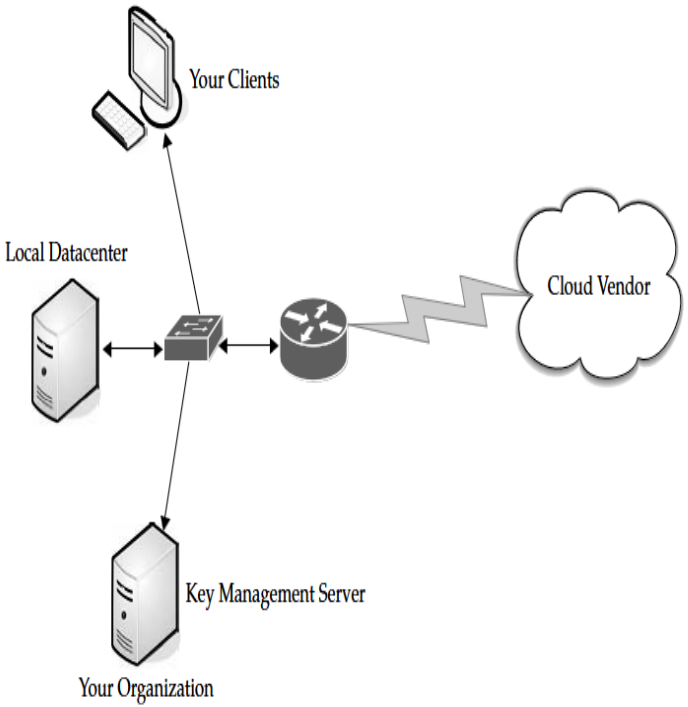
## Key Management

- With your data stored off-site, there's certainly opportunity for your data to be compromised. Your applications, compute cycles, and storage are not under your direct control, so while cloud vendors aspire to keep your data safe, you can never really be 100 percent sure that it's not at risk.
- Add to that the possibility that there may just be an accident that causes your data to be seen by others. Further, when you are done with data and try to purge it, there's no guarantee that it will be eradicated.
- Many cloud services simply do not erase freed storage and some do not even initialize storage when they assign it to you. In the event of a hardware or software failure, some cloud providers may not destroy data on failed machines.
- There are also concerns stemming from man-in-the-middle attacks. The point here is not to scare you away from cloud computing, but to remind you that safeguards must be taken and the tough questions asked.
- It's imperative that you cryptographically authenticate remote services and servers. This is accomplished through client and server certificates that let you know you are connecting securely to your cloud assets.
- Remote services must also be cryptographically protected. You use an authorization infrastructure, like Kerberos, to ensure that you are properly authenticated.




Cloud computing key management diagram

- With cloud storage, be sure to protect it cryptographically as well.
- This includes encrypting the data you store and ensuring that data is set up to be destroyed when the storage key is destroyed.
- This process will make your data more secure, but it also requires a lot of keys. Keys on the server include
- Transport keys
- Authentication keys
- Authorization tokens
- File encryption keys
- Hardware storage keys
- Revocation keys
- Certificates

**Basic Public Internet**

- The first option is the pipe most of us have coming into our office or homes. The public Internet is the most basic choice for cloud connectivity.
- This is the type of access that you buy from an Internet service provider (ISP) and connect with via broadband or dial-up, based on your location.
- There are no extras like Transmission Control Protocol (TCP) acceleration, advanced compression, or application-specific optimization.

**Advantages:**

- There's a large audience. Anyone with Internet access can use this solution.
- It's highly fault tolerant.
- Many provider options are available.
- Secure Sockets Layer (SSL)–based, Hypertext Transport Protocol Over Secure
- Sockets Layer (HTTPS), encrypted access provides confidentiality.
- It's cost-effective.

**Disadvantages:**

- Lack of end-to-end quality of service (QoS), thus making end-to-end service-level agreements (SLAs) difficult to reach.
- Probability of poor response over high-latency connections. This is worsened by protocol inefficiencies in TCP, HTTP, and web services, Downtime that might be out of your control.

## The Accelerated Internet

- Employing advanced application delivery features on top of your Internet connection can benefit both the service provider and the client.
- Cloud improvement can increase by 20 percent to 50 percent by offloading network-related functions from the server.
- SSL termination and TCP connection management remove a significant amount of processing from the front-line servers.
- Additionally, dynamic caching, compression, and prefetching results in better than a 50 percent performance increase for end users.

