CHAPTER 2

Communication as a Service (CaaS)

Communications as a Service (CaaS) is an outsourced enterprise communications solution that can be leased from a single vendor. Such communications can include voice over IP (VoIP or Internet telephony), instant messaging (IM), collaboration and videoconference applications using fixed and mobile devices. CaaS has evolved along the same lines as Software as a Service (SaaS).

CaaS brings social networking, cloud computing, and smartphones together, providing cloud-technologies that let users communicate via voice, text, and rich media on whatever device they prefer to use. To compete in this marketplace, software vendors, enterprises, and service providers must introduce communications-enhanced services that meet a surging need for value, efficiency, cost reduction, and convenience.

Through the hosted model, the CaaS provider manages everything, from the telecommunications infrastructure to the software integration platform for delivering communications offered at a guaranteed Quality of Service (QoS). As a result, businesses can selectively deploy communications features, applications, and devices on a pay-as-you-go, as-needed basis, reducing risks while eliminating capital costs associated with new services.

CaaS offers flexibility and expandability that small and medium-sized business might not otherwise afford, allowing for the addition of devices, modes or coverage on demand. The network capacity and feature set can be changed from day to day if necessary so that functionality keeps pace with demand and resources are not wasted. There is no risk of the system becoming obsolete and requiring periodic major upgrades or replacement

Advantages of Communication as a Service (CaaS)

- **Fully Integrated Enterprise Class Unified Communication:** By managing the LAN/WAN, the vendor can guarantee consistent Quality of Service (QoS) from the desktop across the VoIP backbone and back again. Advanced Unified Communications features such as Outlook integration, soft phones, real-time presence, chat, multimedia conferencing, video calling, unified messaging and mobility are also part of a standard CaaS deployment. And with CaaS, the feature set can continue to evolve. Development and introduction of new features and applications are faster, easier and more economical because the service provider is doing the work for multiple end users across a scalable platform
- **No Upfront Capital Expenses:** Since cloud services are supposed to lower capital expenditure and focus more on operating expenditure, by implementing CaaS, consumers can build up their communication infrastructure without any upfront cost. They just need to pay it as a service.
- **Flexibility in Features:** Since cloud is a multi-tenant architecture, cloud vendors have to manage multiple customers and look after the features that they want. What this allows cloud vendor is to add more advanced features and flexibility in their service model. Economies of scale also

mean that the service provider is not tied to a single vendor investment and can leverage best-of-breed providers like Cisco, Microsoft and Nortel much more economically than an independent enterprise.

- **No Risk of Obsolescence:** Technology changes rapidly and are obsolete within few years of introduction. With CaaS, companies are always privileged with new technologies as cloud vendors keep on updating their equipment's and technologies to sustain in market.
- **No Data Center Cost:** As a prime advantages of cloud computing, while using CaaS infrastructure, organization need not invest on expensive servers, cooling system and electric equipment. With monthly/ yearly recurring cost, organization can dramatically cut down the management cost of data center as well.
- **Guaranteed Business Continuity:** With CaaS, organization can be hugely benefitted with guaranteed business continuity as cloud service providers proactively plans for Business Continuity Planning for their customers. Service uptime is guaranteed even if any catastrophic disaster strikes.

Unified Communication

Unified Communications (UC) might be defined as communications integrated to optimize business performance, and can describe a seamless set of voice, video and Web collaboration applications designed to enable advanced connectivity between employees, customers, partners and other stakeholders available on any device.

In the large enterprise setting, Unified Communications allow employees to send and receive messages on various medium – guided by presence information or employee preference – switching calls between home lines and a mobile device, or accessing a voicemail via text or email. When well implemented, UC can save money, optimize business processes and improve communications by better connecting devices, media and applications, reducing latency, and opening new forms of collaboration.

Some of the benefits of Unified Communication are as below:

a. **Efficient Communication:** Users can communicate more efficiently by having access to all communications at one time and being free to share, forward, or manage them in the way that's most convenient or effective for the given communication.
b. **Anywhere Access:** Unified messaging provides alternative methods of accessing communications. By merging e-mail, voice, and other communications, users can get voice messages in e-mail, have e-mail dictated over the phone, or access communications via the Web.
c. **Collaboration:** Collaborative approach of communication can be helpful in achieving immediacy, simplicity and interoperability of communication. In this way, business can sense and respond more quickly to changing environment.
d. **Business Process Integration:** Business processes can be integrated to each other for more efficiency. Many business entities and functions can be incorporated in one platform to make processes more agile and responsive.

