




ACE XML Gateway: Technical Deep Dive

Simon Parker

What's new?

Reactivity +  CISCO = ACE XML Gateway

- Acquisition closed March 21st '07
- ACE XML Gateway now an integral part of the ACE product family
- Appliance form-factor **shipping** today...
- *“Cisco's Reactivity acquisition is a logical extension of the company's SONA architecture. There's a move towards delivering appliances that provide out of the box application-integration services.”*

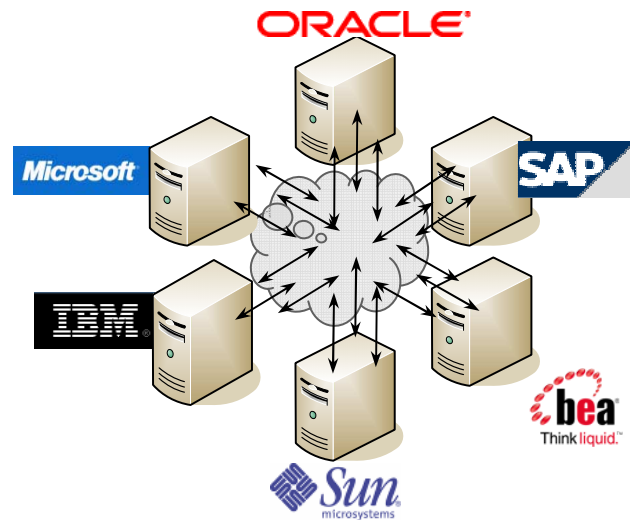
David Greenfield, Editor Network Computing. Feb 07