**Some providers offering this service include**

- AT&T Hosting
- Citrix NetScaler
- F5's WebAccelerator

- Organizations opting for this method of connectivity should look at SLAs and monthly bandwidth charges, rather than worry about what acceleration methods the service provider is adding.

- At the cloud, this method of acceleration requires the installation of a server-side appliance. At the end user, it normally requires the installation of a downloadable client.

## Optimized Internet Overlay

- An optimized Internet overlay approach allows customers to access the cloud via the public Internet, but enhancement occurs on the provider's cloud. Enhancements at these points of presence (POP) include
- Optimized real-time routing. This helps avoid slowdowns, helping to make SLAs easier to attain.
- An SSL session can be stopped so that protocols and payload can be optimized and re-encrypted.
- **Some of the application logic can reside on the POP. This allows for better scalability, fault tolerance, and response time, usually in excess of 80 percent.**
- Content that is frequently accessed can be delivered from local caches.
- Disadvantages of this method include
- It is costlier than public Internet connectivity, sometimes as much as four times as much.
- There is a strong vendor lock-in if the application is distributed into the carrier's network.

## Site-to-Site VPN

- The fourth option is to connect to the service provider directly using a private wide area network (WAN) (normally an MPLS/VPN connection). This setup allows confidentiality, guaranteed bandwidth, and SLAs for availability, latency, and packet loss.

- MPLS can also scale to meet changing bandwidth needs, and QoS can also be written into the SLAs. On the downside, private WANs are not normally more reliable than Internet connections, especially redundant connections to multiple ISPs.

## Cloud Providers

- Cloud providers that use services dispersed across the cloud need a robust connection method. Private tunnels make sure that bandwidth, latency, and loss aren't as likely to affect performance. Encryption and strong authentication offer another benefit.

- Cloud providers that are growing might face big costs as network bandwidth charges increase. This traffic is from traffic both to and from clients as well as traffic among provider sites. Big providers, like Google, are able to sidestep these charges by building their own WANs with multiple peering points with major ISPs.

| Connection Method | Description | Examples of Use |
|---|---|---|
| Basic public internet | Anyone can use it<br>Fault tolerant<br>Multiple providers<br>Cost-effective<br>Performance issues for globally delivered applications | Consumer applications<br>Advertising supported services<br>Applications where "best effort" service is sufficient |
| Accelerated internet | Improved end-user performance<br>Inconsistent performance, based on provider and ISP configuration<br>Low cost | Best for cost-sensitive service where improved response times and bandwidth are necessary |
| Optimized overlay | Consistent performance<br>Ability to have strong SLAs<br>Expensive<br>Limited provider options<br>Provider risk | Business-critical applications that require SLAs delivering promised response times and bandwidth |
| Site-to-site VPN | Ability to have strong SLAs<br>Site-specific delivery<br>Consistent performance<br>Lowest latency<br>Limited reach | Business-critical applications, including server-to-server traffic |

Features of Connectivity Options

**Cloud Consumers**

- Large companies can build their own scalable distributed IT infrastructure in which datacenters are connected with their own private fiber optic connections.
- This depends on distance, bandwidth requirements, and budgets.
- Clients located at major sites normally access applications over the corporate WAN.
- For smaller offices or mobile workers, VPN connections across optimized and accelerated
- Internet services provide a more robust solution.
- VPN tunnels across the Internet are best as a primary link only when high performance is not crucial.

**Pipe Size**

- Bandwidth is, simply put, the transmission speed or throughput of your connection to the Internet.
- There are three factors that are simply out of your control when it comes to how much bandwidth you need:
- The Internet bandwidth between your organization and the cloud
- The round-trip time between your organization and the cloud
- The response time of the cloud

## Upstream/Downstream

- Another factor to consider is whether it is okay for the transfers to be symmetric or asymmetric. If your connection with the cloud is symmetric, then that means you are sending and receiving data at the same rate.

