WEB TECHNOLOGY

SEM IV

QUESTION PAPER SOLUTIONS

MIM 2011 – 2014 Batch

Question Papers :

2011

2010

2007

2006

2003

Collated by Nishant Vyas, Alvito Colasco & Prasad Sampat.

1. Internet has revolutionized the way business is transacted in various industries today as compared to pre-internet era (20m)

   Ans: Worldwide influence of the internet is well-established and acknowledged. Penetration rate of the internet has been phenomenal; almost 1/3rd of Human population are accessing the internet. The way business is conducted in this digital age has changed due to so many people logged on to the internet.

   Advancement in communication and information technology has further strengthen the role of the internet in business. The internet is widely used in organization for marketing and promotion of products and services. The internet is used to deliver customer support, share information and provide training to employees. With the internet becoming a powerful tool for employees, the impact on business is undeniable.

   Internet and Porter's Five Force Model

   Porter's five force model is a framework for industry analysis, business strategy development and study competition. The five forces of the model are the threat from upcoming and future competition, threat from existing substitute, bargaining power of consumers, negotiating power of suppliers and threat of competition. Internet has great Impact on all five force of the model:

   Threat of new entrants: The internet has considerably lowered entry barrier in setting up new enterprise. The setting up of a new company does not require much capital investment, for example, online retail sites, etc. Ever increasing competition has lowered the margins.

   Threat of new substitute: The Internet has reduced the product life cycle; shelf life of products and encouraged innovation is customer serving.

   Bargaining power of customers: The internet has made the customer well informed about products and available substitute. Companies have to be careful in presenting differentiation and pricing.

   Bargaining power of suppliers: Suppliers are well informed about happening in the industry thanks to the internet.

   Threat of competition: The internet has made transparency and honest important factor in success of the company. Customers tend to know more about the company. The internet has lowered the cost of searching new available products.

   Internet and the way business is conducted

   The internet has changed the face of business. It has opened up new avenues of conducting business. Below are some impacts of the internet on business:

Communication: communication technology combined with the internet has given a new dimension to connectivity and dispersion of information. Employees are in constant touch through email, instant messaging, office intranet, etc.

Collaboration: The internet has facilitated collaboration among employees of organization. Geographical boundaries no longer hamper project work and sharing of information.

Business Transaction: The internet has encouraged the culture of online business or e-commerce. In recent years many players have opened shops through e-commerce. Internet banking, payment gateways, etc. are part of normal supply chain transaction.

Work Flexibility: The internet has enabled workers to log in from remote location and home. It has helped on the move employees by remaining in touch with happenings of work.

Web based application: The internet has facilitated the development of concept like cloud computing, which has enabled process and storing of data in large proportion. The internet has helped reduce infrastructure cost of the company.

The internet thus has made a big impact in the way the business gets conducted in both positive as well as a negative way. The internet has made many business obsolete example post offices. Online security issues like hacking, identity theft, etc. are a constant threat to internet users.

- http://www.managementstudyguide.com/impact-of-internet-revolution-in-business.htm
- http://www.forbes.com/sites/michakaufman/2012/10/05/the-internet-revolution-is-the-new-industrial-revolution/
- http://en.wikipedia.org/wiki/Digital_Revolution

2. “You have to be 24x7 shop open at all times in ecommerce age” (10m)

Ans: **Five Trends Driving Traditional Retail Towards Extinction**

The e-commerce behemoth is coming, but that’s no longer news. Amazon is nearly 20 years old now, eBay just a year younger. What is news? The behemoth is arming itself. New tactics, new friends and a hefty war chest mean that the old defenses insulating traditional retailers are no longer enough. Venture funds dished out $242 million to online retail startups in the last quarter alone, more than any other period since 2000. E-commerce, meanwhile, is now a $200 billion-plus industry in the U.S., set to ratchet up 15% a year as consumers realize there’s no reason to trek out to the local strip mall anymore.

In the retail arms race, e-commerce is winning. Here are five trends driving traditional retail towards the grave:

1.) Voluntary Conversion

The smart brick-and-mortar players recognize the inevitable rise of online shopping and are adapting to the new realities. Take Macy's: The 154-year-old retail chain saw online sales rise 40% in 2011 while same-store sales grew just 5.3%. The company is transforming nearly 300 of its stores into distribution centers to speed up shipping for online consumers. Expected to do more than $2 billion in online sales this year, they're even toying around with in-storeonline kiosks to help customers scan and compare prices.

Nordstrom, a whippersnapper compared to Macy's at 111 years old, is taking an even more aggressive approach. With free shipping and free returns in its online store, the company has notched three straight quarters of 35% gains in online sales. Nordstrom is integrating its online and in-store strategies by introducing mobile point-of-sale systems–modified iPod touches–that eliminate lines while helping sales clerks sell customers out-of-stock items. According to Barron's, the company plans to invest $1 billion (one third of its capital expenditures) into online efforts over the next five years.

While adapting their own infrastructure to serve online consumers, Nordstom is also keeping pace with innovation in the space via acquisitions and investments. Last year, the retailer spent $180 million on flash sales siteHauteLook and led a $16.4 million investment in Bonobos, an online retailer of men's clothes.

The online practices of veteran players validate e-commerce in the minds of older consumers while accelerating the industry's growth. It also means they get to survive.

2.) A Losing Cost Structure

When you purchase an item at Bloomingdale's, odds are that it's been marked up at least three times. Once when it changed hands from the factory to the brand, again as it passed from the brand to Bloomingdale's, and once more as it goes from Bloomingdale's into your shopping bag. The result is a purchase price that's some ungodly multiple of the item's actual cost, usually between 2x and 5x.

Brands that operate exclusively online–Frank and Oak, Bonobos, orModCloth for example–eliminate that last markup by selling directly to consumers. By taking ownership of the design, curation and retail aspects of the business, these companies can keep hefty margins for themselves while still undercutting brick-and-mortar competitors on price. And because their stores are made out of bits instead of stone, they don't face the costs of maintaining unwieldy networks of physical locations. As for the legions of sales clerks that retailers pay? A single web developer probably replaces twenty of them.

3.) Free Delivery, Free Returns

Even if shipping costs don't negate the price savings of online shopping, they've long acted as a source of friction. Asking consumers to factor in some uncertain, variable transaction cost is never a good way to do business, and asking them to pay for returns is even worse. The experience of returning an online purchase, paying two-way shipping costs and ending up with nothing–except $15 in the red–is enough to make anyone wary of online shopping.

Tony Hsieh and Zappos figured this out long ago and built a $1.2 billion business on the idea of free shipping and free returns. This policy is now *de rigeur* for serious, full-price e-commerce companies. (Flash sales is a different beast.) The reason is very simple. According to Amanda Bower, a business professor at Washington and Lee University, online shoppers given free returns increase their spend on the same site by 50 to 350 percent in later purchases. When they had to pay for return shipping? The value of their purchases decreased.

Free shipping and returns will be standard for e-commerce companies from now on. One less reason to schlep to the mall.

4.) Subscription Commerce

Call it the "set it and forget it" school of business. The bottom line: People are lazy and certain items just make sense to receive once a month. At the danger of touting a model that has already become a cliche (flash sales was a cliche until it proved itself), I should point out that only certain categories of products work for this model. (Battery Ventures partner Brian O'Malley wrote a fantastic post on this topic.) Razors, as you might imagine, make much more sense as a monthly delivery item than sweaters.

The foundation of the model is recurring revenue, where customers sign up to receive a monthly shipment for a set monthly fee. This is attractive to companies because it creates a steady, predictable revenue stream, not unlikeSaaS businesses. It's attractive to consumers because the system is convenient and usually cost-efficient compared to alternatives. Dollar Shave Club, for example, ships men's razors to customers once a month at a fraction of the cost of an in-store purchase. Men save money and a trip to the convenience store. And because DSC sources their razors directly from the manufacturer and sells them directly to the customer, they still enjoy comfortable margins.

Keep reading on the next page…

Follow me @JJColao and on Facebook. Check out my blog here. Frank and Oak deploys a more complex model that attempts to coax volume from loyal customers. The company allows shoppers to choose three items of clothing from a monthly collection. After receiving the items, customers try them on at home, then decide which they'll keep and which they'll return–all for free of course. Customers then pay for the clothes they want and return the others. Other notable subscription companies include BirchBox,Manpacks and JustFab.

There will be losers in this space as mindless copycats go out of business. But as sensible companies hone their models, subscription commerce will take a dent out of categories previously deemed safe from the digital threat–toiletries, cosmetics, pet food and groceries to name a few.

5.) Fit Without The Fitting Room

There are two categories of players here: Companies that offer custom, tailored clothing online, and those that rely on new technologies to guide customers to a better fit.

The first is popular with men's clothing companies, with startups like J. Hilburn, Indochino and Blank Label selling tailored suits and shirts at a discount to conventional custom options. The appeal here is the sudden accessibility of tailored clothing, both in terms of price and convenience. Because of the price structures discussed above, they can get away comparable quality at reasonable prices while still making a profit.

The second category is more interesting and will have more far-reaching consequences for the future of retail. First we have the incremental innovation of companies like Clothes Horse and True Fit, which ask shoppers for their measurements, along with a tally of their best-fitting clothes, to match them with the right sizes. Frank and Oak, Bonobos and women's retailer Nicole Miller use Clothes Horse while Macy's employs True Fit to increase conversions. True and Co. uses similar methods to match women with well-fitting bras.

Even larger leaps in sizing technology are being made by companies likeAcustom Apparel, which uses 3D body scanners along with pattern-making software to scale the creation of custom-fitted clothing at a digestible price point.

At some point, data about your body type will be saved along with your credit card information and you'll never have to visit a fitting room again.

Bonus Trend: Crowdfunding

Secure, widespread group-paying and crowdfunding applications will make it easy to split the cost of large ticket items over the web. These will also introduce new forms of commerce which have yet be seen. Here's a hint of what's to come.

- Ecommerce in India: http://www.zdnet.com/e-commerce-comes-of-age-in-india-7000012009/
- http://en.wikipedia.org/wiki/E-commerce

- http://www.forbes.com/sites/jjcolao/2012/12/13/five-trends-driving-traditional-retail-towards-extinction/print/
- Everything about Ecommerce: http://www.dawninfotek.com/resources/pdf/The.pdf

3. Explain the workflow in eprocurement application. Discuss advantage of the Internet in this business function in terms of business benefits. (10m)

E-procurement (**electronic procurement**, sometimes also known as supplier exchange) is the business-to-business or business-to-consumer purchase and sale of supplies and services through the Internet as well as other information and networking systems, such as Electronic Data Interchange and Enterprise Resource Planning. Typically, e-procurement Web sites allow qualified and registered users to look for buyers or sellers of goods and services. Depending on the approach, buyers or sellers may specify costs or invite bids. Transactions can be initiated and completed. Ongoing purchases may qualify customers for volume discounts or special offers. E-procurement software may make it possible to automate some buying and selling. Companies participating expect to be able to control parts inventories more effectively, reduce purchasing agent overhead, and improvemanufacturing cycles. E-procurement is expected to be integrated with the trend toward computerized supply chain management.

There are six main types of e-procurement:

- **Web-based ERP (Electronic Resource Planning)**: Creating and approving purchasing requisitions, placing purchase orders and receiving goods and services by using a software system based on Internet technology.
- **e-MRO (Maintenance, Repair and Operating)**: The same as web-based ERP except that the goods and services ordered are non-product related MRO supplies.
- **e-sourcing**: Identifying new suppliers for a specific category of purchasing requirements using Internet technology.
- **e-tendering**: Sending requests for information and prices to suppliers and receiving the responses of suppliers using Internet technology.
- **e-reverse auctioning**: Using Internet technology to buy goods and services from a number of known or unknown suppliers.
- **e-informing**: Gathering and distributing purchasing information both from and to internal and external parties using Internet technology.

The e-procurement value chain consists of Indent Management, eTendering, eAuctioning, Vendor Management, Catalogue Management, and Contract Management. Indent Management is the workflow involved in the preparation of tenders. This part of the value chain is optional, with individual procuring departments defining their indenting process. In works procurement, administrative approval and technical sanction are obtained in electronic format. In goods procurement, indent generation activity is done online. The end result of the stage is taken as inputs for issuing the NIT.

Elements of e-procurement include Request For Information, Request For Proposal, Request for Quotation, RFx (the previous three together), and eRFx (software for managing RFx projects).

Advantages of adopting E-Procurement (Systems)

- E-Procurement helps with the decision-making process by keeping relevant information neatly organized and time-stamped. Most are template-driven which makes all transactions standardized and trackable. Keeping track of all bids means leveraging your knowledge to obtain better pricing. Companies can focus on their most lucrative trading partners and contracts. [8]
- E-Procurement enhances the comparability of suppliers and prices. [9]
- E-Procurement reduces the energy expended. Especially at purchasing office equipment and other class C commodities.
- Well-managed E-procurement helps reduce inventory levels. Knowing product numbers, bid prices and contact points can help businesses close a deal while other suppliers are struggling to gather their relevant data.
- Effective E-Procurement minimizes process costs by fast transaction of the purchasing orders. [10]
- E-Procurement systems that allow multiple access levels and permissions help managers organize administrative users by roles, groups, or tasks. Procurement managers do not need to be as highly trained or paid because such systems are standardized and easy to learn. [11]

Ordinary adoption strategies

Some firms have discovered that many of their transactions still take place on paper, and they have run into problems ranging from content management to supplier participation in their systems. Most companies who desire to make the switch fall into two camps. The first are the slow step-by-step adopters. They implement one piece of their system at a time and slowly bring trading partners on board. The others follow the total replacement model. They build a totally parallel system, test it, then switch over to it when it works. There is usually some pain involved and some mistakes are discovered, but by and large these are absorbed and the business continues.

CONCLUSION

Adopting a complex E-procurement system should only be considered if you have the time and resources to implement this. The possible advantages are described in the text above. If not, stick to an incremental approach.[14] You can´t expect an immediate return on investment. A short-tem gain may be noticeable, but it may be eaten up by the cost of staff training and equipment purchases. A year or two down the road and a larger ROI should be evident.

- http://en.wikipedia.org/wiki/E-procurement
- http://en.ecommercewiki.info/fundamentals/market_places/e_procurement
- http://www.fusiontoad.com/products/eproc-applications.html

4. Business Models on Internet. Explain various revenue generation avenues. (5m)

Ans: Internet Business Models

The Internet has given rise to new kinds of business models while at the same time reinventing tried-and-true models. There are Internet business models that result in passive income and those that work through active income (exchanging hours for dollars).

Today, let's discuss five of the most popular and successful Internet business models:

1. Social Media Model

Of course Facebook, with over 800 million users, is the most successful. But there's also LinkedIn, Twitter, Google Plus, Pinterest, and many more. But how do these companies generate revenue?

This social media business model works by offering a free online service (in this case the service is social networking) and then selling targeted ads to the users. The users do not pay anything to use the service. As Facebook's home page reads, "It's free and it always will be."

The reason advertising is effective on social networks is because companies can buy ads on a pay-per-click basis (similar to Google's PPC ads). And these ads can be laser focused to a very specific target market. Effectively, it's the billboard business model version two.

Last year Facebook generated $4.27 billion and $3.8 billion was from advertising ($470 million was made from "Facebook Credits", a virtual-currency program that lets users buy items in games.)

Virtual goods sales are increasing rapidly and represent a very different business model than the targeted billboarding of internet advertising.

2. Affiliate Model

The affiliate business model is another very successful Internet business model in use today.

Here's how it works:

A business sets up an "affiliate program" where it offers a financial incentive to affiliates for each visitor or customer brought about by the affiliate's own marketing efforts. Typically the affiliate is given a unique "affiliate link" which is tracked by the business.

Every time a sale is made as a result of this process the affiliate receives a percentage of the sale. This Internet business model is well-suited for trusted sites that have large followings. A good example is Pat Flynn from Smart Passive Income.

Thousands of people consider Pat to be a trusted authority on how to make passive income online. In January 2012 Pat earned $38,038 from his affiliate marketing efforts. To view his detailed monthly income report click here.

Here are some other examples of affiliate marketing sites: Illuminated Mind,ShoeMoney, DIY Themes.

3. Subscription Model

Websites that use the subscription business model require users to pay a fee (typically monthly or yearly) to access a service or product. With over 24 million subscribers, Netflix is one the most successful companies that use the subscription business model. In 2011 Netflix generated $876 million.

Another way companies profit from a subscription business model is by combining free content with "premium" (i.e., member-only) content. In this freemium business model, companies like LinkedIn use this strategy to encourage usership and charge the best users.. Most of LinkedIn's 150 million users are basic (free) members but the social media company did make $28.4 million in Q3 2011 (total revenue for Q3 2011 was $139 million) from paid memberships.

4. Merchant Model

The Amazon…oh excuse me, I mean the merchant business model is one of the most profitable Internet business models. The merchant model is a business model that goes back thousands of years. But the Internet has provided a tremendous opportunity for merchants to grow at an almost unbelievable rate.

In the merchant model a merchant simply sells products directly to buyers. It could be clothes, CDs, or cars but the concept is the same. Again this business model is not new but savvy business owners have figured out how to leverage the buying power of customers on the Internet.

Let's compare two merchant business models real quick: Wal-Mart and Amazon. Last year at 48 years old, Wal-Mart's revenue was $416 billion. Amazon at only 16 years old already had a revenue of $32 billion. It took Wal-Mart 15 years to reach annual sales of $1 billion; Amazon did it in only 5.

Internet business models that rely on the merchant model may face some challenges in the upcoming years as the sales tax debate heats up. Should internet merchants be taxed like brick and mortar merchants, the model may be adversely affected. Personally, I believe all internet purchases will be charged sales tax. The loophole will be closed for two reasons: 1) the interstate commerce provision providing for the loophole is archaic and conceived long before anyone dreamed of the internet, and, 2) the government needs the money.

Closure of the loophole will put some internet business models out of business and merely slow growth of strong merchants like Amazon.

5. Advertising Model

Again we have another old school business model that's been applied to the Internet. The advertising business model is an extension of the traditional media broadcast model. But now the "media" company is a website (i.e. Google, Yahoo!). And just like in radio or TV the "media" company provides viewers, or users, with free content and services.

The more people the media company has watching them (or using their service) the more money they can charge for targeted advertising, or hire targeted advertising companies to market for them.. Google has the market on the Internet advertising model. In 2010 their annual revenue was $29.3 billion (compared to about $100 million in 2001).

This Internet business model relies on heavy traffic to the website. A company using this model must provide a valuable service that millions of people use on a regular basis (i.e. Google search, Gmail) in order to command high prices from ad space.

Internet Business Models in the Future

While there are other Internet business models out there these five are the most popular. And as you can see some of these Internet business models overlap. For example Facebook fits the definition of a social model and an advertising model.

What business models will we see 10 years from now? Will the tried-and-true prevail or will new models emerge as savvy business owners discover new ways to do business online? Only time will tell.

- http://businessmodelinstitute.com/internet-business-models/

5. Social issues with advent of Internet era (5m)

[Group 9 PPT]

6. Issues in implementing an Internet / Web application (5m)

The main challenges for implementing Semantic Web technologies

1. Integrating noisy and heterogeneous data - "The majority of applications rely on data integration, but in order to imple- ment it, expensive human intervention is necessary and knowledge about reason- ing and inferencing needs to be acquired by the software engineers." Three particular problems are discussed: 1.Use of non-standard (undefined) terms 2. Incorrect usage of vocabularies (contrary to their intended usage) 3.Multiple URIs for the same objects (identifiers aren't unique)

Furthermore, data integration may require multiple components, such as a crawler and a search service, in addition to the integration service itself.

2. Mismatch of data models and APIs between components - The data models need to be mapped--e.g. relational databases, object oriented data, RDF (graph data model). While web applications benefit from existing mappings, the Semantic Web developer may be obliged to "provide an abstraction layer on top of the RDF data model himself."

3. Missing or belated conventions and standards - "There are many different export and access mechanisms for RDF data, from putting an RDF dump on a web server, embedding links to RDF data in HTML or providing a SPARQL endpoint." and "Authoritative recommendations for making RDF accessible over the Web were not available until 2006, when Tim-Berners Lee published a design note([www.w3.org/DesignIssues/LinkedData.html www.w3.org/DesignIssues/LinkedData.html]) which established the Linked Data principles."

4. Distribution of application logic across computers - Inferencing and reasoning, formal vocabularies, and RDF query language may be used, which "results in the application logic being distributed across the different components."

- http://acawiki.org/Implementing_Semantic_Web_applications:_reference_architecture_and_challenges

7. Convergence and its issues (5m)

Ans: **Technological convergence** is the tendency for different technological systems to evolve toward performing similar tasks. Convergence can refer to previously separate technologies such as voice (and telephony features), data (and productivity applications), and video that now share resources and interact with each other synergistically.

The rise of digital communication in the late 20th century has made it possible for media organizations (or individuals) to deliver text, audio, and video material over the same wired, wireless, or fiber-optic connections. At the same time, it inspired some media organizations to explore multimedia delivery of information. This digital convergence of news media, in particular, was called "Mediamorphosis" by researcher Roger Fidler [2], in his 1997 book by that name. Today, we are surrounded by a multi-level convergent media world where all modes of communication and information are continually reforming to adapt to the enduring demands of technologies, "changing the way we create, consume, learn and interact with each other".

Convergence in this instance is defined as the interlinking of computing and other information technologies, media content, and communication networks that has arisen as the result of the evolution and popularization of the Internet as well as the activities, products and services that have emerged in the digital media space. Many experts view this as simply being the tip of the iceberg, as all facets of institutional activity and social life such as business, government, art, journalism, health, and education are increasingly being carried out in these digital media spaces across a growing network of information and communication technology devices.

Challenges in Convergent World

Technological convergence has raised a number of issues of adjustment to the new environment by telecom operators, service providers, policymakers, regulators, and users.

a) New Regulatory Framework

The combination of services over the same platform is challenging common perceptions about the best means to license and regulate providers. Traditionally, regulatory frameworks were designed for an era when clear functional differences existed between services and infrastructure, but these regulations are increasingly inadequate for dealing with today's world. At first glance, interoperability, interconnection, consumer protection and universal access appear as the most relevant challenges. Existing interconnection mechanisms focus basically on interconnection of telecom networks based on circuit switching technologies, while for instance broadcasting networks are either unregulated or subject to different types of regulation. Additionally, in a convergent environment, which relies greatly on packet switched networks, circuits are neither connected nor provided. In this way distance and time become less determinants as cost factors, requiring adoption of new units of measurement.

b) Bandwidth Shortage and Infrastructure Upgrade

Convergence gives rise to new services and applications which are bandwidth intensive, requiring an existence of broadband infrastructure. Only with broadband access is the use of complex services (e.g. multimedia services) attractive or possible in the first place. While developed economies may not face a bandwidth shortage dilemma, the same may not be said about most of the developing economies where telecommunication infrastructures are still relying on narrowband technologies. These countries face the 14challenge of having to upgrade their infrastructure or miss on the benefits of the technological convergence. In meeting this challenge, as it was in the past, financial constraints will continue to be a problem.

c) Strategic Alignment by Operators and Service Providers

As barriers to market access are significantly reduced, allowing an increased number of new players to enter the market and provide a wide variety of different service packages, established operators and services providers are required to reassess their business models and strategies not only to face these new providers, but also to upgrade their networks to integrate it into their own offering. Another challenge lies in convincing consumers of the value added by the new services for which they must pay

d) Privacy, Security and Reliability

As society becomes increasingly interconnected and dependent of ICT networks, cybercriminals continue to invent increasingly cunning ways to exploit human and computer vulnerabilities to their malicious benefits. This, challenges operators, service providers and users to take measures to minimize risks of network intrusions, attacks and viruses. In a similar way, as technologies and systems become complex, the higher is the risk of their instability. Product designers, manufacturers and operators are challenged to guarantee the reliability of these new technologies.

- http://en.wikipedia.org/wiki/Technological_convergence
- http://www.itu.int/osg/spu/youngminds/2007/essays/PapadakisSteliosYM2007.pdf

8. Internet Security Importance and Aspects (5m)

Internet security protects a computer's Internet account and files from being accessed by an unknown and potentially unwanted user. Internet security also serves to protect the user against the pirating of his identity, passwords and private data.

On-line Risk

- Every time your computer connects to a network and communicates with other computers, you place yourself and loved ones at risk. By adopting security measures, you can minimize this risk, which takes essentially one of three forms. One is infection of your computer's hard drive with software designed for malicious purposes. A second risk is identity theft, which has led in some cases to actual monetary theft. A third risk is reaching and attracting minors over the Internet.

Malicious Software

- Malicious software includes two main categories of programs. Some programs are designed to spy on other computers. These programs can gather personal data, which is then used to send spam to your mailbox. The other category of programs includes viruses, Trojans and bots. These programs affect the proper running of a computer. Many of them serve no purpose other than to do destruction.

Identity Theft

- Identity theft is stealing personal information, such as bank account numbers, credit card numbers and social security numbers. The thief then poses as the owner of these numbers in order to steal from the victim. Law enforcement authorities estimate that billions or even trillions of dollars change hand on-line every day. Computer users who fail to take security precautions against cyber criminals risk losing their savings.

Targeting Minors

- One of the most insidious practices on the Internet involves targeting minors. Web "stalkers," adults who go onto the Internet with the attention of attracting unsuspecting children, may lure children to sites containing violence, pornography or other unsuitable material. In the worst cases, these sick individuals attempt to make personal contact with a child.

Security Measures

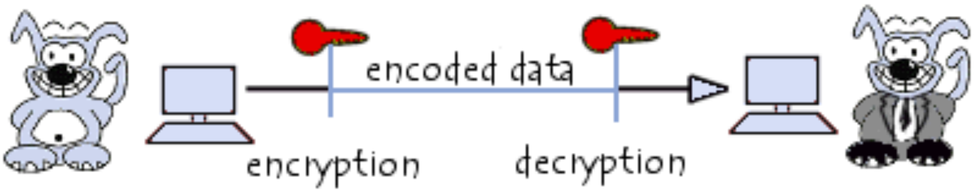
- Fortunately, security measures exist for combating these on-line threats. You can install anti-virus and anti-spy-ware programs on your computer that will lessen your risk of malicious software and spying. Firewall software can protect against identity theft and viruses. Finally, computer operating systems all come with parental controls. In Windows Vista, parental controls appears under "User Accounts and Family Safety" in the Control Panel. The settings found there enable you to control and monitor sites your child visits.

  - http://www.ehow.com/about_6584857_internet-security-important_.html
  - http://en.wikipedia.org/wiki/Internet_security

9. Public / Private key cryptography technique (5m)

   Private key cryptography / Symmetric encryption

Symmetric encryption (also called *private-key encryption* or *secret-key encryption*) involves using the same key for encryption and decryption.



Encryption involves applying an operation (an algorithm) to the data to be encrypted using the private key to make them unintelligible. The slightest algorithm (such as an exclusive OR) can make the system nearly tamper proof (there being so such thing as absolute security).

However, in the 1940s, *Claude Shannon* proved that to be completely secure, private-key systems need to use keys that are at least as long as the message to be encrypted. Moreover, symmetric encryption requires that a secure channel be used to exchange the key, which seriously diminishes the usefulness of this kind of encryption system.

