MIRACLE
SOFTWARE SYSTEMS

LAYER 7
TECHNOLOGIES
a CA Technologies company

Sreevidhya Poola
Sumavarsha Padamuthamu
Geetha Madhuri Gadamboyina
APIM Developer
Miracle Software Systems, Inc.

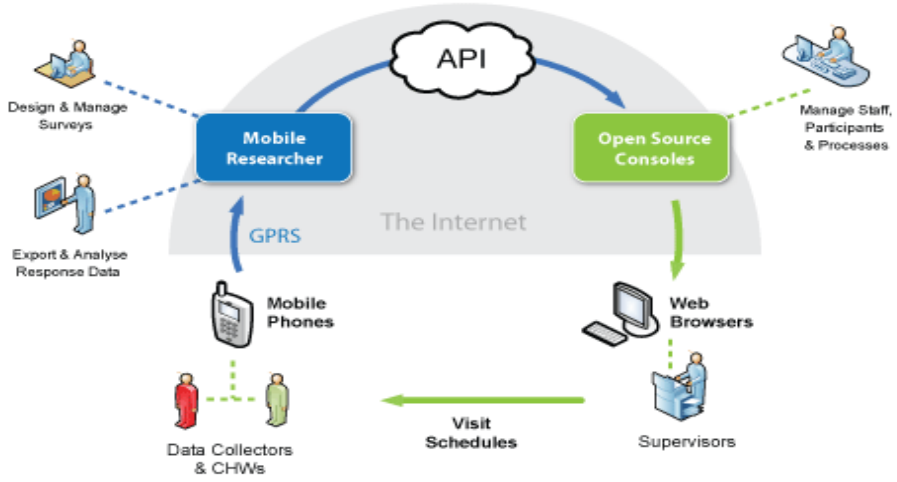
INDEX

APPLICATION PROGRAMMING INTERFACE (API):

An application programming interface (**API**) is a set of routines, protocols, and tools for building software and applications.

It is an architecture that makes it easy for one application to **consume** capabilities or data from another application.

APIs enable developers to easily access and reuse application logic built by other developers. Application developers call API functions and use them by defined protocols like REST and SOAP architectural styles.



API MANAGEMENT (API M):

API Management is the process of publishing, promoting and overseeing application programming interfaces (**APIs**) in a secure, scalable environment. It also includes the creation of end user support resources that define and document the **API**.

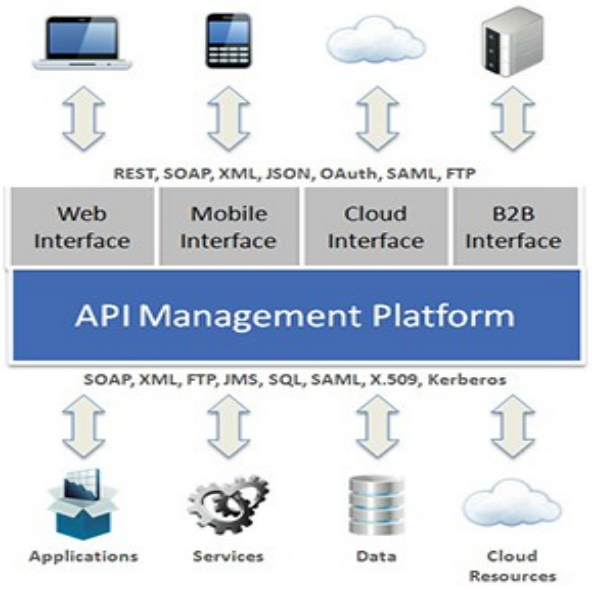
The goal of API management is to allow an organization that publishes an API to monitor the interface's life cycle and make sure the needs of developers and applications using the API are being met.

API management software tools typically provide the following functions:

1. Automate and control connections between an API and the applications that use it.
2. Ensure consistency between multiple API implementations and versions.

3.Monitor traffic from individual apps.

4.Provide memory management and caching mechanisms to improve application performance.