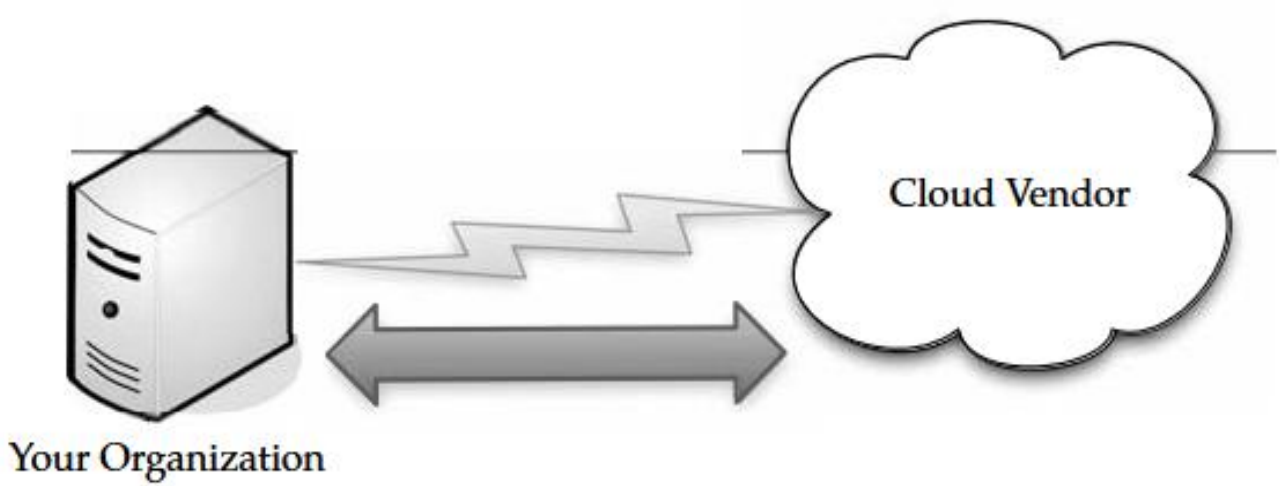
- If your connection is asymmetric, then data is sent from your organization at a slower rate than you're receiving it. For instance, ADSL connections send and receive data at different rates. The "A" in ADSL stands for asymmetric. Depending on what service we're talking about, data can be received at 1.5Mbps while it is sent at 750Mbps.

- Your organization is likely connecting to its ISP using something more robust than DSL, and in most cases those connections are symmetrical.

- Consider also that the Internet changes from one moment to the next in ways that are impossible to predict. Data moves through different routers and network appliances.

- Your speed will vary from time to time. It may not be noticeable, but it does fluctuate. As such, even though you're paying for a T1 line, don't call the phone company to complain right away there's always a delay somewhere.

- The best rule of thumb is that if you are consistently measuring 85 percent of your nominal bandwidth, then you're doing okay. Perform an Internet connection test several times a day. Try it first thing in the morning,




Be cognizant of how fast data is able to be sent
in addition to how fast you are able to receive data.

## How Much Do We Need?

- How much data will be moving in and out of the cloud at any given time, and then decide how big of a pipe you need to move that data.
- Chances are good that you have a beefy enough Internet connection to make cloud computing viable.
- However, realize that the more you do on the cloud, the more demand will be placed on your Internet connection. If you do not have enough capacity, then everyone will experience a slowdown.
- Take the time to figure out how much capacity you'll use, and make sure you have enough resources to accommodate that need.
- It's important to secure an SLA that meets your bandwidth requirements. This not only ensures that you are getting the speed that you need, but if the ISP fails to meet those levels, there can be some sort of remediation in it for you.