The main disadvantage of a secret-key cryptosystem is related to the exchange of keys. Symmetric encryption is based on the exchange of a secret (keys). The problem of key distribution therefore arises:

Moreover, a user wanting to communicate with several people while ensuring separate confidentiality levels has to use as many private keys as there are people. For a group of *N* people using a secret-key cryptosystem, it is necessary to distribute a number of keys equal to *N * (N-1) / 2*.

In the 1920s, Gilbert Vernam and Joseph Mauborgne developed the *One-Time Pad* method (sometimes called "One-Time Password" and abbreviated *OTP*), based on a randomly generated private key that is used only once and is then destroyed. During the same period, the Kremlin and the White House were connected by the famous red telephone, that is, a telephone where calls were encrypted thanks to a private key according to the *one-time pad* method. The private key was exchanged thanks to the diplomatic bag (playing the role of secure channel).

Types of symmetric-key algorithms

Symmetric-key encryption can use either stream ciphers or block ciphers.

- Stream ciphers encrypt the digits (typically bits) of a message one at a time.
- Block ciphers take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the block size. Blocks of 64 bits have been commonly used. The Advanced Encryption Standard (AES) algorithm approved by NIST in December 2001 uses 128-bit blocks.

Public-key cryptography

Public-key cryptography refers to a cryptographic system requiring two separate keys, one of which is secret and one of which is public. Although different, the two parts of the key pair are mathematically linked. One key locks or encrypts the plaintext, and the other unlocks or decrypts the ciphertext. Neither key can perform both functions by itself. The public key may be published without compromising security, while the private key must not be revealed to anyone not authorized to read the messages.

Public-key cryptography uses asymmetric key algorithms and can also be referred to by the more generic term "asymmetric key cryptography." The algorithms used for public key cryptography are based on mathematical relationships (the most notable ones being the integer factorization and discrete logarithm problems) that presumably have no efficient solution. Although it is computationally easy for the intended recipient to generate the public and private keys, to decrypt the message using the private key, and easy for the sender to encrypt the message using the public key, it is extremely difficult (or effectively impossible) for anyone to derive the private key, based only on their knowledge of the public key. This is why, unlike symmetric key algorithms, a public key algorithm does *not* require a secure initial exchange of one (or more) secret keys between the sender and receiver. The use of these algorithms also allows the authenticity of a message to be checked by creating adigital signature of the message using the private key, which can then be verified by using the public key. In practice, only a hash of the message is typically encrypted for signature verification purposes.

Public-key cryptography is widely used. It is an approach used by many cryptographic algorithms andcryptosystems. It underpins such Internet standards as Transport Layer Security (TLS), PGP, and GPG. There are three primary kinds of public key systems: public key distribution systems, digital signaturesystems, and public key cryptosystems, which can perform both public key distribution and digital signature services. Diffie–Hellman key exchange is the most widely used public key distribution system, while the Digital Signature Algorithm is the most widely used digital signature system.

How it works

The distinguishing technique used in public-key cryptography is the use of asymmetric key algorithms, where thekey used to encrypt a message is not the same as the key used to decrypt it. Each user has a pair ofcryptographic keys – a public encryption key and a private decryption key. The publicly available encrypting-key is widely distributed, while the private decrypting-key is known only to its proprietor. The keys are related mathematically, but the parameters are chosen so that calculating the private key from the public key is either impossible or prohibitively expensive.

In contrast, symmetric-key algorithms – variations of which have been used for thousands of years – use a*single* secret key, which must be shared and kept private by both the sender and the receiver, for both encryption and decryption. To use a symmetric encryption scheme, the sender and receiver must securely share a key in advance.

Because symmetric key algorithms are nearly always much less computationally intensive than asymmetric ones, it is common to exchange a key using a key-exchange algorithm, then transmit data using that key and a symmetric key algorithm. PGP and the SSL/TLS family of schemes use this procedures, and are thus called *hybrid cryptosystems*

- http://en.wikipedia.org/wiki/Symmetric-key_algorithm
- http://en.kioskea.net/contents/crypto/cleprivee.php3
- http://en.wikipedia.org/wiki/Public-key_cryptography
- www.csie.kuas.edu.tw/course/CS/old/english/ch-16.ppt

10. Firewalls (5m)

A firewall controls access between networks. It generally consists of gateways and filters which vary from one firewall to another. Firewalls also screen network traffic and are able to block traffic that is dangerous. Firewalls act as the intermediate server between SMTP and HTTP connections.

Role of firewalls in Internet security and web security

Firewalls impose restrictions on incoming and outgoing packets to and from private networks. All the traffic, whether incoming or outgoing, must pass through the firewall; only authorized traffic is allowed to pass through it. Firewalls create checkpoints between an internal private network and the public Internet, also known as *choke points*. Firewalls can create choke points based on IP source and TCP port number. They can also serve as the platform for IPsec. Using tunnel mode capability, firewall can be used to implement VPNs. Firewalls can also limit network exposure by hiding the internal network system and information from the public Internet.

Types of firewalls

Packet filters :Packet filters are one of several different types of firewalls that process network traffic on a packet-by-packet basis. Their main job is to filter traffic from a remote IP host, so a router is needed to connect the internal network to the Internet. The router is known as a screening router, which screens packets leaving and entering the network.

Circuit-level gateways : The circuit-level gateway is a proxy server that statically defines what traffic will be allowed. Circuit proxies always forward packets containing a given port number, provided the port number is permitted by the rules set. This gateway operates at the network level of an OSI model. The main advantage of a proxy server is its ability to provide Network Address Translation (NAT), which can hide the user's IP address from the Internet, effectively protecting all internal information from the Internet.

Application-level gateways : An application-level gateway is a proxy server operating at the TCP/IP application level. A packet is forwarded only if a connection is established using a known protocol. Application-level gateways are notable for analyzing entire messages rather than individual packets of data when the data are being sent or received.

- http://en.wikipedia.org/wiki/Internet_security#Firewalls

11. Ethical Hacking and some of the antivirus package (5m)

- An ethical hacker is a computer and network expert who attacks a security system on behalf of its owners, seeking vulnerabilities that a malicious hacker could exploit. To test a security system, ethical hackers use the same methods as their less principled counterparts, but report problems instead of taking advantage of them. Ethical hacking is also known as*penetration testing*, *intrusion testing* and *red teaming*. An ethical hacker is sometimes called a white hat, a term that comes from old Western movies, where the "good guy" wore a white hat and the "bad guy" wore a black hat.

- One of the first examples of ethical hackers at work was in the 1970s, when the United States government used groups of experts called *red teams* to hack its own computer systems. According to Ed Skoudis, Vice President of Security Strategy for Predictive Systems' Global Integrity consulting practice, ethical hacking has continued to grow in an otherwise lackluster IT industry, and is becoming increasingly common outside the government and technology sectors where it began. Many large companies, such as IBM, maintain employee teams of ethical hackers.

- In a similar but distinct category, a hacktivist is more of a vigilante: detecting, sometimes reporting (and sometimes exploiting) security vulnerabilities as a form of social activism.

Antivirus Packages [Printout attached]

http://searchsecurity.techtarget.com/definition/ethical-hacker

12. RSS Feeds

Ans: RSS Rich Site Summary (originally RDF Site Summary, often dubbed Really Simple Syndication) is a family ofweb feed formats used to publish frequently updated works—such as blog entries, news headlines, audio, and video—in a standardized format.[2] An RSS document (which is called a "feed", "web feed",[3] or "channel") includes full or summarized text, plus metadata such as publishing dates and authorship.

RSS feeds benefit publishers by letting them syndicate content automatically. A standardized XML file format allows the information to be published once and viewed by many different programs. They benefit readers who want to subscribe to timely updates from favorite websites or to aggregate feeds from many sites into one place.

RSS feeds can be read using software called an "RSS reader", "feed reader", or "aggregator", which can be web-based, desktop-based, or mobile-device-based. The user subscribes to a feed by entering into the reader the feed's URI or by clicking a feed icon in a web browser that initiates the subscription process. The RSS reader checks the user's subscribed feeds regularly for new work, downloads any updates that it finds, and provides auser interface to monitor and read the feeds. RSS allows users to avoid manually inspecting all of the websites they are interested in, and instead subscribe to websites such that all new content is automatically checked for and advertised by their browsers as soon as it is available.

OR

RSS is an open method for delivering regularly changing web content. Many news-related sites, weblogs and other online publishers syndicate their content as an RSS Feed to whoever wants it.

Any time you want to retrieve the latest headlines from your favorite sites, you can access the available RSS feeds via a desktop RSS reader. You can also make an RSS feed for your own site if your content changes frequently.

In brief:

- RSS is a protocol that provides an open method of syndicating and aggregating Web content.
- RSS is a standard for publishing regular updates to web-based content.
- RSS is a Syndication Standard based on a type of XML file that resides on an internet server.
- RSS is an XML application, conforms to the W3C's RDF specification and is extensible via XML.

- You can also download RSS feeds from other sites to display updated news items on your site, or use a desktop or online reader to access your favorite RSS feeds.

What does RSS stand for? It depends on what version of RSS you are using.

- **RSS Version 0.9** - Rich Site Summary
- **RSS Version 1.0** - RDF Site Summary
- **RSS Versions 2.0, 2.0.1 and 0.9x** - Really Simple Syndication

What is RSS Feed?

- The RSS feed is a text XML file that resides on an Internet server.
- The RSS feed file includes basic information about a site (title, URL, description), plus one or more item entries that include - at a minimum - a title (headline), a URL, and a brief description of the linked content.
- There are various flavors of RSS feed depending on RSS Version. Another XML feed format is called ATOM.
- RSS Feeds are registered with an RSS registry to make them more available to viewers interested in your content area.
- RSS feeds can have links back to your website which will result in a high traffic to your site.
- RSS feeds are updated hourly (Associated Press and News Groups), some RSS feeds are updated daily, and others are updated weekly or irregularly.

How Does RSS Work?

This is how RSS works:

- A website willing to publish their content using RSS, creates one RSS feed and keeps it on an web server. RSS Feeds can be created manually or with software.
- A website visitor will subscribe to read your RSS feed. An RSS feed will be read by a RSS feed reader.
- The RSS Feed Reader reads the RSS Feed file and displays it. The RSS Reader displays only new items from the RSS Feed
- The RSS Feed Reader can be customized to show you content related to one or more RSS feeds and based on your own interest.

Advantages

RSS gives benefits to both readers (users) and web publishers.

- It gives you the latest updates. Whether it is about the weather, new music, software upgrade, local news, or a new posting from a rarely-updates site learn about the latest as soon as it comes out.
- It gives the power of subscription to the user. Users are given a free-hand on which websites to subscribe in their RSS aggregators which they can change at any time they decide differently.
- It saves on surfing time. Since an RSS feed provides a summary of the related article, it saves the user's time by helping s/he decide on which items to prioritize when reading or browsing the net.
- It is spam free. Unlike email subscriptions, RSS does not make use of your email address to send updates thus your privacy is kept safe from spam mails.
- Unsubscribing is hassle-free. Unlike email subscriptions where the user is asked questions on why she/he is unsubscribing and then the user would be asked to confirm unsubscribing, all you have to do is to delete the RSS feed from your aggregator.
- It can be used as an advertising or marketing tool. Users who subscribe or syndicate product websites receive the latest news on products and services without the website sending spam mail. This is advantageous to both the web user and the website owner since advertising becomes targeted; those who are actually interested in their products are kept posted.

Disadvantages

The disadvantages of RSS use are brought about by its being a new technology and some user-preference concerns.

- Some users prefer receiving email updates over an RSS feed.
- Graphics and photos do not appear in all RSS feeds. For conciseness and ease of publication, RSS feeds do not display the photos from the original site in announcing the update except for some web-based aggregators.
- The identity of the source website can be confusing. Since RSS feeds do not display the actual URL or name of the website, it can sometimes get confusing on what feed a user is actually reading.
- Publishers cannot determine how many users are subscribed to their feed and the frequency of their visits. Moreover, they would not know the reasons why users unsubscribe which could be important in improving their advertising.
- RSS feeds create higher traffic and demands on the server. Most readers still prefer the whole update over a brief summary of the entry, thus they still access the site.
- Since it is a new technology, many sites still do not support RSS.

Example

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<rss version="2.0">
<channel>
 <title>RSS Title</title>
 <description>This is an example of an RSS feed</description>
 <link>http://www.someexamplerssdomain.com/main.html</link>
 <lastBuildDate>Mon, 06 Sep 2010 00:01:00 +0000 </lastBuildDate>
 <pubDate>Mon, 06 Sep 2009 16:45:00 +0000 </pubDate>
 <ttl>1800</ttl>

 <item>
  <title>Example entry</title>
  <description>Here is some text containing an interesting description.</description>
  <link>http://www.wikipedia.org/</link>
  <guid>unique string per item</guid>
  <pubDate>Mon, 06 Sep 2009 16:45:00 +0000 </pubDate>
 </item>

</channel>
</rss>
```

- http://en.wikipedia.org/wiki/RSS

a. 10 CRM [Printout Attached]

13. 10 ERP : http://en.wikipedia.org/wiki/List_of_ERP_software_packages

Free and Open Source ERP software

ERP Package	Language Base	License	Other Info	Developer Country
A1 ERP	Java	Alliance Technologies Open License	ERP for Public Sector, Academia, Healthcare, Logistics A1 ERP	Worldwide
Adaxa Suite	Java	GPL	Integrated ERP built on Adempiere	Australia/New Zealand
Adempiere	Java	GPL	started as a fork of Compiere	Spain
Compiere	Java	GPL/Commercial	Acquired by Consona Corporation in June 2010	US
Dolibarr	PHP, MySQL	GPL		
ERP5	Python, Zope, MySQL	GPL	based on unified model	Brazil, France, Germany, Japan Sénégal
ERPNEXT	Python, JavaScript, MySQL	GPL	ERP for small and medium businesses	India
Fedena	Ruby, MySQL	Apache License	ERP for Schools/Universities	India
GNU Enterprise	Python	GPLv3		
HeliumV	Java	AGPL	ERP for small and medium businesses	Austria, Germany
JFire	Java	LGPL		
Kuali Foundation	Java	ECL	for higher education, by higher education	

ERP Package	Language Base	License	Other Info	Developer Country
LedgerSMB	Perl, PostgreSQL	GPL	started as a fork of SQL-Ledger in 2006	Worldwide
OFBiz	Apache, Java	Apache License 2.0	ERP for small and medium businesses	
Openbravo	Java	Openbravo Public License (OBPL), a free software license based on the Mozilla Public License (MPL)		Spain
OpenERP	Python, PostgreSQL	AGPLv3	OpenERP version 7.0 was released on 12/21/12, OpenERP was formerly known as Tiny ERP	Belgium, India, USA
Phreedom	PHP, Javascript, MySQL	GPLv3	Expanded from Phreebooks accounting engine	USA
Postbooks	C++, JavaScript, PostgreSQL	CPAL	Produced by XTuple, uses Qt framework	
SQL-Ledger	Perl, PostgreSQL	GPL		
Tryton	Python	GPLv3	started as a fork of OpenERP	
WebERP	PHP, MySQL	GPLv2	LAMP based system	

14. IP Address

- An **Internet Protocol address** (**IP address**) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.[1] An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: "*A name indicates what we seek. An address indicates where it is. A route indicates how to get there.*"[2]

- The designers of the Internet Protocol defined an IP address as a 32-bit number[1] and this system, known asInternet Protocol Version 4 (IPv4), is still in use today. However, due to the enormous growth of the Internet and the predicted depletion of available addresses, a new version of IP (IPv6), using 128 bits for the address, was developed in 1995.[3] IPv6 was standardized as RFC 2460 in 1998,[4] and its deployment has been ongoing since the mid-2000s.

- IP addresses are binary numbers, but they are usually stored in text files and displayed in human-readablenotations, such as 172.16.254.1 (for IPv4), and 2001:db8:0:1234:0:567:8:1 (for IPv6).

- The Internet Assigned Numbers Authority (IANA) manages the IP address space allocations globally and delegates five regional Internet registries (RIRs) to allocate IP address blocks to local Internet registries (Internet service providers) and other entities.

- IPv6 Features and Benefits

  IPv6 was designed to build on and improve the existing features of IPv4 and to introduce new capabilities:

  - Larger address space - IP addressing increased to 128 bits, greatly increasing the total amount of unique address space.
  - End-to-end transparency – Due to the increased amount of available addressing, the need for translation technologies has been reduced.
  - Automatic configuration for “plug and play” support.
  - Enabling implementation of IP Security (IPSec) – IPSec extension headers provide integrity, authentication and privacy services. Improved support for IP mobility – Enabled support for mobile device users to keep a permanent IP address while roaming in foreign networks.

15. SMTP – Simple Mail Transfer Protocol

- SMTP is a core Internet protocol used to transfer e-mail messages between servers (first defined in RFC 821 in 1982). This contrasts with protocols such as POP3 and IMAP, which are used by messaging clients to retrieve e-mail.

- SMTP servers look at the destination address of a message and contact the target mail server directly. Of course, this means the Domain Name Service (DNS) has to be configured correctly otherwise mail could be handed to the wrong server - potentially a big problem because, unless you have encrypted your messages, your e-mail will be in plain text!
- SMTP was designed to be a reliable message delivery system. Reliable in this case means that a message handled by SMTP is intended to get to its destination or generate an error message accordingly. This is not the same as a guaranteed delivery service, it just does its best. To guarantee delivery requires all sorts of data exchanges that would add considerable communications overhead that would be pointless for everyday purposes.
- SMTP communications are transported by TCP to ensure reliable end-to-end transport. RFC 822 defines the format of SMTP messages.
- RFC 822 is a straightforward specification that breaks the message into headers and bodies separated by a blank line. In the header are a number of keywords and values that define the sending date, sender's address, where replies should go, and so on, while the body contains the data.
- To send an SMTP message requires an exchange between the sender and receiver. First, the sending server says "HELO." Honest - SMTP servers are very polite. The sender should announce the domain it is sending from, and the receiver should reply with a completion code of 200 if it is willing to talk.

From An inside look at the Simple Mail Transfer Protocol, Network World, 01/31/00.

Additional resources SMTP Tutorial, Topic: Messaging

16. WML

Wireless Markup Language (WML), based on XML, is a markup language intended for devices that implement the Wireless Application Protocol (WAP) specification, such as mobile phones. It provides navigational support, data input, hyperlinks, text and image presentation, and forms, much like HTML(HyperText Markup Language). It preceded the use of other markup languages now used with WAP, such as HTML itself, and XHTML (which are gaining in popularity as processing power in mobile devices increases).

WML markup

WML documents are XML documents that validate against the WML DTD (Document Type Definition)[4] . The W3C Markup Validation service (http://validator.w3.org/) can be used to validate WML documents (they are validated against their declared document type).

For example, the following WML page could be saved as "example.wml":

```
<?xml version="1.0"?> <!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
"http://www.wapforum.org/DTD/wml_1.1.xml" > <wml>    <card id="main" title="First
Card">    <p mode="wrap">This is a sample WML page.</p>   </card> </wml>
```

A WML document is known as a “deck”. Data in the deck is structured into one or more “cards” (pages) – each of which represents a single interaction with the user.

WML decks are stored on an ordinary web server configured to serve the text/vnd.wap.wml MIME type in addition to plain HTML and variants. The WML cards when requested by a device are accessed by a bridge WAP gateway, which sits between mobile devices and the World Wide Web, passing pages from one to the other much like a proxy. The gateways send the WML pages on in a form suitable for mobile device reception (WAP Binary XML). This process is hidden from the phone, so it may access the page in the same way as a browser accesses HTML, using a URL (for example, http://example.com/foo.wml). (Provided the mobile phone operator has not specifically locked the phone to prevent access of user-specified URLs.)

WML has a scaled down set of procedural elements which can be used by the author to control navigation to other cards.

Consider a service that lets you enter a zip code, and obtain a list of clickable phone numbers of pizza parlors and taxicabs in your immediate location:

```
<card id="cM" title="MY_DOMAIN.com">    <p>       '''Call A Taxi:'''<br />       <a
href="wtai://wp/mc;%2B19035551212">903-555-1212</a>  </p> </card>
```

Mobile devices are moving towards support for greater amounts of XHTML and even standard HTML as processing power in handsets increases. These standards are concerned with formatting and presentation. They do not however address cell-phone or mobile device hardware interfacing in the same way as WML.

17. XML

Extensible Markup Language (**XML**) is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. It is defined in the XML 1.0 Specification[3]produced by the W3C, and several other related specifications,[4] all gratis open standards.[5]

The design goals of XML emphasize simplicity, generality, and usability over the Internet.[6] It is a textual data format with strong support via Unicode for the languages of the world. Although the design of XML focuses on documents, it is widely used for the representation of arbitrary data structures, for example in web services.

Many application programming interfaces (APIs) have been developed to aid software developers with processing XML data, and several schema systems exist to aid in the definition of XML-based languages.

As of 2009, hundreds of document formats using XML syntax have been developed,[7] including RSS, Atom,SOAP, and XHTML. XML-based formats have become the default for many office-productivity tools, includingMicrosoft Office (Office Open XML), OpenOffice.org and LibreOffice (OpenDocument), and Apple's iWork. XML has also been employed as the base language for communication protocols, such as XMPP

The Difference Between XML and HTML

- XML is not a replacement for HTML.
- XML and HTML were designed with different goals:
- XML was designed to transport and store data, with focus on what data is
- HTML was designed to display data, with focus on how data looks
- HTML is about displaying information, while XML is about carrying information.

XML Does Not DO Anything

Maybe it is a little hard to understand, but XML does not DO anything. XML was created to structure, store, and transport information.

The following example is a note to Tove, from Jani, stored as XML:

```
<note>
<to>Tove</to>
<from>Jani</from>
```

```
<heading>Reminder</heading>
<body>Don't forget me this weekend!</body>
</note>
```

The note above is quite self descriptive. It has sender and receiver information, it also has a heading and a message body.

But still, this XML document does not DO anything. It is just information wrapped in tags. Someone must write a piece of software to send, receive or display it.

With XML You Invent Your Own Tags

The tags in the example above (like <to> and <from>) are not defined in any XML standard. These tags are "invented" by the author of the XML document.

That is because the XML language has no predefined tags.

The tags used in HTML are predefined. HTML documents can only use tags defined in the HTML standard (like <p>, <h1>, etc.).

XML allows the author to define his/her own tags and his/her own document structure.

XML is Not a Replacement for HTML

XML is a complement to HTML.

It is important to understand that XML is not a replacement for HTML. In most web applications, XML is used to transport data, while HTML is used to format and display the data.

My best description of XML is this:

XML is a software- and hardware-independent tool for carrying information.

XML is a W3C Recommendation

XML became a W3C Recommendation on February 10, 1998.

To read more about the XML activities at W3C, please read our W3C Tutorial.

XML is Everywhere

XML is now as important for the Web as HTML was to the foundation of the Web.

XML is the most common tool for data transmissions between all sorts of applications.

An Example XML Document

XML documents use a self-describing and simple syntax:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<note>
 <to>Tove</to>
```

```
  <from>Jani</from>
  <heading>Reminder</heading>
  <body>Don't forget me this weekend!</body>
</note>
```

The first line is the XML declaration. It defines the XML version (1.0) and the encoding used (ISO-8859-1 = Latin-1/West European character set).

The next line describes the **root element** of the document (like saying: "this document is a note"):

```
<note>
```

The next 4 lines describe 4 **child elements** of the root (to, from, heading, and body):

```
<to>Tove</to>
<from>Jani</from>
<heading>Reminder</heading>
<body>Don't forget me this weekend!</body>
```

And finally the last line defines the end of the root element:

```
</note>
```

You can assume, from this example, that the XML document contains a note to Tove from Jani.

Don't you agree that XML is pretty self-descriptive?

XML Documents Form a Tree Structure

XML documents must contain a **root element**. This element is "the parent" of all other elements.

The elements in an XML document form a document tree. The tree starts at the root and branches to the lowest level of the tree.

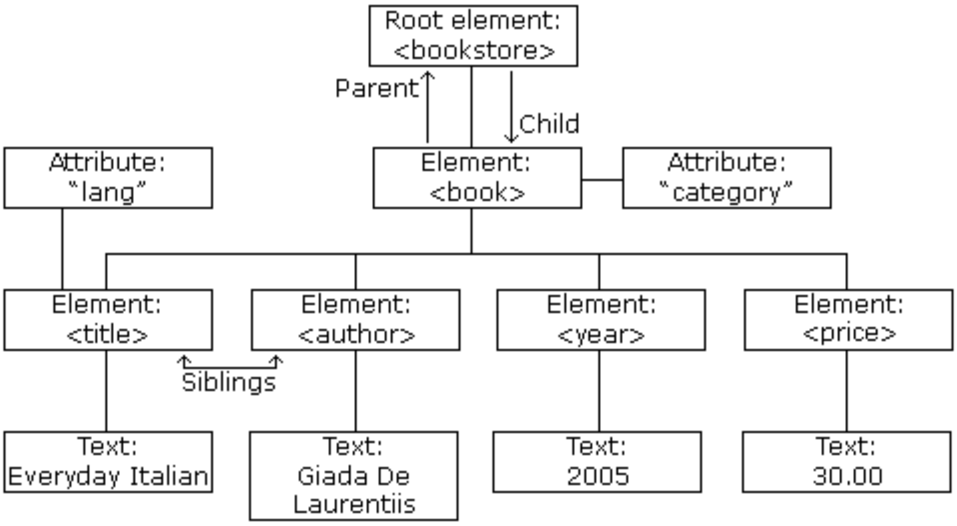
All elements can have sub elements (child elements):

```
<root>
  <child>
    <subchild>.....</subchild>
  </child>
</root>
```

The terms parent, child, and sibling are used to describe the relationships between elements. Parent elements have children. Children on the same level are called siblings (brothers or sisters).

All elements can have text content and attributes (just like in HTML).

Example:



The image above represents one book in the XML below:

```
<bookstore>
 <book category="COOKING">
  <title lang="en">Everyday Italian</title>
  <author>Giada De Laurentiis</author>
  <year>2005</year>
  <price>30.00</price>
 </book>
 <book category="CHILDREN">
  <title lang="en">Harry Potter</title>
  <author>J K. Rowling</author>
  <year>2005</year>
  <price>29.99</price>
 </book>
 <book category="WEB">
  <title lang="en">Learning XML</title>
  <author>Erik T. Ray</author>
  <year>2003</year>
  <price>39.95</price>
 </book>
</bookstore>
```

The root element in the example is <bookstore>. All <book> elements in the document are contained within <bookstore>.

The <book> element has 4 children: <title>,< author>, <year>, <price>.