Introduction to Web Services

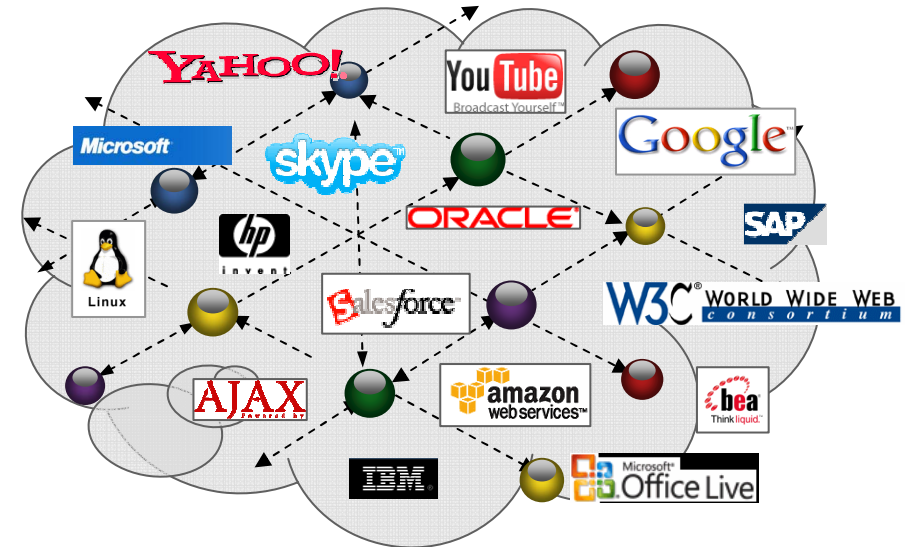


Applications Transition to SOA & Web 2.0

Siloed



Collaborative



- **Web 1.0**

 - Siloed Applications**

 - Making each app work on its own is challenging enough**

 - Limited data sharing between applications**

 - Challenges with Scalability, Security and Control**

- **Web 2.0 & SOA**

 - Collaborative personalized User Experience**

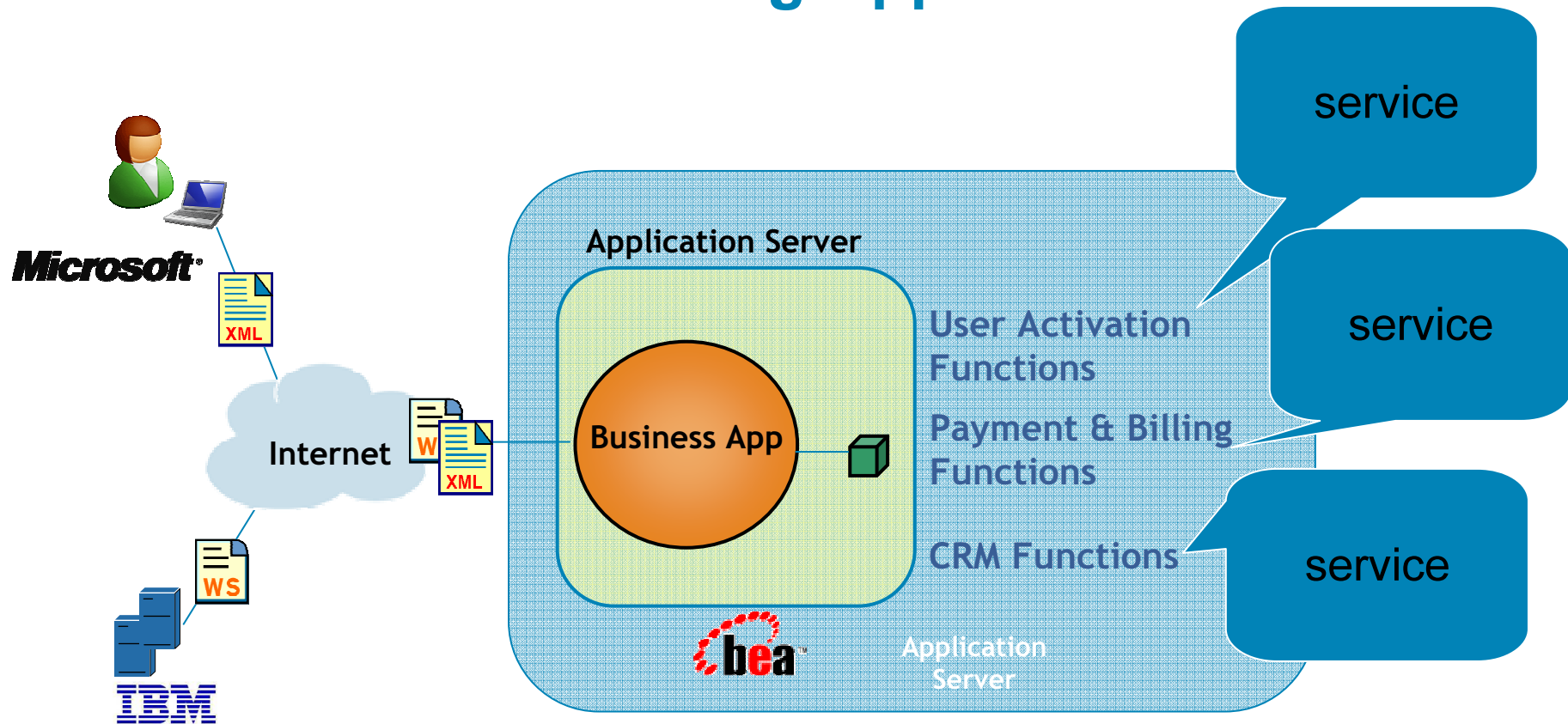
 - Inherently Internet/Web Services based**

 - Dynamic Content, Rich Media**

You said Service Oriented Architecture?

- Service Oriented Architecture: nothing new!
 - RPC, DCE, DCOM, CORBA, JMS, RMI
- Enabler for distributed applications
- Attempt to facilitate exchange of information between apps, or between producers and consumers
- How? Decouples business logic from actual application implementation

Example: Cell Phone Provisioning Application



Today: Monolithic and Tightly Coupled apps

wouldn't it be good if we could expose the billing, CRM, etc APIs independently?

