The widespread availability of Wi-Fi-enabled devices combined with the ubiquity of Wi-Fi hotspots represents a significant business opportunity for service providers — one that can help them complement existing mobile broadband services, distribute traffic intelligently across licensed and unlicensed spectrum, and improve the customer experience by providing choice and ensuring the same high-quality experience regardless of access type.

Given the strategic importance of Wi-Fi for data growth strategies, a proven, carrier-grade solution for getting customers onto the network quickly and securely is a must. While there are legacy Wi-Fi authentication solutions available, most were designed to handle enterprise Wi-Fi requirements and do not support the scale and performance required to support tens of millions of subscribers. Beyond scale and performance considerations, service providers need a Wi-Fi control platform that can be easily extended to support dynamic, real-time controls for introducing innovative services, such as Premium Wi-Fi.

The Amdocs Wi-Fi Control solution enables service providers to roll out Wi-Fi services to their customers quickly and cost-effectively by providing secure, carrier-grade network control functions, including: authentication, authorization, and accounting (AAA) functions for ensuring a transparent and secure single-sign on experience; real-time policy control for supporting innovative Wi-Fi services for data monetization; and 3G/4G offload capabilities for distributing traffic across mobile and Wi-Fi networks. The Amdocs solution also supports Wi-Fi roaming controls, a key capability as service providers look to extend the reach of their Wi-Fi coverage through strategic partnerships.

Why Wi-Fi for Mobile Service Providers?

• Provide customers with flexibility, convenience and choice on all their devices — while ensuring a high-quality experience across all access networks
• Leverage unlicensed Wi-Fi spectrum to manage mobile network capacity and enable innovative new Wi-Fi services
• Increase subscriber loyalty and satisfaction by providing multiple convenient options for access
• Offer greater customer value and gain greater share of subscriber wallet through innovative service offerings
Solution Architecture

Network control functions, such as AAA, policy control and subscriber data management, are business-critical carrier functions that provide subscribers with fast, efficient and secure access to data networks and services. The Amdocs Wi-Fi Control solution provides the flexible underlying network control infrastructure required to support scalable, high-performance Wi-Fi services targeting consumer and enterprise markets alike.

The solution includes the Amdocs Service Controller, the Amdocs Subscriber Data broker, and the Amdocs Policy Controller, which provide end-to-end security for Wi-Fi network access, QoS prioritization, usage metering, and the ability to manage a common set of subscriber entitlements.

Amdocs Service Controller

The Amdocs Service Controller is the industry’s leading service control product, proven in more than 150 service provider deployments globally. The most scalable and robust solution of its kind, the Service Controller supports secure network access control, including authentication, authorization, and accounting (AAA) for devices and subscribers across multiple access networks, including fixed, 3G, 4G and Wi-Fi. The Service Controller supports an extensive set of authentication methods and protocols to ensure support for a full range of devices and diverse network environments.

Amdocs Subscriber Data Broker

The Amdocs Wi-Fi Control solution is anchored by the Amdocs Subscriber Data Broker™, a carrier-grade, subscriber and device identity management solution. It combines the ability to manage a wealth of subscriber and device data, such as location, security entitlements, profile and usage, with the sophisticated tools to broker that data to multiple systems and applications.

Why Amdocs for Wi-Fi Control?

- Best-of-breed service provider pedigree - industry’s leading multi-access AAA solution proven in more than 150 service provider deployments, across fixed, Wi-Fi, 3G and 4G access networks and supporting an extensive set of authentication methods
- Extensive interoperability with leading Wi-Fi vendors and devices (including, access points, wireless access gateways, and security gateways) to reduce time to market and deployment costs
- Support for roaming between partner hotspots. Subscriber authentication information can be proxied from partner networks and centrally authenticated
- Supports flexible policy-driven access control decisions aligned with subscriber entitlements, dynamic state, device type, location, and other parameters
- Carrier-grade performance and scalability — from 5000 to 100M+ subscribers and devices
- Deployable in weeks — ensuring critical time-to-market advantage
Amdocs Policy Controller

The Amdocs Policy Controller is a highly flexible and scalable policy server designed to help manage the impact of mobile data growth in fixed and mobile networks and give network operators the real-time controls they need to offer innovative new services for data monetization. In the Amdocs Wi-Fi Control solution, the Policy Controller is the engine that drives Wi-Fi service innovation. Key real-time policy controls include:

- Metering subscriber usage flexibly based on multiple criteria, including volume, time and application
- Applying dynamic QoS changes on a per-subscriber basis
- Improving customer transparency with real-time notifications

These controls can be used to support innovative use cases for Wi-Fi, including premium Wi-Fi services based on quality of service (QoS), day passes based on time or volume, and application-based services.