18. PHP

- PHP is a server scripting language, and is a powerful tool for making dynamic and interactive Web pages.
- PHP is a widely-used, free, and efficient alternative to competitors such as Microsoft's ASP.
- What is PHP?
  - PHP stands for **P**HP: **H**ypertext **P**reprocessor
  - PHP is a widely-used, open source scripting language
  - PHP scripts are executed on the server
  - PHP is free to download and use

- What is a PHP File?
  - PHP files can contain text, HTML, JavaScript code, and PHP code
  - PHP code are executed on the server, and the result is returned to the browser as plain HTML
  - PHP files have a default file extension of ".php"

- What Can PHP Do?
  - PHP can generate dynamic page content
  - PHP can create, open, read, write, and close files on the server
  - PHP can collect form data
  - PHP can send and receive cookies
  - PHP can add, delete, modify data in your database
  - PHP can restrict users to access some pages on your website
  - PHP can encrypt data
  - With PHP you are not limited to output HTML. You can output images, PDF files, and even Flash movies. You can also output any text, such as XHTML and XML.

- Why PHP?
  - PHP runs on different platforms (Windows, Linux, Unix, Mac OS X, etc.)

  - PHP is compatible with almost all servers used today (Apache, IIS, etc.)
  - PHP has support for a wide range of databases
  - PHP is free. Download it from the official PHP resource: www.php.net
  - PHP is easy to learn and runs efficiently on the server side.

- The PHP script is executed on the server, and the plain HTML result is sent back to the browser.

- **Basic PHP Syntax**

A PHP script can be placed anywhere in the document.
A PHP script starts with **<?php** and ends with **?>**:

```
<?php
// PHP code goes here
?>
```

The default file extension for PHP files is ".php".
A PHP file normally contains HTML tags, and some PHP scripting code.

19. VOIP

Voice over IP (**VoIP**, abbreviation of **voice over Internet Protocol**) commonly refers to the communication protocols, technologies, methodologies, and transmission techniques involved in the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are *IP telephony*, *Internet telephony*, *voice over broadband* (VoBB), *broadband telephony*, *IP communications*, and*broadband phone*.

Internet telephony refers to communications services—voice, fax, SMS, and/or voice-messaging applications—that are transported via the Internet, rather than the public switched telephone network (PSTN). The steps involved in originating a VoIP telephone call are signaling and media channel setup, digitization of the analog voice signal, encoding, packetization, and transmission as Internet Protocol (IP) packets over a packet-switched network. On the receiving side, similar steps (usually in the reverse order) such as reception of the IP packets, decoding of the packets and digital-to-analog conversion reproduce the original voice stream.[1] Even though IP telephony and VoIP are used interchangeably, IP telephony refers to all use of IP protocols for voice communication by digital telephony systems, while VoIP is one technology used by IP telephony to transport phone calls.[2]

Early providers of voice over IP services offered business models (and technical solutions) that mirrored the architecture of the legacy telephone network. Second generation providers, such as Skype have built closed networks for private user bases, offering the benefit of free calls and convenience, while denying their users the ability to call out to other networks. This has severely limited the ability of users to mix-and-match third-party hardware and software. Third generation providers, such as Google Talk have adopted[3] the concept of Federated VoIP – which is a complete departure from the architecture of the legacy networks. These solutions typically allow arbitrary and dynamic interconnection between any two domains on the Internet whenever a user wishes to place a call.

VoIP systems employ session control protocols to control the set-up and tear-down of calls as well as audio codecs which encode speech allowing transmission over an IP network as digital audio via an audio stream. The choice of codec varies between different implementations of VoIP depending on application requirements and network bandwidth; some implementations rely on narrowband and compressed speech, while others support high fidelitystereo codecs. Some popular codecs include u-law and a-law versions of G.711, G.722 which is a high-fidelity codec marketed as HD Voice by Polycom, a popular open source voice codec known as iLBC, a codec that only uses 8 kbit/s each way called G.729, and many others.

VoIP is available on many smartphones and Internet devices so that users of portable devices that are not phones, may place calls or send SMS text messages over 3G or Wi-Fi.

UNANSWERED QUESTIONS :

1. 10 SCM
2. 10 Web programming languages
3. 10 Web application servers
4. Multi tier architure in context of web Technologies
5. DHTML

APRIL 2007

1. E-Business Strategies

- First Mover Advantage.
- Obtaining Market Lock-up,
- Cost of switching,
- Sticky Eyeballs
- Bricks and Clicks
- Winner Take All Markets

(http://www.jackmwilson.com/eBusiness/eBusinessBook/Strategies.htm)

First Mover Advantage.

If there is one thing that characterizes eBusiness, it is the importance of the first mover advantage. Those who have the idea, the resources, and the gumption to get to market first often have a huge advantage over the latecomers. In many cases Metcalf's Law accounts for much of the advantage. If your network of customers or clients is twice as large as your competitors then your network has four times the economic value. This of course attracts more customers to your site, which disproportionately increases your value even further relative to your competitor. This kind of positive feedback loop quickly locks in your competitive advantage. Systems of this type are often referred to as "network economies." Positive feedback systems are often referred to as exhibiting the "Matthew effecti[1]" from Matthew verses 13:12 "For whosoever hath, to him shall be given, and he shall have more abundance: but whosoever hath not, from him shall be taken away even that he hath." Positive feedback systems give to those who have and take from those who have not. That is often how competitive advantages are obtained in eBusiness.

Frank and Cook in "The Winner-Take-All Society" identify a number of factors for the development of winner-take-all markets.ii[2] These are: Production Cloning, Network Economies, Lock-in through Learning and Investment, Other self-reinforcing processes, Decision Leverage, Natural Limits on the Size of the Agenda, Habit formation or Acquired Tastes, Purely Positional (Status) Concerns, Gifts and Special Occasions, Avoidance of Regret, and Concentrated Purchasing Power.

Modifying that list in the light of the eBusiness experience yields the ten imperatives for sustaining a competitive advantage in eBusiness:

1. Production scale

2. Network Economies
3. Lock-in through Learning and Investment
4. Decision Leverage
5. Natural Limits on the Size of the Agenda
6. Habit formation or Acquired Tastes
7. Purely Positional (Status) Concerns
8. Avoidance of Regret
9. Concentrated Purchasing Power

Production Cloning: Competitive advantage can often come because there are significant economies of scale. Often the first copy of something can be enormously expensive, but every succeeding copy can be reproduced at a very small cost. The first copy of Microsoft Windows 2000, the Intel 64 bit chip, etc. can be remarkably expensive, while every succeeding copy cost pennies. This implies huge costs advantages to those with the largest markets and huge barriers to entry for those without.

Network Economies: The formation of auction communities such as eBay illustrates the inherent advantages to size. Once eBay had established a first mover advantage, it was enormously difficult for others to compete. A seller could find the most buyers on eBay and a buyer could find the most sellers. Why would anyone go to another auction site? eBay provides a place for buyers and sellers to meet to exchange goods through auction. The more buyers and sellers that participate, the more liquid the market and the better opportunity to get a good deal in buying and selling your goods. The first mover advantage enjoyed by eBay made it hard for buyers and sellers to switch to another site with fewer participants. Yahoo and Microsoft are both communities with lots of participants, but neither has yet been able to wrest leadership from eBay in on-line auctions.

In order to defend one's network advantage, it is important to try to raise the cost(pain) of switching outside of the network. You want to be sure that your customers feel a loss if they leave. If they can get all the same advantages while not being part of your network, then the cost of switching is low and you will find it difficult to defend your network advantage. AOL has an enormous network advantage because of its commanding market share of users, and one of the most valued AOL perks is the ability to IM (Instant Message) your on-line friends. People want to be on AOL since so many other people are already there, and they do not want to be left out.

If you are trying to break down someone else's network advantage, then you will try to lower the cost of switching. Phone companies do this to an absurd extreme by paying customers to switch to their networks. If you are one of the networks competing with AOL (MSN, Yahoo, etc) then you have t find a way to lower switching costs. A key element of that strategy is to allow your customers to IM AOL customers. Thus networks have created their own IM systems that they hope to make compatible with AOL IM. Since AOL wants to defend it advantage under Metcalf's Law, it would be to its advantage if their rivals were unable to do that. AOL has made a systematic effort to frustrate this access while justifying its actions as "defending the integrity of their user's experience." More cynical observers have attributed their actions to a desire to make it difficult to switch out of AOL.

Cumulative advantage through learning and investment: A company that establishes a competitive advantage can often maintain that competitive advantage through learning and investment. The rate at which any technology is improved is related to how dominant it is in the market. The dominant technologies are improved faster than the also-rans. This results in a cumulative advantage that can quickly become overwhelming. Microsoft Windows is a classic example of a technology that was very slow to be adopted until is had achieved a certain market penetration. At that point the cumulative investment of Windows developers created such a rich set of applications that no other operating systems could compete. Similarly, the Oracle database did not originally enjoy a commanding market position, but once an advantage developed it began to drive the market for database applications and attract the lion's share of investment.

Decision Leverage: There are times when a very small difference in ability might lead to a very large difference in value. By any objective measure Michael Jordan was only slightly better than his very talented competitors. He really could not jump that much higher than others. He was not that much more graceful. Not that much faster. But, when you put it all together and watched him play against his competitors those very small differences meant that he almost always came out on top in any one on one basketball contest. He made the others look like they were running in mud! His very slight advantage was worth almost any amount in salary because the consequences of his excellence were so dramatic. An executive like Jack Welch at GE is only slightly better than many many other middle level executives at GE, but the leverage of his decisions have such huge implications that no one would settle for second best at any price!

Natural Limits on the Size of the Agenda: There are only so many things that a single person can keep in memory. Thus the familiar has an enormous advantage over the unfamiliar. A person who is looking for a book on-line is likely to remember the address Amazon.com, but far less likely to remember any of the many other sites that also sell books. Why should they have to remember lists of names? Just type in Amazon.com and forget the rest! Amazon's familiarity comes from its market position and first mover advantage.

An eCommerce business may simply be familiar because of general use unrelated to the site. There was a long and bitter battle over the ownership of the address "Sex.com" because it was the easiest thing to imagine typing in if you were an internet user interested in sex. Battles over familiar web site names have become commonplace in eBusiness. Enterprising individuals bought up the rights to many domain names that are common trademarks for established businesses. In many cases the business had to pay millions to acquire the domain names from the original owners. In other cases businesses failed to recognize the value inherent in domain names and then were forced to acquire the domain name later. When Alta Vista discovered that someone else trademarked the name, they negotiated to buy the trademark from the owner, but failed to recognize the value of the domain name. Later they had to acquire the domain name for millions.

Habit formation or Acquired Tastes: Once you have learned to use a search engine or other application, it is often difficult to convince yourself to change to an alternative. Yahoo established a significant first mover advantage in search engines and then in portals built around search engines. Although much better products eventually came to market like Alta Vista and XXXXX, they could not overcome the advantage that Yahoo gained by having so many persons who knew how to use Yahoo and were comfortable in using the site.

Learning lock in is a characteristic of many markets in the technology area. It explains why no company has been able to break the domination of Microsoft Office, why the Apple Macintosh continues to dominate the education market, and why computer keyboards still use a key arrangement specifically designed to slow down typists to avoid stuck keys.

Avoidance of Regret: Many years ago, the best advice given to new employees in the IT areas of corporations was "No one ever gets fired for buying IBM." This piece of advice implies that the purchase of IBM equipment is the safe choice and the expected choice. If someone offers you a little better performance or a little better price, you had better think twice before accepting that offer. If it works you may be a minor hero. If it fails, you will surely be made to regret the purchase. Today the safe purchase might be a Microsoft operating system, a Cisco router, and Intel Inside PC, or an Oracle database. Competitors have a higher bar to clear.

Concentrated Purchasing Power: After Jim Clark founded Silicon Graphics, Netscape and then Healtheon, he came up with the idea for myCFO.com. His plan was to use the concentrated purchasing power of the wealthiest persons in the world to gain advantage over the suppliers of the financial and other services. He defined the wealthiest as those with over $10 million in net assets, and he called them the "wealthy masses." He assumed there were over 180,000 persons in the “wealthy masses” and that they controlled over 15 trillion dollars in assets. He explained that “The power of that money is huge. You could go and cut deals with banks or brokerage firms or insurance companies or anyone else who wanted to do business with the money” His argument of concentrated purchasing power was so persuasive that, with no business plan, he persuaded John Chambers, CEO of CISCO, Tom Jermoluk, CEO of @Home, Jim Barksdale, CEO of Netscape, and John Doerr, of the Kleiner Perkins Venture Capital Group, to finance the venture!

Purely Positional (Status) Concerns: This can occur when there is a status that can accrue with one brand that is not enjoyed by another. This explains why Tommy Hilfiger clothing became so ubiquitous on urban teens and young adults in the late 90s.

Gifts and Special Occasions: Why do diamonds enjoy a special place in our purchasing patterns? Because they have become the special symbol of certain occasions and nothing else will really do.

Obtaining Market Lock-up,

There is one strategy for obtaining market lock-up that is particularly advantageous to eBusinesses, and that strategy stems directly from the three driving laws, Moore’s Law, the Bandwidth Law, and Metcalf’s Law. EBusiness is one area of the economy which generally experiences declining unit costs for many of the elements of products and services. This allows a lock-up strategy based upon creative use of long-term contracts and systematic renewal of contracts. If a supplier has a long-term contract with a vendor, then there is often an opportunity for the supplier to go to that vendor and offer attractive terms for early renewal. No alternative supplier can make the same offer at that time, since the contract already in force makes the costs of switching to a new provider prohibitive to the consumer. The supplier is able to offer the consumer a contract that will reduce the consumer’s costs over the existing contract since the unit cost of delivering the products or services has decreased. The consumers have a huge incentive to renew the contract because they stand to save money immediately.

The astute consumer will realize what is happening, but faces a difficult choice. Suppose the supplier and consumer have a three year contract for a certain service. Suppose also that the unit cost of providing that service has halved over the first 18 months of the contract. The supplier can then offer the consumer a new three year contract at a significant discount (say 25%) to the existing contract and still make a profit. The consumer can either agree and immediately reduce the costs of the contract for the remaining 18 months of the contract, or can chose to pay the higher price for the remaining 18 months in hopes of obtaining an even lower cost of service for the next three year contract. If the consumers elect to renew early, the supplier has effectively locked in the consumers. If the consumers chose not to renew, they pay a higher price for the remainder of the contract and then the supplier has to meet the market at the end of the contract. This is almost a no-lose situation for the supplier, because the supplier will continue to have other advantages based upon the cost of switching and should have a favorable position vis-à-vis other suppliers that are trying to win the business. The only possible disadvantage is the chance of upsetting the customer, but customers rarely become upset when offered lower prices.

Cost of switching

As we have seen, raising the cost of switching is an important aspect of obtaining market lock-up. Once your organization has the advantage of Metcalf's Law, it needs to ensure that the cost of switching to another has more cost and more pain than the customer is willing to bear. This needs to be done quite delicately, since ham handed attempts to trap customers are usually obvious and often lead to the opposite effect of lowering switching costs. A customer that feels trapped is willing to pay a bit for freedom. The best way to keep a customer in your network is to offer better, more, and lest costly service than competitors. If the customer know that he or she can get more from your firm than from any other, then the cost of switching will always be too high.

Sticky Eyeballs:

The investment community began to refer to the customers using the websites as "eyeballs." The job of the sites was to "grab eyeballs." The more eyeballs the better Metcalf's law treated you. It was soon discovered that grabbing them was not enough. Once you got them to your site you needed to keep them there. Investors wanted sites with "sticky eyeballs." The theory was that if you could keep them on your site, they were likely to bring you revenue.

Bricks and Clicks

At first it was thought that one reason Amazon.com had a huge advantage over Barnes and Noble was because it did not have a huge capital investment in "bricks and mortar." Over time, that became less clearly an advantage. There was certainly the advantage of the lower capital investment, but there was a disadvantage in not being able to get product into the customers hands more quickly. Over the last two years we have seen the "brick and mortar" companies launch their own eCommerce arms using a variety of strategies. Some kept them as part of the bricks. Some spun them out into separate companies. The former had the advantage of building on the established brand name and closely integrating the strategies of the traditions retail with that of the eBusiness. The latter had the advantage of being unencumbered by the old ways of thinking, operating, financing and so on. In some cases the identification of the eBusiness with the tradition brand may not have been an advantage.

2. AJAX

Asynchronous JavaScript and XML, is a group of interrelated web development techniques used on the client-side to create asynchronous web applications. With Ajax, web applications can send data to, and retrieve data from, a server asynchronously (in the background) without interfering with the display and behavior of the existing page. Data can be retrieved using the XMLHttpRequest object. Despite the name, the use of XML is not required (JSON is often used instead), and the requests do not need to be asynchronous.

Google made a wide deployment of standards-compliant, cross browser Ajax with Gmail (2004) and Google Maps (2005).

On 5 April 2006 the World Wide Web Consortium (W3C) released the first draft specification for the XMLHttpRequest object in an attempt to create an official web standard.

Technologies: The term Ajax has come to represent a broad group of web technologies that can be used to implement a web application that communicates with a server in the background, without interfering with the current state of the page. The term Ajax explained that the following technologies are incorporated:

HTML (or XHTML) and CSS for presentation, The Document Object Model (DOM) for dynamic display of and interaction with data, XML for the interchange of data, and XSLT for its manipulation, The XMLHttpRequest object for asynchronous communication and JavaScript to bring these technologies together.

Drawbacks:

1. Depending on the nature of the Ajax application, dynamic page updates may interfere disruptively with user interactions, especially if working on an unstable Internet connection.

2. Dynamic web page updates also make it difficult to bookmark and return to a particular state of the application.

3. In pre-HTML5 browsers, pages dynamically created using successive Ajax requests did not automatically register themselves with the browser's history engine, so clicking the browser's "back" button may not have returned the browser to an earlier state of the Ajax-enabled page, but may have instead returned to the last full page visited before it. Such behavior — navigating between pages instead of navigating between page states — may be desirable, but if fine-grained tracking of page state is required then a pre-Ajax workaround was to use invisible iframes to trigger changes in the browser's history.

4. Because most web crawlers do not execute JavaScript code, publicly indexable web applications should provide an alternative means of accessing the content that would normally be retrieved with Ajax, thereby allowing search engines to index it.

5. Any user whose browser does not support JavaScript or XMLHttpRequest, or simply has this functionality disabled, will not be able to properly use pages which depend on Ajax. Devices such as smartphones and PDAs may not have support for the required technologies, though this is becoming less of an issue.

6. Some web applications which use Ajax are built in a way that cannot be read by screen-reading technologies, such as JAWS.

7. Screen readers that are able to use Ajax may still not be able to properly read the dynamically generated content.

8. The same origin policy prevents some Ajax techniques from being used across domains, although the W3C has a draft of the XMLHttpRequest object that would enable this functionality.

9. The asynchronous callback-style of programming required can lead to complex code that is hard to maintain, to debug and to test.

3. FTP

File Transfer Protocol (**FTP**) is a standard network protocol used to transfer files from one host or to another host over a TCP-based network, such as the Internet.

FTP is built on a client-server architecture and uses separate control and data connections between the client and the server.[1] FTP users may authenticate themselves using a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that hides (encrypts) the username and password, and encrypts the content, FTP is often secured with SSL/TLS ("FTPS"). SSH File Transfer Protocol ("SFTP") is sometimes also used instead, but is technologically different.

The first FTP client applications were command-line applications developed before operating systems had graphical user interfaces, and are still shipped with most Windows, Unix, and Linux operating systems.[2][3] Dozens of FTP clients and automation utilities have since been developed for desktops, servers, mobile devices, and hardware, and FTP has been incorporated into hundreds of productivity applications, such as Web page editors.

History

The original specification for the File Transfer Protocol was written by Abhay Bhushan and published as RFC 114 on 16 April 1971 and later replaced by RFC 765 (June 1980) and RFC 959 (October 1985), the current specification. Several proposed standards amend RFC 959, for example RFC 2228 (June 1997) proposes security extensions and RFC 2428 (September 1998) adds support for IPv6 and defines a new type of passive mode.[4]

Protocol overview

Communication and data transfer

The protocol was first specified June 1980 and updated in RFC 959,[2] which is summarized here.[5]

The server responds over the control connection with three-digit status codes in ASCII with an optional text message. For example "200" (or "200 OK") means that the last command was successful. The numbers represent the code for the response and the optional text represents a human-readable explanation or request (e.g. <Need account for storing file>).[1] An ongoing transfer of file data over the data connection can be aborted using an interrupt message sent over the control connection.

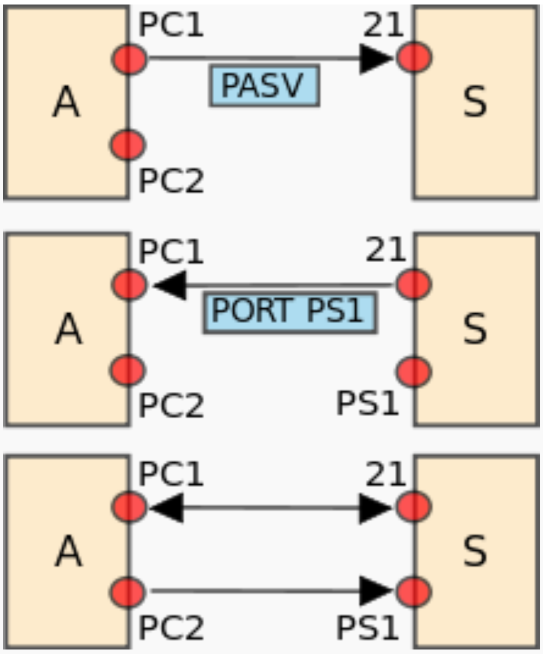


Illustration of starting a passive connection using port 21

FTP may run in *active* or *passive* mode, which determines how the data connection is established.[6] In active mode, the client creates a TCP control connection to the server and sends the server the client's IP address and an arbitrary client port number, and then waits until the server initiates the data connection over TCP to that client IP address and client port number.[7] In situations where the client is behind a firewall and unable to accept incoming TCP connections, *passive mode* may be used. In this mode, the client uses the control connection to send a PASV command to the server and then receives a server IP address and server port number from the server,[7][6] which the client then uses to open a data connection from an arbitrary client port to the server IP address and server port number received.[5] Both modes were updated in September 1998 to support IPv6. Further changes were introduced to the passive mode at that time, updating it to *extended passive mode*.[8]

While transferring data over the network, four data representations can be used:

- ASCII mode: used for text. Data is converted, if needed, from the sending host's character representation to "8-bit ASCII" before transmission, and (again, if necessary) to the receiving host's character representation. As a consequence, this mode is inappropriate for files that contain data other than plain text.
- Image mode (commonly called Binary mode): the sending machine sends each file byte for byte, and the recipient stores the bytestream as it receives it. (Image mode support has been recommended for all implementations of FTP).

- EBCDIC mode: use for plain text between hosts using the EBCDIC character set. This mode is otherwise like ASCII mode.
- Local mode: Allows two computers with identical setups to send data in a proprietary format without the need to convert it to ASCII

For text files, different format control and record structure options are provided. These features were designed to facilitate files containing Telnet or ASA

Data transfer can be done in any of three modes:[1][2]

- Stream mode: Data is sent as a continuous stream, relieving FTP from doing any processing. Rather, all processing is left up to TCP. No End-of-file indicator is needed, unless the data is divided into records.
- Block mode: FTP breaks the data into several blocks (block header, byte count, and data field) and then passes it on to TCP.[4]
- Compressed mode: Data is compressed using a single algorithm (usually run-length encoding).

Login

FTP login utilizes a normal usernames and password scheme for granting access.[2] The username is sent to the server using the USER command, and the password is sent using the PASS command.[2] If the information provided by the client is accepted by the server, the server will send a greeting to the client and the session will commence.[2] If the server supports it, users may log in without providing login credentials, but the same server may authorize only limited access for such sessions.[2]

Anonymous FTP

A host that provides an FTP service may provide anonymous FTP access.[2] Users typically log into the service with an 'anonymous' (lower-case and case-sensitive in some FTP servers) account when prompted for user name. Although users are commonly asked to send their email address instead of a password,[3] no verification is actually performed on the supplied data.[9] Many FTP hosts whose purpose is to provide software updates will provide anonymous logins.[3]

NAT and firewall traversal

FTP normally transfers data by having the server connect back to the client, after the PORT command is sent by the client. This is problematic for both NATsand firewalls, which do not allow connections from the Internet towards internal hosts.[10] For NATs, an additional complication is that the representation of the IP addresses and port number in the PORT command refer to the internal host's IP address and port, rather than the public IP address and port of the NAT.

There are two approaches to this problem. One is that the FTP client and FTP server use the PASV command, which causes the data connection to be established from the FTP client to the server.[10] This is widely used by modern FTP clients. Another approach is for the NAT to alter the values of the PORT command, using an application-level gateway for this purpose.[10]

Differences from HTTP

FTP is considered an *out-of-band* protocol, as opposed to an *in-band* protocol such as HTTP.[11]

Web browser support

Most common web browsers can retrieve files hosted on FTP servers, although they may not support protocol extensions such as FTPS.[3][12] When an FTP—rather than an HTTP—URL is supplied, the accessible contents on the remote server are presented in a manner that is similar to that used for other Web content. A full-featured FTP client can be run within Firefox in the form of an extension called FireFTP

Syntax

FTP URL syntax is described in RFC1738,[13] taking the form: ftp://[<user>[:<password>]@]<host>[:<port>]/<url-path>[13] (The bracketed parts are optional.) For example: ftp://public.ftp-servers.example.com/mydirectory/myfile.txt

or: ftp://user001:secretpassword@private.ftp-servers.example.com/mydirectory/myfile.txt

More details on specifying a username and password may be found in the browsers' documentation, such as, for example, Firefox [14] and Internet Explorer.[15]By default, most web browsers use passive (PASV) mode, which more easily traverses end-user firewalls.

Security

FTP was not designed to be a secure protocol—especially by today's standards—and has many security weaknesses.[16] In May 1999, the authors of RFC 2577 listed a vulnerability to the following problems: Brute force attacks, Bounce attacks, Packet capture (sniffing), Port stealing, Spoof attacks & Username protection.

FTP is not able to encrypt its traffic; all transmissions are in clear text, and usernames, passwords, commands and data can be easily read by anyone able to perform packet capture (sniffing) on the network.[2][16] This problem is common to many of the Internet Protocol specifications (such as SMTP, Telnet, POP and IMAP) that were designed prior to the creation of encryption mechanisms such as TLS or SSL.[4] A common solution to this problem is to use the "secure", TLS-protected versions of the insecure protocols (e.g. FTPS for FTP, TelnetS for Telnet, etc.) or a different, more secure protocol that can handle the job, such as the SFTP/SCP tools included with most implementations of the Secure Shell protocol.

Secure FTP

There are several methods of securely transferring files that have been called "Secure FTP" at one point or another.

FTPS

Explicit FTPS is an extension to the FTP standard that allows clients to request that the FTP session be encrypted. This is done by sending the "AUTH TLS" command. The server has the option of allowing or denying connections that do not request TLS. This protocol extension is defined in the proposed standard:RFC 4217. Implicit FTPS is a deprecated standard for FTP that required the use of a SSL or TLS connection. It was specified to use different ports than plain FTP.