Problems with the traditional model

- Tied to the underlying architecture
- Binary or proprietary message formats
- Compatibility issues
- Expensive
- Not extensible
- Complex
- Performance costs
- Not firewall friendly

Solutions to the Problem

- Open standard-driven mechanisms that are both programming language and platform independent.
- Make sure these standards are created by an independent standards body to minimize compatibility and patent issues.
- Make these standards robust enough to handle the job and yet simple enough to facilitate widespread adoption.

XML lends itself very well to this approach

Why XML Web Services?

- XML is plain ASCII
 - Introduces non-binary messaging
- XML messaging rides on top of existing application protocols
- XML over HTTP solves the problem of distributed applications across firewalls
- Guess what the 'Web' in Web Services is for? The communications can run over HTTP. SOAP is XML over HTTP – more on this topic in a few slides ...

Loosely-coupled apps that use open standards to describe an interface for accessing them and a messaging format for communication

XML in 10 seconds

- HTML = a set of tags to *format* data (eg: bold , tables <td><tr>, colors , etc.) – entirely focused on formatting rather than data
- XML = focuses on *content* rather than format. XML does not have any predefined tags. No such thing as , <h1> etc.

HTML

```
<pre>
<h1>Customer</h1>
<h2>Title</h2>Mr.
<h2>Name</h2>
John Doe
<h2>Address</h2>
123 ABC Street
Anytown
Ca
95134
```

XML

```
<customer>
  <name>
    <title>Mr.</title>
    <first-name>John</first-name>
    <last-name>Doe</last-name>
  </name>
  <street>123 ABC Street</street>
  <city>Anytown</city>
  <state>Ca</state>
  <zipcode>95134</zipcode>
</customer>
```

Giving XML meaning: XML Schemas

- Schemas are rules that an XML document must abide by
- Popular ways to define schemas include Document Type Definition (DTD) or W3C XML Schema
- W3C XML Schema fare more prevalent for data-oriented style documents (e.g. restricting content, explicit data types)
- Provides a very convenient way to inform clients about the data types and ranges accepted by my exposed services

Exchanging data in a WS world: SOAP

- Simple Object Access Protocol
- XML-based messaging format
- Rides on top of HTTP
- SOAP = XML over HTTP

HTTP Headers for the request

```
POST HacmeBank_v2_WS/Webservices/AccountManagement.asmx HTTP/1.1
Host: 172.25.89.157
Connection: Keep-Alive
User-Agent: PHP-SOAP/5.2.3
Content-Type: text/xml charset=utf-8
SOAPAction: "http://tempuri.org/GetLoanRates"
Content-Length: 220
```