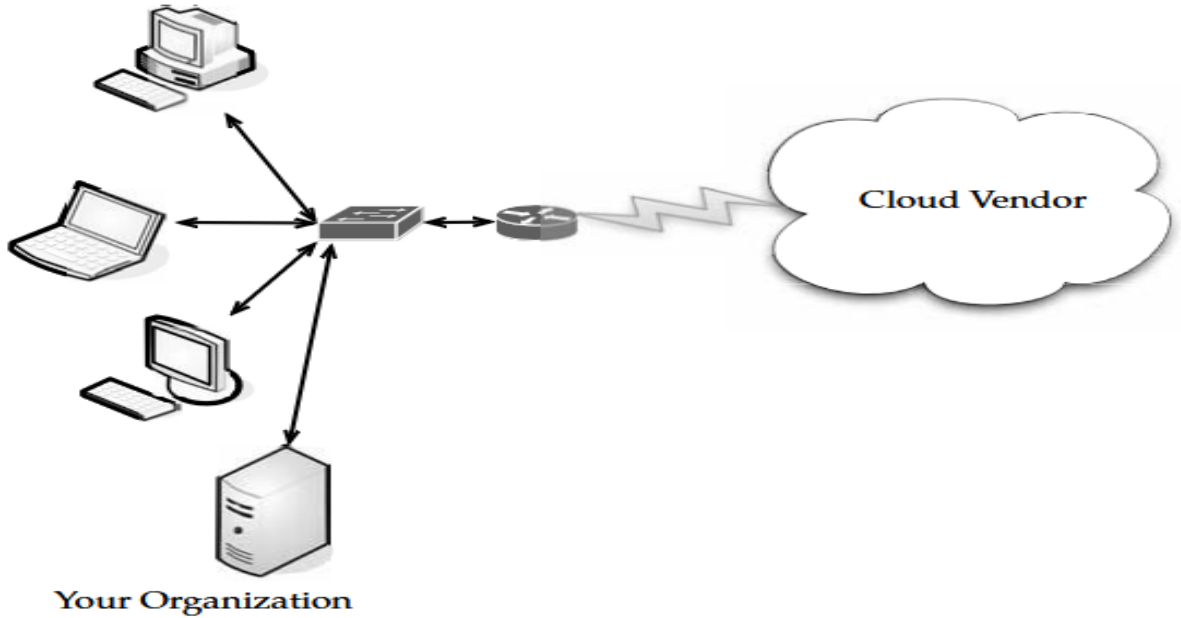
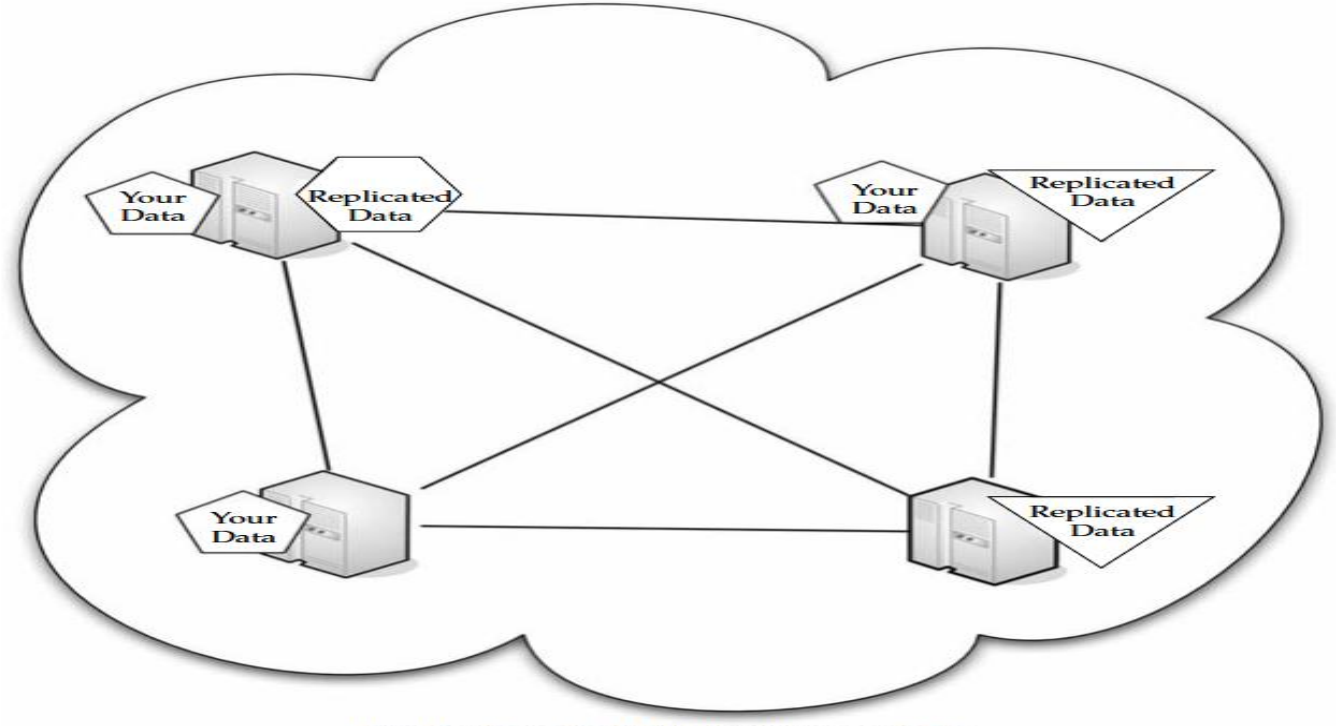



Figure out how much capacity all your clients will use when accessing the cloud, and ensure you have a big enough pipe to accommodate that need.

