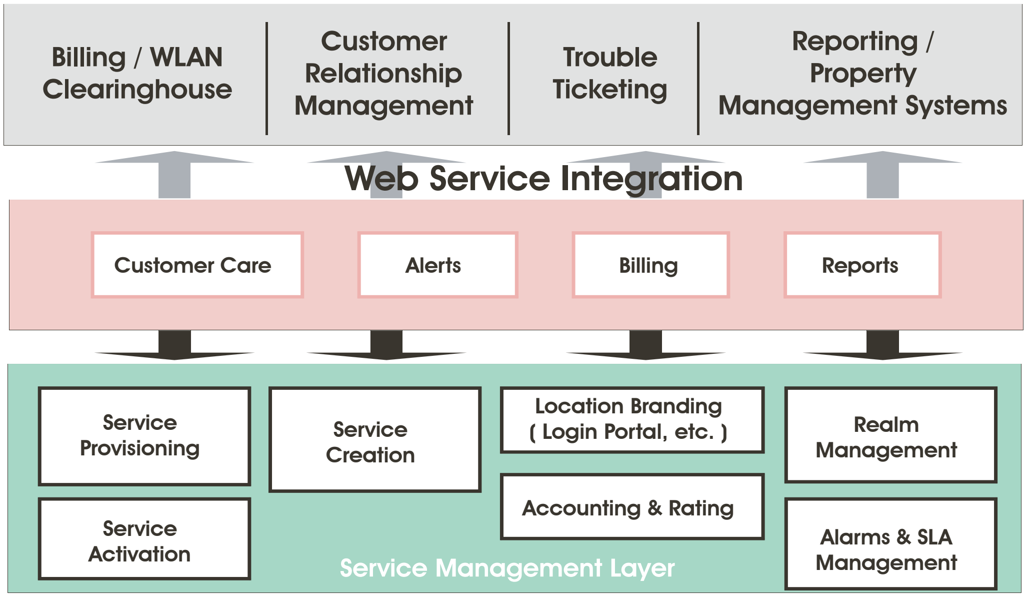

Figure 6: Using Web Services to exchange information externally

Acronyms

802.11	The family of Wireless LAN specifications (802.11a, 802.11b, 802.11g, etc.)
AP	Access Point
API	Application Program Interface
SSID	Basic Service Set Identifier (same as the controller MAC address)
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
EAP	Extensible Authentication Protocol
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
HC	Hotspot Controller
HNS	Hotspot Networking System
HTML	HyperText Markup Language
HTTPS	HyperText Transfer Protocol Secure sockets
IP	Internet Protocol
IPSec	Internet Protocol Security
IEEE	Institute of Electrical and ElectronicsEngineers
JAAS	Java Authentication and Authorization
LAN	Local Area Network
MIB	Management Information Base
MSN	Microsoft Network
NAT	Network Address Translation
NMS	Network Management System
NOC	Network Operations Center
OA&M	Operations, Administration & Maintenance
OSS	Operations Support System (preferred) also Operating Support System and Operation Support System
QoS	Quality of Service
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial In User Service
SIM	Subscriber Identify Module
SMS	Short Message Service
SOAP	Simple Object Access Protocol
SS7	Signaling System 7
SSID	Service Set Identifier (wireless LAN ID) Same as Net+ID or ESS
SSL	Secure Socket Layer
TMF	Telecommunications Management Forum
TOM	Telecommunications Operation Map (created by the TMF)
Wi-Fi	Wireless Fidelity
WISP	Wireless Internet Service Provider
WLAN	Wireless LAN
WSDL	Web Services Definition Language

Pronto Networks
Corporate Headquarters
4637 Chabot Drive, Suite 350
Pleasanton, CA 94588
925 227 5500

For more information:
www.prontonetworks.com
info@prontonetworks.com