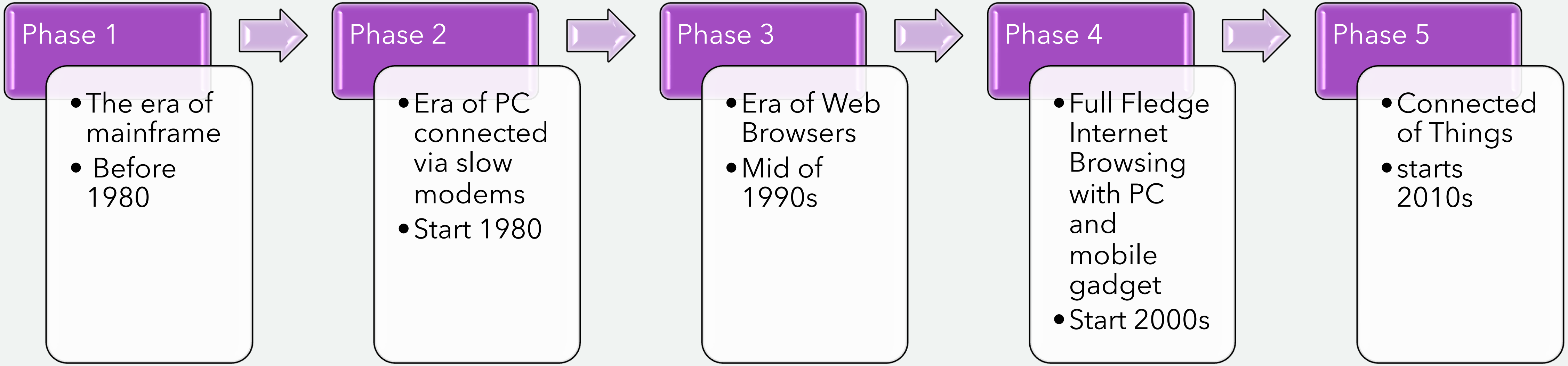
Foundations of Cloud Computing and Information Security

I Gde Dharma Nugraha, Ph.D

Outlined

- Historical Evolution
- Network Protocol for Cloud Computing
- Data Center Architecture and Connectivity
- IT Evolution
- Server Operation in Data Center
- Evolution of Service Orientation Architecture
- Basic Concept of Cloud Computing Security

Historical Evolution



Phase 1

- The era of mainframe
- Before 1980

Phase 2

- Era of PC connected via slow modems
- Start 1980

Phase 3

- Era of Web Browsers
- Mid of 1990s

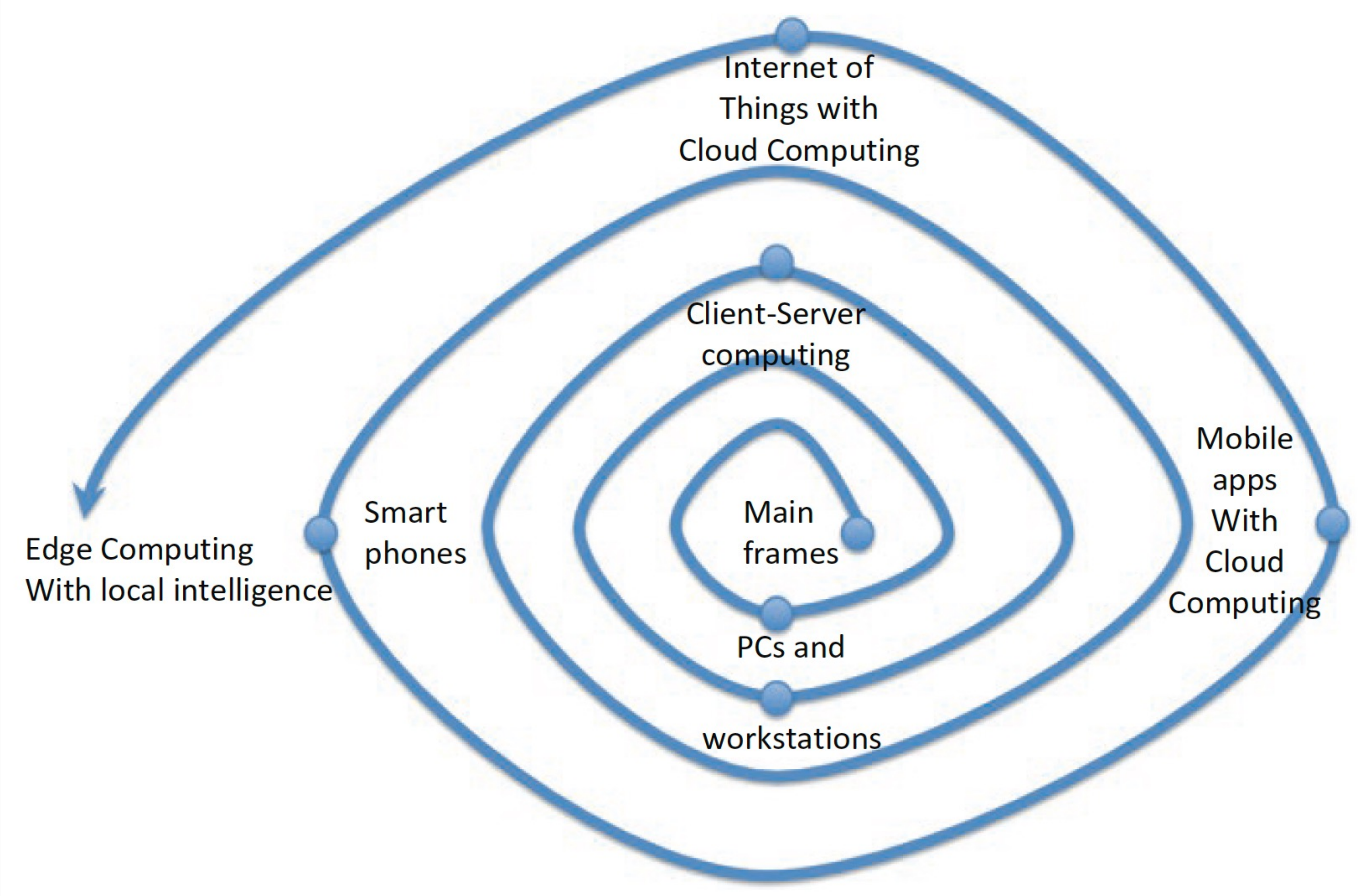
Phase 4

- Full Fledge Internet Browsing with PC and mobile gadget
- Start 2000s

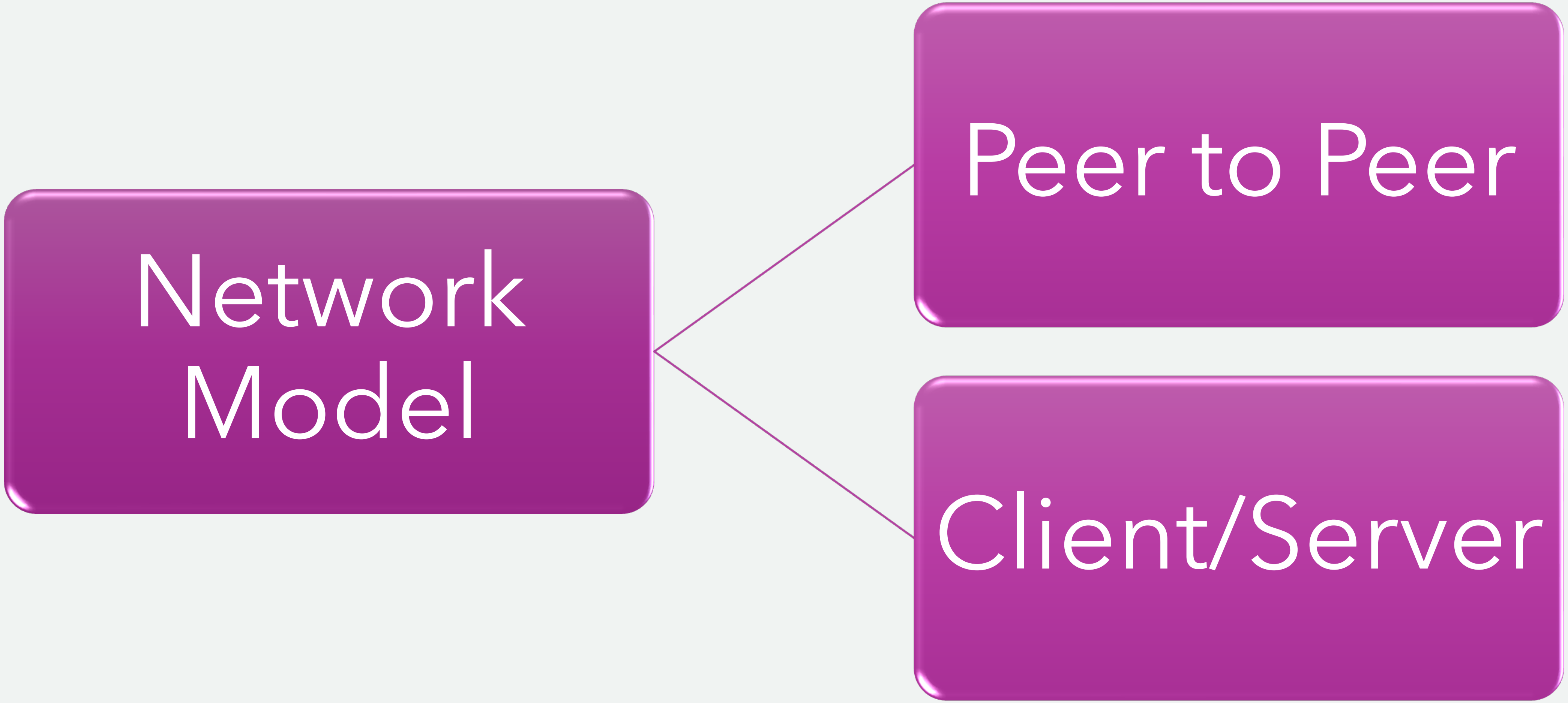
Phase 5

- Connected of Things
- starts 2010s

Historical Evolution


Main frames
PCs and workstations
Client-Server computing
Smart phones
Internet of Things with Cloud Computing
Mobile apps With Cloud Computing
Edge Computing With local intelligence