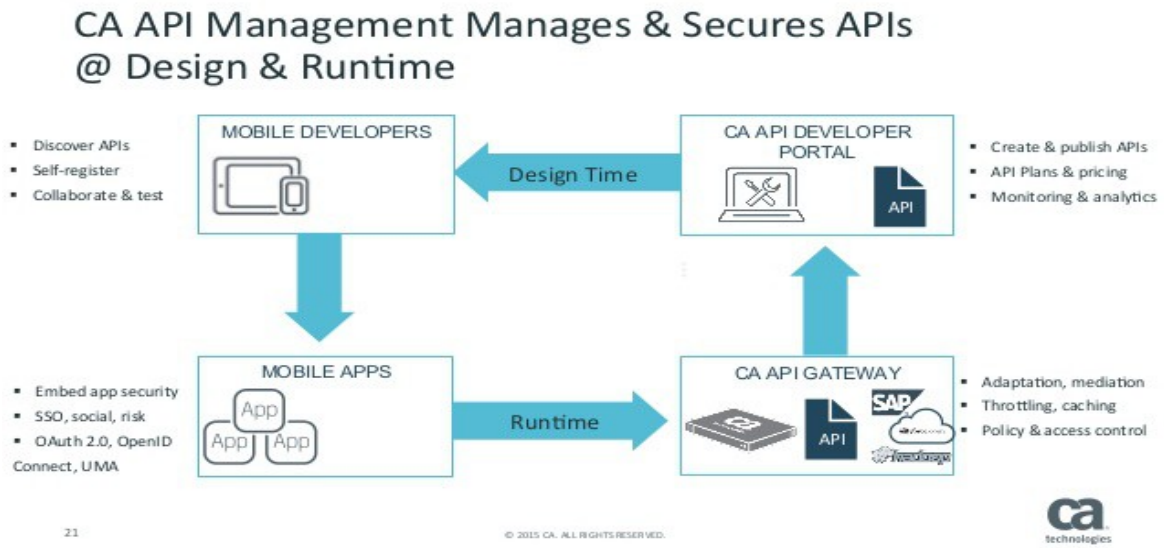
LAYER7 API MANAGEMENT

- It is also called CA API Management.
- LAYER7 is the top most platform used in API Management.
- The acquisition of layer7 will enable CA technologies to manage and secure the API
- Layer7 technologies provide secure integration technology that enable hybrid enterprise.
- Their services range from integration, security management, performance management, mobile API gateways, mobile optimization and developer portals. CA's support for mobile applications.

APIs are the building blocks of digital transformation:-

To compete successfully and thrive today, enterprises across every industry need to transform. This process is not just about incremental improvement, but about evolving core businesses to meet the demands of today's connected world. CA API Management accelerates this digital transformation by providing the capabilities you need to bring systems together, secure these integrations, deliver better customer experiences faster and capitalize on new opportunities.

Reference link: http://www.ca.com/us/products/api-management.html



Create APIs and integrate everything:-

Digital initiatives based on APIs are all about providing scalable, reliable connectivity between data, people, apps and devices. CA API Management helps you solve the challenge of integrating systems, adapting services, orchestrating data and rapidly creating modern, enterprise-grade APIs from different sources.

Reference link: http://www.ca.com/us/products/api-management.html

Secure the open enterprise:-

Today's open enterprises must be secured completely, from the app to the API—without getting in the way of a streamlined user experience. CA API Management offers trusted, consistent and repeatable security when integrating across apps, devices and businesses.

Reference link: http://www.ca.com/us/products/api-management.html

Accelerate mobile and IoT development:-

Web, mobile and IoT applications must be delivered faster and more efficiently than ever before. CA API Management provides the capabilities and tools needed to streamline development and reduce app time-to-market.

Reference link: http://www.ca.com/us/products/api-management.html

Unlock the value of data :-

API-based ecosystems can help you reach new customers, develop new products and create new revenue channels. CA API Management provides a foundation for these efforts with robust analytics, monetization and developer enablement features.