Infrastructure as a Service

Infrastructure as a Service (IaaS) is one of the three fundamental service models of cloud computing alongside Platform as a Service (PaaS) and Software as a Service (SaaS).

Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. Clients are able to self-provision this infrastructure, using a Web-based graphical user interface that serves as an IT operations management console for the overall environment. API access to the infrastructure may also be offered as an option.

A typical Infrastructure as a Service offering can deliver the following features and benefits:

- **Scalability**; resource is available as and when the client needs it and, therefore, there are no delays in expanding capacity or the wastage of unused capacity
- **No investment in hardware**; the underlying physical hardware that supports an IaaS service is set up and maintained by the cloud provider, saving the time and cost of doing so on the client side
- **Utility style costing**; the service can be accessed on demand and the client only pays for the resource that they actually use
- **Location independence**; the service can usually be accessed from any location as long as there is an internet connection and the security protocol of the cloud allows it
- **Physical security of data center locations**; services available through a public cloud, or private clouds hosted externally with the cloud provider, benefit from the physical security afforded to the servers which are hosted within a data center
- **No single point of failure**; if one server or network switch, for example, were to fail, the broader service would be unaffected due to the remaining multitude of hardware resources and redundancy configurations. For many services if one entire data center were to go offline, never mind one server, the IaaS service could still run successfully.

On Demand Computing: On-demand (OD) computing is an increasingly popular enterprise model in which computing resources are made available to the user as needed. The resources may be maintained within the user's enterprise, or made available by a service provider. The on-demand model evolved to overcome the challenge of being able to meet fluctuating resource demands efficiently. Because demand for computing resources can vary drastically from one time to another, maintaining sufficient resources to meet peak requirements can be costly.

On-demand computing products are rapidly becoming prevalent in the marketplace. Computer Associates, HP, IBM, Microsoft, and Sun Microsystems are among the more prominent on-demand

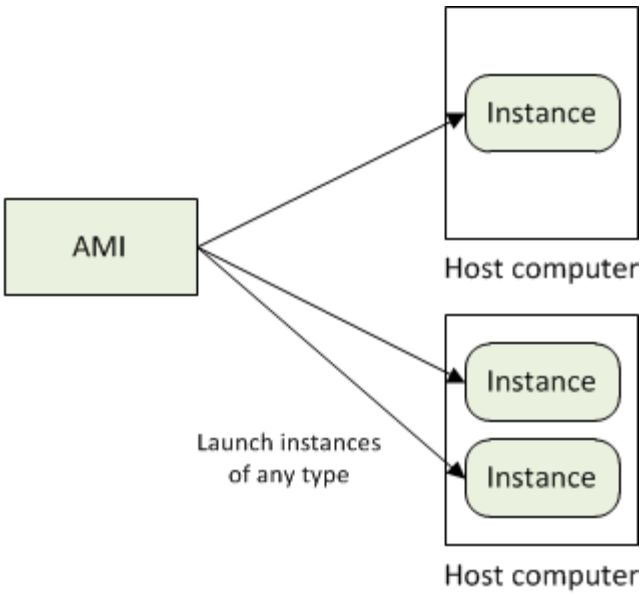
vendors. These companies refer to their on-demand products and services by a variety of names. Concepts such as grid computing, utility computing, autonomic computing, and adaptive management seem very similar to the concept of on-demand computing.

The major advantage of On Demand Computing (ODC) is low initial cost, as computational resources are essentially rented when they are required. This provides cost savings over purchasing them outright.

(Amazon EC2): Amazon Elastic Compute Cloud (EC2) is a central part of Amazon cloud computing platform Amazon Web Services (AWS). EC2 allows users to rent virtual computers on which to run their own computer applications. EC2 allows scalable deployment of applications by providing a Web service through which a user can boot an Amazon Machine Image to create a virtual machine, which Amazon calls an "instance", containing any software desired. A user can create, launch, and terminate server instances as needed, paying by the hour for active servers, hence the term "elastic".