Network Protocols for Cloud Computing



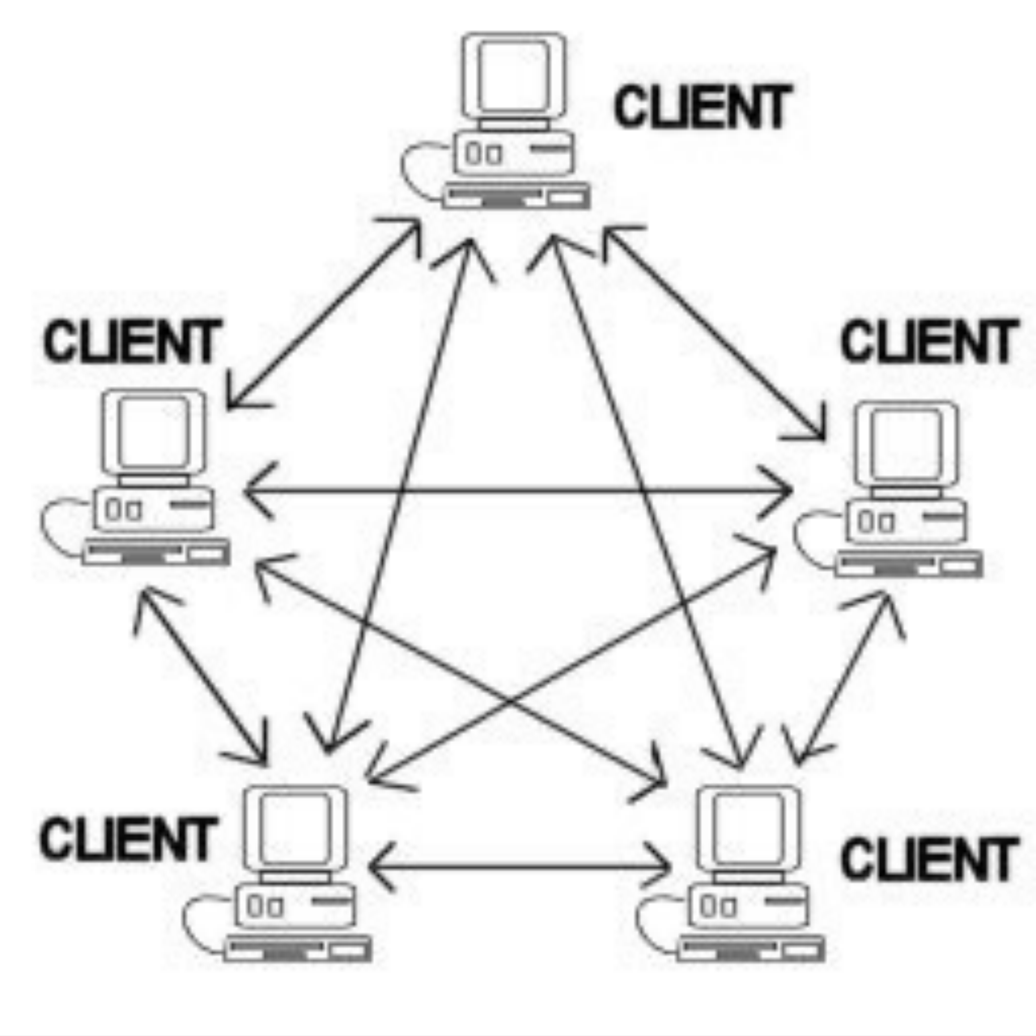
Network Model

Peer to Peer

Client/Server

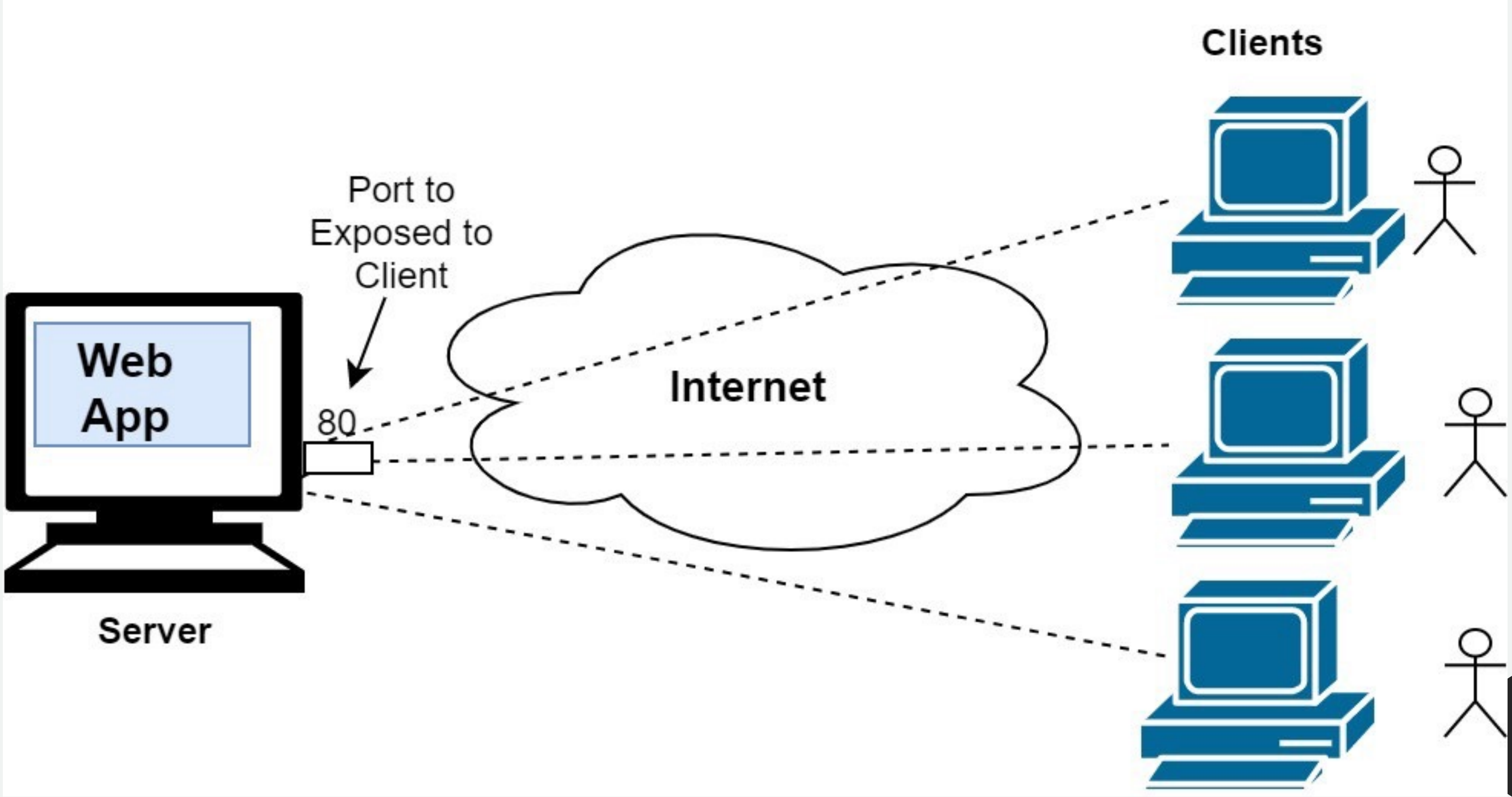
Network Protocols for Cloud Computing

- Peer to Peer Model

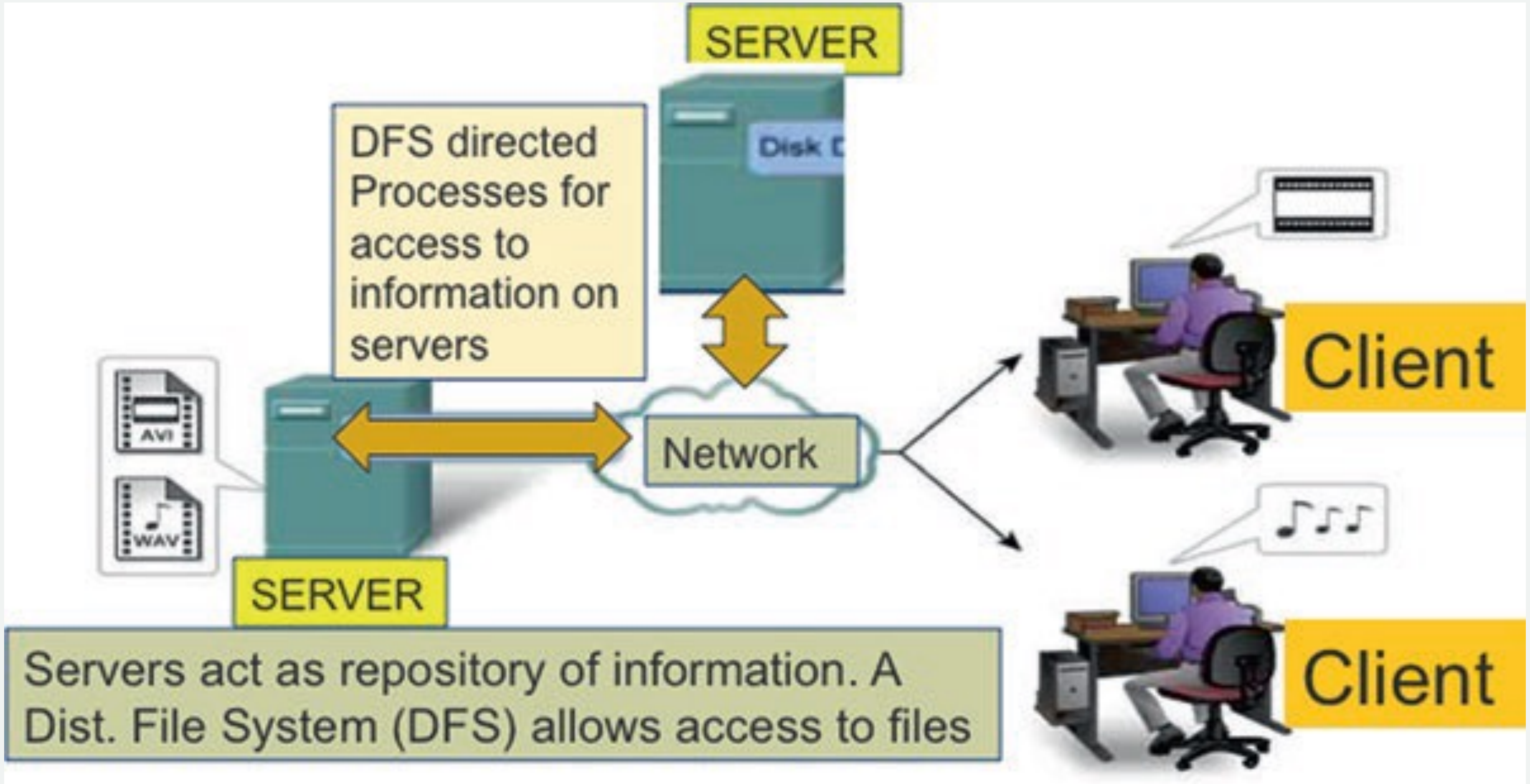