## Redundancy

- When formulating your cloud infrastructure, be sure to consider the issue of reliability and uptime and ask your service provider to configure your computing infrastructure for redundancy and failover.
- Redundancy used to mean that another server or two were added to the data center in case there was a problem.
- These days with virtualization, redundancy might mean a virtual server being cloned onto the same device, or all the virtual servers of one machine being cloned onto a second physical server.
- It becomes more complex in the cloud. While you may think of your server being hosted at the datacenter of your cloud provider, it’s not as easy to nail down.
- Parts of your data may be housed in one location and other parts scattered throughout the country.
- When the provider adds a redundant system, again the data is scattered throughout their cloud. So it’s not an issue of the service provider wheeling in a new server to provide redundant services. Rather, they simply reallocate resources to give you a redundant system.




The cloud vendor is likely to have your data and its redundant clone in geographically dispersed locations.

**Services :**

- There are different services you will need to run, depending on your cloud provider and what your organization does. Also, these services will likely affect how your cloud infrastructure is deployed.

**Identity :**

- No matter where an application runs—in-house or on the cloud—it needs to know about its users. To accomplish this, the application asks for a digital identity—a set of bytes—to describe the user.

- Based on this information, the application can determine who the user is and what he or she is allowed to do. In-house applications rely on services like Active Directory to provide this information.

- Clouds, however, have to use their own identity services. For instance, if you sign on to Amazon cloud services, you have to sign on using an Amazon-defined identity. Google's App Engine requires a Google account, and Windows uses Windows Live ID for use with Microsoft's cloud applications.

- Identity services need not be proprietary. OpenID is an open, decentralized, single sign-on standard that allows users to log in to many services using the same digital identity.

- An OpenID is in the form of a uniform resource locator (URL) and does not rely on a central authority to authenticate a user's identity.

- Since a specific type of authentication is not required, nonstandard forms of authentication may be used, including smart cards, biometric, or passwords.

OpenID authentication is used by many organizations, including:

- Google
- IBM
- Microsoft
- Yahoo


OpenID is a means to keep login information consistent across several sites.

**Integration :**

- Applications talking among themselves have become highly common. Vendors come up with all sorts of on-premises infrastructure services to accomplish it. These range from technologies like message queues to complex integration servers.
- Integration is also on the cloud and technologies are being developed for that use, as well. For example, Amazon's Simple Queue Service (SQS) provides a way for applications To exchange messages via queues in the cloud.
- SQS replicates messages across several queues, so an application reading from a queue may not see all messages from all queues on a given request. SQS also doesn't guarantee in-order delivery.
- In fact it's these simplifications that make SQS more scalable, but it also means that developers must use SQS differently from on-premises messaging. Instead of using queuing, BizTalk Services utilizes a relay service in the cloud, allowing applications to communicate through firewalls.
- Cloud-based integration requires communicating through different organizations, the ability to tunnel through firewalls is an important problem to solve.

**Mapping :**

- Maps are becoming more and more popular in web applications. For instance, hotel and restaurant web sites show their locations on their web sites and allow visitors to enter their addresses to get customized directions.

- The guy who developed the web site likely didn't have the time or money to make his own mapping database. Enough organizations want this functionality, however, so it is offered as a cloud application.

- Google Maps and Microsoft's Virtual Earth provide this cloud-based function, allowing developers to embed maps in web pages.

**Payments :**

- Another cloud service that you might want to plan for and configure your hardware appropriately for is payments. Depending on your organization, you may or may not want to accept online payments from customers. Luckily, there is no lack of ways to get paid online.

- You can simply sign up with a service to accept credit cards, or you can go the route of PayPal. With an online payment service, customers can send money directly to your organization.


These services are really just additions to existing web sites.

**Search :**

- The ability to embed search options in a web site is certainly nothing new, but it is rich feature that you might want to employ in your own web or application development.
- Microsoft's Live Search allows on-site and cloud applications to submit searches and then get the results back.
- Searching is limited only to the organization and what it does. For instance, a company might develop an application that does both.
- For instance, let's say a company has a database of movie information.
- By typing in the name of the movie, you can search its own database as well as a search of the Internet to give you two types of results what's stored in the company database as well as what's on the entire Web.
- If you were to use a single computer to access the cloud, the requirements are pretty minimal all you need is a computer and an Internet connection.