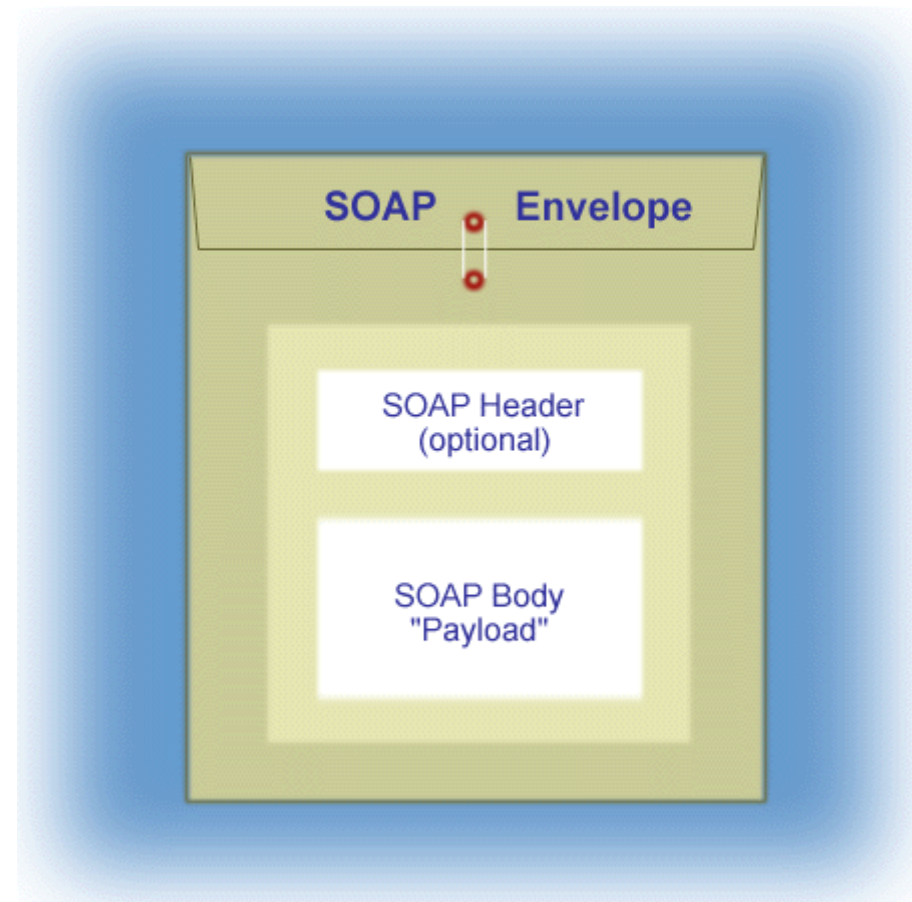
HTTP Body of the request

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns1="http://tempuri.org/"><SOAP-ENV:Body>ns1:GetLoanRates/></SOAP-ENV:Body></SOAP-ENV:Envelope>
```

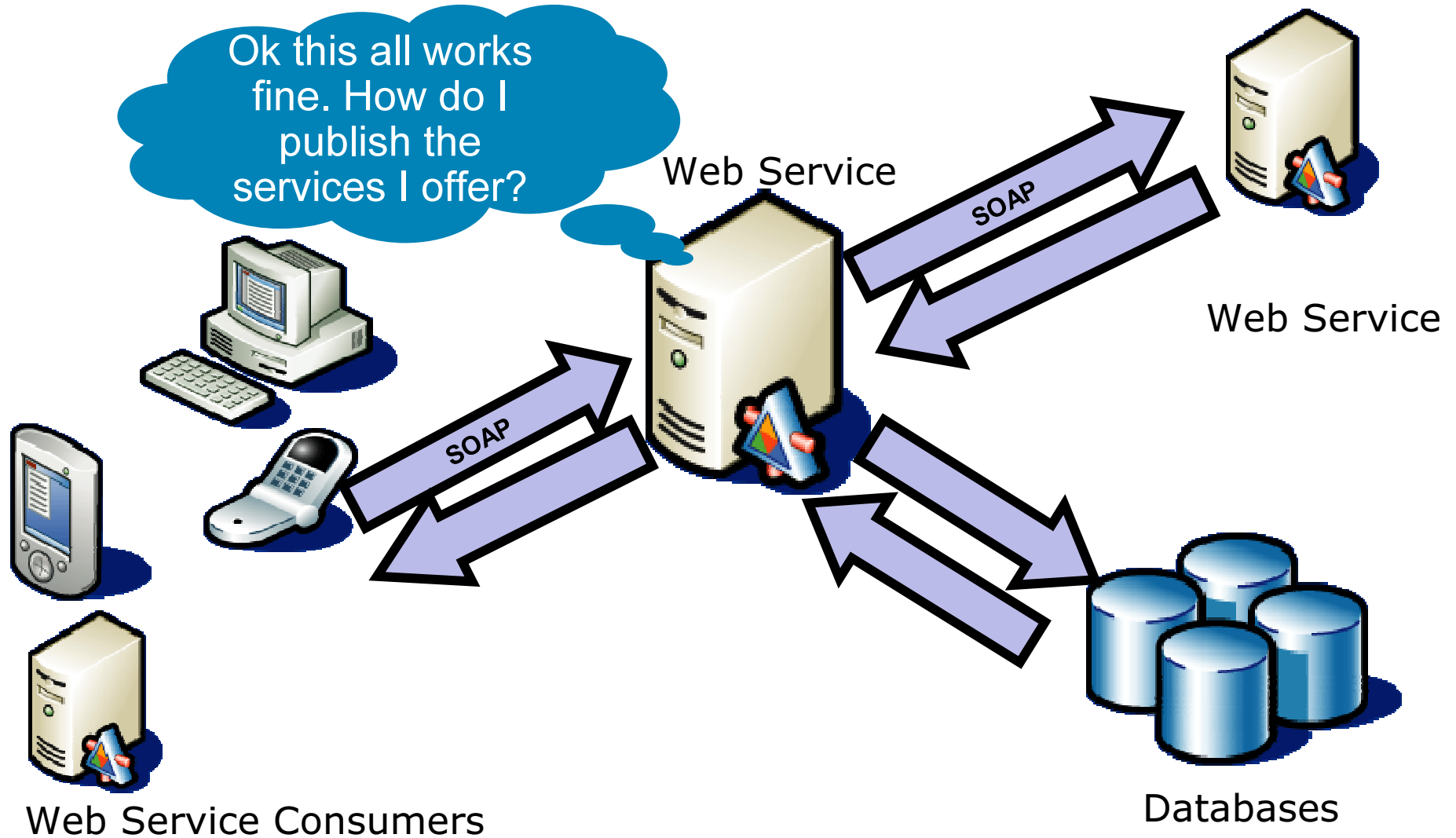
<http://172.25.89.140/WS/soapheaders.php?ARG=req>

What's inside SOAP?

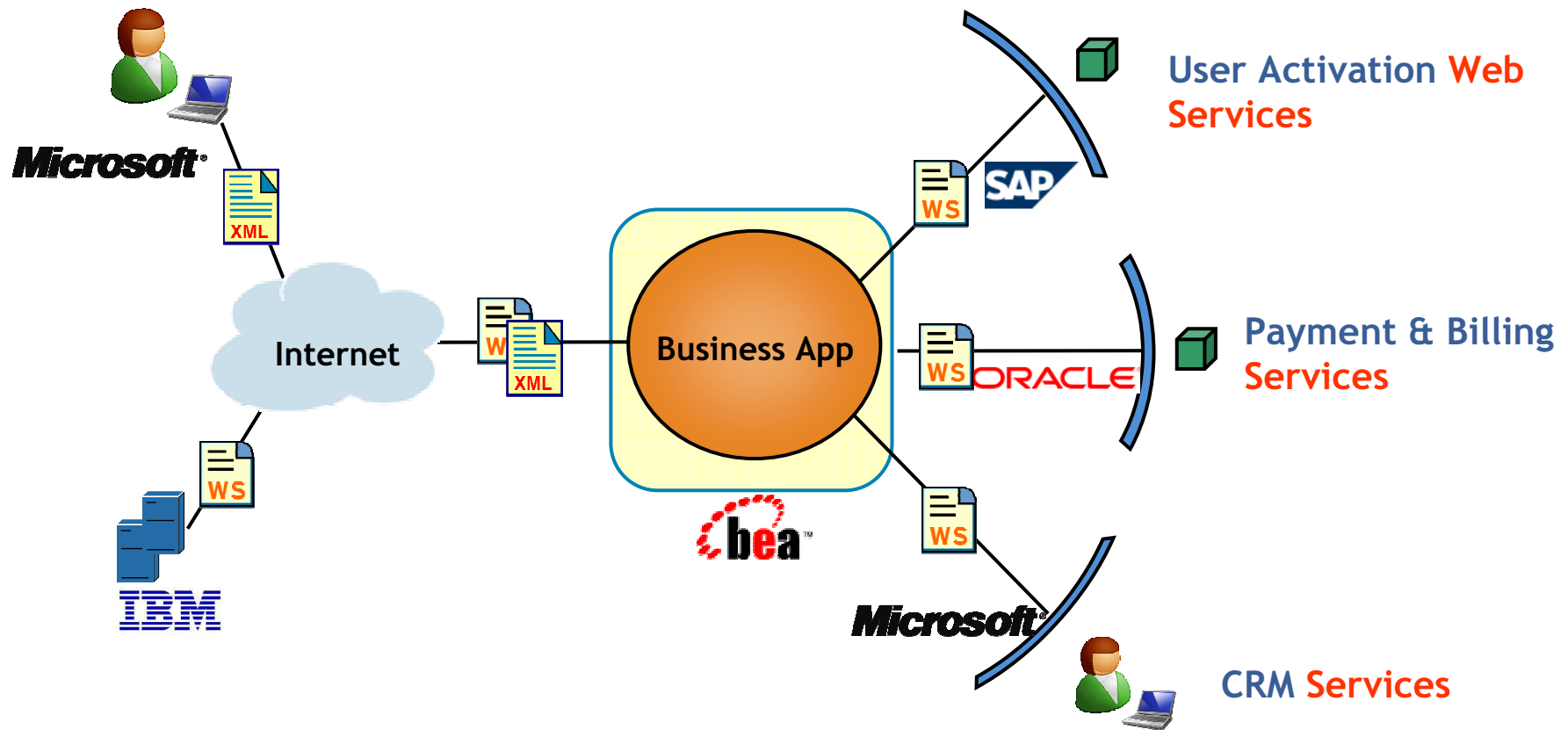
- Required SOAP Body and Envelope
- Optional SOAP Header



Web Services In Action



WS-enabled Cell Phone Provisioning Application



Collaborative and Loosely Coupled

SOA: it's happening today!

SOA: capitalizing on the enterprise's core competency

XML usage is increasing

“XML accounted for 15% of internet traffic in 2005. By 2008, it is expected to account for 50%” – 451 Group

Some numbers