Network Protocols for Cloud Computing

- Client/Server Architecture



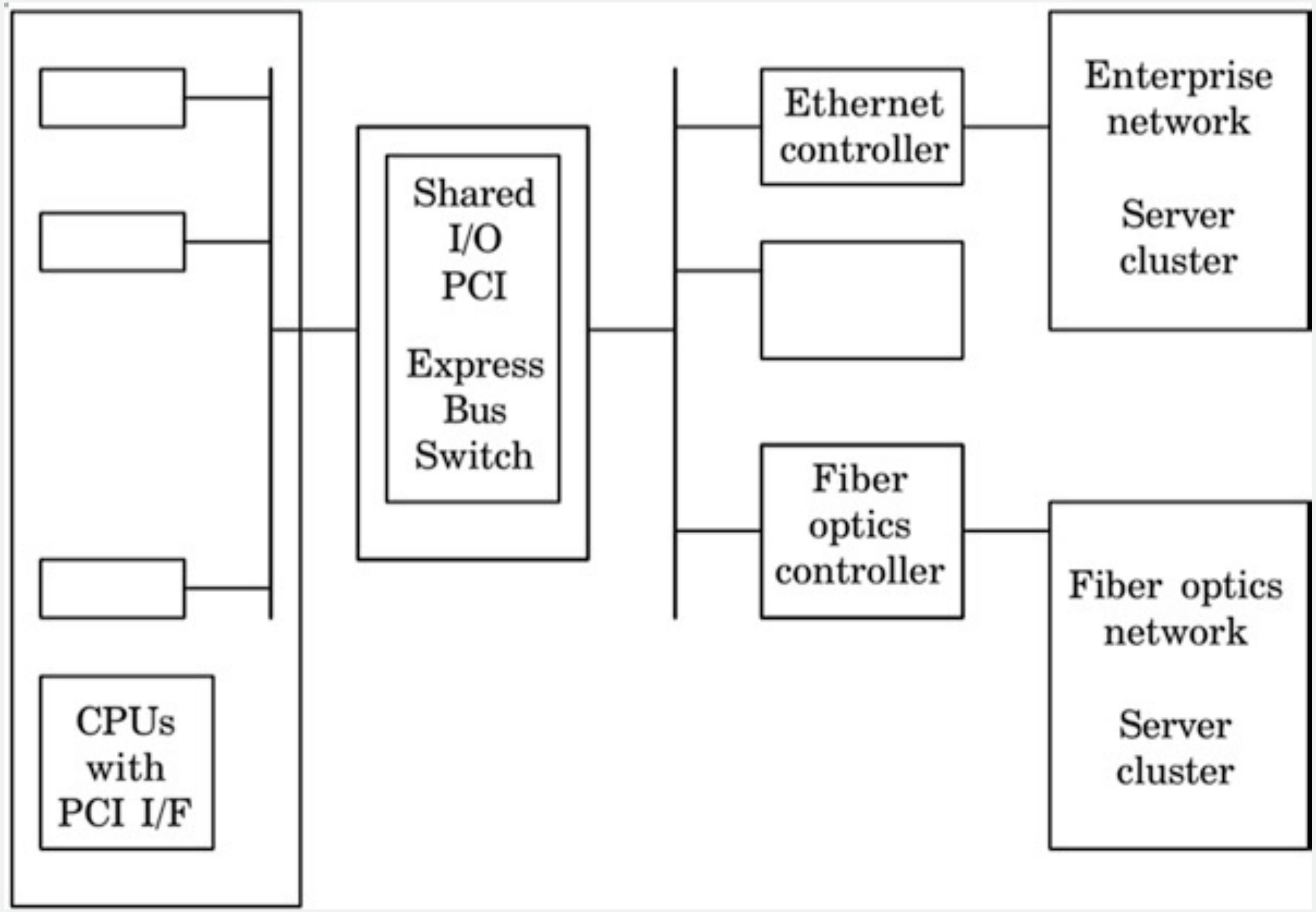
Typical Network Model in Data Center



Servers act as repository of information. A Dist. File System (DFS) allows access to files