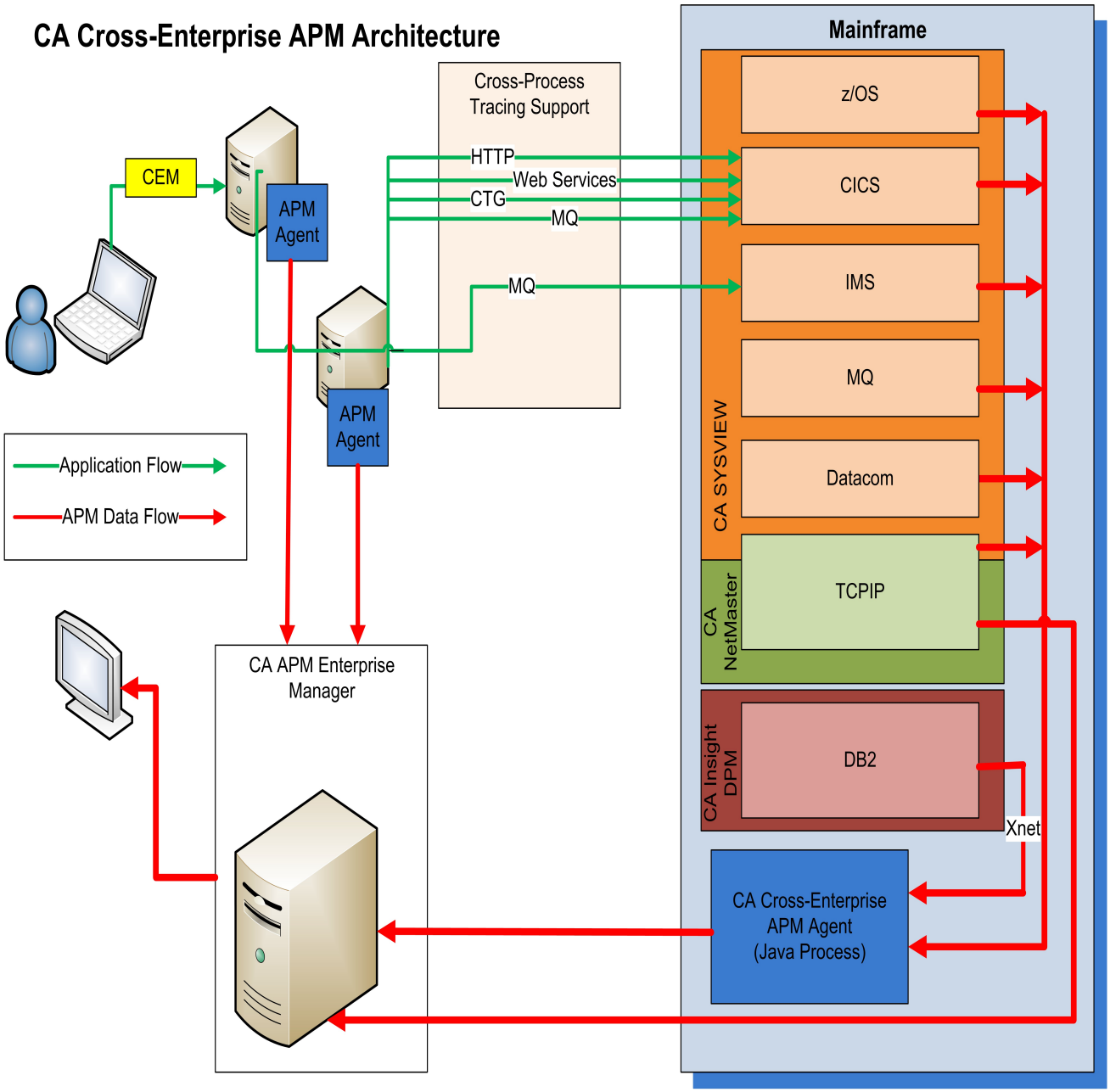
Reference link: http://www.ca.com/us/products/api-management.html

