Lesson 2 – Introduction to SOAP

Service Oriented Architectures Security

Module 1 - Basic technologies

Unit 1 - Introduction

Ernesto Damiani

Università di Milano
Basic problems to solve (1)

• How to make the service invocation part of the language in a more or less transparent manner
• How to exchange data between machines that might use different representations for different data types
  – This involves two aspects: data type formats (e.g., byte orders in different architectures) and data structures (need to be flattened and then reconstructed)
Basic problems to solve (2)

- How to find the service one actually wants among a potentially large collection of services and servers. The client does not necessarily need to know where the server resides or even which server provides the service.
- How to deal with errors in the service invocation in a more or less elegant manner:
  - server is down or busy
  - communication is down
  - duplicated requests
CORBA invocations
DCOM invocations

- Client
  - Client proxy
  - COM runtime
  - MIDDLEWARE
  - SCM
  - DCE RPC

- Identifying and locating services

- Registry

- Server stub
  - COM runtime
  - MIDDLEWARE
  - SCM
  - DCE RPC

- Service (server)

SCM = Service Control Manager

Local Area Network
DCOM runtime

• Installed by default
  – Windows XP, 2k, (98, Me)

• Not installed by default
  – Windows NT

• But installed with other apps (ex. IE)
• DCOM Configuration Tool
• View installed DCOM-enable applications list
List of DCOM-enabled apps

DCOM-enabled apps:
- Defrag FAT engine
- Defrag NTFS engine
- Event Object Change
- HTML Application
- Image Document
- Internet Explorer V1.0
- Logagent
- Logical Disk Manager Administrative Service
- Logical Disk Manager Remote Client
- Media Player
- MediaCatalogDB OLE DB Provider
- Microsoft Agent Server 2.0
- Microsoft Clip Organizer
- Microsoft Excel Application
- Microsoft Graph Application
- Microsoft PowerPoint Presentation
- Microsoft WBEM Active Scripting Event Consumer Provider
- Microsoft WBEM Server
- Microsoft WBEM Unsecured Apartment
Windows built-in DCOM apps

- Internet Explorer
- Windows Media Player
- Windows Scripting Host
- Sound recorder
- WordPad
  - and more...
Other applications

• Word
• Excel
• Outlook
• PowerPoint
  – and more ...
COM components on Windows

- Windows has many COM components
- They are registered under
  "\HKEY_CLASSES_ROOT\CLSID" in the registry
COM components in Registry
Distributed apps by using DCOM
The COM/DCOM scalability (1)

- In the same process
  - Fast, direct function calls

- On the same machine
  - Fast, secure IPC
• Across machines
  – Secure, reliable and flexible DCE-RPC based DCOM protocol
DCOM transports
DCOM security
DCOM architecture (1)

- **Multiplexing** - Single Port per-protocol, per server process, regardless of # of objects
- **Scalable** - Connection-Less Protocols like UDP Preferred
- **Established Connection-Oriented** (TCP) Sessions Reused by same client
DCOM architecture (2)

- Low bandwidth
  - Header is 28 bytes over DCE-RPC
  - Keep-Alive Messages bundled for all connections between machines
What’s right with COM?

• Focus is on binary object standard and scalable/fine-grained component re-use
• Concreteness and depth of definition, for example security, lifetime management, activation, installation & deployment
• Architected extensibility
What’s wrong with CORBA/IIOP?

- Focus is on cross-node or network reuse/integration
  - in practice useful for vertical solutions, not horizontal reuse/integration
- Incomplete specification
  - marshaling format of certain types of data-structures
  - implications of lack of services (e.g. Naming, Events, Lifetime management)
- No architected extensibility
Application Management

- Distribution of Code + Data + Configuration Information
- Security and Security Delegation
  - Security “roles” and re-use of components
- Performance Monitoring
- Runtime Environment
• What’s the next programming model layer to vastly improve ease-of-use?
  – Transactions?
  – Auto-caches & state management?
  – Auto-distribution & -execution?
Ease-of-Use: first steps

MTS = easier servers
COM/DCOM Reading list

•[Box 1 97]

•[Box 2 97]

•[Brockschmidt 93]

•[Brown 96]
  N. Brown, C. Kindel, Distributed Component Object Model Protocol -- DCOM/1.0