- **Salesforce.com:** reports on their blog that over 40% of all of Salesforce.com traffic comes from their API.
- **Amazon:** 140,000 registered developers. [Information Week](#) article reported 3rd party sellers generated 28% of Amazon's Q2 unit sales, or \$490 million.
- **eBay:** Over 25,000 developers with 1,900 certified applications. A [TechWeb story](#) notes that during Q4CY05, eBay handled more than 8 billion Web service requests, up from less than 1 billion for the entire CY02.

<http://blog.programmableweb.com/?p=277>

XML adoption

How fast is it growing?

Traffic growth

- 2005: XML accounted for 15% of data centre traffic
- 2008: XML will account for 50% of data centre traffic

The logo for 'the 451 group' is displayed on a dark blue rectangular background. The text 'the' and 'group' are in a white, lowercase, sans-serif font. The number '451' is enclosed in a white circle, also in a lowercase, sans-serif font.

XML appliance market size

- 2007: \$100m
- 2008: \$200m
- 2009: \$400m



zapthink

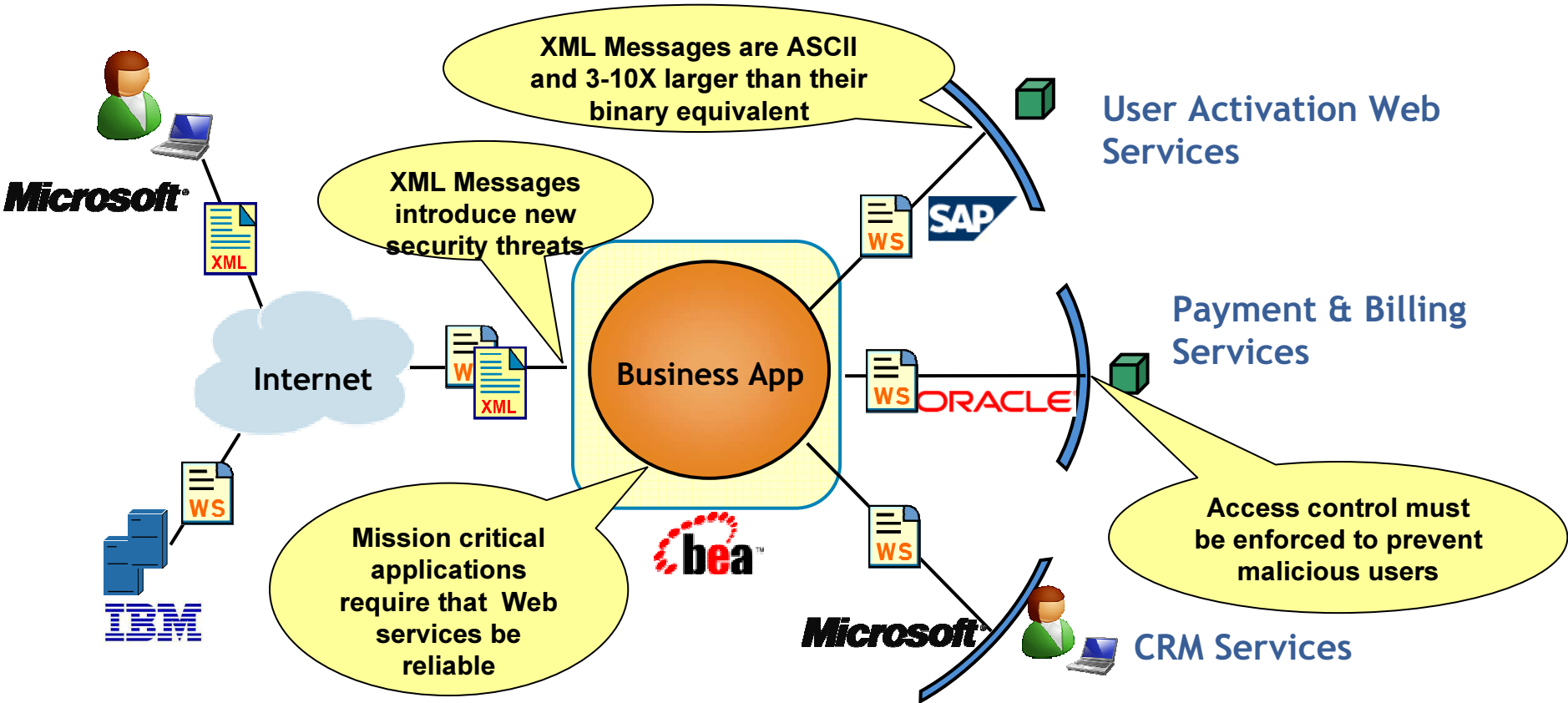
Service Orientation Advisory, Research, and Expertise
Intelligence for IT Vendors, Service Providers & Enterprises

Challenges



XML Challenges

Example: Cell Phone Provisioning Application



The Challenges of XML

- Interoperability comes at a price - **poor application performance**
 - XML documents are cumbersome for machines to process
- Increasingly open systems create **new security problems**
 - No single point of enforcement of security policy
- Increased system interaction **increases latency**
 - Applications exist as part of an interconnected community

XML Threat Categories

- **Format Attacks**

 - Main focus: Buffer overflow, Overload and Denial of Service

 - Documents of extreme depth, breadth, length, number of nodes

- **Content Attacks**

 - Main focus: Command execution

 - Exploiting insecure business logic (e.g. SQL Injection)

- **Denial of Service**

 - Main focus: Consuming all system resources

 - Exploiting processing issues to overwhelm capacity

Format Attack: Entity Expansion

Entity Expansion Attack

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE foobar [
<!ENTITY x0 "hello">
<!ENTITY x1 "&x0;&x0;">
<!ENTITY x2 "&x1;&x1;">
<!ENTITY x3 "&x2;&x2;">
<!ENTITY x4 "&x3;&x3;">
...
<!ENTITY x98 "&x97;&x97;">
<!ENTITY x99 "&x98;&x98;">
<!ENTITY x100 "&x99;&x99;"> ]>


<foobar>&x100;</foobar>
```