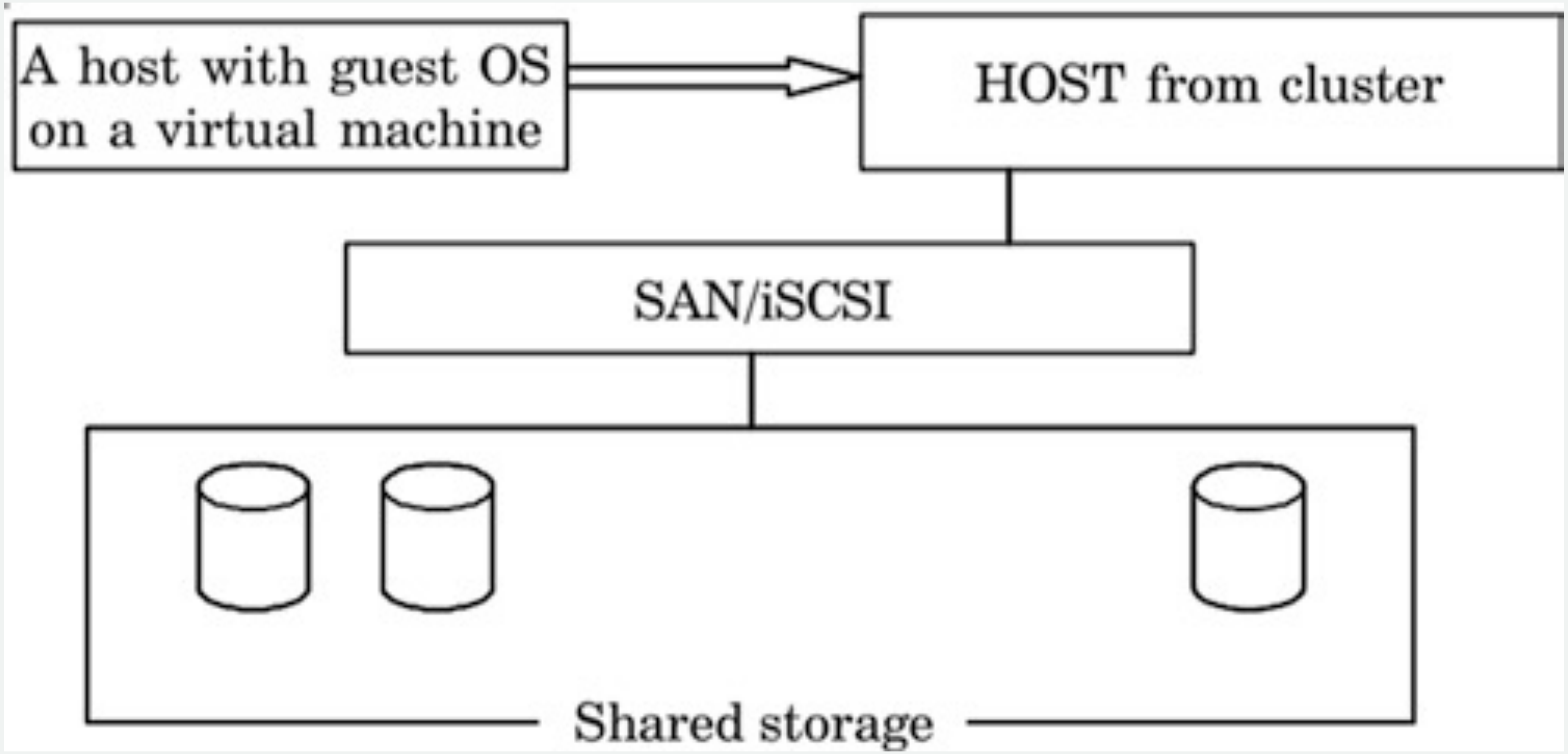
Typical Network Model in Data Center

- Server Cluster



Typical Network Model in Data Center

- Shared Storage

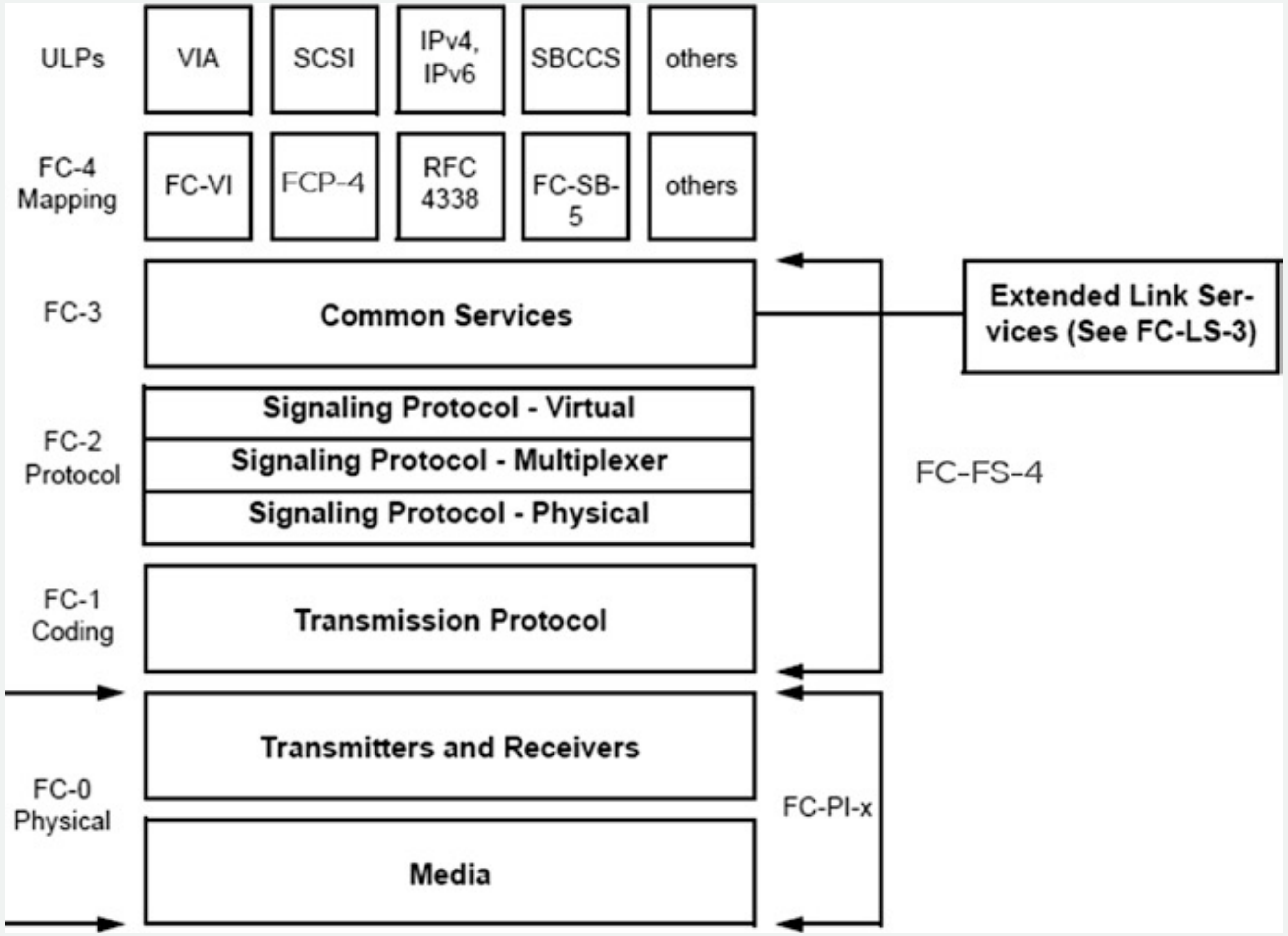


Role of Internet Protocols in a Data Center

- Many public data centers need to share their hardware among different customers, to optimize their infrastructure investments.
- One way to enable this sharing, while preserving isolation and privacy between their customers, data center operators use virtualization.
- The purposes are Isolation and Security, so VLAN is used.
- However, it also can lead to heavy network traffic in a Data Center, so Fibre Channels (FC) are used.

Role of Internet Protocols in a Data Center

- Layers of Fibre Channel Technology Implementation



Role of Internet Protocols in a Data Center

- Layers of Fibre Channel Technology Implementation
- Fibre Channel does not follow the OSI model layers and, is split into five layers:
  - *FC-4 – Protocol-mapping layer, in which upper-level protocols are grouped into Information Units (IUs) for delivery to FC-2.*
  - *FC-3 – Common services layer, a thin layer that implements functions like encryption or RAID redundancy algorithms; multiport connections.*
  - *FC-2 – Signaling Protocol consists of the low-level Fibre Channel protocols; port-to-port connections.*
  - *FC-1 – Transmission Protocol, which implements line coding of signals.*
  - *FC-0 – PHY includes cabling, connectors, etc.*

Data Center Architecture and Connectivity

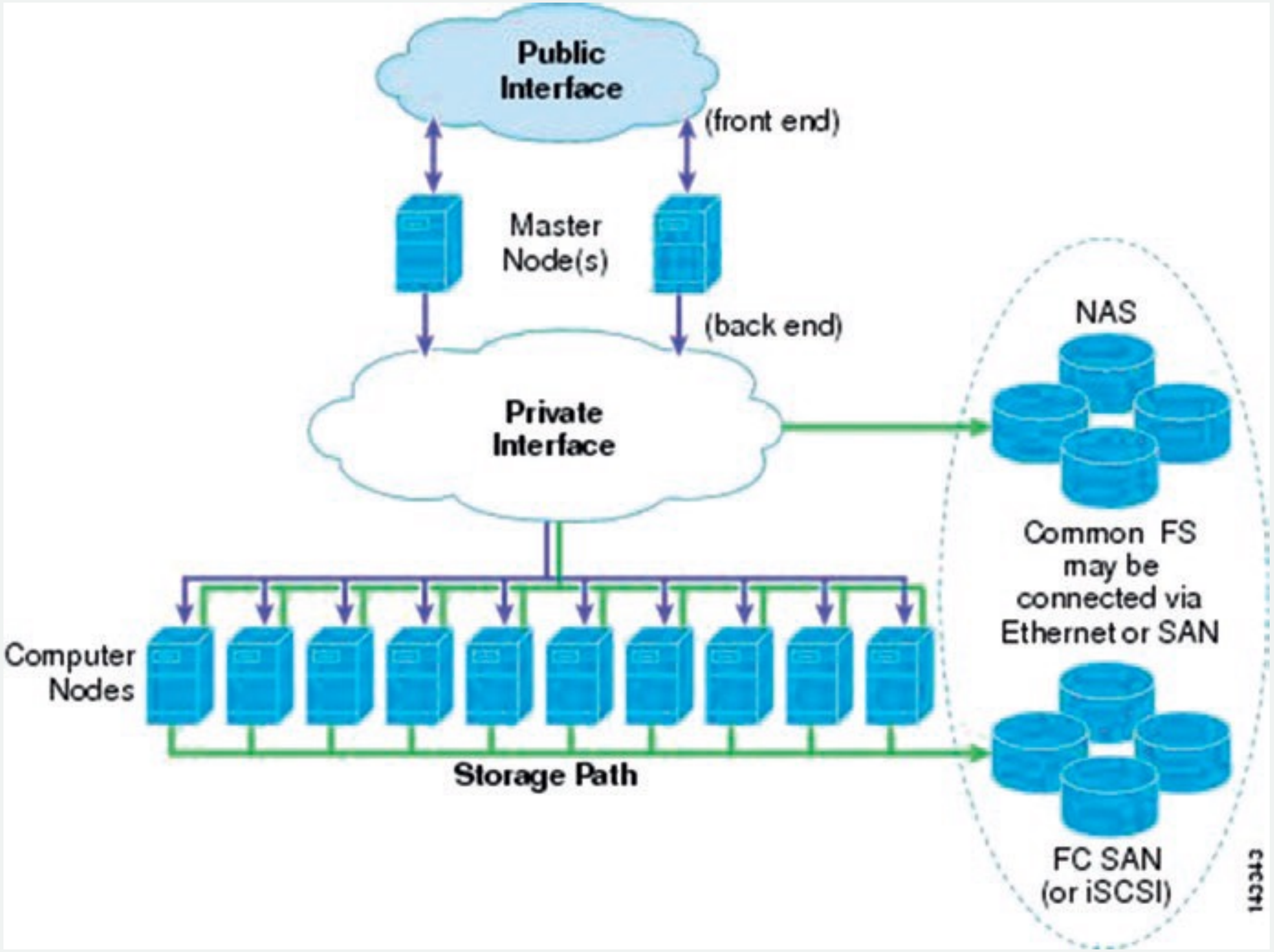
- Data center architecture is the physical and logical layout of the resources and equipment within a data center facility.
- A comprehensive design takes into account:
    1. Power and cooling requirements
    2. Racks of servers
    3. Storage arrays
    4. Network switches
    5. Security aspects
    6. IT management practices

Data Center Architecture and Connectivity

- Typically, the goal of a data center is to support one or more business services while considering the following factors:

  1. *Scalability: ability to increase compute or storage capacity as demand grows*
  2. *Performance*
  3. *Flexibility*
  4. *Resiliency*
  5. *Maintenance aspects*

Data Center Architecture and Connectivity



IT Evolution

- In regards Cloud Computing, evolution happen for:

Enterprise IT

Web Services

Enterprise IT

- Enterprise computing refers to business-oriented information technology that is critical to a company's day-to-day operations.
- One key aspect of enterprise computing is its high availability, as crash of a hardware or software component can lead to loss of revenue and customer base.
- Thus, multiple redundant computers exist for mission critical applications, as well as regular data backups are taken to ensure that there is no single point of failure within an enterprise.
- Nowadays, IT is the lifeblood of successful enterprise.

Web Services

- A Web service is an interface described by some form of service from a remote provider.
- These evolved from client-server and distributed computing concepts, to offer a "Web of Services," such that distributed applications can be assembled from a Web of software services in the same way that Websites are assembled from a Web of HTML pages.
- The advent of the Internet is based on a set of open standards, some of which are:

1. **TCP/IP**: Transmission Control Protocol/Internet Protocol, for network applications to exchange data packets in real time. Data is packed in byte packages, ranging up to 64 K (65,535 bytes). These are sent and acknowledged and, if not acknowledged, then sent again with multiple retries, until each packet arrives at the destination. These packets are then reassembled to create a complete copy of the information content in whole.
2. **RPC**: Remote Procedure Call allows functions written in C, Java, or any other procedural languages to involve each other across a network, allowing software services to reach other servers across the network.