SFTP

SFTP, the "SSH File Transfer Protocol," is not related to FTP except that it also transfers files and has a similar command set for users. SFTP, or secure FTP, is a program that uses Secure Shell (SSH) to transfer files. Unlike standard FTP, it encrypts both commands and data, preventing passwords and sensitive information from being transmitted openly over the network. It is functionally similar to FTP, but because it uses a different protocol, standard FTP clients cannot be used to talk to an SFTP server, nor can one connect to an FTP server with a client that supports only SFTP.

FTP over SSH (not SFTP)

FTP over SSH (not SFTP) refers to the practice of tunneling a normal FTP session over an SSH connection.[16] Because FTP uses multiple TCP connections (unusual for a TCP/IP protocol that is still in use), it is particularly difficult to tunnel over SSH. With many SSH clients, attempting to set up a tunnel for the *control channel* (the initial client-to-server connection on port 21) will protect only that channel; when data is transferred, the FTP software at either end will set up new TCP connections (*data channels*), which bypass the SSH connection and thus have no confidentiality or integrity protection, etc.

Otherwise, it is necessary for the SSH client software to have specific knowledge of the FTP protocol, to monitor and rewrite FTP control channel messages and autonomously open new packet forwardings for FTP data channels. Software packages that support this mode include:

- Tectia ConnectSecure (Win/Linux/Unix) of SSH Communications Security's software suite
- Tectia Server for IBM z/OS of SSH Communications Security's software suite
- FONC (the GPL licensed)
- Co:Z FTPSSH Proxy

FTP over SSH is sometimes referred to as *secure FTP*; this should not be confused with other methods of securing FTP, such as SSL/TLS (FTPS). Other methods of transferring files using SSH that are not related to FTP include SFTP and SCP; in each of these, the entire conversation (credentials and data) is always protected by the SSH protocol.

4. HTTP

The Hypertext Transfer Protocol is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

Hypertext is a multi-linear set of objects, building a network by using logical links (the so-called hyperlinks) between the nodes (e.g. text or words). HTTP is the protocol to exchange or transfer hypertext.

HTTP functions as a request-response protocol in the client-server computing model. A web browser, for example, may be the client and an application running on a computer hosting a web site may be the server.

A web browser is an example of a user agent (UA). Other types of user agent include the indexing software used by search providers (web crawlers), voice browsers, mobile apps and other software that accesses, consumes or displays web content.

HTTP is designed to permit intermediate network elements to improve or enable communications between clients and servers. High-traffic websites often benefit from web cache servers that deliver content on behalf of upstream servers to improve response time. Web browsers cache previously accessed web resources and reuse them when possible to reduce network traffic. HTTP proxy servers at private network boundaries can facilitate communication for clients without a globally routable address, by relaying messages with external servers.

Request methods

An HTTP request made using telnet. The request, response headers and response body are highlighted.

HTTP defines methods (sometimes referred to as verbs) to indicate the desired action to be performed on the identified resource. What this resource represents, whether pre-existing data or data that is generated dynamically, depends on the implementation of the server. Often, the resource corresponds to a file or the output of an executable residing on the server.

GET HEAD POST PUT DELETE TRACE OPTIONS CONNECT PATCH

Safe methods

Some methods (for example, HEAD, GET, OPTIONS and TRACE) are defined as safe, which means they are intended only for information retrieval and should not change the state of the server. In other words, they should not have side effects, beyond relatively harmless effects such as logging, caching, the serving of banner advertisements or incrementing a web counter.

By contrast, methods such as POST, PUT and DELETE are intended for actions that may cause side effects either on the server, or external side effects such as financial transactions or transmission of email.

HTTP session state - HTTP is a stateless protocol. A stateless protocol does not require the HTTP server to retain information or status about each user for the duration of multiple requests. However, some web applications implement states or server side sessions using one or more of the following methods:

HTTP cookies.

Query string parameters, for example, /index.php?session_id=some_unique_session_code.

Hidden variables within web forms.

Secure HTTP - There are three methods of establishing a secure HTTP connection: HTTP Secure, Secure Hypertext Transfer Protocol and the HTTP/1.1 Upgrade header.

Request message - The request message consists of the following:

A request line, for example GET /images/logo.png HTTP/1.1, which requests a resource called /images/logo.png from the server.

Response message - The response message consists of the following:

A Status-Line (for example HTTP/1.1 200 OK, which indicates that the client's request succeeded).

5. SOAP

Simple Object Access Protocol, is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks. It relies on Extensible Markup Language (XML) for its message format, and usually relies on other Application Layer protocols, most notably Hypertext Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission.

Characteristics

SOAP can form the foundation layer of a web services protocol stack, providing a basic messaging framework upon which web services can be built. This XML based protocol consists of three parts: an envelope, which defines what is in the message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing procedure calls and responses.

SOAP has three major characteristics:

Extensibility (security and WS-routing are among the extensions under development),

Neutrality (SOAP can be used over any transport protocol such as HTTP, SMTP, TCP, or JMS)

Independence (SOAP allows for any programming model).

SOAP originally stood for 'Simple Object Access Protocol' but this acronym was dropped with Version 1.2 of the standard.

After SOAP was first introduced, it became the underlying layer of a more complex set of Web Services, based on Web Services Description Language (WSDL) and Universal Description Discovery and Integration (UDDI).

Specification

The SOAP specification defines the messaging framework which consists of:

The SOAP processing model defining the rules for processing a SOAP message

The SOAP extensibility model defining the concepts of SOAP features and SOAP modules

The SOAP underlying protocol binding framework describing the rules for defining a binding to an underlying protocol that can be used for exchanging SOAP messages between SOAP nodes

The SOAP message construct defining the structure of a SOAP message.

Processing model

The SOAP processing model describes a distributed processing model, its participants, the SOAP nodes, and how a SOAP receiver processes a SOAP message. The following SOAP nodes are defined:

SOAP sender: A SOAP node that transmits a SOAP message.

SOAP receiver: A SOAP node that accepts a SOAP message.

SOAP message path: The set of SOAP nodes through which a single SOAP message passes.

Initial SOAP sender (Originator): The SOAP sender that originates a SOAP message at the starting point of a SOAP message path.

SOAP intermediary: A SOAP intermediary is both a SOAP receiver and a SOAP sender and is targetable from within a SOAP message. It processes the SOAP header blocks targeted at it and acts to forward a SOAP message towards an ultimate SOAP receiver.

Ultimate SOAP receiver: The SOAP receiver that is a final destination of a SOAP message. It is responsible for processing the contents of the SOAP body and any SOAP header blocks targeted at it. In some circumstances, a SOAP message might not reach an ultimate SOAP receiver, for example because of a problem at a SOAP intermediary. An ultimate SOAP receiver cannot also be a SOAP intermediary for the same SOAP message.

Transport methods

Both SMTP and HTTP are valid application layer protocols used as Transport for SOAP, but HTTP has gained wider acceptance as it works well with today's Internet infrastructure; specifically, HTTP works well with network firewalls. SOAP may also be used over HTTPS.

Message format

XML was chosen as the standard message format because of its widespread use by major corporations and open source development efforts.

Advantages:

1. SOAP is versatile enough to allow for the use of different transport protocols. The standard stacks use HTTP as a transport protocol, but other protocols such as JMS and SMTP are also usable.

2. Since the SOAP model tunnels fine in the HTTP post/response model, it can tunnel easily over existing firewalls and proxies, without modifications to the SOAP protocol, and can use the existing infrastructure.

Disadvantages:

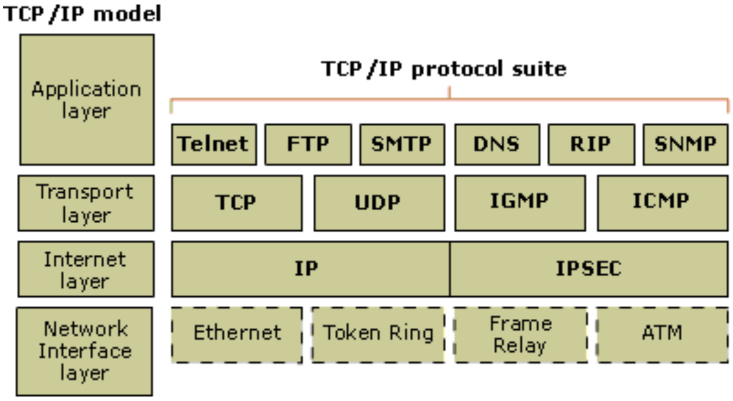
1. Because of the verbose XML format, SOAP can be considerably slower than competing middleware technologies such as CORBA or ICE. This may not be an issue when only small messages are sent.

2. When relying on HTTP as a transport protocol and not using WS-Addressing or an ESB, the roles of the interacting parties are fixed. Only one party (the client) can use the services of the other.

6. Various Protocols in TCP/IP Model:

TCP/IP is based on a four-layer reference model. All protocols that belong to the TCP/IP protocol suite are located in the top three layers of this model.

As shown in the following illustration, each layer of the TCP/IP model corresponds to one or more layers of the seven-layer Open Systems Interconnection (OSI) reference model proposed by the International Standards Organization (ISO).



The types of services performed and protocols used at each layer within the TCP/IP model are described in more detail below:

1. Application

Defines TCP/IP application protocols and how host programs interface with transport layer services to use the network.

HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows, other application protocols

2. Transport

Provides communication session management between host computers. Defines the level of service and status of the connection used when transporting data.

TCP, UDP, RTP

3. Internet

Packages data into IP datagrams, which contain source and destination address information that is used to forward the datagrams between hosts and across networks. Performs routing of IP datagrams.

IP, ICMP, ARP, RARP

4. Network interface

Specifies details of how data is physically sent through the network, including how bits are electrically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted-pair copper wire.

Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35.

2003

What is VPN?

A Virtual Private Network (VPN) is a network technology that creates a secure network connection over a public network such as the Internet or a private network owned by a service provider. Large corporations, educational institutions, and government agencies use VPN technology to enable remote users to securely connect to a private network.

A VPN can connect multiple sites over a large distance just like a Wide Area Network (WAN). VPNs are often used to extend intranets worldwide to disseminate information and news to a wide user base. Educational institutions use VPNs to connect campuses that can be distributed across the country or around the world.

In order to gain access to the private network, a user must be authenticated using a unique identification and a password. An authentication token is often used to gain access to a private network through a personal identification number (PIN) that a user must enter. The PIN is a unique authentication code that changes according to a specific frequency, usually every 30 seconds or so.

Protocols

There are a number of VPN protocols in use that secure the transport of data traffic over a public network infrastructure. Each protocol varies slightly in the way that data is kept secure.

IP security (IPSec) is used to secure communications over the Internet. IPSec traffic can use either transport mode or tunneling to encrypt data traffic in a VPN. The difference between the two modes is that transport mode encrypts only the message within the data packet (also known as the payload) while tunneling encrypts the entire data packet. IPSec is often referred to as a "security overlay" because of its use as a security layer for other protocols.

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) use cryptography to secure communications over the Internet. Both protocols use a "handshake" method of authentication that involves a negotiation of network parameters between the client and server machines. To successfully initiate a connection, an authentication process involving certificates is used. Certificates are cryptographic keys that are stored on both the server and client.

Point-To-Point Tunneling Protocol (PPTP) is another tunneling protocol used to connect a remote client to a private server over the Internet. PPTP is one of the most widely used VPN protocols because of it's straightforward configuration and maintenance and also because it is included with the Windows operating system.

Layer 2 Tunneling Protocol (L2TP) is a protocol used to tunnel data communications traffic between two sites over the Internet. L2TP is often used in tandem with IPSec (which acts as a security layer) to secure the transfer of L2TP data packets over the Internet. Unlike PPTP, a VPN implementation using L2TP/IPSec requires a shared key or the use of certificates.

VPN technology employs sophisticated encryption to ensure security and prevent any unintentional interception of data between private sites. All traffic over a VPN is encrypted using algorithms to secure data integrity and privacy. VPN architecture is governed by a strict set of rules and standards to ensure a private communication channel between sites. Corporate network administrators are responsible for deciding the scope of a VPN, implementing and deploying a VPN, and ongoing monitoring of network traffic across the network firewall. A VPN requires administrators to be continually be aware of the overall architecture and scope of the VPN to ensure communications are kept private.

Advantages

A VPN is a inexpensive effective way of building a private network. The use of the Internet as the main communications channel between sites is a cost effective alternative to expensive leased private lines. The costs to a corporation include the network authentication hardware and software used to authenticate users and any additional mechanisms such as authentication tokens or other secure devices. The relative ease, speed, and flexibility of VPN provisioning in comparison to leased lines makes VPNs an ideal choice for corporations who require flexibility. For example, a company can adjust the number of sites in the VPN according to changing requirements.

Disadvantages

There are several potential disadvantages with VPN use. The lack of Quality of Service (QoS) management over the Internet can cause packet loss and other performance issues. Adverse network conditions that occur outside of the private network is beyond the control of the VPN administrator. For this reason, many large corporations pay for the use of trusted VPNs that use a private network to guarantee QoS. Vendor interoperability is another potential disadvantage as VPN technologies from one vendor may not be compatible with VPN technologies from another vendor. Neither of these disadvantages have prevented the widespread acceptance and deployment of VPN technology.

History of the Internet

The history of the Internet began with the development of electronic computers in the 1950s. The public was first introduced to the concepts that would lead to the Internet when a message was sent over the ARPANet from computer science Professor Leonard Kleinrock's laboratory at University of California, Los Angeles (UCLA), after the second piece of network equipment was installed at Stanford Research Institute (SRI). Packet switched networks such as ARPANET, Mark I at NPL in the UK, CYCLADES, Merit Network, Tymnet, and Telenet, were developed in the late 1960s and early 1970s using a variety of protocols. The ARPANET in particular led to the development of protocols for internetworking, where multiple separate networks could be joined together into a network of networks.

In 1982, the Internet protocol suite (TCP/IP) was standardized, and consequently, the concept of a world-wide network of interconnected TCP/IP networks, called the Internet, was introduced. Access to the ARPANET was expanded in 1981 when the National Science Foundation (NSF) developed the Computer Science Network (CSNET) and again in 1986 when NSFNET provided access to supercomputer sites in the United States from research and education organizations. Commercial Internet service providers (ISPs) began to emerge in the late 1980s and early 1990s. The ARPANET was decommissioned in 1990. The Internet was commercialized in 1995 when NSFNET was decommissioned, removing the last restrictions on the use of the Internet to carry commercial traffic.

Since the mid-1990s, the Internet has had a revolutionary impact on culture and commerce, including the rise of near-instant communication by electronic mail, instant messaging, Voice over Internet Protocol (VoIP) "phone calls", two-way interactive video calls, and the World Wide Web with its discussion forums, blogs, social networking, and online shopping sites. The research and education community continues to develop and use advanced networks such as NSF's very high speed Backbone Network Service (vBNS), Internet2, and National LambdaRail. Increasing amounts of data are transmitted at higher and higher speeds over fiber optic networks operating at 1-Gbit/s, 10-Gbit/s, or more. The Internet's takeover over the global communication landscape was almost instant in historical terms: it only communicated 1% of the information flowing through two-way telecommunications networks in the year 1993, already 51% by 2000, and more than 97% of the telecommunicated information by 2007. Today the Internet continues to grow, driven by ever greater amounts of online information, commerce, entertainment, and social networking.

FTP

File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host or to another host over a TCP-based network, such as the Internet.

FTP is built on a client-server architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves using a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that hides (encrypts) the username and password, and encrypts the content, FTP is often secured with SSL/TLS ("FTPS"). SSH File Transfer Protocol ("SFTP") is sometimes also used instead, but is technologically different.

The first FTP client applications were command-line applications developed before operating systems had graphical user interfaces, and are still shipped with most Windows, Unix, and Linux operating systems.[2][3] Dozens of FTP clients and automation utilities have since been developed for desktops, servers, mobile devices, and hardware, and FTP has been incorporated into hundreds of productivity applications, such as Web page editors.

FTP may run in active or passive mode, which determines how the data connection is established. In active mode, the client creates a TCP control connection to the server and sends the server the client's IP address and an arbitrary client port number, and then waits until the server initiates the data connection over TCP to that client IP address and client port number. In situations where the client is behind a firewall and unable to accept incoming TCP connections, passive mode may be used. In this mode, the client uses the control connection to send a PASV command to the server and then receives a server IP address and server port number from the server, which the client then uses to open a data connection from an arbitrary client port to the server IP address and server port number received.

Active Server Pages (ASP)

Active Server Pages (ASP), also known as Classic ASP or ASP Classic, was Microsoft's first server-side script engine for dynamically generated web pages. Initially released as an add-on to Internet Information Services (IIS) via the Windows NT 4.0 Option Pack (ca. 1996), it was subsequently included as a free component of Windows Server (since the initial release of Windows 2000 Server). ASP.NET has superseded ASP.

It is a server-side scripting environment that you can use to create and run dynamic, interactive Web server applications. With ASP, you can combine HTML pages, script commands, and COM components to create interactive Web pages and powerful Web-based applications that are easy to develop and modify.

Server-side scripting is a technique used in website design which involves embedding scripts in an HTML source code which results in a user's (client's) request to the server website being handled by a script running server-side before the server responds to the client's request. The scripts can be written in any of a number of server-side scripting languages available (see below). Server-side scripting differs from client-side scripting where embedded scripts, such as JavaScript, are run client-side in the web browser.

Server-side scripting is usually used to provide an interface and to limit client access to proprietary databases or other data sources. These scripts may assemble client characteristics for use in customizing the response based on those characteristics, the user's requirements, access rights, etc. Server-side scripting also enables the website owner to reduce user access to the source code of server-side scripts which may be proprietary and valuable in itself. The down-side to the use of server-side scripting is that the server website computer needs to provide most of the computing resources before sending a page to the client computer for display via its web browser.

When the server serves data in a commonly used manner, for example according to the HTTP or FTP protocols, users may have their choice of a number of client programs (most modern web browsers can request and receive data using both of those protocols). In the case of more specialized applications, programmers may write their own server, client, and communications protocol, that can only be used with one another.

Some of the advantages of server-side scripting are:

1. It does not require the user to download plugins like Java or Flash (client-side scripting).

2. You can create a single website template for the entire website. Each new dynamic page you create will automatically use it.

3. You can configure a site to use a content management system, which simplifies the editing, publishing, adding of images, and creation of web applications. Many apps are often available in the form of extensions or addons.

4. Load times are generally faster than client-side scripting.
5. Your scripts are hidden from view. Users only see the HTML output, even when they view the source.

Java Platform independent ?

Java solves the problem of platform-independence by using byte code. The Java compiler does not produce native executable code for a particular machine like a C compiler would. Instead it produces a special format called byte code. Java byte code written in hexadecimal, byte by byte, looks like this:
CA FE BA BE 00 03 00 2D 00 3E 08 00 3B 08 00 01 08 00 20 08

This looks a lot like machine language, but unlike machine language Java byte code is exactly the same on every platform. This byte code fragment means the same thing on a Solaris workstation as it does on a Macintosh PowerBook. Java programs that have been compiled into byte code still need an interpreter to execute them on any given platform. The interpreter reads the byte code and translates it into the native language of the host machine on the fly. The most common such interpreter is Sun's program java (with a littlej). Since the byte code is completely platform independent, only the interpreter and a few native libraries need to be ported to get Java to run on a new computer or operating system. The rest of the runtime environment including the compiler and most of the class libraries are written in Java.

Features

1. Compiled and Interpreter:- has both Compiled and Interpreter Feature Program of java is First Compiled and Then it is must to Interpret it .First of all The Program of java is Compiled then after Compilation it creates Bytes Codes rather than Machine Language. Then After Bytes Codes are Converted into the Machine Language is Converted into the Machine Language with the help of the Interpreter So For Executing the java Program First of all it is necessary to Compile it then it must be Interpreter
2. Platform Independent:- Java Language is Platform Independent means program of java is Easily transferable because after Compilation of java program bytes code will be created then we have to just transfer the Code of Byte Code to another Computer.

3. Object-Oriented:- We Know that is purely OOP Language that is all the Code of the java Language is Written into the classes and Objects So For This feature java is Most Popular Language because it also Supports Code Reusability, Maintainability etc.
4. Robust and Secure:- The Code of java is Robust andMeans ot first checks the reliability of the code before Execution When We trying to Convert the Higher data type into the Lower Then it Checks the Demotion of the Code the It Will Warns a User to Not to do this So it is called as Robust

   Secure : When We convert the Code from One Machine to Another the First Check the Code either it is Effected by the Virus or not or it Checks the Safety of the Code if code contains the Virus then it will never Executed that code on to the Machine.
5. Distributed:- Java is Distributed Language Means because the program of java is compiled onto one machine can be easily transferred to machine and Executes them on another machine because facility of Bytes Codes So java is Specially designed For Internet Users which uses the Remote Computers For Executing their Programs on local machine after transferring the Programs from Remote Computers or either from the internet.
6. Simple Small and Familiar:- is a simple Language Because it contains many features of other Languages like c and C++ and Java Removes Complexity because it doesn't use pointers, Storage Classes and Go to Statements and java Doesn't support Multiple Inheritance
7. Multithreaded and Interactive:- Java uses Multithreaded Techniques For Execution Means Like in other in Structure Languages Code is Divided into the Small Parts Like These Code of java is divided into the Smaller parts those are Executed by java in Sequence and Timing Manner this is Called as Multithreaded In this Program of java is divided into the Small parts those are Executed by Compiler of java itself Java is Called as Interactive because Code of java Supports Also CUI and Also GUI Programs
8. Dynamic and Extensible Code:- Java has Dynamic and Extensible Code Means With the Help of OOPS java Provides Inheritance and With the Help of Inheritance we Reuse the Code that is Pre-defined and Also uses all the built in Functions of java and Classes
9. Distributed:- Java is a distributed language which means that the program can be design to run on computer networks. Java provides an extensive library of classes for communicating ,using TCP/IP protocols such as HTTP and FTP. This makes creating network connections much easier than in C/C++. You can read and write objects on the remote sites via URL with the same ease that programmers are used to when read and write data from and to a file. This helps the programmers at remote locations to work together on the same project.
10. Secure: Java was designed with security in mind. As Java is intended to be used in networked/distributor environments so it implements several security mechanisms to protect you against malicious code that might try to invade your file system.

11. Architectural Neutral: One of the key feature of Java that makes it different from other programming languages is architectural neutral (or platform independent). This means that the programs written on one platform can run on any other platform without having to rewrite or recompile them. In other words, it follows 'Write-once-run-anywhere' approach. Java programs are compiled into byte-code format which does not depend on any machine architecture but can be easily translated into a specific machine by a Java Virtual Machine (JVM) for that machine. This is a significant advantage when developing applets or applications that are downloaded from the Internet and are needed to run on different systems.
12. Portable : The portability actually comes from architecture-neutrality. In C/C++, source code may run slightly differently on different hardware platforms because of how these platforms implement arithmetic operations. In Java, it has been simplified.
13. Interpreted : Unlike most of the programming languages which are either complied or interpreted, Java is both complied and interpreted The Java compiler translates a java source file to bytecodes and the Java interpreter executes the translated byte codes directly on the system that implements the Java Virtual Machine. These two steps of compilation and interpretation allow extensive code checking and improved security.
14. High performance: Java programs are complied to portable intermediate form know as bytecodes, rather than to native machine level instructions and JVM executes Java bytecode on. Any machine on which it is installed. This architecture means that Java programs are faster than program or scripts written in purely interpreted languages but slower than C and C++ programs that compiled to native machine languages.

Types of Java Program

There are two types of Java programs

1. Application Programs
2. Applet Programs

Application Programs

Application programs are stand-alone programs that are written to carry out certain tasks on local computer such as solving equations, reading and writing files etc. The application programs can be executed using two steps

1. Compile source code to generate Byte code using Javac compiler.
2. Execute the byte code program using Java interpreter.

```
import java.io.*;
```

```
public class Example {

public static void main(String[] args) {

//desired code
    }
}
```

Applet programs:

Applets are small Java programs developed for Internet applications. An applet located in distant computer can be downloaded via Internet and executed on a local computer using Java capable browser. The Java applets can also be executed in the command line using appletviewer, which is part of the JDK.

Following example demonstrates how to create a basic Applet by extending Applet Class. You will need to embed another HTML code to run this program.

```
import java.applet.*;
import java.awt.*;

public class Main extends Applet{
  public void paint(Graphics g){
    g.drawString("Welcome in Java Applet.",40,20);
  }
}
```

Now compile the above code and call the generated class in your HTML code as follows:

```
<HTML>
<HEAD>
</HEAD>
<BODY>
<div >
<APPLET CODE="Main.class" WIDTH="800" HEIGHT="500">
</APPLET>
</div>
```

```
</BODY>
</HTML>
```

Symmetric and Asymmetric Encryption

Symmetric Encryption

Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

Asymmetric Encryption

The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is asymmetric encryption, in which there are two related keys--a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it.

Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key.

This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.

ColdFusion

ColdFusion is the name of a commercial rapid web application development platform invented by Jeremy and JJ Allaire in 1995. (The programming language used with that platform is also commonly called ColdFusion, though is more accurately known as CFML.) ColdFusion was originally designed to make it easier to connect simple HTML pages to a database.

Main features

ColdFusion provides a number of additional features out of the box. Among them:

- Simplified database access
- Client and server cache management
- Client-side code generation, especially for form widgets and validation
- Conversion from HTML to PDF and FlashPaper
- Data retrieval from common enterprise systems such as Active Directory, LDAP, SMTP, POP, HTTP, FTP, Microsoft Exchange Server and common data formats such as RSS and Atom
- File indexing and searching service based on Apache Solr
- GUI administration
- Server, application, client, session, and request scopes
- XML parsing, querying (XPath), validation and transformation (XSLT)
- Server clustering
- Task scheduling
- Graphing and reporting
- Simplified file manipulation including raster graphics (and CAPTCHA) and zip archives (introduction of video manipulation is planned in a future release)
- Simplified web service implementation

ColdFusion Markup Language, more commonly known as CFML, is a scripting language for web development that runs on the JVM, the .NET framework, and Google App Engine. Multiple commercial and open source implementations of CFML engines are available, including Adobe ColdFusion, New Atlanta BlueDragon (who makes both a Java-based and a .NET-based version), Railo, and Open BlueDragon as well as other CFML server engines.

CFML tags have a similar format to HTML tags. They are enclosed in angle brackets (< and >) and generally have zero or more named attributes, though some tags (e.g. cfset, cfif) contain an expression rather than attributes. Many CFML tags have bodies; that is, they have beginning and end tags with text to be processed between them. For example:

```
<cfoutput>
  #value# Bob!
```

```
</cfoutput>
```

Other tags, such as cfset and cfftp, never have bodies; all the required information goes between the beginning (<) character and the ending (>) character in the form of tag attributes (name/value pairs), as in the example below. If it is legal for tags not to have a body, it is syntactically acceptable to leave them unclosed as in the first example, though many CFML developers choose to self-close tags as in the second example to (arguably) make the code more legible.

```
<cfset value = "Hello">
<cfset value = "Hello" />
```

Even if the tag can have a body, including a body may not be necessary in some instances because the attributes specify all the required information. In these cases, as with the second example above, the end tag (and hence, the tag body) may be omitted and the tag may be self-closing as in the following example:

```
<cfexecute name="C:\\winNT\\System32\\netstat.exe" arguments="-e"
outputfile="C:\\Temp\\out.txt" timeout="1" />
```

Various tags offer the ability to type-check input parameters (e.g. cffunction, cfparam, cfqueryparam) if the programmer declares their type specifically. This functionality is used with cfqueryparam to secure web applications and databases from hackers and malicious web requests such as SQL injection.