ARCHITECTURE OF CA API MANAGEMENT

CA Cross-Enterprise Application Performance Management (CA Cross-Enterprise APM) architecture looks like the following diagram. The diagram illustrates how each component connects to the other components. On each monitored z/OS system, one or more of the following software is running

- CA SYSVIEW® Performance Management (CA SYSVIEW) (requires the agent)
- CA Insight™ Database Performance Monitor for DB2 for z/OS (CA Insight DPM) (requires the agent)
- CA NetMaster® Network Management for TCP/IP (CA NetMaster NM for TCP/IP) (does *not* require the agent)

CA Cross-Enterprise APM Architecture



The agent allows the tracing of transactions across the multiple tiers of an application that invokes transactions on the mainframe. These components are:

- HTTP calls into CICS
- Web Services calls into CICS
- CICS Transaction Gateway (CTG) using channels invoking the CICS transactions
- WebSphere MQ Series messages sent to CICS or IMS transactions, which the mainframe transaction retrieves

On the mainframe, CA Cross-Enterprise APM Agent collects information for analysis from the following product components:

- z/OS
- CICS
- IMS
- WebSphere MQ
- CA Datacom®/DB
- DB2

These collections are done using CA SYSVIEW and CA Insight DPM.

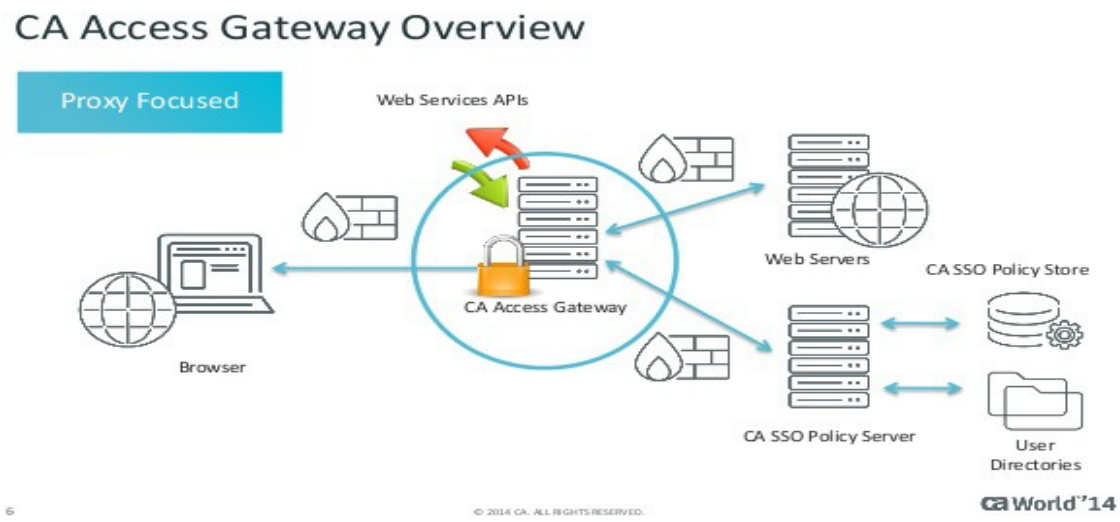
Xnet (Execution Manager Network) provides a communications subsystem that CA Database Management Solutions for DB2 for z/OS shares. Xnet executes as a started task between CA Insight DPM and other CA products. Xnet is required for CA Cross-Enterprise APM to interface with CA Insight DPM to collect DB2 information.

CA NetMaster NM for TCP/IP allows information to be collected for TCP/IP.

PRODUCTS OF LAYER7

CA API GATEWAY:-

Expose, secure and manage backend applications, network systems or infrastructure via APIs:-



The industry-leading family of API gateways from CA Technologies offers unmatched flexibility, performance and security. Building on the foundation of its industry-leading SOA application gateway technology for exposing, securing and managing backend applications, network systems or infrastructure via APIs, CA Technologies has added critical mobile, cloud and REST composition features. With this additional functionality, CA API Gateways represent the best available solution for enterprises looking to open data and services to partners, developers, mobile apps, cloud services

and smart devices. All CA API Gateways are available in hardware, virtual appliance, software and Amazon Machine Image form factors.