Web Services

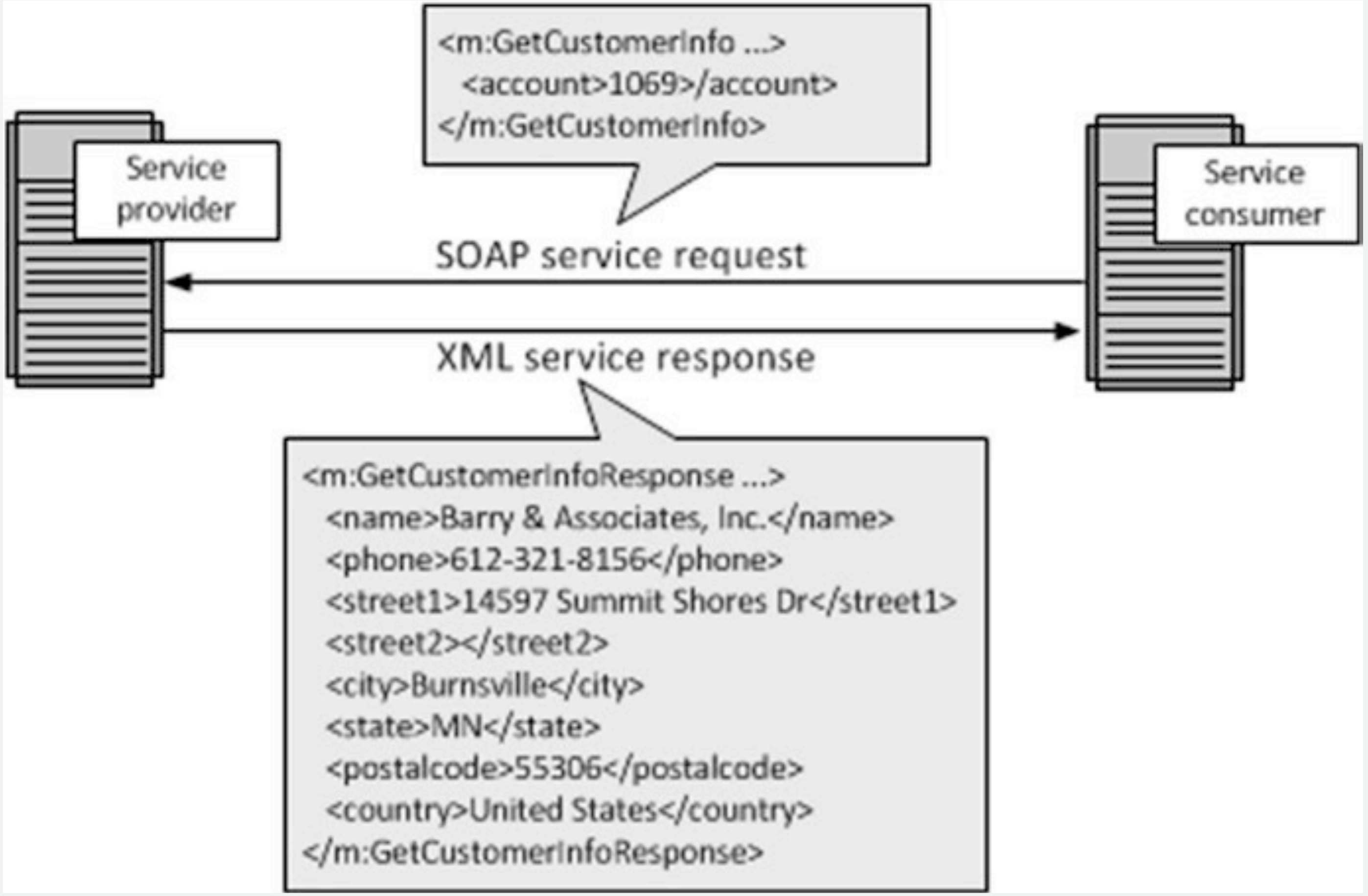
- The advent of the Internet is based on a set of open standards, some of which are:

3. **HTTP**: Hypertext Transport Protocol, for sharing data between machines based on top of TCP/IP protocol.
4. **HTML**: Hypertext Markup Language, the format for representing data in a browser-friendly manner.
5. **XML**: It stands for Extensible Markup Language. It enables any data to be represented in a simple and portable way. Users can define their own customized markup language, to display documents on the Internet.

Web Services

- The advent of the Internet is based on a set of open standards, some of which are:

6. **<u>SOAP</u>**: Service-Oriented Architecture Protocol, for connecting computers. It allows message passing between endpoints and may be used for RPC or document transfer. These messages are represented using XML and can be sent over a transport layer, e.g., HTTP or SMTP. An example of communication using SOAP and XML is shown in Figure.



```
<m:GetCustomerInfo ...>
  <account>1069>/account>
</m:GetCustomerInfo>
```

Service provider

Service consumer

SOAP service request

XML service response

```
<m:GetCustomerInfoResponse ...>
  <name>Barry & Associates, Inc.</name>
  <phone>612-321-8156</phone>
  <street1>14597 Summit Shores Dr</street1>
  <street2></street2>
  <city>Burnsville</city>
  <state>MN</state>
  <postalcode>55306</postalcode>
  <country>United States</country>
</m:GetCustomerInfoResponse>
```

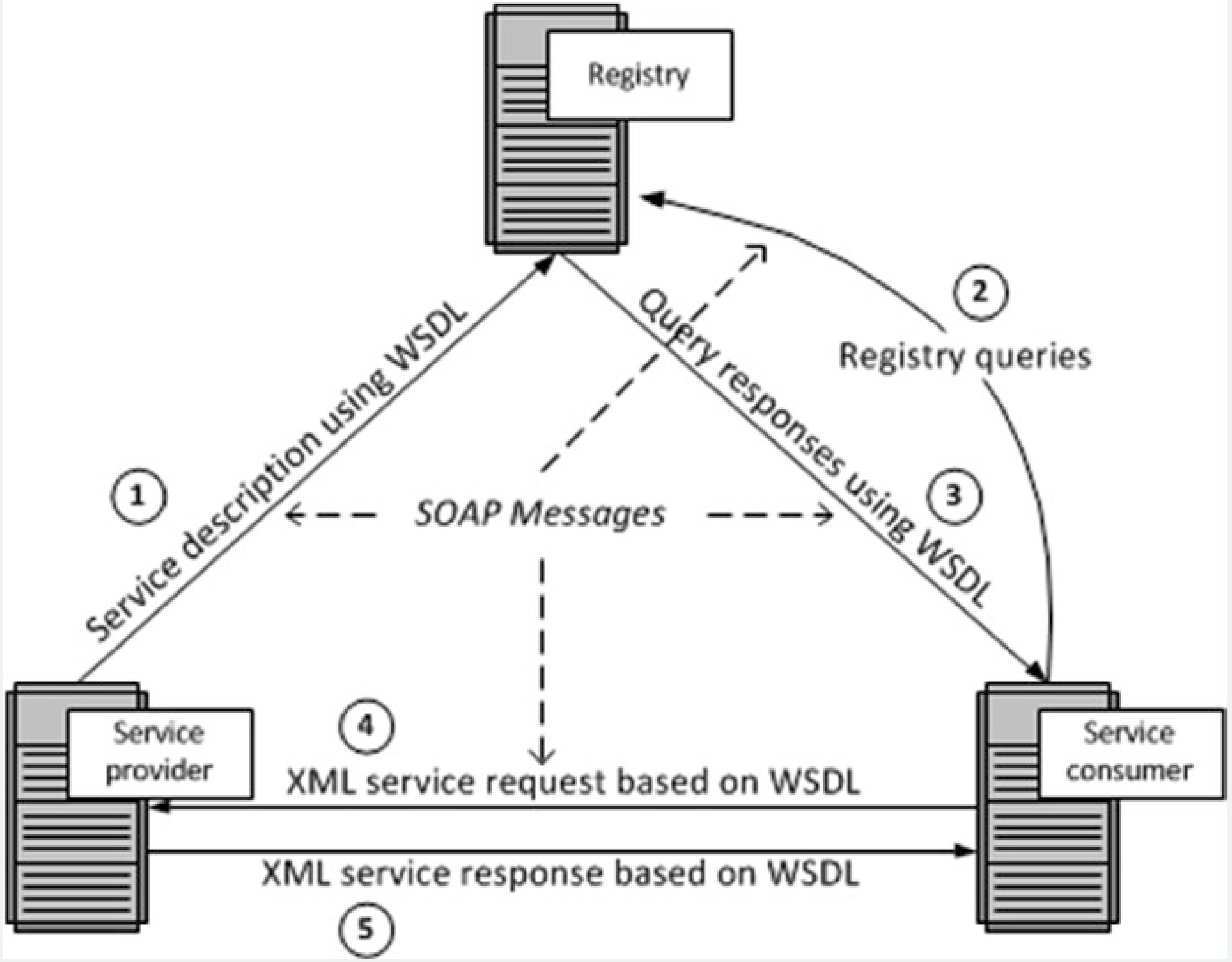
Web Services

- The advent of the Internet is based on a set of open standards, some of which are:

7. **UDDI**: Universal Description, Discovery, and Integration is an XML-based registry for businesses to list themselves on the Internet. It can streamline online transactions by enabling companies to find one another on the Web and make their systems interoperable for e-commerce.
8. **WSDL**: Web Services Description Language is used to describe a Web service in a document. It uses an XML format for describing network services as a set of end points operating on messages. These can contain either document-oriented or procedure-oriented information. The operations and messages are described abstractly and then bound to a concrete network protocol and message format to define an end point. The Web Services Description Language (WSDL) forms the basis for the original Web Services specification.