- Overwhelms CPU and memory usage of XML parser
- This document will render current IE and Firefox unusable
- All J2EE app servers will choke on this document unless a manual property is changed

Content Attack: SQL Injection

Strategy: insert SQL statements into otherwise valid XML to cause problems on database back end

```
<customer>
  <customerName>BigCo</customerName>
  <customerID>12345</customerID>
</customer>
```



```
<customer>
  <customerName>BigCo</customerName>
  <customerID>12345; drop table users; --</customerID>
</customer>
```

```
SqlQuery = "Select * from userTable where ID ="
          + myCustomer.CustomerID + ";"
```

- Eg. of a general class of threats: Command Injection, LDAP...

XML Denial of Service (XDoS)

- Swamping a server with illegitimate messages that consume resources that would otherwise be used to process legitimate messages

- Resources

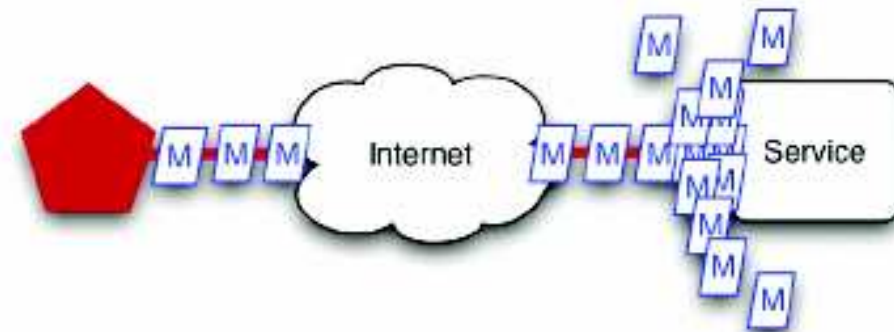
 - Server CPU (parsing, SSL processing, signature validation, etc.)

 - Server network Connections

 - Server memory

 - Server storage

- Inadvertent, non-malicious XDoS



XML Threats Are Already Here!

Vulnerabilities and Threats

Internet security problems are abundant but at *WebServicesSummit.com* we put a spotlight on vulnerabilities related to XML processing and XML messaging, such as web services. This is not a comprehensive list, which had grown to more than **13,000 known vulnerabilities by the end of 2003.**

Potential threats and security holes may take several forms. Failure to install security fixes invites unauthorized entry as much as leaving a safe or briefcase open and unattended.

<http://www.webservicessummit.com/Vulnerabilities.htm>

Introducing the ACE XML Gateway

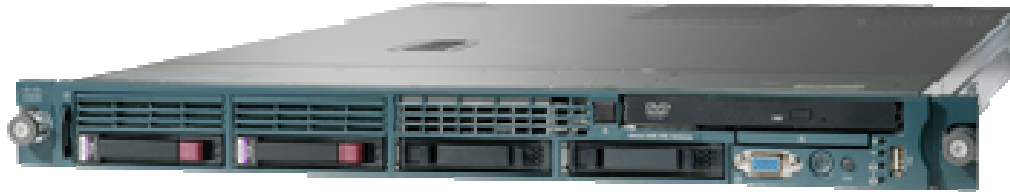


Network device that *simplifies* XML and Web Service application deployments

- **Secure** - Prevents threats to application – XML Firewall, message inspection access control
- **Accelerate** - Offloads XML and message processing from application servers
- **Scale** - Reduce end-to-end application latency and improve concurrency – 30,000 TPS and 40,000 concurrent connection
- **Manage** - Policy-driven message enforcement of how and when applications may be accessed. Intuitive GUI to define and monitor service execution.

Industry's Highest Performing XML Firewall
30,000 XML schema validations per second!

ACE XML Gateway: XML Firewall Capabilities



XML Intrusion Prevention

Thwart malicious XML attacks

Access Control

Locks downs access to web services

Message Level Encryption & SSL

Ensures message privacy

Extensive Security Logging

Forensics & Audit

Federated ID - SSO Management

Improved User Experience

Best XML Firewall in Its Class