It reduces the time required to obtain and boot new server instances to minutes, allowing customers to quickly scale capacity as their computing demands dictate. It changes the economics of computing by allowing clients to pay only for capacity they actually use. It provides developers the tools needed to build failure-resilient applications and isolate themselves from common failure scenarios.

To use the EC2, a subscriber creates an Amazon Machine Image (AMI) containing the operating system, application programs and configuration settings. Then the AMI is uploaded to the Amazon Simple Storage Service (Amazon S3) and registered with Amazon EC2, creating a so-called AMI identifier (AMI ID). Once this has been done, the subscriber can requisition virtual machines on an as-needed basis. Capacity can be increased or decreased in real time from as few as one to more than 1000 virtual machines simultaneously. Billing takes place according to the computing and network resources consumed.



The idea of EC2 is to lighten the cost of buying servers to host a system, but more importantly to eliminate the wasted time systems engineers devote to managing hard assets. Instead of buying servers to increase capacity or add new features, you simply buy more gigabytes on EC2. Amazon sells it in subscription form, with subscriptions based on how much capacity you use.

Characteristics of Amazon EC2

(http://en.wikipedia.org/wiki/Amazon_ec2)

a. Persistent Storage
b. Elastic IP Addresses
c. Amazon Cloud Watch
d. Automated Scaling
e. Reliability

Monitoring as a Service

Monitoring-as-a-Service is an outsourced service to provide security mainly to platforms that are run on the Internet for conducting business. Maas became highly popular in the last decade. Since the advent of Cloud Computing, its popularity has increased even more. Safe monitoring involves protecting a company or other institution / organization from cyber threats, in which a team prepared is crucial to maintain the confidentiality, integrity and access to IT assets.

Many industry regulations require organizations to monitor their security environment, server logs, and other information assets to ensure the integrity of these systems. However, conducting effective security monitoring can be a daunting task because it requires advanced technology, skilled security experts, and scalable processes—none of which come cheap. MaaS security monitoring services offer real-time, 24/7 monitoring and nearly immediate incident response across a security infrastructure—they help to protect critical information assets of their customers

Protection against Internal and External Threats

Security monitoring services can improve the effectiveness of a customer security infrastructure by actively analyzing logs and alerts from infrastructure devices around the clock and in real time. Typical services provided by many MaaS vendors are described below.

Early Detection

An early detection service detects and reports new security vulnerabilities shortly after they appear. Generally, the threats are correlated with third-party sources, and an alert or report is issued to customers. This report is usually sent by email to the person designated by the company. Security vulnerability reports, aside from containing a detailed description of the vulnerability and the platforms affected, also include information on the impact the exploitation of this vulnerability would have on the systems or applications previously selected by the company receiving the report. Most often, the report also indicates specific actions to be taken to minimize the effect of the vulnerability, if that is known.

Platform, Control, and Services Monitoring

Platform, control, and services monitoring is often implemented as a dashboard interface and makes it possible to know the operational status of the platform being monitored at any time. It is accessible from a web interface, making remote access possible. Each operational element that is monitored usually provides an operational status indicator, always taking into account the critical impact of each element. This service aids in determining which elements may be operating at or near capacity or beyond the limits of established parameters. By detecting and identifying such problems, preventive measures can be taken to prevent loss of service.

Intelligent Log Centralization and Analysis

Intelligent log centralization and analysis is a monitoring solution based mainly on the correlation and matching of log entries. Such analysis helps to establish a baseline of operational performance and provides an index of security threat. Alarms can be raised in the event an incident moves the established baseline parameters beyond a stipulated threshold. These types of sophisticated tools are used by a team of security experts who are responsible for incident response once such a threshold has been crossed and the threat has generated an alarm or warning picked up by security analysts monitoring the systems.

Vulnerabilities Detection and Management

Vulnerabilities detection and management enables automated verification and management of the security level of information systems. The service periodically performs a series of automated tests for the purpose of identifying system weaknesses that may be exposed over the Internet, including the possibility of unauthorized access to administrative services, the existence of services that have not been updated, the detection of vulnerabilities such as phishing, etc. The service performs periodic follow-up of tasks performed by security professionals managing information systems security and provides reports that can be used to implement a plan for continuous improvement of the systems security level.