CFML allows language extensions in the form of custom tags, which are tags created by the developer that are not part of the CFML language itself. Custom tags are regular CFML files which are intended to be invoked as tags, although it is possible to treat a template as both a custom tag and a regular template. Custom tags are written in CFML and are typically invoked by prefixing the custom tag's file name with *cf_*, although there are other ways to invoke custom tags.

If a template is invoked as a custom tag, the attributes used to invoke that tag are available within the tag in a special *attributes* structure and the variables contained in the calling page are accessible via the *caller* structure.

For example, if writing an *add* tag which takes two attributes and adds them together, the sum.cfm page would look like this:

```
<cfset caller.sum = attributes.first + attributes.second />
```

Assuming the template and tag are in the same directory, the tag can be invoked thus:

```
<cf_sum first="1" second="2">
```

Style sheets

Style sheets represent a major breakthrough for Web page designers, expanding their ability to improve the appearance of their pages. In the scientific environments in which the Web was conceived, people are more concerned with the content of their documents than the presentation. As people from wider walks of life discovered the Web, the limitations of HTML became a source of continuing frustration and authors were forced to sidestep HTML's stylistic limitations. While the intentions have been good -- to improve the presentation of Web pages -- the techniques for doing so have had unfortunate side effects. These techniques work for some of the people, some of the time, but not for all of the people, all of the time. They include:

- Using proprietary HTML extensions
- Converting text into images
- Using images for white space control
- Use of tables for page layout
- Writing a program instead of using HTML

These techniques considerably increase the complexity of Web pages, offer limited flexibility, suffer from interoperability problems, and create hardships for people with disabilities.

Style sheets solve these problems at the same time they supersede the limited range of presentation mechanisms in HTML. Style sheets make it easy to specify the amount of white space between text lines, the amount lines are indented, the colors used for the text and the backgrounds, the font size and style, and a host of other details.

For example, the following short CSS style sheet (stored in the file "special.css"), sets the text color of a paragraph to green and surrounds it with a solid red border:

```
P.special {
color : green;
border: solid red;
}
```

Authors may link this style sheet to their source HTML document with the LINK element:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
  "http://www.w3.org/TR/html4/strict.dtd">
<HTML>
```

```
 <HEAD>
  <LINK href="special.css" rel="stylesheet" type="text/css">
 </HEAD>
 <BODY>
  <P class="special">This paragraph should have special green text.
 </BODY>
</HTML>
```

HTML 4 provides support for the following style sheet features:

Flexible placement of style information

Placing style sheets in separate files makes them easy to reuse. Sometimes it's useful to include rendering instructions within the document to which they apply, either grouped at the start of the document, or in attributes of the elements throughout the body of the document. To make it easier to manage style on a site basis, this specification describes how to use HTTP headers to set the style sheets to be applied to a document.

Independence from specific style sheet languages

This specification doesn't tie HTML to any particular style sheet language. This allows for a range of such languages to be used, for instance simple ones for the majority of users and much more complex ones for the minority of users with highly specialized needs. The examples included below all use the CSS (Cascading Style Sheets) language, but other style sheet languages would be possible.

Cascading

This is the capability provided by some style sheet languages such as CSS to allow style information from several sources to be blended together. These could be, for instance, corporate style guidelines, styles common to a group of documents, and styles specific to a single document. By storing these separately, style sheets can be reused, simplifying authoring and making more effective use of network caching. The cascade defines an ordered sequence of style sheets where rules in later sheets have greater precedence than earlier ones. Not all style sheet languages support cascading.

Media dependencies

HTML allows authors to specify documents in a media-independent way. This allows users to access Web pages using a wide variety of devices and media, e.g., graphical displays for computers running Windows, Macintosh OS, and X11, devices for television sets, specially adapted phones and PDA-based portable devices, speech-based browsers, and braille-based tactile devices.

Style sheets, by contrast, apply to specific media or media groups. A style sheet intended for screen use may be applicable when printing, but is of little use for speech-based browsers. This specification allows you to define the broad categories of media a given style sheet is applicable to. This allows user agents to avoid retrieving inappropriate style sheets. Style sheet languages may include features for describing media dependencies within the same style sheet.

Alternate styles

Authors may wish to offer readers several ways to view a document. For instance, a style sheet for rendering compact documents with small fonts, or one that specifies larger fonts for increased legibility. This specification allows authors to specify a preferred style sheet as well as alternates that target specific users or media. User agents should give users the opportunity to select from among alternate style sheets or to switch off style sheets altogether.

Performance concerns

Some people have voiced concerns over performance issues for style sheets. For instance, retrieving an external style sheet may delay the full presentation for the user. A similar situation arises if the document head includes a lengthy set of style rules.

The current proposal addresses these issues by allowing authors to include rendering instructions within each HTML element. The rendering information is then always available by the time the user agent wants to render each element.

In many cases, authors will take advantage of a common style sheet for a group of documents. In this case, distributing style rules throughout the document will actually lead to worse performance than using a linked style sheet, since for most documents, the style sheet will already be present in the local cache. The public availability of good style sheets will encourage this effect.

Process Models

The large and growing body of software development organizations implement process methodologies. Many of them are in the defense industry, which in the U.S. requires a rating based on 'process models' to obtain contracts.

The international standard for describing the method of selecting, implementing and monitoring the life cycle for software is ISO/IEC 12207.

A decades-long goal has been to find repeatable, predictable processes that improve productivity and quality. Some try to systematize or formalize the seemingly unruly task of writing software. Others apply project management techniques to writing software. Without project management, software projects can easily be delivered late or over budget. With large numbers of software projects not meeting their expectations in terms of functionality, cost, or delivery schedule, effective project management appears to be lacking.

Organizations may create a Software Engineering Process Group (SEPG), which is the focal point for process improvement. Composed of line practitioners who have varied skills, the group is at the center of the collaborative effort of everyone in the organization who is involved with software engineering process improvement.

Software development activities

Planning

Planning is an objective of each and every activity, where we want to discover things that belong to the project. An important task in creating a software program is extracting the requirements or requirements analysis. Customers typically have an abstract idea of what they want as an end result, but not what *software* should do. Skilled and experienced software engineers recognize incomplete, ambiguous, or even contradictory requirements at this point. Frequently demonstrating live code may help reduce the risk that the requirements are incorrect.

Once the general requirements are gathered from the client, an analysis of the scope of the development should be determined and clearly stated. This is often called a scope document.

Certain functionality may be out of scope of the project as a function of cost or as a result of unclear requirements at the start of development. If the development is done externally, this document can be considered a legal document so that if there are ever disputes, any ambiguity of what was promised to the client can be clarified.

Implementation, testing and documenting

Implementation is the part of the process where software engineers actually program the code for the project.

Software testing is an integral and important phase of the software development process. This part of the process ensures that defects are recognized as soon as possible.

Documenting the internal design of software for the purpose of future maintenance and enhancement is done throughout development. This may also include the writing of an API, be it external or internal. The software engineering process chosen by the developing team will determine how much internal documentation (if any) is necessary. Plan-driven models (e.g., Waterfall) generally produce more documentation than Agile models.

Deployment and maintenance

Deployment starts after the code is appropriately tested, approved for release, and sold or otherwise distributed into a production environment. This may involve installation, customization (such as by setting parameters to the customer's values), testing, and possibly an extended period of evaluation.

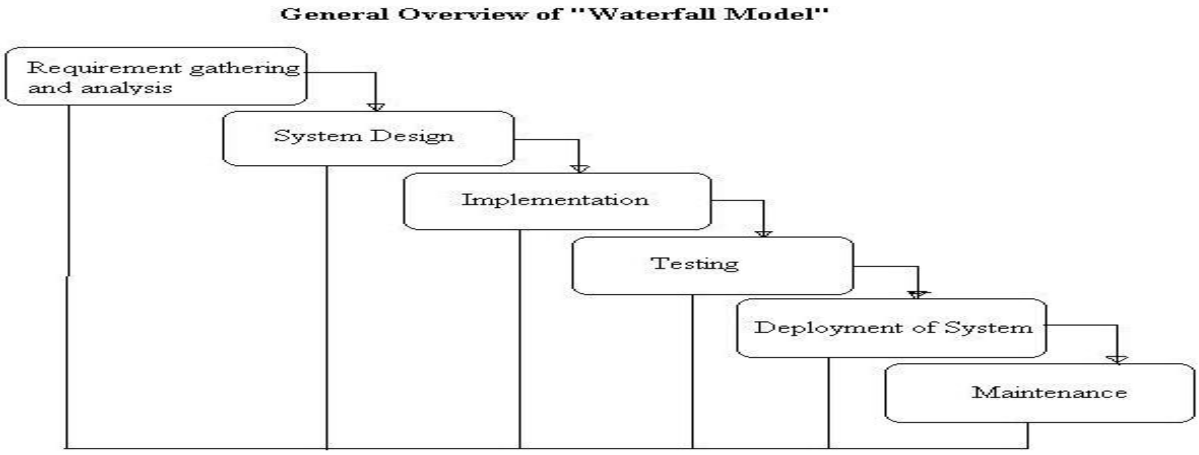
Software training and support is important, as software is only effective if it is used correctly.

Maintaining and enhancing software to cope with newly discovered faults or requirements can take substantial time and effort, as missed requirements may force redesign of the software.

Waterfall model- advantages, disadvantages

The Waterfall Model was first Process Model to be introduced. It is also referred to as a **linear-sequential life cycle model**. It is very simple to understand and use. In a waterfall model, each phase must be completed fully before the next phase can begin. At the end of each phase, a review takes place to determine if the project is on the right path and whether or not to continue or discard the project. In waterfall model phases do not overlap.

Diagram of Waterfall-model:


General Overview of "Waterfall Model"
Requirement gathering and analysis
System Design
Implementation
Testing
Deployment of System
Maintenance

Advantages of waterfall model:

- Simple and easy to understand and use.
- Easy to manage due to the rigidity of the model – each phase has specific deliverables and a review process.
- Phases are processed and completed one at a time.
- Works well for smaller projects where requirements are very well understood.

Disadvantages of waterfall model:

- Once an application is in the testing stage, it is very difficult to go back and change something that was not well-thought out in the concept stage.
- No working software is produced until late during the life cycle.
- High amounts of risk and uncertainty.
- Not a good model for complex and object-oriented projects.
- Poor model for long and ongoing projects.
- Not suitable for the projects where requirements are at a moderate to high risk of changing.

When to use the waterfall model:

- Requirements are very well known, clear and fixed.
- Product definition is stable.
- Technology is understood.
- There are no ambiguous requirements
- Ample resources with required expertise are available freely
- The project is short.

What is Prototyping Model SDLC?

In Prototyping model, a prototype is made first and based on it final product is developed. A prototype is a model or a program which is not based on strict planning, but is an early approximation of the final product or software system. A prototype acts as a sample to test the process. From this sample we learn and try to build a better final product. Please note that this prototype may or may not be completely different from the final system we are trying to develop.

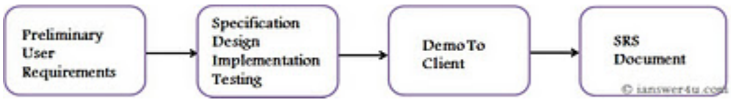
There are several steps in the Prototyping Model:

1. The new system requirements are defined in as much detail as possible. This usually involves interviewing a number of users representing all the departments or aspects of the existing system.

2. A preliminary design is created for the new system.
3. A first prototype of the new system is constructed from the preliminary design. This is usually a scaled-down system, and represents an approximation of the characteristics of the final product.
4. The users thoroughly evaluate the first prototype, noting its strengths and weaknesses, what needs to be added, and what should to be removed. The developer collects and analyzes the remarks from the users.
5. The first prototype is modified, based on the comments supplied by the users, and a second prototype of the new system is constructed.
6. The second prototype is evaluated in the same manner as was the first prototype.
7. The preceding steps are iterated as many times as necessary, until the users are satisfied that the prototype represents the final product desired.
8. The final system is constructed, based on the final prototype.
9. The final system is thoroughly evaluated and tested. Routine maintenance is carried out on a continuing basis to prevent large-scale failures and to minimize downtime.

Need of Prototyping Model

This type of System Development Method is employed when it is very difficult to obtain exact requirements from the customer(unlike waterfall model, where requirements are clear). While making the model, user keeps giving feedbacks from time to time and based on it, a prototype is made. Completely built sample model is shown to user and based on his feedback, the SRS(System Requirements Specifications) document is prepared. After completion of this, a more accurate SRS is prepared, and now development work can start using Waterfall Model. Now lets discuss the disadvantages and advantages of the Prototype model in Software Development Method.


Preliminary User Requirements
Specification Design Implementation Testing
DemoTo Client
SRS Document
© ianswer4u.com

Prototyping Process Model

Advantages of Prototyping Model

1) When prototype is shown to the user, he gets a proper clarity and 'feel' of the functionality of the software and he can suggest changes and modifications.

2) This type of approach of developing the software is used for non-IT-literate people. They usually are not good at specifying their requirements, nor can tell properly about what they expect from the software.

3) When client is not confident about the developer's capabilities, he asks for a small prototype to be built. Based on this model, he judges capabilities of developer.
4) Sometimes it helps to demonstrate the concept to prospective investors to get funding for project.
5) It reduces risk of failure, as potential risks can be identified early and mitigation steps can be taken.
6) Iteration between development team and client provides a very good and conductive environment during project.
7) Time required to complete the project after getting final the SRS reduces, since the developer has a better idea about how he should approach the project.

Disadvantages of Prototyping Model:

1) Prototyping is usually done at the cost of the developer. So it should be done using minimal resources. It can be done using Rapid Application Development (RAD) tools. Please note sometimes the start-up cost of building the development team, focused on making prototype, is high.
2) Once we get proper requirements from client after showing prototype model, it may be of no use. That is why, sometimes we refer to the prototype as "Throw-away" prototype.
3) It is a slow process.
4) Too much involvement of client, is not always preferred by the developer.
5) Too many changes can disturb the rhythm of the development team.

Preliminary analysis

The main objectives of preliminary analysis is to identify the customer's needs, evaluate system concept for feasibility, perform economic and technical analysis, perform cost benefit analysis and create system definition that forms the foundation for all subsequent engineering works. There should be enough expertise available for hardware and software for doing analysis.

While performing analysis, the following questions arise.

- How much time should be spent on it?
  As such, there are no rules or formulas available to decide on this. However, size, complexity, application field, end-use, contractual obligation are few parameters on which it should be decided.
- Other major question that arises is who should do it.
  Well an experienced well-trained analyst should do it. For large project, there can be an analysis team.

After the preliminary analysis, the analyst should report the findings to management, with recommendations outlining the acceptance or rejection of the proposal.

Create a web page

Validate the web page

Languages or technologies used

Techniques to maintain secrecy and security of data

Disk Encryption

Disk encryption refers to encryption technology that encrypts data on a hard disk drive. Disk encryption typically takes form in either software (see disk encryption software] or hardware (see disk encryption hardware). Disk encryption is often referred to as on-the-fly encryption ("OTFE") or transparent encryption.

Hardware based Mechanisms for Protecting Data

Software based security solutions encrypt the data to prevent data from being stolen. However, a malicious program or a hacker may corrupt the data in order to make it unrecoverable, making the system unusable. Hardware-based security solutions can prevent read and write access to data and hence offers very strong protection against tampering and unauthorized access.

Hardware based or assisted computer security offers an alternative to software-only computer security. Security tokens such as those using PKCS(*public-key cryptography standards*) may be more secure due to the physical access required in order to be compromised. Access is enabled only when the token is connected and correct PIN is entered (see two factor authentication). However, dongles can be used by anyone who can gain physical access to it. Newer technologies in hardware based security solves this problem offering fool proof security for data.

Working of Hardware based security: A hardware device allows a user to log in, log out and to set different privilege levels by doing manual actions. The device uses biometric technology to prevent malicious users from logging in, logging out, and changing privilege levels. The current state of a user of the device is read by controllers in peripheral devices such as harddisks. Illegal access by a malicious user or a malicious program is interrupted based on the current state of a user by harddisk and DVD controllers making illegal access to data impossible. Hardware based access control is more secure than protection provided by the operating systems as operating systems are vulnerable to malicious attacks by viruses and hackers. The data on harddisks can be corrupted after a malicious access is obtained. With hardware based protection, software cannot manipulate the user privilege levels, it is impossible for a hacker or a malicious program to gain access to secure data protected by hardware or perform unauthorized privileged operations. The hardware protects the operating system image and file system privileges from being tampered. Therefore, a completely secure system can be created using a combination of hardware based security and secure system administration policies.

Backups

Backups are used to ensure data which is lost can be recovered.

Data Masking

Data Masking of structured data is the process of obscuring (masking) specific data within a database table or cell to ensure that data security is maintained and sensitive information is not exposed to unauthorized personnel. This may include masking the data from users (for example so banking customer representatives can only see the last 4 digits of a customers national identity number), developers (who need real production data to test new software releases but should not be able to see sensitive financial data), outsourcing vendors, etc.

Data Erasure

Data erasure is a method of software-based overwriting that completely destroys all electronic data residing on a hard drive or other digital media to ensure that no sensitive data is leaked when an asset is retired or reused.

Also read encryption above

Unanswered:

Expansion from India to USA, Norway and Argentina. Legal and administrative hurdles faced? Solutions for implementation?

Q1 Explain a)XML:

XML is a simplified version of SGML and a cousin of HTML. It was developed by members of the W3C and released as a recommendation by the W3C in February 1998.
SGML, the parent of XML, is an international standard that has been in use as a markup language primarily for technical documentation and government applications since the early 1980s. It was developed to standardize the production process for large document sets.

XML is a way of adding intelligence to your documents.
It lets you identify each element using meaningful tags and it lets you add information ("metatdata") about each element.
XML is very much a part of the future of Web, and part of the future for all electronic information.
XML is a syntax for marking up data and it works with many other technologies to display and process information. It looks and feels very much like HTML.
You'll still need to use CSS--Cascading Style Sheets-- (with XML) to define font colors or JavaScript (again, with XML) to make your images fly around.
XML lets you make documents smarter, more portable, and more powerful.
XML allows you to use your own tags to define parts of a document. That is, XML describes what something is rather than performing an action.

For example, take a look at the front page of a newspaper. You'll see different font sizes, different sections, and columns.
If you were to create a Web page for that newspaper--using the same formatting and styles--you would use tags such as <H1> and <font color="red"> to define the size and color of a large headline, or <i> to italicize a word such as a byline, in order to distinguish it from the rest of the text.
But just try to write tags that actually explain that you've got a Headline and that the words "John Smith" make up a byline. HTML won't know what you're talking about if you create tags such as <Headline> or <byline> or <advertisement>.
XML, with help from other technologies such as CSS, understands what the elements are and how to display them.
That means, in the future, when you're searching on the web for say, a Barbie doll for your niece's birthday, you'll get Barbie the DOLL instead of some other type of Barbie, because the Barbie doll page might be marked up like this:

<DOLL>Barbie</DOLL>.

XML documents can be moved to any format on any platform -- without the elements losing their meaning. That means you can publish the same information to a web browser, a PDA, or a network-enabled bread machine and each device would use the information appropriately.

The design goals of XML, taken from the XML **Specification** are:

- XML shall be straightforwardly usable over the Internet.
- XML shall support a wide variety of applications.
- XML shall be compatible with SGML.
- It shall be easy to write programs which process XML documents.
- The number of optional features in XML is to be kept to the absolute minimum, ideally zero.
- XML documents should be human-legible and reasonably clear.
- The XML design should be prepared quickly.
- The design of XML shall be formal and concise.
- XML documents shall be easy to create.
- Terseness in XML markup is of minimal importance.

In other words, XML is easy to create, easy to read, and designed for use over the Internet. What more could a Web designer ask for?

What Does XML Look Like?