Reference link: http://www.ca.com/us/products/ca-api-gateway.html

CA API MOBILE GATEWAY:-

Simplify the process of adapting internal data, application functionality and security infrastructure for mobile use:

CA Mobile API Gateway is a low-latency middleware appliance that provides a central point for controlling enterprise policies that secure and manage information assets exposed via mobile-friendly APIs. It helps solve mobile-specific challenges around API composition, security, identity, adaptation, optimization and integration.

The CA Mobile API Gateway is designed to help your enterprise create apps that support bring-your-own-device (BYOD), enable innovative business strategies and leverage the Internet of Things (IoT). And it provides a manageable system for exposing backend data and application functionality in formats that can easily be consumed by mobile developers as well as the apps they create.

Read more at http://www.ca.com/us/products/ca-mobile-api-gateway.html

CA API DEVELOPER PORTAL:-

Gain maximum value from APIs by establishing a complete, secure platform for developer onboarding, engagement and management:-

CA API Developer Portal simplifies API discovery for developers and provides them with access to enterprise data so they can get to building apps fast. In the portal you can manage developer registration and API consumption through business plans and packages which can be monetized. Developers can engage with interactive development and educational tools including an API catalog, sample applications, mobile device SDKs and code generation—all designed to help streamline the development process.

Reference link: http://www.ca.com/us/products/ca-api-developer-portal.html

SaaS FROM CA TECHNOLOGIES:

SaaS solutions from CA implement security measures at all layers of the deployed architecture and service to meet the increasingly stringent service security objectives that customers require of their cloud services. The following broad topics provide more information on the security features

implemented SaaS from CA:

• Secure data center

• Certification and compliance

Secure Data Center

CA Technologies SaaS solutions are delivered from data centers that exceed Tier III standards as measured by the Uptime Institute (**http://uptimeinstitute.com**). Our facilities and control processes have been engineered to meet or exceed typical large enterprise standards, ensuring availability and security.

SOLUTION BRIEF: CA SOFTWARE-AS-A-SERVICE (SAAS)

The key benefits of our SaaS data centers are:

• Security

— Physical security and Closed Circuit TV (CCTV) monitoring

— 128 Bit or higher Secure Socket Layer (SSL) encryption

— Fully managed firewalls and Intrusion Detection Systems (IDS)

— Ongoing security management and policy enforcement

• Reliability and availability

— Redundant, multi-homed tier 1 network connectivity

— Redundant switching, routing and load balancing

— Redundant Uninterrupted Power Supply (UPS) systems and generators

— Geographically distributed data centers

Secure data center facilities

Data center premises are secured using a number of defined controls and processes:

- Data centers are monitored and recorded using CCTV systems
- All access points are controlled by people or by entry/exit systems
- Facilities are staffed around the clock by security officers
- Authorized visitors are screened and escorted to locations as authorized

Data center power and environment

Our SaaS data center facilities are carefully selected and then environments are closely monitored to maintain optimal performance of our computing resources:

- Controls provide appropriate levels of airflow, temperature and humidity
- Redundant UPS and generator backups are available for all systems
- Heating Ventilation and Air Conditioning (HVAC) systems are made available and configured for redundancy to ensure environment conditions do not fail

SOLUTION BRIEF: CA SOFTWARE-AS-A-SERVICE (SAAS)

Fire detection and suppression

To guard against the potential damage of fires, our SaaS data centers are equipped with these following capabilities:

- Multi-zoned fire suppression systems that will only discharge according to specific fire alarm locations from where the fire occurs
- Monitors are employed to sample air and provide alarms prior to pressurization
- Dual alarm activation is setup for required water pressurization

Staff vetting and management

SaaS solutions from CA along with our third party data center providers perform background checks on full-time and part-time employees before they are employed. These checks cover the areas of credit, criminal record and general background information, including former address, alias and education. Background screening includes at least the following:

- Two full reference verifications
- A five year county criminal check
- Social security number verification (applicable to US data centers only)

Security training

Education is a key part of a solid protection framework. Consequently, all employees working on customer data are required to take additional security training based on Information Technology Infrastructure Library (ITIL) v3, as well as the standard CA Technologies training curriculum.