Continuous System Patching/Upgrade

Security posture is enhanced with continuous system patching and upgrading of systems and application software. New patches, updates, and service packs for the equipment operating system are necessary to maintain adequate security levels and support new versions of installed products. Keeping abreast of all the changes to all the software and hardware requires a committed effort to stay informed and to communicate gaps in security that can appear in installed systems and applications.

Intervention, Forensics, and Help Desk Services

Quick intervention when a threat is detected is crucial to mitigating the effects of a threat. This requires security engineers with ample knowledge in the various technologies and with the ability to support applications as well as infrastructures on a 24/7 basis. MaaS platforms routinely provide this service to their customers. When a detected threat is analyzed, it often requires forensic analysis to determine what it is, how much effort it will take to fix the problem, and what effects are likely to be seen. When problems are encountered, the first thing customers tend to do is pick up the phone. Help desk services provide assistance on questions or issues about the operation of running systems. This service includes assistance in writing failure reports, managing operating problems, etc.

Real-Time Log Monitoring Enables Compliance

Security monitoring services can also help customers comply with industry regulations by automating the collection and reporting of specific events of interest, such as log-in failures. Regulations and industry guidelines often require log monitoring of critical servers to ensure the integrity of confidential data. MaaS provider’s security monitoring services automate this time consuming process.

Platform as a Service

Platform as a service (PaaS) is a category of cloud computing services that provide a computing platform and a solution stack as a service. Along with software as a service (SaaS) and infrastructure as a service (IaaS), it is a service model of cloud computing. PaaS offerings facilitate the deployment of applications without the cost and complexity of buying and managing the underlying hardware and software and provisioning hosting capabilities.

Technically, a PaaS is an Application Platform comprised of an operating system, middleware and other software that allows applications to run on the cloud with much of the management, security, scaling and other stack related headaches abstracted away. This allows you to focus on two things: customers and developing your application. Let the PaaS deal with system administration details like setting up servers or VMs, installing libraries or frameworks, configuring testing tools, etc.

Platform as a Service allows users to create software applications using tools supplied by the provider. PaaS services can consist of preconfigured features that customers can subscribe to; they can choose to include the features that meet their requirements while discarding those that do not. PaaS works on top of IaaS and will do all of that work automatically.

The Traditional On-Premises Model

The traditional approach to developing and running applications on-premises has always been complex, expensive and risky. Producing your own solution never brought any guarantee of success. Each application has been designed to meet their specific requirements within each business. Each solution requires a specific programming hardware, an operating system, a database, often a middle-ware package, mail and web servers, etc. Once environment was created in hardware and software, a team of developers had to navigate a complex programming platform to build their own applications. Additionally, a team of network, database and system management was needed to keep everything in perfect driving conditions. Inevitably, developers were forced to change the application on behalf of a detail of the business, generating new cycles of testing before being distributed.

PaaS model offers a choice of faster and more cost-effective application development and delivery. Furthermore, PaaS provides all the infrastructure needed to run applications over the Internet. Just like Google, iTunes and Youtube, this cloud computing model allows new functionality to be delivered in emerging markets through web browsers. PaaS is based on a model of mediation or subscription, and users only pay for what they use. The PaaS model in its range also includes other facilities such as, application design and development, testing, deployment and hosting as well as integration, security, scalability, storage, status management, control panel, etc.

Characteristics of PaaS

1. **Multi-tenant architecture**
   A PaaS offering must be multi-tenanted. A multi-tenant platform is one that uses common computing resources including hardware, operating system, software (i.e. application code), and a single underlying database with a shared schema to support multiple customers simultaneously. This is in direct contrast to the traditional client/server architecture, which requires an entire stack of hardware and software to be dedicated to each tenant (customer).

2. **Customizable /Programmable User Interface**
   PaaS offering should provide the ability to construct highly flexible user interfaces via a simple "drag & drop" methodology that permits the creation and configuration of UI components on the fly. Furthermore, given the growing set of Web devices, additional flexibility to use other technologies such as CSS, AJAX and Adobe Flex to specify the appearance of the application's interface should be available to the UI designer.