Web Services

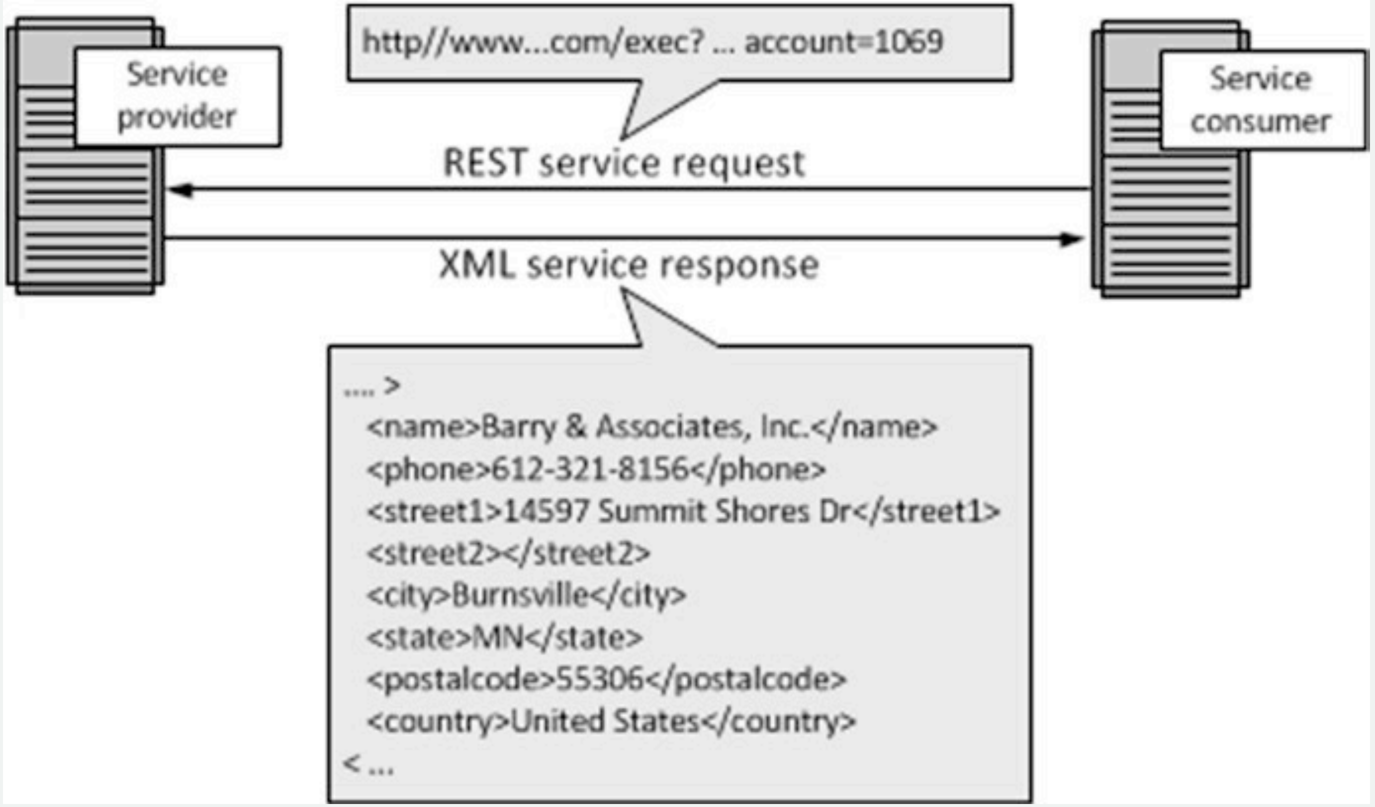
- Message Protocol using WSDL


Registry
2
Registry queries
Query responses using WSDL
3
1
Service description using WSDL
SOAP Messages
4
XML service request based on WSDL
Service provider
Service consumer
XML service response based on WSDL
5

Web Services

- The advent of the Internet is based on a set of open standards, some of which are:

9. **<u>REST</u>**: Representational State Transfer is a protocol used to create and communicate with the Web services. REST is language independent. Developers prefer REST due to a simpler style that makes it easier to use than SOAP. It is less verbose so less data wrappers are sent when communicating. An interaction is illustrated in Figure.

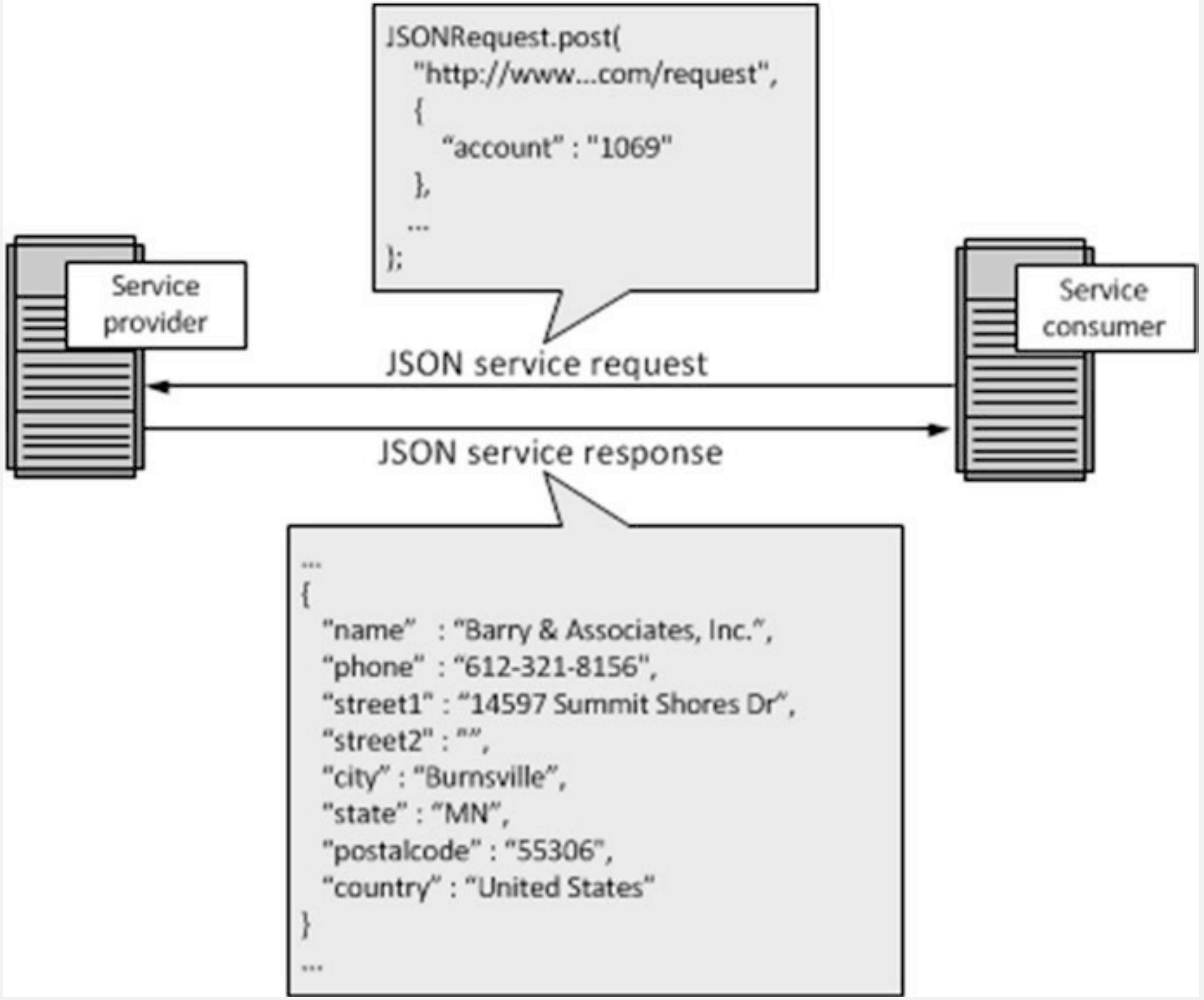


```
.... >
  <name>Barry & Associates, Inc.</name>
  <phone>612-321-8156</phone>
  <street1>14597 Summit Shores Dr</street1>
  <street2></street2>
  <city>Burnsville</city>
  <state>MN</state>
  <postalcode>55306</postalcode>
  <country>United States</country>
< ...
```

Web Services

- The advent of the Internet is based on a set of open standards, some of which are:

10. **<u>JSON</u>**: JavaScript Object Notation uses a subset of JavaScript. An example is shown in Figure. It uses name/value pairs and is similar to tags used by XML. Also, like XML, JSON provides resilience to changes and avoids the brittleness of fixed record formats. These pairs do not need to be any specific order.



```
JSONRequest.post(
  "http://www...com/request",
  {
    “account” : "1069"
  },
  ...
);
```

```
...
{
  “name”   : “Barry & Associates, Inc.”,
  “phone” : “612-321-8156”,
  “street1” : “14597 Summit Shores Dr”,
  “street2” : “”,
  “city” : “Burnsville”,
  “state” : “MN”,
  “postalcode” : “55306”,
  “country” : “United States”
}
...
```

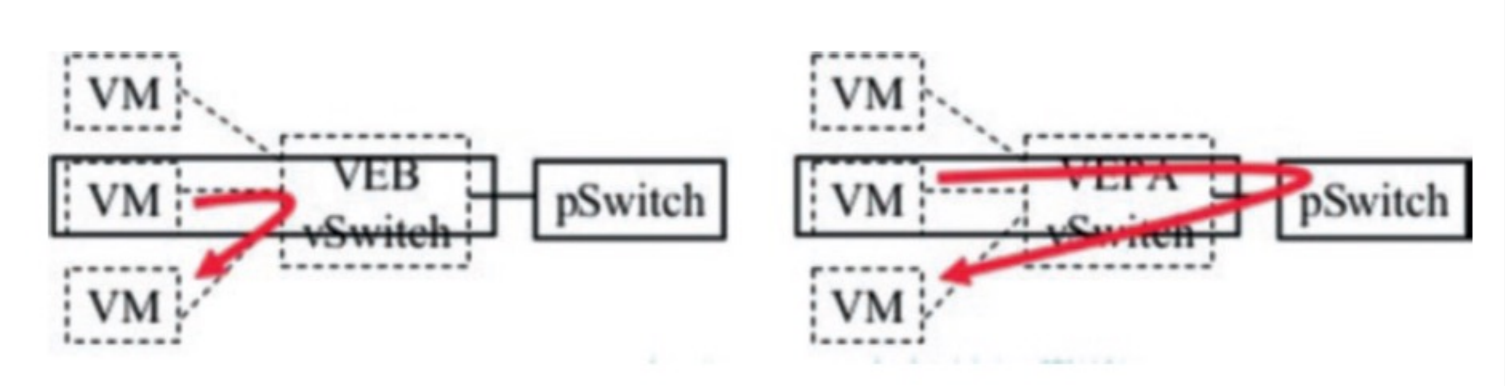
Web Services

- The advent of the Internet is based on a set of open standards, some of which are:

11. **DCB**: Datacenter Bridging (DCB) is a set of enhancements to the Ethernet protocol for use with clustering and storage area networks. Ethernet was originally designed to be a best-effort-based network, which can experience packet loss when the network or devices are preoccupied. TCP/IP adds end-to-end reliability to Ethernet but lacks the finer granularity to control the bandwidth allocation. This is especially required with a move to 10 Gbit/sec and even faster transmission rates, as such a network pipe can't be utilized fully by TCP/IP. DCB eliminates loss due to queue overflows (hence, called lossless Ethernet). It also includes a Priority-based Flow Control (PFC), an IEEE 802.1 standard that provides a link-level control mechanism.