Additionally, the signing of confidentiality and non-disclosure agreements (NDA) are conditions of employment at CA Technologies and the third party vendors.

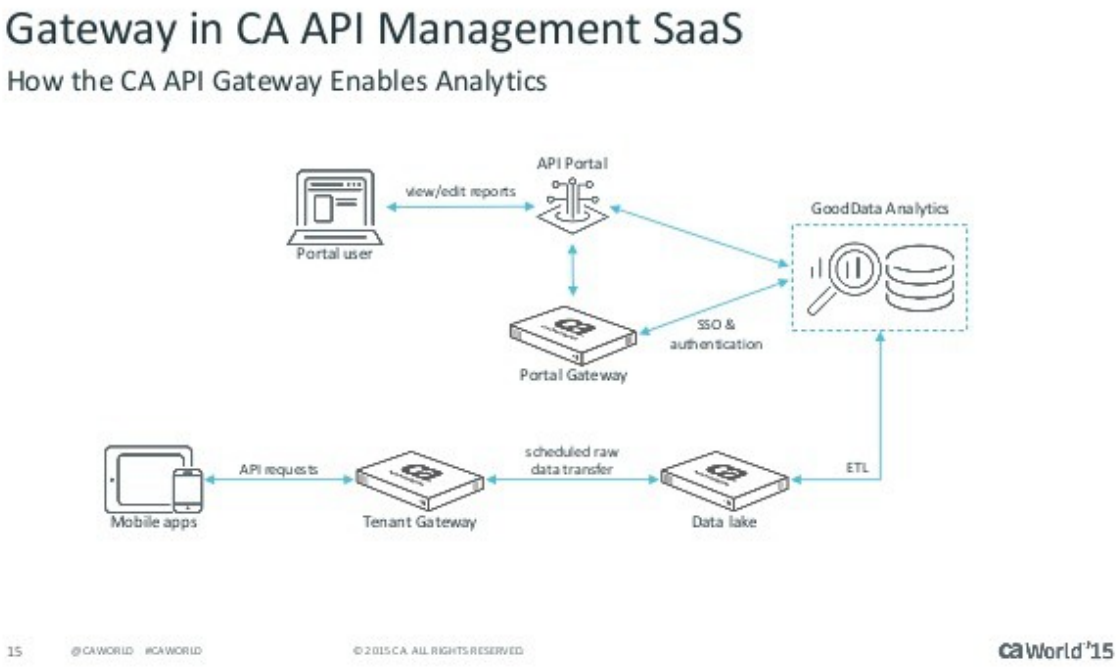
Certification and Compliance

At CA Technologies, we understand that security is a top concern when evaluating cloud-based applications, which is why our SaaS operations worldwide conform to rigorous certification,compliance and security programs and processes. In addition, we contract with independent auditors to regularly evaluate and validate the security of our service. High risks are identified, validated and remediated before production systems are made available to paying customers. Medium risks are evaluated and resolved on a priority basis keeping customer concerns in mind.

The following are the important certification and compliance standards our SaaS solutions comply with when providing cloud-based services:

- Statement on Standards for Attestation Engagements No.16 (SSAE 16)

• Payment Card Industry (PCI) Data Security Standard (DSS), where applicable
• Federal Risk and Authorization Management Program (FedRAMP), where applicable
• Safe Harbor



COMPONENTS OF LAYER7

API Gateway

An API Gateway is a networking component (either hardware or virtual)

The API Management functionality required of a Gateway will vary depending on the specific architectural layers it supports but is likely to include features for:

- **Security –** Protecting exposed backend systems against attack and hijack

- **Performance –** Maximizing API and client app efficiency and minimizing downtime
- **Data transformation–** Converting backend systems into API and app-friendly formats
- **Orchestration –** Composing new APIs from multiple backend resources
- **Logging –** Recording message-based events for analysis and auditing

An API Gateway supports layered API architecture by providing a central point to which these kinds of API Management functionality can be abstracted, away from the interface implementation as such.