3. **Unlimited Database Customizations**
   Database used by application should have option of customization for more flexibility in application development. Specifying relationships between objects, a key requirement of any sophisticated business application, must be possible through the declarative Web-based interface. Other mandatory functions include the ability to incorporate validation rules and permissions at the object/field level and the ability to specify auditing behavior.

4. **Automation**
   PaaS environments automate the process of deploying applications to infrastructure, configuring application components, provisioning and configuring supporting technology like load balancers and databases, and managing system change based on policies set by the user. While IaaS is known for its ability to shift capital costs to operational costs through outsourcing, only PaaS is able to cut down costs across the development, deployment and management aspects of the application lifecycle.

5. **Security**
   The PaaS offering should provide a flexible access control system that allows detailed control over what users of the SaaS application can see and the data each user can access. Definition of access from the application level (including tabs, menus, objects, views, charts, reports and workflow actions) to the individual field level should be possible. Defining an access control model should be possible through the creation of groups and roles and the assignment of users to either groups or roles.

6. **Runtime Framework:**
   This is the "software stack" aspect of PaaS, and perhaps the aspect that comes first to mind for most people. The PaaS runtime framework executes end-user code according to policies set by the application owner and cloud provider. PaaS runtime frameworks come in many flavors, some based on traditional application runtimes, others based on 4GL and visual programming concepts, and some with pluggable support for multiple application runtimes.

Software as a Service

Software as a service , sometimes referred to as "on-demand software", is a software delivery model in which software and associated data are centrally hosted on the cloud. SaaS is typically accessed by users using a thin client via a web browser.

In this model, the software is not hosted on the customers' individual computers. Under the SaaS model, a vendor is responsible for the creation, updating, and maintenance of software. Customers buy a subscription to access it, which includes a separate license, or seat, for each person that will use the software.

SaaS has become a common delivery model for many business applications, including accounting, collaboration, customer relationship management (CRM), management information systems(MIS), enterprise resource planning (ERP), invoicing, human resource management (HRM), content management (CM) and service desk management.

The emergence of SaaS as an effective software-delivery mechanism creates an opportunity for IT departments to change their focus from deploying and supporting applications to managing the services that those applications provide.

Unlike traditional software which is conventionally sold as a perpetual license with an up-front cost (and an optional ongoing support fee), SaaS providers generally price applications using a subscription fee, most commonly a monthly fee or an annual fee. Consequently, the initial setup cost for SaaS is typically lower than the equivalent enterprise software. SaaS vendors typically price their applications based on some usage parameters, such as the number of users ("seats") using the application. However, because in a SaaS environment customers' data reside with the SaaS vendor, opportunities also exist to charge per transaction, event, or other unit of value.

Benefits of SaaS (Hope now you can explain all):

- Save money by not having to purchase servers or other software to support use.
- Focus Budgets on competitive advantage rather than infrastructure.
- Monthly obligation rather than up front capital cost.
- Reduced need to predict scale of demand and infrastructure investment up front as available capacity matches demand.
- Multi-Tenant efficiency
- Flexibility and scalability
- Security

Characteristics of SaaS

- **Simple and quick system implementation:** As Saas sits on top of PaaS and IaaS, deploying any enterprise level software becomes easy and quick as SaaS inherits all the features of underlying infrastructure. Also since SaaS is scalable, any user request can be addressed with required elasticity.
- **Transparent and low pricing:** With common infrastructure, cloud vendor can leverage their infrastructure with lower cost and transparency. End result of this directly impacts customer cost of software implementation as they gets it cheaper with enhanced security and high availability.
- **Multitenant Architecture:** A multitenant architecture, in which all users and applications share a single, common infrastructure and code base that is centrally maintained. Because SaaS vendor clients are all on the same infrastructure and code base, vendors can innovate more quickly and save the valuable development time previously spent on maintaining numerous versions of outdated code.
- **Easy software maintenance and Customization:** The ability for each user to easily customize applications to fit their business processes without affecting the common infrastructure. Because of the way SaaS is architected, these customizations are unique to each company or user and are always preserved through upgrades. That means SaaS providers can make upgrades more often, with less customer risk and much lower adoption cost.
- **Better Access:** Improved access to data from any networked device while making it easier to manage privileges, monitor data use, and ensure everyone sees the same information at the same time.