Web Services

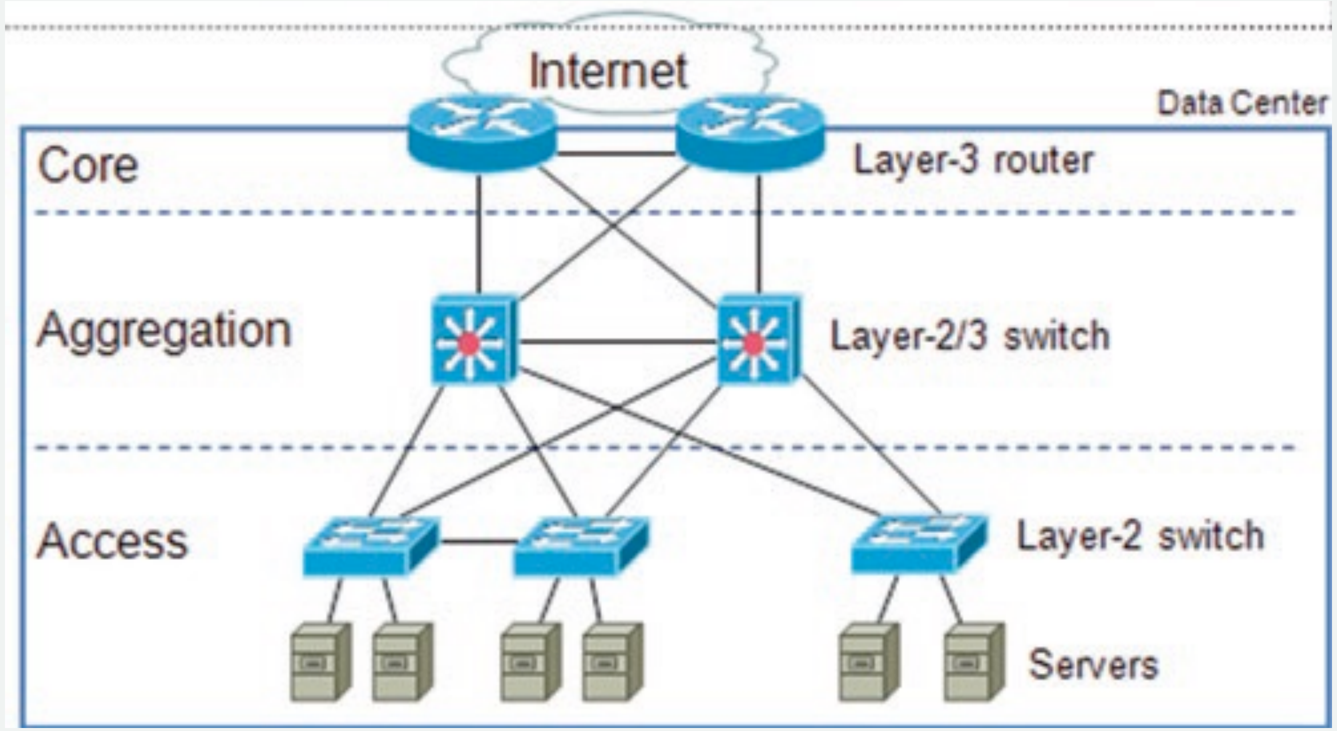
- Two methods for inter-VM communications



1. *Virtual Edge Bridge (VEB):* Switch internally in a VMM using CPU instructions.
2. *Virtual Ethernet Port Aggregator (VEPA):* An external switch that could be in a network interface card.

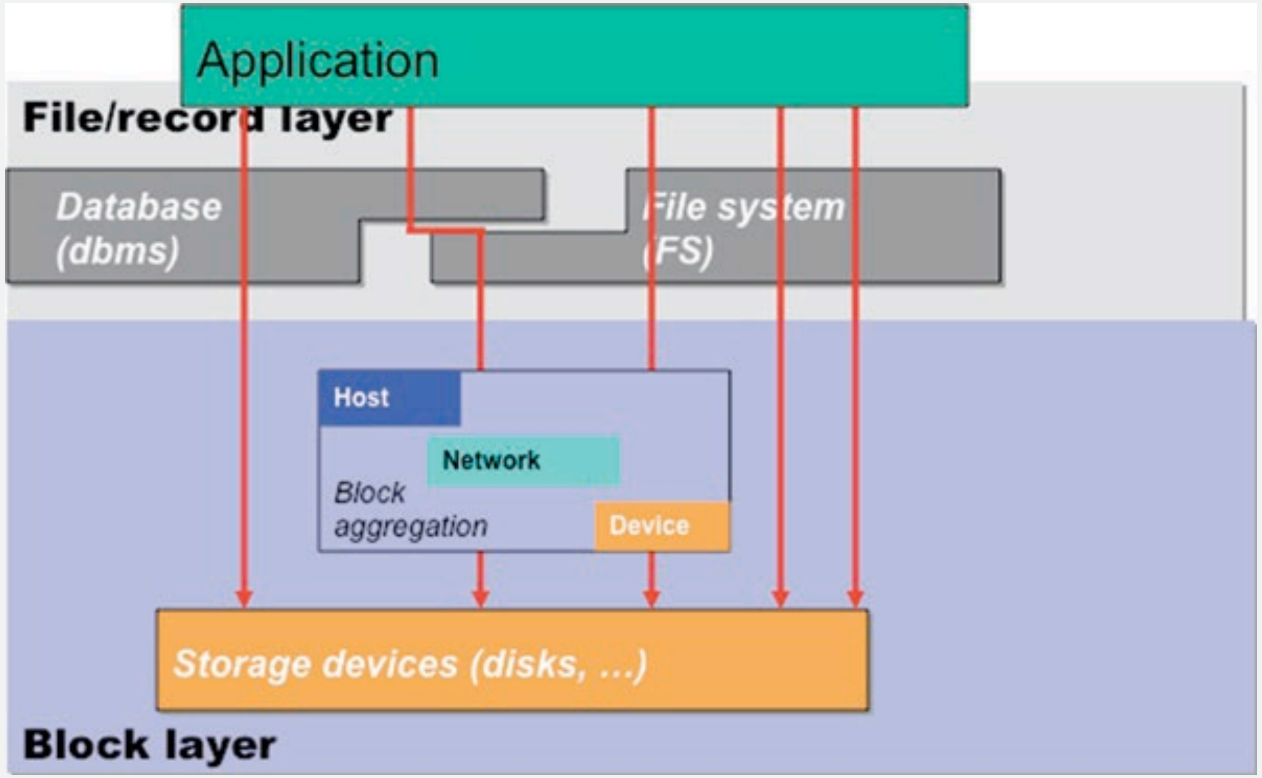
Server Operations in a Data Center

- The server stores or has access to a database, for which clients initiate queries from terminals.
- To support many servers in one place, in turn serving many users spread across a large area, one needs a lot of servers, routers, and switches. These server clusters are also called data centers (DCs).



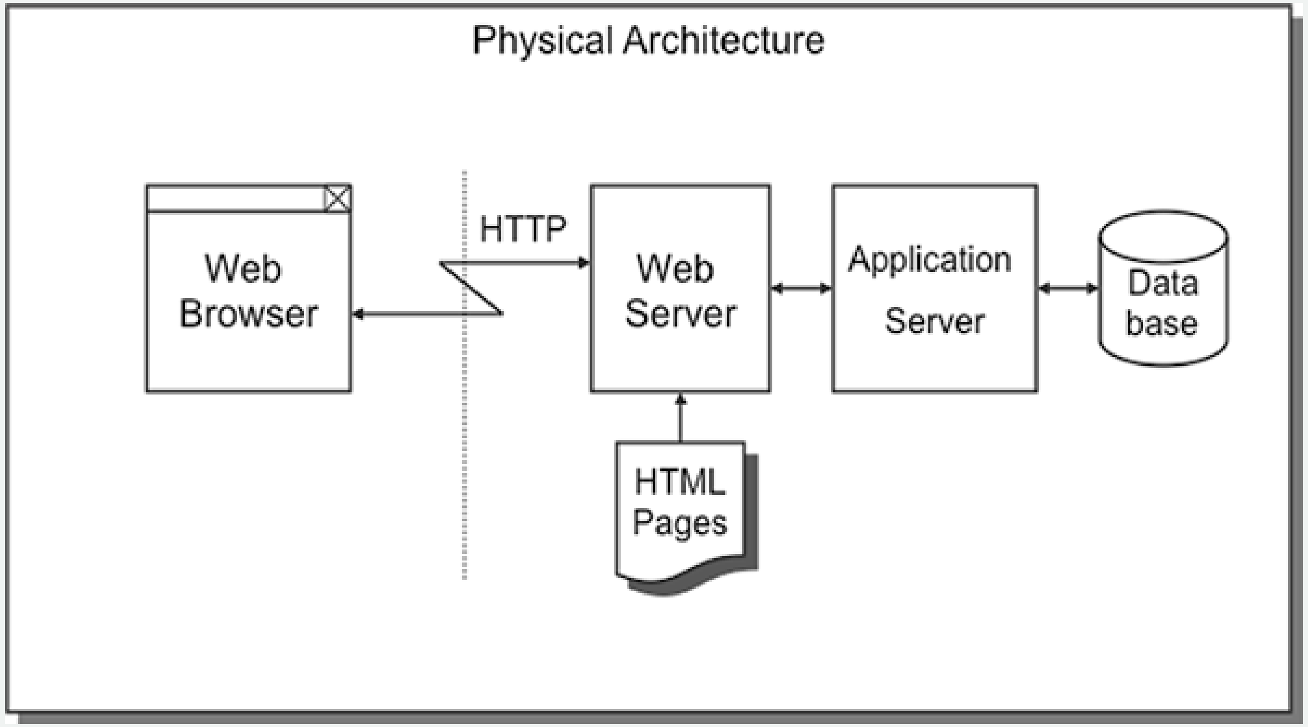
Server Operations in a Data Center

- These servers need to have massive storage, connectivity, and traffic management capability using switches. Of these, storage is a key capability required to provide large amounts of data needed by remote users, for which SNIA (Storage Networking Industry Association) has recommended storage architecture, as depicted in Figure.