Abstracting key API functionality out to the Gateway removes the need to build this functionality into each new API, making the processes of API design, implementation and management considerably simpler and more consistent.

A key advantage of this approach is "loose coupling" between exposed resources and client applications. Each API call must pass through every architectural layer encapsulated by the Gateway before reaching the interface, so resources and apps do not interact directly.

Aside from its security benefits, loose coupling simplifies the entire process of API design, implementation and management by providing a place for data transformation, where messages can be translated between backend, API and app formats and protocols.

Again, centralization is the key – legacy backend systems do not need to be updated and APIs do not need to be designed with every potential client platform in mind. The Gateway provides a central data transformation point through which all traffic is translated to the required protocol or format.

Centralization creates various other benefits for architects managing API programs, including:

- Providing a place for applying a consistent set of API Management policies
- Minimizing the amount of code and infrastructural components to be supported
-

APIPORTAL

As discussed in API Design Lesson 102: The Developer Experience, one of the keys to a successful API program is making sure client application developers can quickly and easily leverage APIs to create apps that offer something of real value.

While an API Gateway will support most of the architectural functionality required for composing, implementing and managing APIs, it cannot entirely satisfy the requirement to engage and enable client app developers.

API publishers also need ways to engage, onboard, educate and manage developers – whether these developers are inside or outside the API-owning organization itself. This will generally mean delivering registration services, documentation, analytics and other resources.

The best way to make these resources available to developers is via a purpose-built Web site – usually referred to as a "developer portal" or "API Portal". A full-featured portal will offer a range of functionality for developers and API owners, including:

- **Discovery –** Making it simple for developers to find and learn about APIs
- **Onboarding –** Allowing developers to sign-up for owner-denied API usage plans

- **Education –** Providing developers with the information they need to make use of APIs
- **Examples –** Illustrating functionality with sample applications and code fragments
- **Community –** Enabling developers to share best practices via forums
- **Analytics –** Delivering insight into API and app usage and performance

An API Portal may be built entirely in-house or based on one of several available white-label portal solutions. Building a portal in-house allows complete control over site functionality as well as look-and-feel. However, it can also lead to a great deal of development overhead.

Luckily, the API Portal market is now mature enough to include providing solutions that offer a broad range of customization options. Furthermore, a white-label portal solution can often be delivered fully integrated with an API Gateway.

- Together a Gateway and Portal significantly simplify the process of managing APIs and developers in order to minimize integration costs, maintain the secure functioning of backend systems and facilitate the creation of truly valuable client applications.

These components are powerful individually but are especially useful when they are integrated to work together.

Layer 7 Solves the Mobile Enterprise App Challenge

From the two sides of the globe, CA Technologies -- owner of the Layer 7 API Management Suite-- has announced new API services aimed at providing developers and enterprises with a full mobile suite platform. At DeveloperWeek in San Francisco, Dana Crane, senior product manager at CA Technologies, launched the General Availability of the API Portal; at Mobile World Congress in Barcelona, Dimitri Sirota, Layer 7 cofounder, talked to *Programmable Web* about the launch of the API Gateway.

We have had these products available for some time, but we are now making them General Availability and launching them as an enterprise mobile cloud suite of services," Sirota told *Programmable Web* on the eve of the announcement at Mobile World Congress.

Most organizations are moving to multiple apps, but, in many cases, each app may need multiple databases -- it's like access to a mashup. So for any apps that an enterprise is building, the API Portal provides a facility for a central registry, with quick access to code and APIs to speed the development process, similar to a registry of atomic building blocks.

Then, the API Gateway can pull information from the cloud and internal enterprise databases and put that into a format that can be consumed by an app. The API Gateway then layers in all the security that can address employee app security and help enterprises deal with securing data on employee devices and apps.