Features and Benefits

- **Policy Engine:** Flexible network, service, subscriber and device policies can be defined at many levels of granularity including domains, user or device groups, individuals, wholesale, enterprise and consumers.
- **Multiple Extensible Authentication Protocols (EAP):** Broad and flexible security policy support, ensuring secure network attachment.
- **Wi-Fi Roaming Support:** Enables broad Wi-Fi coverage by supporting Wi-Fi roaming between partner hotspots. Subscriber authentication information can be proxied from partner networks and centrally authenticated.
- **Enforcement Point Support:** Enables policy rules to be executed on many different types of enforcement points, including wireless access gateways (WAG), DPIs, and optimization servers.
- **Dynamic Mid-session Modifications:** Provides granular policy controls that can be applied in real time on a per-subscriber and per-session basis to enable innovative new Wi-Fi services.
- **Push-and-Pull Policy Decision Point (PDP):** Allows subscriber and device entitlements to be managed and enforced through profile-associated attributes and credentials including security, QoS, location and subscriber, and device entitlements.
- **Real-time Session Management:** Provides mobility, roaming, security, and usage tracking.
- **Multiprotocol:** Dual RADIUS and Diameter support.
- **Intelligent RADIUS Proxy:** Minimizes the operational impact of non-performing proxy targets.
- **Centralized Subscriber Management:** The Amdocs Subscriber Data Broker provides the foundation for differentiated services, hierarchical subscriber and device administration, and granular, profile-based control of subscriber and device entitlements.
- **Deployment Architecture Options:** High availability, database replication, system redundancy, and application decoupling.
- **Hierarchical Device Modeling:** Allows flexible grouping of similar devices, and provides extensive scalability and the ability to support complex hierarchical groups of similar devices based on entitlements and requirements.
Wi-Fi Authentication — How It Works
1. User connects to service provider Wi-Fi access point using a Wi-Fi-enabled smartphone.
2. The Wireless Access Gateway (WAG) sends the authentication request to the Amdocs Service Controller.
3. Service Controller retrieves authentication vectors from the HLR to authenticate the user and caches these vectors for fast.
4. Service Controller retrieves a WLAN profile from the Subscriber Data Broker to assign a QoS profile.
5. Service Controller authorizes the user based on service entitlements.
6. User is allowed on Wi-Fi network.

Wi-Fi Premium Services — How It Works
1. A subscriber with a Premium Wi-Fi plan accesses the network using a tablet. The subscriber’s Wi-Fi plan includes 5 GB of data usage per month with a guaranteed speed of 7 Mbps.
2. Wireless Access Gateway (WAG) sends an authentication request to Amdocs Service Controller (AAA).
3. Service Controller retrieves authentication vectors from the HLR to authenticate the user and caches these vectors for fast re-authentication.
4. Service Controller retrieves a WLAN profile from the Subscriber Data Broker to assign a QoS profile that meets the user’s plan.
5. Service Controller authorizes the user based on service entitlements.
6. Policy Controller begins metering the subscriber’s monthly usage via the Gx interface to the WAG.
Wi-Fi Offload — How It Works

1. The subscriber device is connected on the 3G network.
2. The device detects a Wi-Fi network.
3. The Security Gateway sends an authentication request to the Authentication, Authorization and Accounting function (AAA).
4. The AAA retrieves authentication vectors from the HLR to authenticate the user; It caches authentication vectors for fast re-authentication.
5. The AAA retrieves a WLAN profile from the Subscriber Data Store to assign a QoS profile.
6. The AAA authenticates the user against service entitlements from the HLR.
7. The subscriber connects to the Wi-Fi network transparently without having to log in separately.

Standards Support

**Authentication and authorization accounting administration**
- RADIUS - RFC 2866 (RADIUS)
- RFC 2868 (RADIUS Attributes for Tunnel Protocol Support)
- RFC 3576 (RADIUS Dynamic Authorization Extensions)
- Draft RFC for PPTP/L2TP Tunneling via RADIUS
- Multiple configurable virtual server architecture (VSA) definitions for simultaneous support in a multi-vendor architecture

**Diameter**
- RFC 3588 (Diameter Base Protocol)
- RFC 4005 (NASreq)
- RFC 4072 (Diameter EAP Application)
- RFC 4006 (Diameter Credit Control Application (DCCA))

**Accounting**
- RFC 2866 (RADIUS Accounting)
- RFC 2867 (RADIUS Accounting Modifications for Tunnel Protocol Support)
- RFC 2868 (RADIUS Attributes for Tunnel Protocol Support)
- RFC 2869 (RADIUS Extensions)

**Administration**
- Command line interface and GUI for Windows 2000, XP, or better
- Web-based corporate manager and user self-administration (IE 5.0 or Netscape Navigator 6.0 or higher)
- APIs for OSS/BSS integration

**3GPP/ETSI**
- TS 29.061 (PLMN–PDN Interworking)
- TS 23.234 R7 (WLAN Interworking)
- TS 32.299 (Diameter charging applications)
3GPP2
- X.S0011-D v1.0 (CDMA2000 Wireless IP)
- X.S0028-100-0 (WLAN Interworking) IETF
- RFC 821 (SMTP)
- RFC 822 (ARPA text)
- RFC 959 (FTP)
- RFC 1939 (POP v3)
- RFC 2068 (HTTP v1.1)
- RFC 2251 (LDAP v3)
- RFC 2548 (MS RADIUS Attributes)
- RFC 2617 (HTTP Basic and Digest Access Authentication)

EAP
- EAP-MD5 (RFC 3748–Simple CHAP)
- LEAP (Proprietary Cisco wireless support)
- PEAP (PEAPv0/EAP–MSCHAPv2)
- EAP-TLS (RFC 2716–Transport Layer Security)
- EAP-TTLS (EAP–Tunneled Transport Layer Security)
- EAP-SIM (RFC 4186-EAP Method for GSM for Mobile Communications Subscriber Identity Modules)
- EAP-AKA (RFC 4187–3G Authentication and Key Agreement)

SNMP
- RADIUS Authentication Client MIB (RFC 2618)
- RADIUS Authentication Server MIB (RFC 2619)
- RADIUS Accounting Client MIB (RFC 2620)
- RADIUS Accounting Server MIB (RFC 2621)

Technical Specifications

Operating System Support
- Linux Red Hat (RHEL 5.4 x86 64-bit)
- Solaris 10

Hardware Support
- Oracle’s Sun T2-based hardware
- IBM x3650 M3
- IBM HS22 Servers in BCH chassis
- Cisco UCS C210 M Series
- Cisco UCS B-Series Blade Servers in UCS 5100 Series Blade Server Chassis