Server Operations in a Data Center

- Web services are provisioned from a client's browser to access applications and data resident on remote servers in a remote data center. Figure represent this linkage.



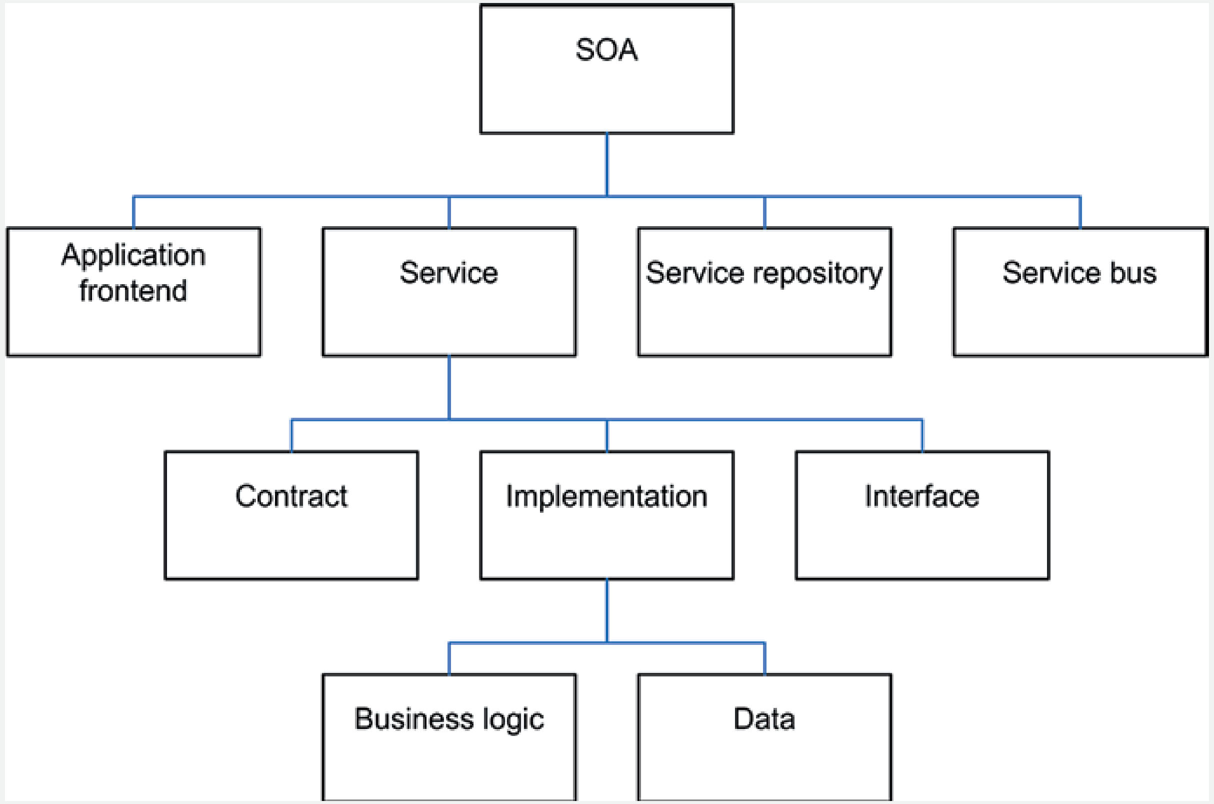
Evolution of Service-Oriented Architecture

- **A service-oriented architecture (SOA)** is a style of software design where services are provided to the other components by **application components**, through a **communication protocol** over a network.
- SOA is composed of loosely coupled set of services with well-defined interfaces. These services communicate with each other and are used for building higher-level applications.
- A service has four properties according to one of the many definitions of SOA:

1. It logically represents a business activity with a specified outcome.
2. It is self-contained.
3. It is a black box for its consumers.
4. It may consist of other underlying services.

Evolution of Service-Oriented Architecture

- Different services can be used in conjunction to provide the functionality of a large software application. So far, the definition could be a definition of modular programming in the 1970s. Service-oriented architecture is about how to compose an application by integration of distributed, separately maintained, and deployed software components, as shown in Figure.

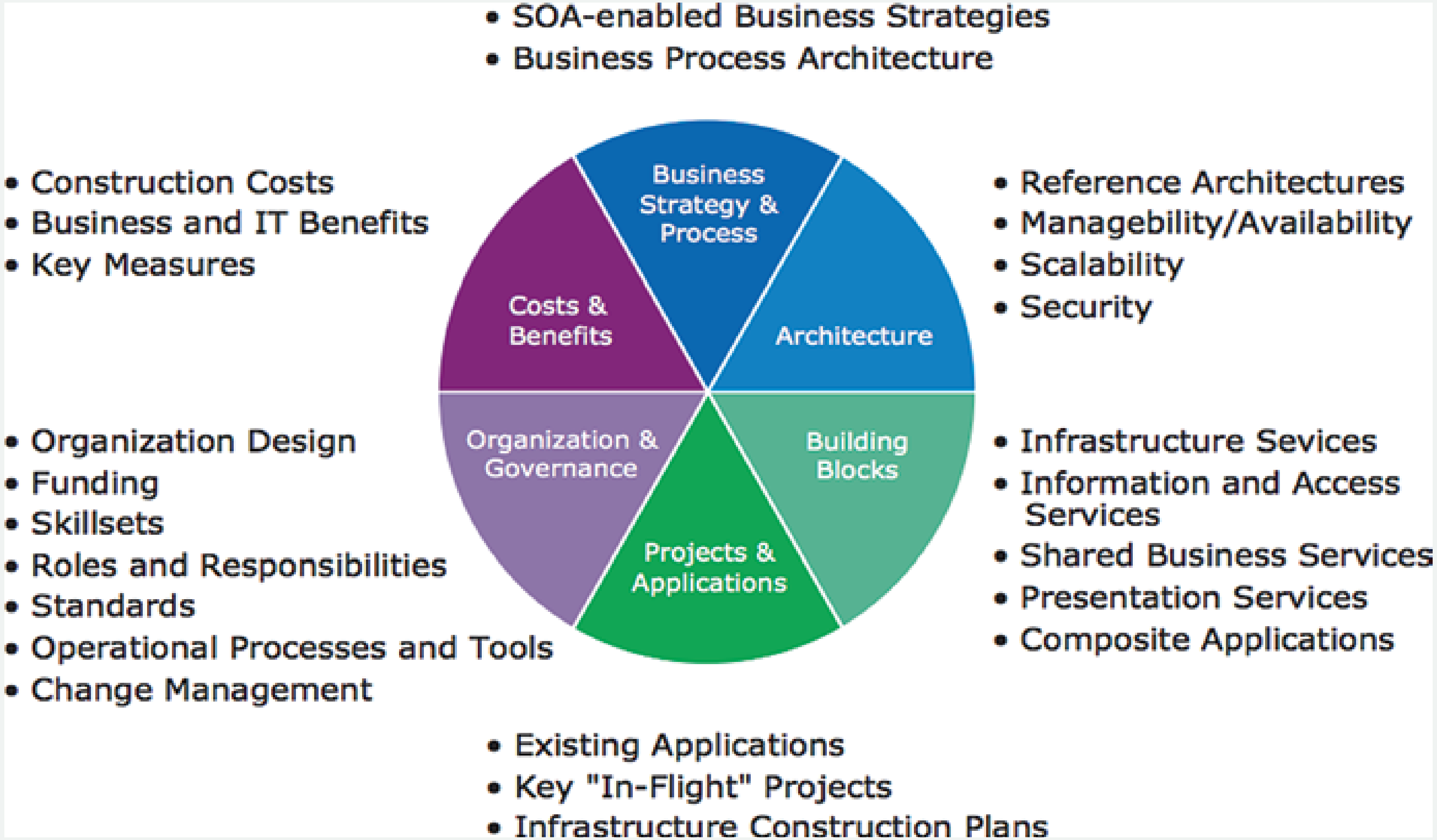


Evolution of Service-Oriented Architecture

- By organizing enterprise IT around services instead of around applications, SOA provides the following key benefits:
- Improves productivity, agility, and speed for both business and IT
- Enables IT to deliver services faster and align closer with business
- Allows the business to respond quicker and deliver optimal user experience

Evolution of Service-Oriented Architecture

- Six SOA Domains as Follow:



- SOA-enabled Business Strategies
- Business Process Architecture

- Construction Costs
- Business and IT Benefits
- Key Measures

- Reference Architectures
- Managebility/Availability
- Scalability
- Security

- Organization Design
- Funding
- Skillsets
- Roles and Responsibilities
- Standards
- Operational Processes and Tools
- Change Management

- Infrastructure Sevices
- Information and Access Services
- Shared Business Services
- Presentation Services
- Composite Applications

- Existing Applications
- Key "In-Flight" Projects
- Infrastructure Construction Plans

Transition from SOA to Cloud Computing

- SOA accelerates and supports Cloud Computing through the following vectors:

1. Faster application development
2. Reuse of services
3. Reduction of application maintenance
4. Reduced integration costs
5. Support of application portfolio consolidation

Basic Concept of Cloud Computing Security

- The previously defined Cloud Computing business models and implementation architectures have extended access to a wide variety of capabilities. Consequently, its security needs have also extended beyond the basic information security issues.
- However, basic security concepts still apply. Information security or INFOSEC begins with access control.
- Access control is based upon identity authentication.

  The entity to be identified can be a person, a device, or a computational process.
- These factors involve answering the four key questions of identity authentication:

1. What you have?
2. What you know?
3. What you are?
4. Where you are?

Basic Concept of Cloud Computing Security

- The next category of security for Cloud Computing is protecting information both during transmission and during storage.
- Protection of information includes keeping secrets and private data away from unauthorized entities, preventing changes by unauthorized entities, and detection of attempts at tampering with the data.
- Separate from security is the detection of errors due to transmission noise or equipment problems.
- While access control and information protection are required for preventing security breaches, some security attacks will occur.
- The detection of positional attacks and an appropriate response mechanism is required.