•[Chappell 96]

•[COM 95] The Component Object Model Specification,

•[DCE 95]
  AES/Distributed Computing - Remote Procedure Call, Revision B, Open Software Foundation,
  [http://www.osf.org/mall/dce/free_dce.htm](http://www.osf.org/mall/dce/free_dce.htm)

•[Rogerson 96]

•[Wang 97]
  Y. M. Wang, COM/DCOM Resources,
  [http://www.research.att.com/~vmwang/resources/resources.htm](http://www.research.att.com/~vmwang/resources/resources.htm)
Problems with previous solutions

- RPC, CORBA, DCOM, even Java, use different mechanisms and protocols for communicating. All of them map to TCP or UDP one way or another, but use different syntax for marshalling, serializing and packaging messages
  - The problem is that these mechanisms are a legacy from the time when communications were mostly within LANs and within homogeneous systems
  - Building a B2B environment combining the systems of different companies becomes difficult because the protocols available in RPC, CORBA, or DCOM are too low level and not compatible among each other (gateways are needed, etc.)
The SOAP solution

- To address this problem, XML was used to define SOAP
  - SOAP is conceptually quite simple: RPC using HTTP
  - (at the client) turn an RPC call into an XML document
  - (at the server) turn the XML document into a procedure call
  - (at the server) turn the procedure’s response into an XML document
  - (at the client) turn the XML document into the response to the RPC
  - use XML to serialize the arguments following the SOAP specification
• SOAP was originally conceived as the minimal possible infrastructure necessary to perform RPC through the Internet: use of XML as intermediate representation between systems
  – very simple message structure
  – mapping to HTTP for tunneling through firewalls and using the Web infrastructure
The idea was to avoid the problems associated with CORBA’s IIOP/GIOP (which fulfilled a similar role but using a non-standard intermediate representation and had to be tunneled through HTTP anyway)

- The goal was to have an extension that could be easily plugged on top of existing middleware platforms to allow them to interact through the Internet rather than through a LAN as in the original case. Hence the emphasis on RPC from the very beginning (essentially all forms of middleware use RPC at one level or another)

Eventually SOAP started to be presented as a generic vehicle for computer driven message exchanges through the Internet and then it was opened to support interactions other than RPC and protocols other than HTTP
SOAP invocation

- **CLIENT** call
  - stubs, runtime service location
  - SOAP system
    - Serialized XML doc
  - Wrap doc in HTTP POST request
  - HTTP support (web client)

- **SERVER** service
  - stubs, runtime adapters
  - SOAP system
    - Serialized XML doc
  - Retrieve doc from HTTP response
  - HTTP support (web server)

This could be RPC, CORBA, DCOM, using SOAP as protocol

INTERNET

SOAP covers the following main areas:

- **Message construct**: a message format for one-way communication describing how a message can be packed into an XML document

- **Processing model**: rules for processing a SOAP message and a simple classification of the entities involved in processing a SOAP message. Which parts of the messages should be read by whom and how to react in case the content is not understood

- **Extensibility model**: how the basic message construct can be extended with application specific constructs
• **Protocol binding framework**: allows SOAP messages to be transported using different protocols (HTTP, SMTP, ...)
  - a concrete binding for HTTP
  - conventions on how to turn an RPC call into a SOAP message and
  - back as well as how to implement the RPC style of interaction
SOAP facts (1)

- SOAP is “a lightweight protocol intended for exchanging structured information [...]”, “a stateless, one-way message exchange paradigm”
  - defines the general format of a message and how to process it
  - RPC is implemented on top of the core specification following conventions of the “SOAP RPC representation”
• SOAP ≠ RPC: since Version 1.1, SOAP abstracts from the RPC programming model
• SOAP ≠ HTTP: since Version 1.1, SOAP abstracts from the protocol used to transport the messages
  - HTTP is one of many possible transports
• A SOAP message can pass through multiple hops on the way from the initial sender to the ultimate receiver
• The entities involved in transporting the message are called SOAP nodes
• SOAP intermediaries forward the message and may manipulate it
SOAP message path (2)

• Every SOAP node assumes a certain role which influences the message processing at the node

- SOAP nodes: Initial sender
- Intermedaries
- Ultimate receiver