```
<?xml version="1.0"?>
<CANTERBURY-TALES>
<SECTION name="physician">
The Physician's Tale
<LINE number="282">
That no man woot therof but God and he.
</LINE>
</SECTION>
</CANTERBURY-TALES>
```

The tags simply define that:

1) This document is the Canterbury Tales.

2) This section is the Physician's Tale.

3) Each line of the Physician's Tale is defined.

4) Each line ends, and the Physician's Tale and The Canterbury Tales end.

If the entire document were marked up such as this, you could easily jump to a certain line or section. The entire document is annotated for easy reference and searching, and instead of viewing the entire document, users could request only specific sections of a document--simply by calling the specific tags they want.

XML Syntax

Tagging an XML document is, in many ways, similar to tagging an HTML document. Here are some of the most important guidelines to follow.

Rule #1: Remember the XML declaration

This declaration goes at the beginning of the file and alerts the browser or other processing tools that this document contains XML tags. The declaration looks like this:

<?xml version="1.0" standalone="yes/no" encoding="UTF-8"?>

You can leave out the encoding attribute and the processor will use the UTF-8 default.

Rule #2: Do what the DTD instructs

If you are creating a valid XML file, one that is checked against a DTD, make sure you Know what tags are part of the DTD and use them appropriately in your document. Understand what each does and when to use it. Know what the allowable values are for each. Follow those rules. The XML document will validate against the specified DTD.

Rule #3: Watch your capitalization

XML is case-sensitive. <P> is not the same as <p>. Be consistent in how you define element names. For example, use ALL CAPS, or use Initial caps, or use all lowercase. It is very easy to create mis-matching case errors.

Also, make sure starting and ending tags use matching capitalization, too. If you start a paragraph with the <P> tag, you must end it with the </P> tag, not a </p>.

Rule #4: Quote attribute values

In HTML there is some confusion over when to enclose attribute values in quotes. In XML the rule is simple: enclose all attribute values in quotes, like this:

<NAME dob="1960">Ben Johnson</NAME>

Rule #5: Close all tags

In XML you must close all tags. This means that paragraphs must have corresponding end paragraph tags. Anchor names must have corresponding anchor end tags. A strict interpretation of HTML says we should have been doing this all along, but in reality, most of us haven't.

Rule #6: Close Empty tags, too

In HTML, empty tags, such as <br> or <img>, do not close. In XML, empty tags do close. You can close them either by adding a separate close tag (</tagname>) or by combining the open and close tags into one tag. You create the open/close tag by adding a slash, /, to the end of the tag, like this: <br/>

Examples

This table shows some HTML common tags and how they would be treated in XML.

Tag	Comment	End-Tag
<P>	Technically, in HTML, you're supposed to close this tag. In XML, it's essential to close it.	</P>
<ELEMENT>	All Elements in XML must have a Start-tag and an end-tag.	</ELEMENT>
<LI>	This tag must be closed in XML in order to ensure a Well-Formed XML document.	</LI>
<META name="keywords" content="XML, SGML, HTML">	META tags are considered empty elements in XML, and they must close.	<META name="keywords" content="XML, SGML, HTML"/>
<BR>	Break tags are considered empty elements.	<BR/>
<IMG src= "coolpictures.html">	This is an empty element tag.	<IMG src= "coolpictures.html"/>

Source : portal.aauj.edu/portal_resources/downloads/xml/what_is_xml.doc

Q2) Technology in tiers from Microsoft and java

Ans : Microsoft : N-Tier Data Applications Overview

N-tier data applications are data applications that are separated into multiple tiers. Also called "distributed applications" and "multitier applications," n-tier applications separate processing into discrete tiers that are distributed between the client and the server. When you develop applications that access data, you should have a clear separation between the various tiers that make up the application.

A typical n-tier application includes a presentation tier, a middle tier, and a data tier. The easiest way to separate the various tiers in an n-tier application is to create discrete projects for each tier that you want to include in your application. For example, the presentation tier might be a Windows Forms application, whereas the data access logic might be a class library located in the middle tier. Additionally, the presentation layer might communicate with the data access logic in the middle tier through a service such as a service. Separating application components into separate tiers increases the maintainability and scalability of the application. It does this by enabling easier adoption of new technologies that can be applied to a single tier without the requirement to redesign the whole solution. In addition, n-tier applications typically store sensitive information in the middle-tier, which maintains isolation from the presentation tier.

Visual Studio contains several features to help developers create n-tier applications:

- The **Dataset Designer** provides a DataSet Project property that enables you to separate the dataset (data entity layer) and TableAdapters (data access layer) into discrete projects.

- The **Object Relational Designer (O/R Designer)** provides settings to generate the DataContext and data classes into separate namespaces. This enables logical separation of the data access and data entity tiers.

- **LINQ to SQL** provides the **Attach** method that enables you to bring together the DataContext from different tiers in an application. For more information, see **N-Tier and Remote Applications with LINQ to SQL**.

Presentation Tier

The presentation tier is the tier in which users interact with an application. It often contains additional application logic also. Typical presentation tier components include the following:

- Data binding components, such as the **BindingSource** and **BindingNavigator**.

- Object representations of data, such as **LINQ to SQL** entity classes for use in the presentation tier.

The presentation tier typically accesses the middle tier by using a service reference (for example, a **Windows Communication Foundation Services and WCF Data Services in Visual Studio** application). The presentation tier does not directly access the data tier. The presentation tier communicates with the data tier by way of the data access component in the middle tier.

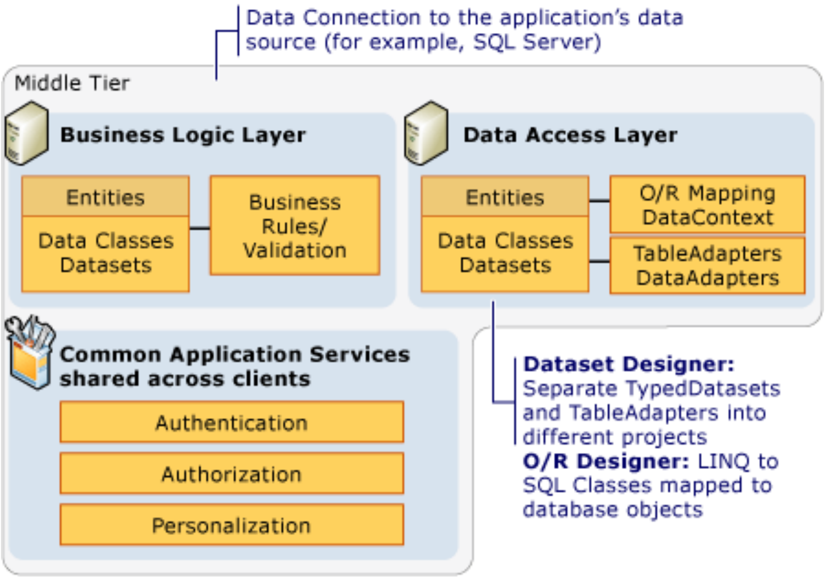
Middle Tier

The middle tier is the layer that the presentation tier and the data tier use to communicate with each other. Typical middle tier components include the following:

- Business logic, such as business rules and data validation.
- Data access components and logic, such as the following:
    - **TableAdapters** and **DataAdapters and DataReaders (ADO.NET)**.
    - Object representations of data, such as **LINQ to SQL** entity classes.
    - Common application services, such as authentication, authorization, and personalization.

The following illustration shows features and technologies that are available in Visual Studio and where they might fit in to the middle tier of an n-tier application.

Middle tier


Data Connection to the application's data source (for example, SQL Server)
Middle Tier
Business Logic Layer
Entities
Data Classes Datasets
Business Rules/ Validation
Data Access Layer
Entities
Data Classes Datasets
O/R Mapping DataContext
TableAdapters DataAdapters
Common Application Services shared across clients
Authentication
Authorization
Personalization
Dataset Designer: Separate TypedDatasets and TableAdapters into different projects
O/R Designer: LINQ to SQL Classes mapped to database objects

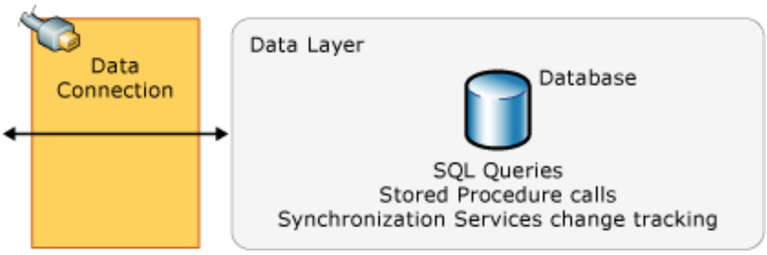
The middle tier typically connects to the data tier by using a data connection. This data connection is typically stored in the data access component.

Data Tier

The data tier is basically the server that stores an application's data (for example, a server running SQL Server).

The following illustration shows features and technologies that are available in Visual Studio and where they might fit in to the data tier of an n-tier application.

Data tier



The data tier cannot be accessed directly from the client in the presentation tier. Instead, the data access component in the middle tier is used for communication between the presentation and data tiers.

Source : MSDN

Q3) Difference between Client-Server application and web based applications?

Ans: Client/Server application:

1. Application runs in two or more machines
2. Application is a menu-driven
3. Connected mode (connection exists always until logout)
4. Limited number of users
5. Less number of network issues when compared to web app.

Web application:

1. Application runs in two or more machines
2. URL-driven
3. Disconnected mode (state less)
4. Unlimited number of users
5. Many issues like hardware compatibility, browser compatibility, version compatibility, security issues, performance issues etc.

Architectural Differences

- According to Information-Management.com, client-server applications are typically two-tiered, consisting of an in-house server loaded with the operating system, a database and application software and a client personal computer loaded with a software application that interacts with the server. Web-based applications are usually three-tiered, consisting of a database server, a Web server and possibly a separate application server. You use an Internet browser to connect to and use the application.

Financial Concerns

- Companies pay for Web-based applications on a subscription or usage basis. Client-server applications, however, are purchased up front, usually with a huge initial cost and ongoing licensing and maintenance fees, which can wind up costing as much as 20 percent per year of the original fee according to The IQ Group.
- Support Considerations
- Servers need regular maintenance such as upgrades, patches and hardware maintenance. All costs to purchase, maintain and upgrade the network for client-server applications are the company's responsibility. A company using a Web-based application through an Application Service Provider, however, is little involved with support.

Source:
http://www.softwaretestinghelp.com/what-is-client-server-and-web-based-testing-and-how-to-test-these-applications/
http://www.ehow.com/facts_7339964_difference-between-web_based-client_server-applications.html

Q 5) History of the Internet [GROUP 2 Presentation] or
Source - **http://www.computerhistory.org/internet_history/index.html**

Q6) ISP services and features? Give optional features too.

In this day and age, no business can succeed without being connected to the Internet. Businesses of all sizes use the Internet to connect with their customers, to stay in touch with their vendors, and to let the public know what is happening in their world.

Internet access companies are commonly known as Internet service providers, or ISPs for short. There are literally thousands of ISPs providing a wide range of Internet services, so when you are shopping around, it pays to do your homework ahead of time. You should know what your company needs in terms of Internet access and features, and look for a provider that meets your business goals and budget.

When shopping for an ISP, make sure they include these basic features:

- E-mail accounts. Look for ISPs that offer the best packages on e-mail accounts, including features and number of e-mail aliases.

- Customer service and support. While many ISP companies are still mom-and-pop shops, look for a provider that can provide the service and support that your business needs. Always consider the worst case scenario, and be sure you have someone you can contact if there are problems.
- High-speed access. You can connect to the Internet in a number of different ways, including dialup, DSL, cable, and even wireless. Over the past decade, thousands of miles of fiber-optic cable have been installed all across the country, allowing more businesses and households to connect to the Internet at a much faster speed. Wireless options are also increasing, and more businesses are including that feature as part of their Internet service package.
- Advanced spam-blocking features. A few years ago, spam blocking features cost extra, but these days they are more likely to be part of the basic features package.

In addition to the regular services, some ISP's offer additional value-added services, including:

- Domain name registration. Many ISPs will include the cost of registering a domain name into their access or hosting packages. Prices for domain name registrations and automatic renewals will also vary, so make sure you get the best price available.
- Web hosting. Your ISP and your Web host don't have to be one and the same, but you may be able to save money and simplify your bookkeeping by getting both services from one place.

If you find yourself getting overwhelmed by the myriad ISP options available, consider retaining a technology consultant. A little time and money spent now may save you lots of money in the future. Whether you do it yourself and hire a consultant, the time to do your research and due diligence is now — not once you're locked in to an unfavorable long-term contract.

What Is An ISP (Internet Service Provider)? What Does It Do?

An ISP is a company that provides access to the internet through modems, ISDN, T1s, etc. It is an organization that provides and sells physical internet access for global users. An ISP arranges access to the Internet for organizations and/or individuals. Access services provided by ISPs may include web hosting, e-mail, VoIP (voice over IP), and support for many other applications. You may have tried one of the traditionally big online services such as AOL, MSN, Prodigy, Compuserve, or WebTV to get access to the Internet. They apparently make every effort to assure that your first Internet experiences give you successful access to the WWW. A time may come when you will want to have your own website, with your own domain, and have it hosted with an Internet Service Provider (ISP). The big online services can connect you to the internet, so do ISPs. The big difference between the two is the kind of content! The online services provide proprietary (company owned) content; that is, large quantities of materials that include ads and promotional presentations. Most ISPs include very little (if any) original or promotional content; and they may do so only when it is “free” or at a very low price. You are expected to provide your own subject matter; regardless of quality. You will probably discover that an ISP can provide you with services that are just as good, or better, at the same price or less than the big online services. Not all ISPs are created with the same characteristics. Some are very good, some are very bad, and some are both good and bad.

Some Things That An Internet Service Provider Can Do:

- Internet Service Providers (ISPs) equip users with access to the internet through a connection to the ISPs computer network.
- ISPs will set up a user with an account user name and password and the account holder can connect to the ISPs computer through an internet connection (usually dial up modems).
- Once the connection has been achieved, the account holder is able to surf the internet and to upload pages of content to a website.
- ISPs virtually always set the user up with one or more e-mail addresses; depending on which service program is chosen.
- ISPs will also supply the account holder with web space for his/her website.

  In summary, the services that an ISP offers vary considerably and Internet users should be mindful of the following:

- Charges for the service, set up, and on-going costs.
- Customer Service or level of support, should things go wrong.
- The kinds of services that are provided, such as webspace, e-mail addresses, FTP uploading, and much more.
- The connection speeds that are provided.
- The kinds of payment plans that are available.
- Access that is reliable. Some ISPs suffer with constantly busy systems. This is a bad sign!

  Here Are Some Questions That You Should Ask of Any Potential ISP Before You Sign Up:

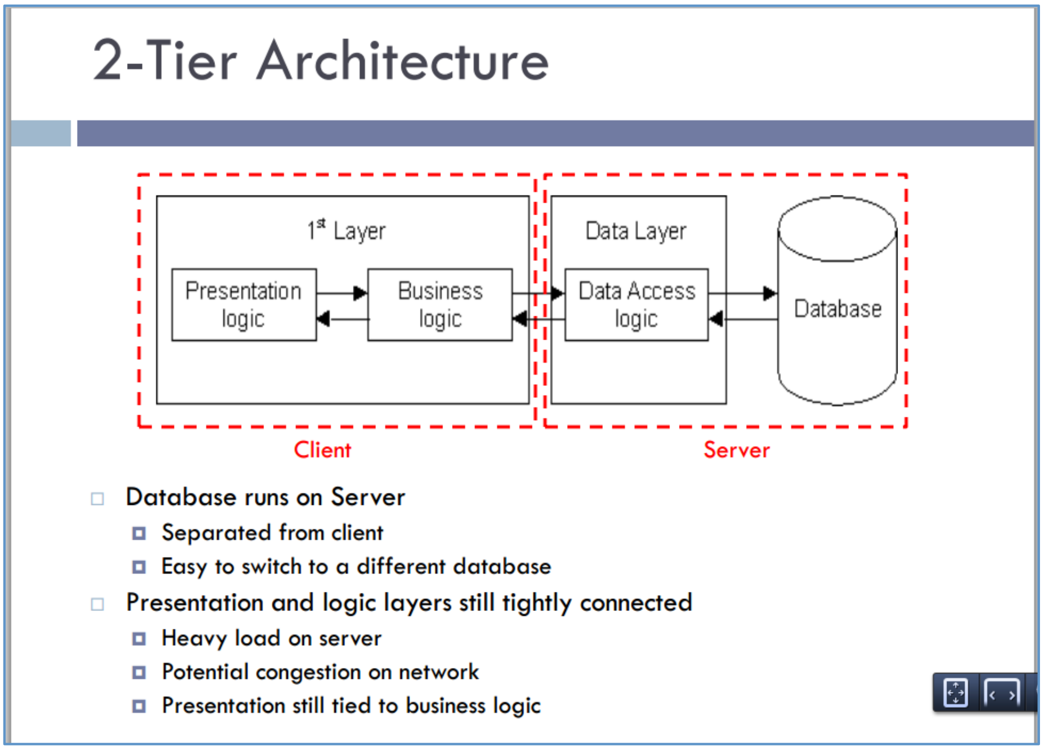
- How much does it cost? This may not be the most important factor but it’s a good place to start. Shop around for the price that is best for you.
- Does it offer discounts if you prepay the entire year up front? This is a good option, providing that it fits into your budget, and if you choose a good ISP. It’s a bad option if the ISP turns out to be less than desirable.
- Does it offer a free trial? Try-before-you-buy is always a good thing.

- What software does the ISP supply? What software will you need? Is there an extra charge if the ISP supplies the software? Most of the software that you need can be obtained on the internet or is included as part of your contract.
- How good is the customer support? Some will provide customer support "24 hours a day, 7 days a week;" with a special toll-free number. Most aren't quite that good.

  Source - **http://www.allbusiness.com/technology/technology-services/11027-1.html**

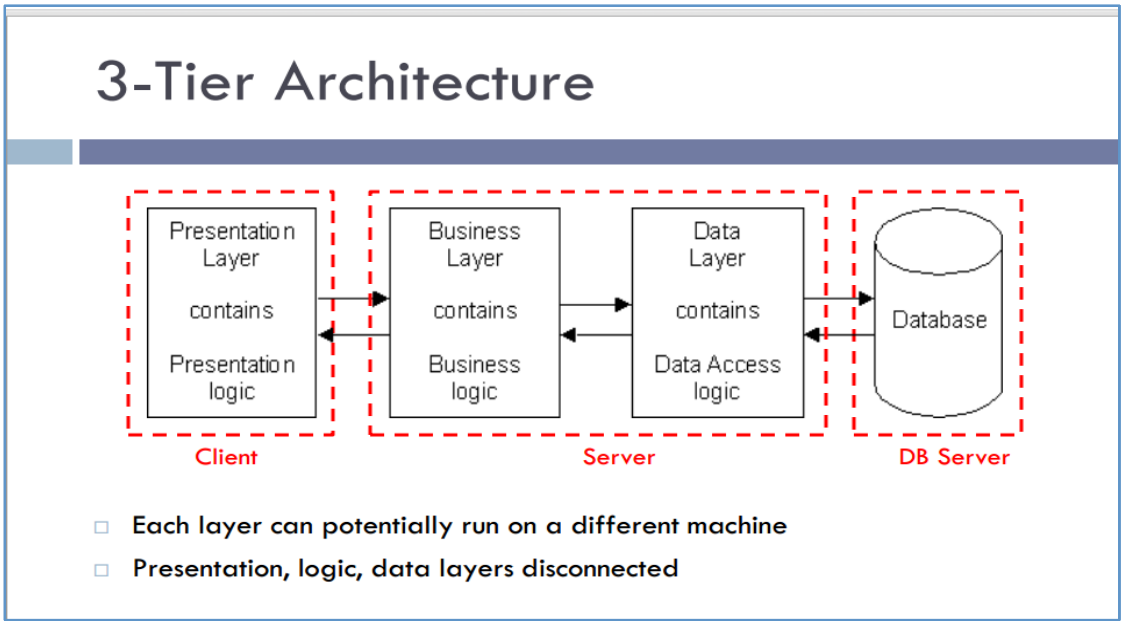
http://www.allbusiness.com/technology/technology-services/11027-1.html

Q7) 3 tier web applications and its adavantage over 2 tier web applications?



2-Tier Architecture

- Database runs on Server
  - Separated from client
  - Easy to switch to a different database
- Presentation and logic layers still tightly connected
  - Heavy load on server
  - Potential congestion on network
  - Presentation still tied to business logic



3-Tier Architecture

Presentation Layer

contains

Presentation logic

Business Layer

contains

Business logic

Data Layer

contains

Data Access logic

Database

Client

Server

DB Server

- Each layer can potentially run on a different machine
- Presentation, logic, data layers disconnected

Technical architecture is concerned about how large software applications can be or should be organized for better performance and ease of development. The commonly used option is a 3 or n tier architecture.

Presentation Tier (or Client-tier) (see **Web Design**)

It implements the "look and feel" of an application. It is responsible for the presentation of data, receiving user events and controlling the user interface. Most ecommerce applications are web-based. The programming languages used are the combination of HTML, CSS and Javascript. JSP or ASP are used for dynamic content.

- HTML is a Web authoring markup language for defining content structures and rendering a web page.
- Javascript is commonly used for client-side validation. Javascript does have some control over the look-and-feel of a page in dynamic HTML.

Application Tier (see **Application Development**)

This layer implements the business logic of the applications. It is usually powered by a Java Application Server (WebLogic or WebSphere). There're several sub-layers within the application layer.

- Control Layer is the interface layer between presentation tier and application tier. The implementation of this layer is dependent on the languages used for implementing the presentation tier.
- Transaction Layer usually implements business processes that may involve many business objects. In J2EE architecture, session beans are commonly used for implementing the

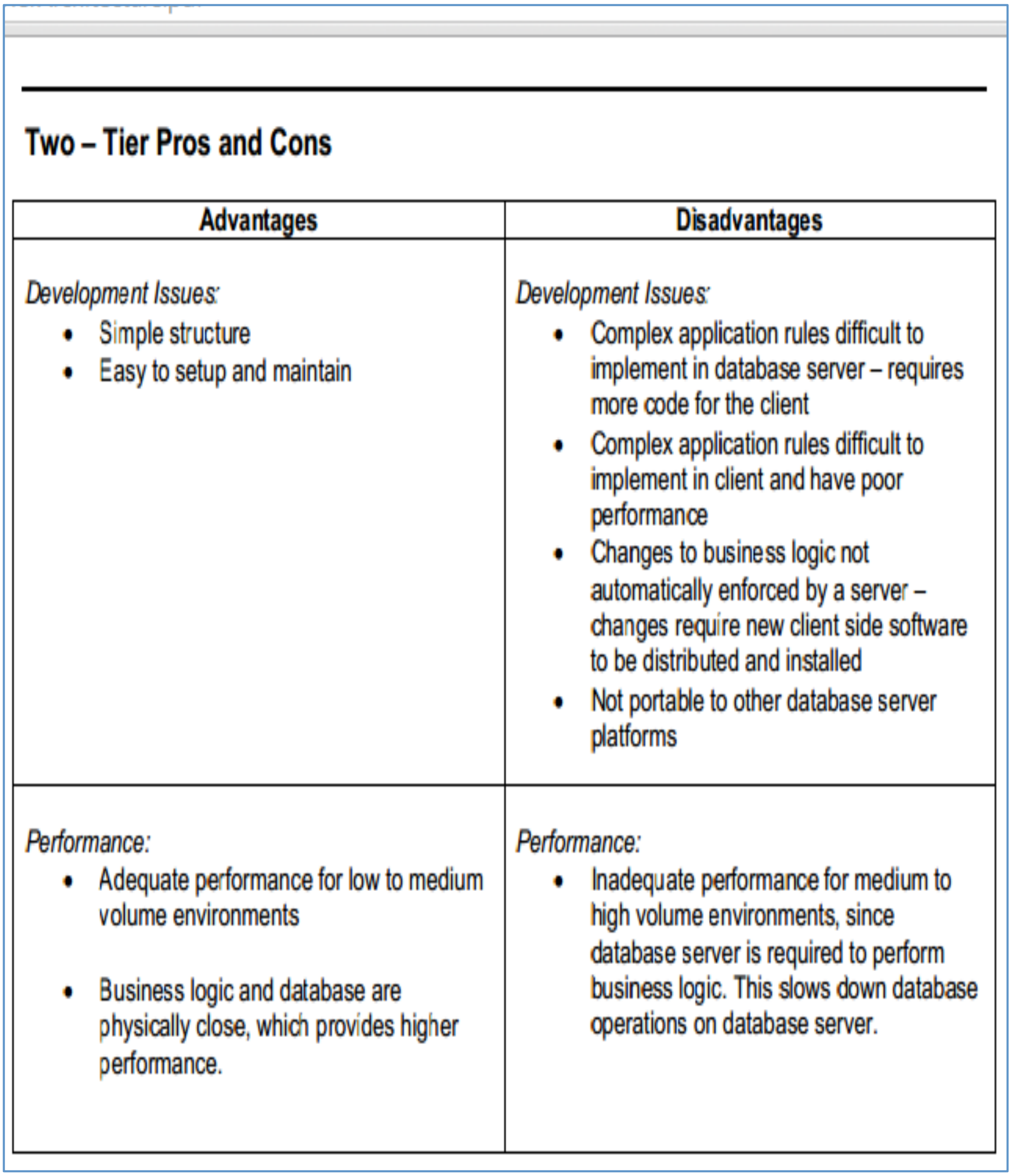
transaction layer. Transaction Layer and Business Object Layer are not constrained by the programming languages for the presentation and the database used for persistence.

- Business Object Layer consists of objects that represent business entities which always should be 100% independent of database used for data persistence.
- Data Access Object (DAO) Layer is the interface between the application tier and persistence tier. Besides the methods for "creating", "retrieving", "updating" and "removing" a business object from database, DAO objects implement other business-specific methods as well. Even with JDBC, DAO objects may not be 100% database independent.

Data Tier

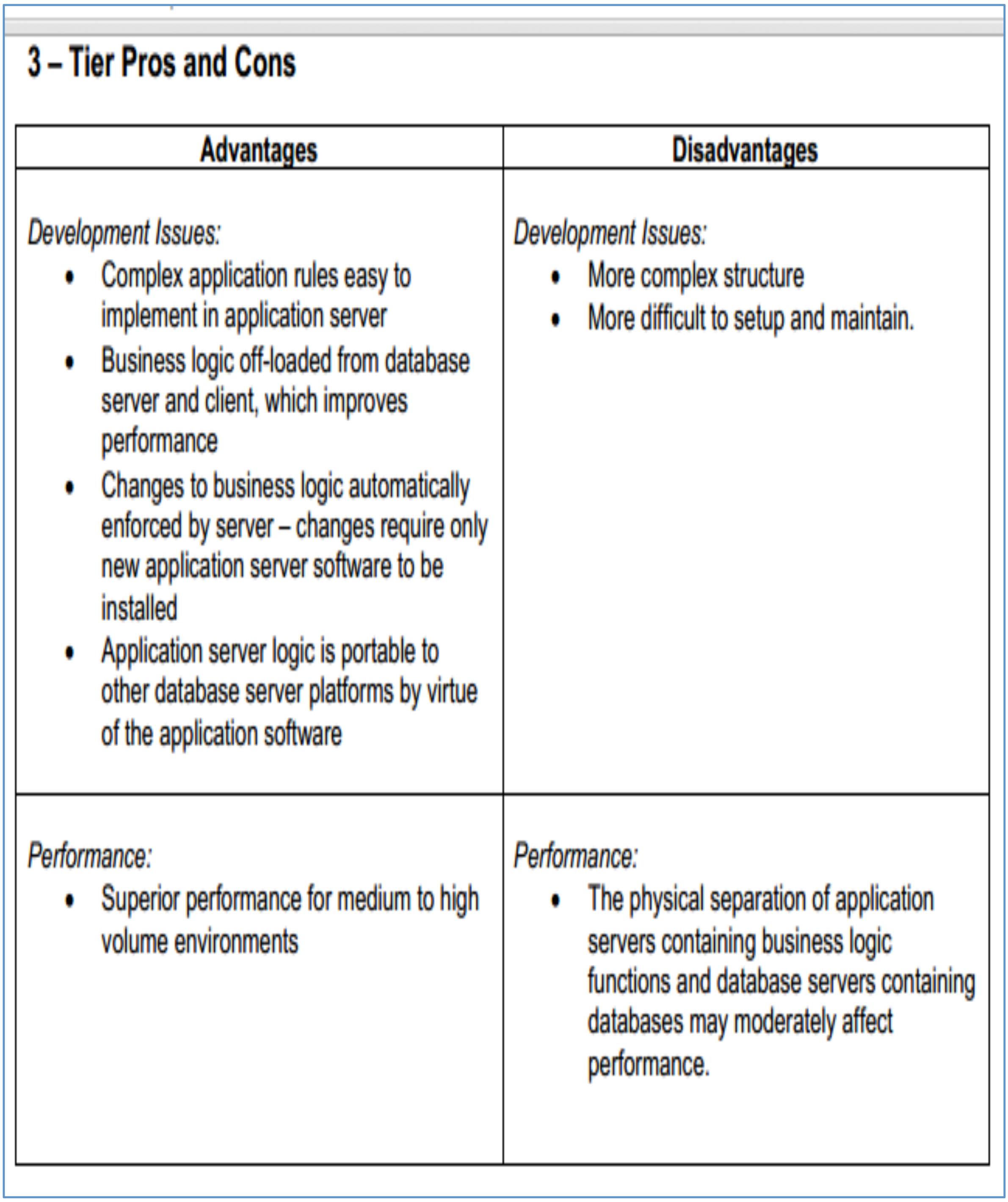
This is the layer that manages the persistence of application information. It is usually powered by a relational database server (Oracle or MS SQLServer).

- Stored Procedures and Functions are used to execute database server-side processes pertinent to data integrity. Business logic processes should be part of application layer in general, not part of data layer.
- Views are better choice than tables for presenting data to applications. They offer some level of security and can be used as alias to hide physical structures of database tables.
- Database Tables are used primarily for storing data.



Two – Tier Pros and Cons

Advantages	Disadvantages
Development Issues: - Simple structure - Easy to setup and maintain	*Development Issues:* - Complex application rules difficult to implement in database server – requires more code for the client - Complex application rules difficult to implement in client and have poor performance - Changes to business logic not automatically enforced by a server – changes require new client side software to be distributed and installed - Not portable to other database server platforms
Performance: - Adequate performance for low to medium volume environments - Business logic and database are physically close, which provides higher performance.	*Performance:* - Inadequate performance for medium to high volume environments, since database server is required to perform business logic. This slows down database operations on database server.



3 – Tier Pros and Cons

Advantages	Disadvantages
Development Issues: • Complex application rules easy to implement in application server • Business logic off-loaded from database server and client, which improves performance • Changes to business logic automatically enforced by server – changes require only new application server software to be installed • Application server logic is portable to other database server platforms by virtue of the application software	*Development Issues:* • More complex structure • More difficult to setup and maintain.
Performance: • Superior performance for medium to high volume environments	*Performance:* • The physical separation of application servers containing business logic functions and database servers containing databases may moderately affect performance.

Source : **http://queens.db.toronto.edu/~papaggel/courses/csc309/docs/lectures/web-architectures.pdf**

http://ecommerce.insightin.com/architecture/technical_architecture.html

Q 8) POP , SMTP? Difference between IMAP and POP?

Different technologies used for mailing.

SMTP - The Simple Mail Transfer Protocol (SMTP) technology pertains specifically to outgoing mail servers because this protocol only allows for sending electronic mail; it does not provide a user the capability of accessing incoming mail, as described at the Email Address Manager website. Another limitation with SMTP is that, depending on your Internet settings and the setup of your network, you may have the restriction of using SMTP only under specific conditions.

POP3 - The Post Office Protocol 3 (POP3) affords those whose e-mail facility uses this function the option of either downloading all e-mail messages to a local computer from the server or leaving copies of the e-mails on the server. This protocol offers both an advantage and a disadvantage. The advantage applies to e-mail facilities that charge in time units, because downloading e-mails allows you to read them without remaining connected to the e-mail server. The disadvantage is that you may also transfer unwanted e-mail content such as viruses and spam.

IMAP - Internet Message Access Protocol (IMAP) retains all e-mail on the outgoing server until the e-mail account holder requests to read a specific e-mail message. This protocol also allows the e-mail account holder to create and organize folders on the outgoing mail server. Because the IMAP protocol makes use of only small data transfers, this e-mail protocol is effective over slow connections such as dial-up Internet service.

HTTP - The Hypertext Transfer Protocol (HTTP) originally allowed those working with Hypertext Markup Language (HTML) pages a means to publish and receive such pages, and evolved to the primary means of information transfer on the worldwide web, as described at the WordIQ website. As such, some outgoing mail servers use this communications protocol as a means for account holders to access their mailbox account. In reference to e-mail, you will also find HTTP called web based e-mail; the free Hotmail e-mail service provides an example of the use of HTTP in an e-mail application as indicated at the Emailaddressmanager website.

1. IMAP and POP are the protocols or technologies using which you can download messages from mail servers on your computer and access them with the help of mail clients such as Microsoft Outlook, Mozilla Thunderbird etc. The main advantage of this technology is that you can access your emails via a feature-rich browser-independent mail client. In case of POP, you get offline access to old mails too.

2. Difference between IMAP and POP

3. IMAP and POP are two different protocols. There are many differences between these two. The main difference is that IMAP(Internet Messaged Access Protocol) always syncs with mail server so that any changes you make in your mail client (Microsoft Outlook, Thunderbird) will instantly appear on your webmail inbox.

4. On the other hand, in POP(Post Office Protocol), your mail client account and mail server are not synced. It means whatever changes you make to your email account in the mail client will not be transferred to the webmail inbox.

5. In simple terms, if you are using IMAP and mark a mail as read, it gets marked as read in your web based inbox too (because the changes are happening on the server). However, this won’t be the case if you are using POP, because the mails are downloaded to your PC and the changes won’t reflect on the server.

The using of IMAP to access your mailbox has advantages over POP3 and the difference of their working mechanism can be summarized in the following table.

POP3	IMAP
Since email needs to be downloaded into desktop PC before being displayed, you may have the following problems for POP3 access: • You need to download all email again when using another desktop PC to check your email. • May get confused if you need to check email both in the office and at home. The downloaded email may be deleted from the server depending on the setting of your email client.	Since email is kept on server, it would gain the following benefits for IMAP access: • No need to download all email when using other desktop PC to check your email. • Easier to identify the unread email.
All messages as well as their attachments will be downloaded into desktop PC during the 'check new email' process.	A whole message will be downloaded only when it is opened for display from its content.
Mailboxes can only be created on desktop PC. There is only one mailbox (INBOX) exists on the server.	Multiple mailboxes can be created on the desktop PC as well as on the server.
Filters can transfer incoming/outgoing messages only to local mailboxes.	Filters can transfer incoming/outgoing messages to other mailboxes no matter where the mailboxes locate (on the server or the PC).
Outgoing email is stored only locally on the desktop PC.	Outgoing email can be filtered to a mailbox on server for accessibility from other machine.
Messages are deleted on the desktop PC. Comparatively, it is inconvenient to clean up your mailbox on the server.	Messages can be deleted directly on the server to make it more convenient to clean up your mailbox on the server.
Messages may be reloaded onto desktop PC several times due to the corruption of system files.	The occurrence of reloading messages from the server to PC is much less when compared to POP3.

Source **http://www.guidingtech.com/2207/difference-between-pop-and-imap/**

http://email.cityu.edu.hk/faq/popimap.htm

Q 9) WAP in business?

Wireless Application Protocol commonly known as WAP is used to enable the access of internet in the mobile phones or PDAs. WAP is an international standard for the devices that use the wireless communications. Nowadays internet has prevailed in our lives so much that it has become difficult to live without it even for a while. But we can not have access to our personal computers all the time to connect to the internet, like when we are on the go or we are out of town for while and we want to check our mail or want to make a flight-reservation online or chat to an associate or a friend. In the situations like these, WAP comes in handy. All we have to do is to carry a WAP enabled mobile phone or PDA. Approximately all the mobile phone carriers have the WAP service these days, therefore all you need to get WAP on your device is to get the configuration settings from your wireless carrier and you are in business. But the use of WAP can be a bit tricky for the beginners as the pages open in your mobile phone are not quiet same to the ones on your pc or laptop because these pages are optimized for mobile phones and PDAs and the images and text is quiet small.

WAP-Applications

There is a need of certain applications to make the full use of WAP in your device. The first thing you need is a WAP browser to access different wap-sites. Most WAP-enabled mobile phones and PDAs have a built-in WAP browser but you can also use a third party wap-browser. A famous browser in Opera-mini which is available free of cost for most of the models available and offers many features that the built-in browsers do not.

Another application that people want to use in their wap-enabled phones is an instant messenger. An instant messenger enables you to do a live chat. The famous instant messaging services are MSN, YAHOO, AOL and GOOGLE. The used of these services in your mobile phone enables you to chat live with your friends and family all around the world. There are number of wap messengers that enable you to avail this service and some of them are even free. The instant messaging is one of the biggest advantages one can avail using a cellular phone.

There are certain applications that connect you to the global positioning system commonly known as GPS so that you can not get lost and you can easily find your destinations all around world.

WAP-Sites

With the use of your WAP browser in your mobile phone you can only access the wap-sites, which means you do not have access to the whole World Wide Web. This is a drawback of the wap as one cant access all the web from his device. But with this technology, all the major online companies have opened their wap sites along with their websites and the count is increasing every single day because the use of wap all around the world has become very popular.

Wireless Application Protocol:

As the bottom line, it is to be said that the use of WAP has made the access to web very easy. The access to the internet has become very easy when you are on the move and the use of mobile phones have become much more worthy.

Source - **http://www.streetdirectory.com/travel_guide/117330/cell_phones/use_of_wap_wireless_application_protocol_in_cell_phones.html**

Q10) Digital certificates and its uses?

The contents of a digital certificate are prescribed by the X.509 standard, developed by the International Standards Organization (ISO) and adopted by the American National Standards Institute (ANSI) and the Internet Engineering Task Force (IETF). The latest version is now X509 v3. The principal elements of a digital certificate are as follows:

- Version number of the certificate format
- Serial number of the certificate
- Signature algorithm identifier
- Issuer of digital certificate: a certificate authority with URL
- Validity period
- Unique identification of certificate holder
- Public key information

Applications using public-key cryptography systems for key exchange or digital signatures need to use digital certificates to obtain the needed public keys. Internet applications of this kind are numerous. Following are brief descriptions of a few of the commonly used Internet applications that use public-key cryptography:

SSL

A protocol that provides privacy and integrity for communications. This protocol is used by :

- Web servers to provide security for connections between Web servers and Web browsers,
- LDAP to provide security for connections between LDAP clients and LDAP servers,
- Host-on-Demand V2 to provide security for connections between the client and the host system.

Additional applications based on this protocol are in development.

SSL uses digital certificates for key exchange, server authentication, and optionally, client authentication.

Client Authentication

Client authentication is an option in SSL that requires a server to authenticate a client's digital certificate before allowing the client to log on or access certain resources. The server requests and authenticates the client's digital certificate during the SSL handshake. At that time the server can also determine whether it trusts the CA that issued the digital certificate to the client.

Secure Electronic Mail

Many electronic mail systems, using standards such as Privacy Enhanced Mail (PEM) or Secure/Multipurpose Internet Mail Extensions (S/MIME) for secure electronic mail, use digital certificates for digital signatures and for the exchange of keys to encrypt and decrypt messages.

Virtual Private Networks (VPNs)

Virtual private networks, also called secure tunnels, can be set up between firewalls to enable protected connections between secure networks over insecure communication links. All traffic destined to these networks is encrypted between the firewalls.

The protocols used in tunneling follow the IP Security (IPsec) standard. For the key exchange between partner firewalls, the Internet key exchange (IKE) standard, previously known as ISAKMP/Oakley, has been defined.

The standards also allow for a secure, encrypted connection between a remote client (for example, an employee working from home) and a secure host or network.

Secure Electronic Transaction (SET)

SET is a standard designed for secure credit card payments using insecure networks, for example, the Internet. Digital certificates are used for card holders (electronic credit cards) and merchants. The use of digital certificates in SET allows for secure, private connections between card holders, merchants, and banks. The transactions created are secure and indisputable, and they cannot be forged. The merchants receive no credit card information that can be misused or stolen.

Source – **http://www.cren.net/crenca/docs/cren-dlf.pdf**

http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.itame2.doc_5.1%2Fss7aumst15.htm

Q1 – Compare competing server side technologies (any 2)

A quick introduction to server-side technology

Choosing which server-side technology to use is an important decision. All of the technologies have similar capabilities and features, but while switching a project from one technology to another is possible, it is also time consuming and often fraught with difficulty. It's impossible to say if one is any *better* than another, but there are certain aspects of each technology, such as ease of learning, availability, cost, and software support, that can help you make up your mind.

merits of the most widely used server-side technologies, namely (in alphabetical order):

- Active Server Pages (ASP)
- ASP.NET
- ColdFusion
- JavaServer Pages (JSP)
- PHP
- Python
- Ruby on Rails

What makes a website dynamic?

The word *dynamic* is often used to describe websites that use a server-side technology. This is because the content of each page often changes in response to user input, such as through a search form. The term, *dynamic* is also applied to web pages that use effects like rollovers, drag-and-drop, and fades, or widgets like accordion panels that slide open and closed to reveal or hide content. These dynamic effects and widgets are controlled by JavaScript in the browser, and are not related in any way to server-side technology. Because they take place in the browser on the user's computer (the *client*), they are known as *client-side technology*.

On the other hand, as its name suggests, server-side technology operates entirely on the web server and sends the results to the browser.

What happens on the server?

Server-side technology can be used in the following main ways:

- To build web pages with HTML

- To serve data to a rich Internet application (RIA), such as a SWF file built in Flash Builder 4 or Flash Professional
- To process user input and send it by email or update the contents of a database

The important thing to understand about using server-side technology is that everything takes place on the server, and the results are sent to the browser or the RIA. If further processing or database queries are required, it always involves a round-trip to the server. It might sound like a statement of the obvious, but it's easy to forget when you see a well-designed dynamic website, which will almost certainly use a combination of client-side and server-side technologies.

Active Server Pages (ASP)

ASP (often referred to as Classic ASP) is Microsoft's original server-side technology, released in 1997. After ASP 3.0 was launched in 2000, Microsoft decided to abandon all further development, and focus instead on ASP.NET. Nevertheless, Classic ASP remained very popular and is still in widespread use.

Contrary to common belief, ASP is not a language. Active Server Pages can be created using either VBScript or JavaScript. Older versions of Dreamweaver include server behaviors in both languages. However, the ASP JavaScript server behaviors have been removed from Dreamweaver CS5, which now supports only ASP VBScript.

Classic ASP is likely to remain in use for many more years; but it is a stagnant technology, and does not make a wise choice for anyone currently contemplating learning a server-side technology. Versions of ASP designed to run on non-Windows servers are no longer officially supported.

ASP.NET

The replacement for Classic ASP bears little resemblance to it apart from the name. The difference is so marked that previous experience of Classic ASP does little to smooth the transition from one technology to the other. ASP.NET uses the Microsoft .NET framework, and can be written in many different computer languages, the most popular being C# and VB.NET.

A major feature of ASP.NET is the use of controls, such as data grids and navigation controls. This makes it a very powerful server-side technology, which is particularly suited to large-scale projects. However, the power comes at the expense of a steep learning curve. ASP.NET is worth serious consideration if you plan a career as a programmer in web application development. On the other hand, if you simply want to add database functionality to small- to medium-size websites, ASP.NET might be overkill..

Adobe ColdFusion

ColdFusion is Adobe's application server that runs on Windows, Mac OS X, and Linux. In the background, it uses Java, a powerful programming language that, in spite of its name, is unrelated to JavaScript. From a web developer's viewpoint, ColdFusion is very easy to use because the application server takes care of most of the complex programming. Commands are written using a tag-based language, ColdFusion Markup Language (CFML), that looks very similar to HTML. To give a simple example, if you have a form on your site where visitors can enter their name, the following code displays the name when the form is submitted:

```
<cfoutput>Hello, #FORM.name#!</cfoutput>
```

A major strength of ColdFusion is its integration with Java. While most users do everything with CFML, and need no knowledge of Java, advanced programmers can access pre-existing Java objects from within a ColdFusion application. If you plan to do a lot of server-side development with ColdFusion, you should consider using the Eclipse-basedColdFusion Builder. ColdFusion is particularly suitable for use with RIAs as it automatically converts data to and from the binary Action Message Format (AMF), which greatly improves the speed of data transfer.

A common misunderstanding surrounding ColdFusion is cost. Because it's a commercial product, a license is required to run a ColdFusion server on the Internet. However, this cost is normally included in the price of a hosting service. The developer version of ColdFusion is free, and is not time-limited.

JavaServer Pages (JSP)

JSP is designed to work with very large, high-volume sites. It uses libraries of Java code known as *servlets*, which reduce the amount of code that needs to be written. JSP is worth considering if you plan a serious career as a programmer.

PHP

PHP is the most popular open-source server-side language. It started out in 1995 as Personal Home Page Tools (PHP Tools), a simple set of utilities that gave users access to their server logs and processed online forms. Since then, it has developed into a sophisticated technology that drives some of the most visited websites, including Facebook, Wikipedia, and Yahoo!. The original name eventually sounded out of place, so PHP now officially stands for PHP: Hypertext Preprocessor.

Like ColdFusion, it is relatively easy to learn, and it also has advanced features that appeal to serious programmers. Unlike ColdFusion, it is not tag-based. Instead, PHP uses traditional programming syntax. However, the basics are easy to grasp. The previous example of displaying a name from a form is written like this in PHP:

```
Hello, <?php echo $_POST['name']; ?>
```

The PHP community is very active, making it easy to find help. The community has also produced powerful content management systems (CMS), such as WordPress, Drupal, and Joomla, that allow even non-programmers to create sophisticated database-driven websites without touching a line of PHP code.

Dreamweaver CS5 has enhanced support for PHP. In addition to the existing server behaviors that work with the open source MySQL database, Dreamweaver CS5 provides real-time checking for syntax errors and code completion for user variables. Code hinting has also been extended to display the PHP documentation, complete with examples, for all built-in functions, methods, and constants (up to PHP 5.2). Other improvements include code introspection to provide code hints for custom functions and classes, as well as external libraries, such as the Zend Framework. Live view also makes it possible to see the output of WordPress, Drupal, and Joomla directly in the Document window.

PHP also makes a suitable back end for an RIA. Flash Builder 4 automatically generates the basic code to transfer data through PHP and Zend_Amf, an independent module of the Zend Framework that handles conversion to and from AMF.

Python

Python is an open-source programming language that claims to combine "remarkable power with very clear syntax." It's a standard component of most Linux distributions and Mac OS X, and can also be installed on Windows. Its users include YouTube, Google, Yahoo!, and NASA. Two popular web development frameworks for Python are Django and Zope. However, neither Dreamweaver CS5 nor Flash Builder 4 has any built-in support for Python.

Ruby on Rails

Ruby on Rails (or Rails, as it's often called) is an open-source web application framework designed to make common development tasks easier through the use of tools, such as scaffolding, which automatically constructs some of the basic elements of a website. A notable feature of Rails is that the ActiveRecord library enables you to write code that works with any supported database, rather than having to write database-specific code, as is common with other server-side technologies. Twitter is perhaps the best known among prominent users of Rails.

Rails can be installed on Windows, Mac OS X (Ruby is preinstalled), and Linux. There is no built-in support for Rails in Dreamweaver CS5 or Flash Builder 4. However, the free RubyWeaver extension for Dreamweaver

Q2) CRM and SCM? Can they work effectively without internet?

CRM is the abbreviation for ***customer relationship management***. CRM entails all aspects of interaction that a company has with its customer, whether it is sales or service-related. CRM is often thought of as a business strategy that enables businesses to:

- Understand the customer
- Retain customers through better customer experience
- Attract new customer
- Win new clients and contractsIncrease profitably
- Decrease customer management costs

How CRM is Used Today

While the phrase *customer relationship management* is most commonly used to describe a business-customer relationship, however CRM systems are used in the same way to manage business contacts, clients, contract wins and sales leads.

CRM solutions provide you with the customer business data to help you provide services or products that your customers want, provide better customer service, cross-sell and up sell more effectively, close deals, retain current customers and understand who the customer is.

Recommended Reading: *Customer Relationship Management (CRM) Reports Explained*.

Technology and the Web has changed the way companies approach CRM strategies because advances in technology have also changed consumer buying behavior and offers new ways for companies to communicate with customers and collect data about them. With each new advance in technology -- especially the proliferation of self-service channels like the Web and smartphones -- customer relationships is being managed electronically.

Many aspects of CRM relies heavily on technology; however the strategies and processes of a good CRM system will collect, manage and link information about the customer with the goal of letting you market and sell services effectively.

Organizations frequently looking for ways to personalize online experiences (a process also referred to as mass customization) through tools such as help-desk software, e-mail organizers and different types of enterprise applications.

Recommended Reading: *Learn more about CRM, business intelligence and business analytics on EnterpriseAppsToday.*

SCM

What is SCM?

You're probably familiar with some aspect of supply chain management (SCM), but perhaps not as well-versed in the detailed processes within SCM. So, what is SCM? Supply chain management integrates supply and demand management within and across companies. It includes important variables such as the planning and management of all activities involved in sourcing and procurement, conversion and all logistics management activities. It can also include coordination and collaboration with channel partners, which can be suppliers, intermediaries, third party service providers and customers.

Five Stages of SCM

Within the overarching umbrella of SCM, there are several stages which identify the exact process from start to finish. These stages include:

Plan - The entire process of supply chain management must be planned out with the primary goal of the organization in mind. The plan should also address how the organization's goods or service will fulfill the needs of their customers.

Develop - A major component of this process is to develop strong relationships with suppliers. The potential suppliers are then contracted and conditions of delivery, payment and transportation are then finalized with them.

Make - The product is finally manufactured, thoroughly tested and packaged and then launched into the market.

Deliver - This involves the transportation of the product through various channels into the hands of the ultimate customer.

Return - Customer queries and complaints are handled subsequently. If there are any defective items present, they are returned to sender.

Benefits of SCM

It's clear that there are many benefits of supply chain management, but what exactly are those benefits? Effective SCM achieves more accurate information, along with the ability to carry out better sales forecasting. Other benefits include building stronger partnerships and supplier networks, balancing out supply and demand, improving business plans and working strategies, predicting transportation requirements, planning daily operations of the company, creating streamlined inventory management and removing irrelevant elements.

While all organizations have supply chain processes of varying degrees, it is important to understand, identify and implement each stage with careful consideration. Variables including the size of the organization and the type of product manufactured affect SCM components, so understanding the most critical business discipline in the world today will greatly benefit you, your business and your bottom line.

For SCM and CRM without internet –Give your opinions.

Source- http://www.webopedia.com/TERM/C/CRM.html

http://www.usanfranonline.com/what-is-scm/

Q3) Networking security has become important part of computariztion . Explain various security aspects

Source : http://www.cs.st-andrews.ac.uk/~jfdm/notes/netsec/#_wireless_lan_an_introduction

Security comes in all shapes and sizes, ranging from problems with software on a computer, to the integrity of messages and emails being sent on the Internet. Network Security is a term to denote the security aspects attributed to the use of computer networks. This involves the protection of the integrity of the communications that are sent over the network, who is able to access the network or information system present, and also what can be sent over the network. There are a multitude of scenarios and areas that a network and its use can be exploited. The problem is that given the OSI Network Model of: **Application**, **Transport**,**Network**, **Datalink** and **Physical**, where amongst this can security be deployed? Should everything be concentrated at the data link or network or transport… layers? or should a **Defense in Depth** strategy be employed? These notes details the various ways in which networks can be made secure. The remainder of this chapter provides some introductory material in relation to networks and their security. First, some terminology:

- **Security Attack**: Any action that compromises the security of information exchanges and systems.
- **Security Service**: A service that enhances the security of information exchanges and systems. A sercurity service makes use of one or more security mechanisms.
- **Security Mechanism***: A mechanism that is designed to detect, prevent or recover from a security attack.

Security Attacks

There exist several attack types and they can be divided into two distinct category's: **Passive** and **Active**, they denote the amount of work that an attacker must do.

Passive Attacks

A **Passive Attack** is one that involves either the eavesdropping or monitoring of data communications. The goal of the malicious entity is to acquire the information or learn more about the communication.

- **Release of Message Contents**: This is when during the transmission of data from one party to another, a third and malicious party intercepts the message and learns its contents.
- **Traffic Analysis**: Traffic analysis is concerned with the analysis of patterns generated by the actions of the parties involved. This may simply involve the detection of an encrypted message being sent from a single party.

Such attacks are difficult to detect, due to their inherent nature. Though one can use encryption in order to inhibit the success-fullness of such attacks.

Active Attacks

Active Attacks are those that involve the modification of the communication channel or the data being sent across the channel.

- **Masquerade**: This is simply the impersonation of a legitimate entity in order to abuse or access the resources accessible by the entity.
- **Replay**: Involves the retransmission of existing and already transmitted data in order to produce an unauthorised effect.
- **Message Modification**: The delay, modification, reorder on a legitimate message such that it produces an unauthorised effect.
- **Denial of Service**: This involves the prevention of or reduction in quality, of a legitimate service. Such attacks may target specific hosts or entire networks.

In contrast to passive attacks, active ones are easy to detect but harder to counter, as it would involve the protection of **all** the communication services offered.

Security Services

A **Security Service**, as defined by X.800, is a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or data transfers. There are five categories mentioned, together with availability:

Availability

The property of a system or a system resource being accessible and usable upon demand by an authorised system entity, according to performance specifications for the system.

Access Control

The prevention of unauthorised use of a resource.

Authentication

This is the assurance that the communicating entity is the one that it claims to be. There are two classes of authentication:

- **Peer Entity** — involves the authentication of a logical entity in a communication process; and
- **Data Origin** — involves assurances relating to the origin of the source of received data.

Data Confidentiality

The protection of data from unauthorised disclosure. This can be further specified as:

- **Connection Confidentiality** — The protection of all user data on a connection.
- **Connectionless Confidentiality** — The protection of all user data in as single data block.
- **Selective-Field Confidentiality** — The confidentiality of selected fields within the user data on a connection or in a single data block.
- **Traffic-Flow Confidentiality** — The protection of the information that might be derived from observation of traffic flows.

Data Integrity

The assurance that data received is in the exact same format as it was when sent by an authorised entity. This can be considered in terms of **Connection Integrity**:

- **Connection Integrity with Recovery** — Provided for the integrity of all user data on a connection and detects any modification, insertion, deletion or replay of any data within an entire data sequence, with recovery attempted.
- **Connection Integrity without Recovery** — As previously but provides only detection without recovery.
- **Selective-Field Connection Integrity** — Provides for the integrity of selected field within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted or replayed.
- **Connectionless Integrity** — Provides for the integrity of a single connectionless data block and may take the form of a detection of data modification. Additionally a limited form of replay detection may be provided.

- **Selective-Field Connectionless Integrity** — Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

Non-repudiation

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. This can imply:

- **Origin Non-repudiation** — Proof that the message was sent by the specified party.
- **Destination Non-repudiation** — Proof that the message was received by the specified party.

Security Mechanisms

Security Mechanisms refer to tools and techniques that can be implemented within a specific protocol layer or outwith the layer that provided some form of security. Some examples are listed below.

Specific Mechanisms

Encryption, Digital Signatures, Access Control, Data Integrity, Authentication Exchange, Traffic Padding, Routing Control, Notarisation

Pervasive Mechanisms

Trusted Functionality, Security Label, Event Detection, Security Audit Trail, Security Recovery

Security Models

There are two main security models that are used when dealing with network security: **Secure Communication** and **Secure Systems**.

1.Secure Communication

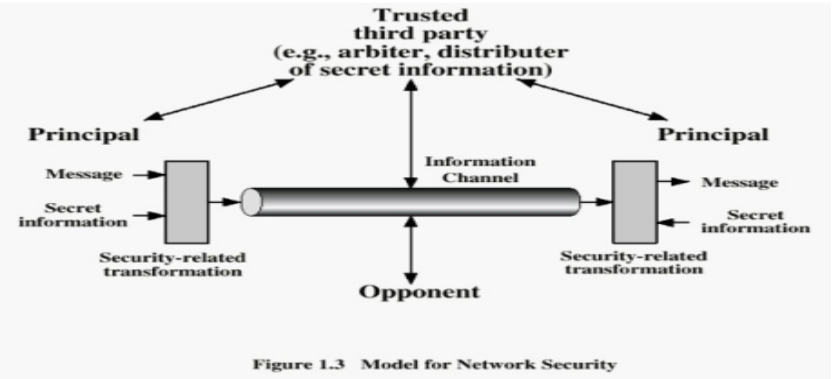

Trusted third party (e.g., arbiter, distributer of secret information)
Principal
Principal
Message
Secret information
Information Channel
Message
Secret information
Security-related transformation
Security-related transformation
Opponent
Figure 1.3 Model for Network Security

Figure 1. Secure Communication

In this model, there are two principal agents i.e. Alice and Bob, who wish to send a message via a information channel to each other that contains some secret information. In order to protect the secret information the parties involved will perform some form of **Security Related Transformation** on the information to be sent, using some form of **shared secret** that is known only by the parties involved. Such activities may involve the use of a **Trusted Third Party** to whom some responsibilities such as distribution of secret information or authorisation/authentication, are entrusted to. This is summarised in the figure above. This model is used for most areas of network security when the transmission of data is concerned. [Stallings2008] mentions that there are four basic task involved in designing a security service using this model:

1. Design an algorithm for performing the security related transformation.
2. Generate the secret information that is to be used.
3. Develop method for distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that utilises the security algorithm and secret information to achieve a particular security service.

2. Secure Systems

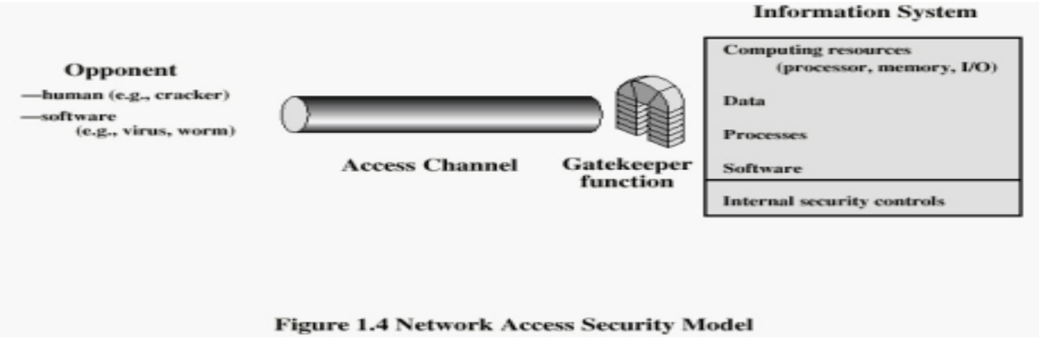


Figure 2. Secure System

The other model reflects the remainder of the security problems that are associated with the protection of an information system i.e. a network, from malicious entities. Such entities can be a hacker that aims to gain access to a system for **fun and profit**, a disgruntled employee who wishes to cause damage or a criminal who wishes to exploit the resources for financial gain. Furthermore this model incorporates the notion of additional software that aims to exploit vulnerabilities in the system and targets applications and utility programs. They can be classed as: **Information access threats** — interception/modification of data; and **Service Threats--** exploitation of service flaws. Moreover in order to protect the information system a **Gatekeeper Function** is used to perform access control and restrict the accessibility of the system. If this fails then some form of internal security controls are needed to identify any, stop the actions of and repair any damage as caused by, intruders.

Q4 : Evolution and development of internet protocols in light of convergence technology – data , video , voice over.

Source : http://vlaurie.com/computers2/Articles/protocol.htm

http://www.ehow.com/about_5488462_types-internet-protocol.html

In order for computers to communicate with one another, standard methods of information transfer and processing have been devised. These are referred to as "protocols" and some of the more common ones such as TCP, IP, UDP, POP, SMTP, HTTP, and FTP are discussed here.

When two humans converse, they may have to use the same language but they generally understand each other without having to adhere to rigid rules of grammar or formal language frameworks. Computers, on the other hand, have to have everything explicitly defined and structured. If computers wish to communicate with one another, they have to know in advance exactly how information is to be exchanged and precisely what the format will be. Therefore, standard methods of transmitting and processing various kinds of information are used and these methods are called "protocols". Protocols are established by international agreement and ensure that computers everywhere can talk to one another. There are a variety of protocols for different kinds of information and functions

TCP/IP

TCP (Transmission Control Protocol) and IP (Internet Protocol) are two different procedures that are often linked together. The linking of several protocols is common since the functions of different protocols can be complementary so that together they carry out some complete task. The combination of several protocols to carry out a particular task is often called a "stack" because it has layers of operations. In fact, the term "TCP/IP" is normally used to refer to a whole suite of protocols, each with different functions. This suite of protocols is what carries out the basic operations of the Web. TCP/IP is also used on many local area networks. The details of how the Web works are beyond the scope of this article but I will briefly describe some of the basics of this very important group of protocols.

When information is sent over the Internet, it is generally broken up into smaller pieces or "packets". The use of packets facilitates speedy transmission since different parts of a message can be sent by different routes and then reassembled at the destination. It is also a safety measure to minimize the chances of losing information in the transmission process. TCP is the means for creating the packets, putting them back together in the correct order at the end, and checking to make sure that no packets got lost in transmission. If necessary, TCP will request that a packet be resent.

Internet Protocol (IP) is the method used to route information to the proper address. Every computer on the Internet has to have it own unique address known as the IP address. Every packet sent will contain an IP address showing where it is supposed to go. A packet may go through a number of computer routers before arriving at its final destination and IP controls the process of getting everything to the designated computer. Note that IP does not make physical connections between computers but relies on TCP for this function. IP is also used in conjunction with other protocols that create connections.

Another member of the TCP/IP suite is User Datagram Protocol (UDP). (A datagram is almost the same as a packet except that sometimes a packet will contain more than one datagram.) This protocol is used together with IP when small amounts of information are involved. It is simpler than TCP and lacks the flow-control and error-recovery functions of TCP. Thus, it uses fewer system resources.

A different type of protocol is Internet Control Message Protocol (ICMP) . It defines a small number of messages used for diagnostic and management purposes. It is also used by Ping and Traceroute.

Mail protocols

Email requires its own set of protocols and there are a variety, both for sending and for receiving mail. The most common protocol for sending mail is Simple Mail Transfer Protocol (SMTP). When configuring email clients such as Outlook Express, an Internet address for an SMTP server must be entered. The most common protocol for receiving mail is Post Office Protocol (POP). It is now in version 3 so it is called POP3. Email clients such as Outlook Express require an address for a POP3 server before they can read mail. The SMTP and POP3 servers may or may not be the same address. Both SMTP and POP3 use TCP for managing the transmission and delivery of mail across the Internet.

A more powerful but less common protocol for reading mail is Interactive Mail Access Protocol (IMAP). This protocol allows for the reading of individual mailboxes at a single account and is more common in business environments. IMAP also uses TCP to manage the actual transmission of mail.

It is increasingly popular to use Web based email such as Yahoo. Web mail, of course, involves the same protocol as a Web page and this is discussed next.

Hypertext Transfer Protocol

Web pages are constructed according to a standard method called Hypertext Markup Language (HTML). An HTML page is transmitted over the Web in a standard way and format known as Hypertext Transfer Protocol (HTTP). This protocol uses TCP/IP to manage the Web transmission.

A related protocol is Hypertext Transfer Protocol over Secure Socket Layer (HTTPS), first introduced by Netscape. It provides for the transmission in encrypted form to provide security for sensitive data. A Web page using this protocol will have *https:* at the front of its URL.

File Transfer Protocol

File Transfer Protocol (FTP) lives up to its name and provides a method for copying files over a network from one computer to another. More generally, it provides for some simple file management on the contents of a remote computer. It is an old protocol and is used less than it was before the Word Wide Web came along. Today, Its primary use is uploading files to a Web site. It can also be used for downloading from the Web but, more often than not, downloading is done via HTTP. Sites that have a lot of downloading (software sites, for example) will often have an FTP server to handle the traffic. If FTP is involved, the URL will have *ftp:* at the front.

News (or Usenet)

Network News Transfer Protocol (NNTP) is used for serving Usenet posts Usenet is similar to the forums that many web sites have. Usenet has forums that are dedicated to specific companies as well as forums that have a wide range of topics. Usenet is divided into several areas. Some of the forums that are included in Usenet are comp. for discussion of computer-related topics, sci. for discussion of scientific subjects, rec. for discussion of recreational activities (e.g. games and hobbies) and talk. for discussion of contentious issues such as religion and politics.

Gopher

Another tool of the Internet is Gopher, a menu-based program that enables you to browse for information without knowing where the material is located. It lets you search a list of resources and then sends the material to you.

Telnet

Telnet lets you log in to a remote computer just as you would if you were there. So any commands that you would be able to run from the remote computer if you were sitting in front of it, you would be able to run from the computer you logged in from.

Q5 a) Manchester Encoding

Src : http://www.erg.abdn.ac.uk/~gorry/eg3567/phy-pages/man.html

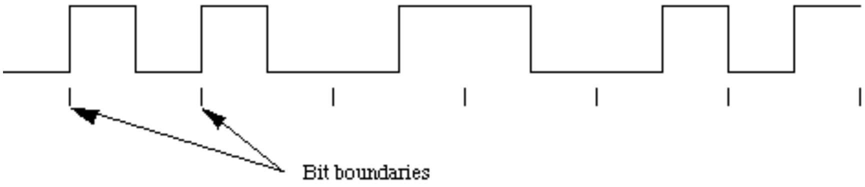
Manchester encoding (first published in 1949) is a synchronous clock encoding technique used by the physical layer to encode the clock and data of a synchronous bit stream. In this technique, the actual binary data to be transmitted over the cable are not sent as a sequence of logic 1's and 0's (known technically as Non Return to Zero (NRZ)). Instead, the bits are translated into a slightly different format that has a number of advantages over using straight binary encoding (i.e. NRZ).

In the Manchester encoding shown, a logic 0 is indicated by a 0 to 1 transition at the centre of the bit and a logic 1 is indicated by a 1 to 0 transition at the centre of the bit. Note that signal transitions do not always occur at the 'bit boundaries' (the division between one bit and another), but that there is always a transition at the centre of each bit. The Manchester encoding rules are summarized below:

Original Data	Value Sent
Logic 0	0 to 1 (upward transition at bit centre)
Logic 1	1 to 0 (downward transition at bit centre)

In some cases you will see the encoding reversed, with 0 being represented as a 0 to 1 transition. The two definitions have co-existed for many years. The Ethernet Blue-Book and IEEE standards (10 Mbps) describe the method in whih a Logic 0 is sent as 0 to 1 transition, and a Logic 1 as a one to zero transition (where a zero is represented by a less negative voltage on the cable). Note that because many physical layers employ an inverting line driver to convert the binary digits into an electrical signal, the signal on the wire is the exact opposite of that output by the encoder. Differential physical layer transmission, (e.g. 10BT) does not suffer this inversion.

The following diagram shows a typical Manchester encoded signal with the corresponding binary representation of the data (1,1,0,1,0,0) being sent.



The waveform for a Manchester encoded bit stream carrying the sequence of bits 110100.

Note that signal transitions do not always occur at the 'bit boundaries' (the division between one bit and another), but that there is **always** a transition at the centre of each bit.The encoding may be alternatively viewed as a phase encoding where each bit is encoded by a postive 90 degree phase transition, or a negative 90 degree phase transition. The Manchester code is therefore sometimes known as a **Biphase Code**.

A Manchester encoded signal contains frequent level transitions which allow the receiver to extract the clock signal using a Digital Phase Locked Loop (DPLL) and correctly decode the value and timing of each bit. To allow reliable operation using a DPLL, the transmitted bit stream must contain a high density of bit transitions. Manchester encoding ensures this, allowing the receiving DPLL to correctly extract the clock signal.

The bi-phase Manchester encoding can consume up to approximately twice the bandwidth of the original signal (20 MHz). This is the penalty for introducing frequent transitions. For a 10 Mbps LAN, the signal spectrum lies between the 5 and 20 MHz. Manchester encoding is used as the physical layer of an Ethernet LAN, where the additional bandwidth is not a significant issue for coaxial cable transmission, the limited bandwidth of CAT5e cable necessitated a more efficient encoding method for 100 Mbps transmission using a 4b/5b MLT code. This uses three signal levels (instead of the two levels used in Manchester encoding) and therfore allows a 100 Mbps signal to occupy only 31 MHz of bandwidth. Gigabit Ethernet utilises five levels and 8b/10b encoding, to provide even more efficient use of the limited cable bandwidth, sending 1 Gbps within 100 MHz of bandwidth.

Example of Manchester Encoding

The pattern of bits " 0 1 1 1 1 0 0 1 " encodes to " 01 10 10 10 10 01 01 10".

Another more curious example is the pattern " 1 0 1 0 1 etc" which encodes to "10 01 10 01 10 " which could also be viewed as "1 00 11 00 11 0 ". Thus for a 10 Mbps Ethernet LAN, the preamble sequence encodes to a 5 MHz square wave! (i.e., One half cycle in each 0.1 microsecond bit period.)

Thinking more about sending bits

A transmission rate of 10 Mbps implies that each bit is sent in 0.1 microseconds. For a coaxial cable, the speed at which the signal travels along the cable is approximately 0.77 times the speed of light (i.e. 0.77x3x10E8). A bit therefore occupies 23 metres of cable. Under the same conditions the smallest frame would be 13.3 km!

If you wish to do the same calculation for a twisted pair cable, you would have to take into consideration that the propagation speed is slower at 1.77x10E8 (0.59c). Increasing the bit rate, for example using 100BTx, decreases the time available to send each bit into the wire, but does not change the speed at which the edge of the bits travel through the cable!

Source : (Also Refer http://en.wikipedia.org/wiki/Manchester_code)

Q5) B) 802.11 PROTOCOL AND SERVICES

The IEEE 802.11 protocol is a network access technology for providing connectivity between wireless stations and wired networking infrastructures. By deploying the IEEE 802.11 protocol and associated technologies, you enable the mobile user to travel to various places and still have access to networked data. Also, beyond the corporate workplace, you enable access to the Internet and even corporate sites can be made available through public wireless “hot spot” networks. Airports, restaurants, rail stations, and common areas throughout cities can be configured to provide this service.

802.11 Architecture

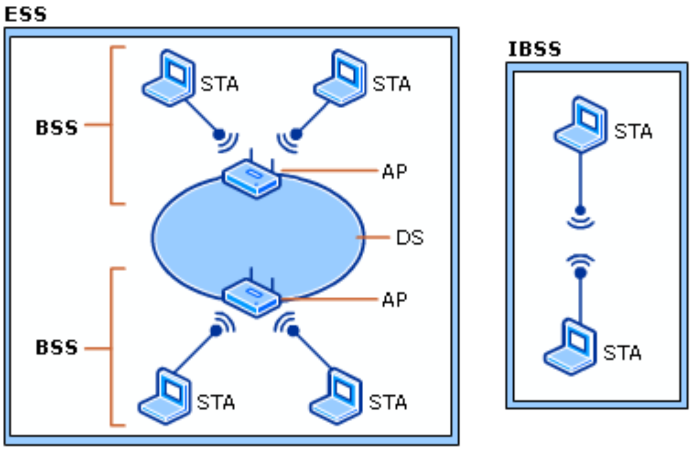
The 802.11 logical architecture contains several main components: station (STA), wireless access point (AP), independent basic service set (IBSS), basic service set (BSS), distribution system (DS), and extended service set (ESS). Some of the components of the 802.11 logical architecture map directly to hardware devices, such as STAs and wireless APs. The wireless STA contains an adapter card, PC Card, or an embedded device to provide wireless connectivity. The wireless AP functions as a bridge between the wireless STAs and the existing network backbone for network access. An IBSS is a wireless network, consisting of at least two STAs, used where no access to a DS is available. An IBSS is also sometimes referred to as an ad hoc wireless network. A BSS is a wireless network, consisting of a single wireless AP supporting one or multiple wireless clients. A BSS is also sometimes referred to as an infrastructure wireless network. All STAs in a BSS communicate through the AP. The AP provides connectivity to the wired LAN and provides bridging functionality when one STA initiates communication to another STA or a node on the DS.

An ESS is a set of two or more wireless APs connected to the same wired network that defines a single logical network segment bounded by a router (also known as a *subnet*).

The APs of multiple BSSs are interconnected by the DS. This allows for mobility, because STAs can move from one BSS to another BSS. APs can be interconnected with or without wires; however, most of the time they are connected with wires. The DS is the logical component used to interconnect BSSs. The DS provides distribution services to allow for the roaming of STAs between BSSs.

The following figure shows the 802.11 architecture.

802.11 Architecture



802.11 Operating Modes

IEEE 802.11 defines the following operating modes:

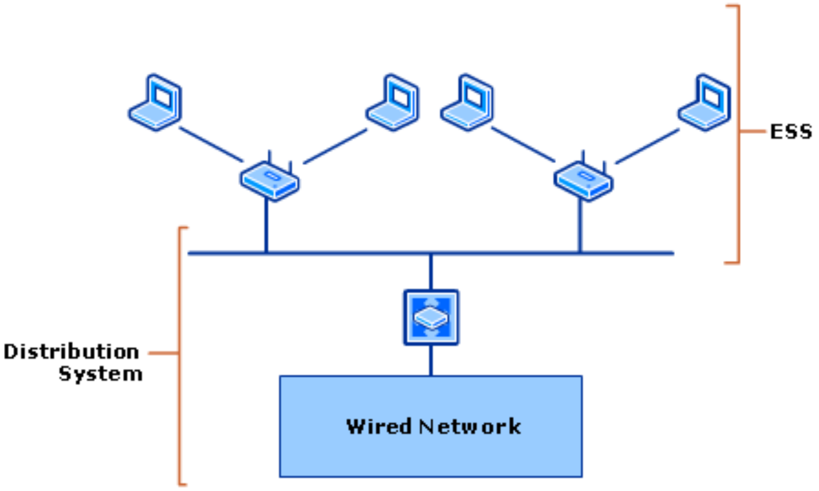
- Infrastructure mode
- Ad hoc mode

In both operating modes, a Service Set Identifier (SSID), also known as the *wireless network name*, identifies the wireless network. The *SSID* is a name configured on the wireless AP (for infrastructure mode) or an initial wireless client (for ad hoc mode) that identifies the wireless network. The SSID is periodically advertised by the wireless AP or the initial wireless client using a special 802.11 MAC management frame known as a *beacon frame*.

802.11 Infrastructure Mode

In *infrastructure mode*, there is at least one wireless AP and one wireless client. The wireless client uses the wireless AP to access the resources of a traditional wired network. The wired network can be an organization intranet or the Internet, depending on the placement of the wireless AP. An extended service set (ESS) is shown in the following figure.

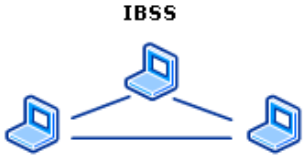
802.11 Infrastructure Mode



802.11 Ad Hoc Mode

In *ad hoc mode*, wireless clients communicate directly with each other without the use of a wireless AP, as shown in the following figure.

802.11 Wireless Clients in Ad Hoc Mode

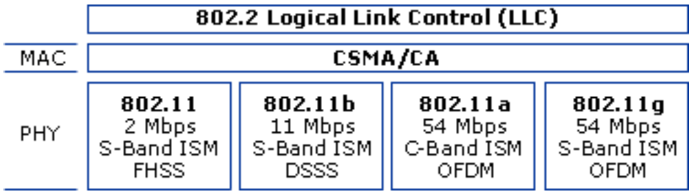


Ad hoc mode is also called *peer-to-peer mod*e. Wireless clients in ad hoc mode form an independent basic service set (IBSS). One of the wireless clients, the first wireless client in the IBSS, takes over some of the responsibilities of the wireless AP. These responsibilities include the periodic beaconing process and the authentication of new members. This wireless client does not act as a bridge to relay information between wireless clients. Ad hoc mode is used to connect wireless clients together when there is no wireless AP present. The wireless clients must be explicitly configured to use ad hoc mode. There can be a maximum of nine members in an ad hoc 802.11 wireless network.

802.11 PHY Sublayer

At the physical (PHY) sublayer, IEEE 802.11 defines a series of encoding and transmission schemes for wireless communications, the most common of which are the Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), and Orthogonal Frequency Division Multiplexing (OFDM) transmission schemes. The following figure shows the 802.11, 802.11b, 802.11a, and 802.11g standards that exist at the PHY sublayer. These standards are described in the sections that follow.

Standards for 802.11 at the PHY Layer



	802.2 Logical Link Control (LLC)			
MAC	CSMA/CA			
PHY	802.11 2 Mbps S-Band ISM FHSS	802.11b 11 Mbps S-Band ISM DSSS	802.11a 54 Mbps C-Band ISM OFDM	802.11g 54 Mbps S-Band ISM OFDM

IEEE 802.11

The bit rate for the original IEEE 802.11 standard is 2 Mbps using the FHSS transmission scheme and the S-Band Industrial, Scientific, and Medical (ISM) frequency band, which operates in the frequency range of 2.4 to 2.5 GHz. However, under less-than-ideal conditions, a lower bit rate speed of 1 Mbps is used.

802.11b

The major enhancement to IEEE 802.11 by IEEE 802.11b is the standardization of the physical layer to support higher bit rates. IEEE 802.11b supports two additional speeds, 5.5 Mbps and 11

Mbps, using the S-Band ISM. The DSSS transmission scheme is used in order to provide the higher bit rates. The bit rate of 11 Mbps is achievable in ideal conditions. In less-than-ideal conditions, the slower speeds of 5.5 Mbps, 2 Mbps, and 1 Mbps are used.

Note

- 802.11b uses the same frequency band as that used by microwave ovens, cordless phones, baby monitors, wireless video cameras, and Bluetooth devices.

802.11a

IEEE 802.11a (the first standard to be ratified, but just now being widely sold and deployed) operates at a bit rate as high as 54 Mbps and uses the C-Band ISM, which operates in the frequency range of 5.725 to 5.875 GHz. Instead of DSSS, 802.11a uses OFDM, which allows data to be transmitted by subfrequencies in parallel and provides greater resistance to interference and greater throughput. This higher-speed technology enables wireless LAN networking to perform better for video and conferencing applications.

Because they are not on the same frequencies as other S-Band devices (such as cordless phones), OFDM and IEEE 802.11a provide both a higher data rate and a cleaner signal. The bit rate of 54 Mbps is achievable in ideal conditions. In less-than-ideal conditions, the slower speeds of 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, and 6 Mbps are used.

802.11g

IEEE 802.11g operates at a bit rate as high as 54 Mbps, but uses the S-Band ISM and OFDM. 802.11g is also backward-compatible with 802.11b and can operate at the 802.11b bit rates and use DSSS. 802.11g wireless network adapters can connect to an 802.11b wireless AP, and 802.11b wireless network adapters can connect to an 802.11g wireless AP. Thus, 802.11g provides a migration path for 802.11b networks to a frequency-compatible standard technology with a higher bit rate. Existing 802.11b wireless network adapters cannot be upgraded to 802.11g by updating the firmware of the adapter — they must be replaced. Unlike migrating from 802.11b to 802.11a (in which all the network adapters in both the wireless clients and the wireless APs must be replaced at the same time), migrating from 802.11b to 802.11g can be done incrementally.

Like 802.11a, 802.11g uses 54 Mbps in ideal conditions and the slower speeds of 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, and 6 Mbps in less-than-ideal conditions.

802.1X Protocol

The IEEE 802.1X standard defines port-based, network access control used to provide authenticated network access for Ethernet networks. This port-based network access control uses the physical characteristics of the switched LAN infrastructure to authenticate devices attached to a LAN port. Access to the port can be denied if the authentication process fails. Although this standard was designed for wired Ethernet networks, it has been adapted to 802.11 wireless LANs.

Components of 802.1X

IEEE 802.1X defines the following terms, as described in the following sections:

- **Port access entity.** A LAN port, also known as *port access entity (PAE)*, is the logical entity that supports the IEEE 802.1X protocol that is associated with a port. A PAE can adopt the role of the authenticator, the supplicant, or both.

- **Authenticator.** An *authenticator* is a LAN port that enforces authentication before allowing access to services accessible using that port. For wireless connections, the authenticator is the logical LAN port on a wireless AP through which wireless clients in infrastructure mode gain access to other wireless clients and the wired network.

- **Supplicant.** The *supplicant* is a LAN port that requests access to services accessible on the authenticator. For wireless connections, the supplicant is the logical LAN port on a wireless LAN network adapter that requests access to the other wireless clients and the wired network by associating with and then authenticating itself to an authenticator.

  Whether for wireless connections or wired Ethernet connections, the supplicant and authenticator are connected by a logical or physical point-to-point LAN segment.

Authentication server. To verify the credentials of the supplicant, the authenticator uses an *authentication server*, which checks the credentials of the supplicant on behalf of the authenticator and then responds to the authenticator, indicating whether or not the supplicant is authorized to access the authenticator's services.

WEP

WEP provides data confidentiality services by encrypting the data sent between wireless nodes. Setting a WEP flag in the MAC header of the 802.11 frame indicates that the frame is encrypted with WEP encryption. WEP provides data integrity by including an integrity check value (ICV) in the encrypted portion of the wireless frame.

WEP defines two shared keys:

- **Multicast/global key.** The *multicast/global key* is an encryption key that protects multicast and broadcast traffic from a wireless AP to all of its connected wireless clients.

- **Unicast session key.** The *unicast session key* is an encryption key that protects unicast traffic between a wireless client and a wireless AP and multicast and broadcast traffic sent by the wireless client to the wireless AP.

WEP encryption uses the RC4 symmetric stream cipher with 40-bit and 104-bit encryption keys. Although 104-bit encryption keys are not specified in the 802.11 standard, many wireless AP vendors support them.

Note

- Some implementations that advertise the use of 128-bit WEP encryption keys are just adding a 104-bit encryption key to the 24-bit initialization vector (IV) and calling it a 128-bit key. The IV is a field in the header of each 802.11 frame that is used during the encryption and decryption process.

Security Issues with WEP and IEEE 802.11

The main problem with WEP is that the determination and distribution of WEP encryption keys are not defined. WEP keys must be distributed by using a secure channel outside of the 802.11 protocol. In practice, WEP keys are text strings that must be manually configured using a keyboard for both the wireless AP and wireless clients. However, this key distribution system does not scale well to an enterprise organization and is not secure.

Additionally, there is no defined mechanism for changing the WEP encryption keys either per authentication or periodically for an authenticated connection. All wireless APs and clients use the same manually configured WEP key for multiple sessions. With multiple wireless clients sending a large amount of data, an attacker can remotely capture large amounts of WEP ciphertext and use cryptanalysis methods to determine the WEP key.

The lack of a WEP key management protocol is a principal limitation to providing 802.11 security, especially in infrastructure mode with a large number of stations. Some examples of this type of network include corporate and educational institutional campuses and public places such as airports and malls. The lack of automated authentication and key determination services also affects operation in ad hoc mode, in which users might want to use in peer-to-peer collaborative communication in areas such as conference rooms.

WPA

Although 802.1X addresses many of the security issues of the original 802.11 standard, issues still exist with regard to weaknesses in the WEP encryption and data integrity methods. The long-term solution to these problems is the IEEE 802.11i standard, which is currently in draft form.

Until the IEEE 802.11i standard is ratified, wireless vendors have agreed on an interoperable interim standard known as Wi-Fi Protected Access (WPA).

The goals of WPA are the following:

- **To require secure wireless networking.** WPA requires secure wireless networking by requiring 802.1X authentication, encryption, and unicast and multicast/global encryption key management.

- **To address WEP issues with a software upgrade.** The implementation of the RC4 stream cipher within WEP is vulnerable to known plaintext attacks. Additionally, the data integrity provided with WEP is relatively weak. WPA solves all the remaining security issues with WEP, yet only requires firmware updates in wireless equipment and an update for wireless clients. Existing wireless equipment is not expected to require replacement.

- **To provide a secure wireless networking solution for small office/home office (SOHO) wireless users.** For the SOHO, there is no RADIUS server to provide 802.1X authentication with an EAP type. SOHO wireless clients must use either shared key authentication (highly discouraged) or open system authentication (recommended) with a single static WEP key for both unicast and multicast traffic. WPA provides a pre-shared key option intended for SOHO configurations. The pre-shared key is configured on the wireless AP and each wireless client. The initial unicast encryption key is derived from the authentication process, which verifies that both the wireless client and the wireless AP have the pre-shared key.

- **To be compatible with the upcoming IEEE 802.11i standard.** WPA is a subset of the security features in the proposed IEEE 802.11i standard. All the features of WPA are described in the current draft of the 802.11i standard.

- **To be available today.** WPA upgrades to wireless equipment and for wireless clients were available beginning in February 2003.

WPA Security Features

WPA contains enhancements or replacements for the following security features:

- Authentication

- Encryption

- Data integrity

Authentication

With 802.11, 802.1X authentication is optional; with WPA, 802.1X authentication is required. Authentication with WPA is a combination of open system and 802.1X authentication, which uses the following phases:

- The first phase uses open system authentication to indicate to the wireless client that it can send frames to the wireless AP.
- The second phase uses 802.1X to perform a user-level authentication. For environments without a RADIUS infrastructure, WPA supports the use of a pre-shared key; for environments with a RADIUS infrastructure, WPA supports EAP and RADIUS.

Encryption

With 802.1X, rekeying of unicast encryption keys is optional. Additionally, 802.11 and 802.1X provide no mechanism to change the global encryption key that is used for multicast and broadcast traffic. With WPA, rekeying of both unicast and global encryption keys is required. The Temporal Key Integrity Protocol (TKIP) changes the unicast encryption key for every frame, and each change is synchronized between the wireless client and the wireless AP. For the multicast/global encryption key, WPA includes a facility for the wireless AP to advertise changes to the connected wireless clients.

TKIP - For 802.11, WEP encryption is optional. For WPA, encryption using TKIP is required. TKIP replaces WEP with a new encryption algorithm that is stronger than the WEP algorithm, yet can be performed using the calculation facilities present on existing wireless hardware. TKIP also provides for the following:

- The verification of the security configuration after the encryption keys are determined.
- The synchronized changing of the unicast encryption key for each frame.
- The determination of a unique starting unicast encryption key for each pre-shared key authentication.

AES - WPA defines the use of the Advanced Encryption Standard (AES) as an optional replacement for WEP encryption. Because adding AES support by using a firmware update might not be possible for existing wireless equipment, support for AES on wireless network adapters and wireless APs is not required.

Data Integrity

With 802.11 and WEP, data integrity is provided by a 32-bit ICV that is appended to the 802.11 payload and encrypted with WEP. Although the ICV is encrypted, it is possible through cryptanalysis to change bits in the encrypted payload and update the encrypted ICV without being detected by the receiver.

Q5) D) PPP protocol

In networking, the Point-to-Point Protocol (PPP) is a data link protocol commonly used in establishing a direct connection between two networking nodes. It can provide connection authentication, transmission encryption (using ECP, RFC 1968), and compression.

PPP is used over many types of physical networks including serial cable, phone line, trunk line, cellular telephone, specialized radio links, and fiber optic links such as SONET. PPP is also used over Internet access connections (now marketed as "broadband").Internet service providers (ISPs) have used PPP for customer dial-up access to the Internet, since IP packets cannot be transmitted over a modem line on their own, without some data link protocol. Two derivatives of PPP, Point-to-Point Protocol over Ethernet(PPPoE) and Point-to-Point Protocol over ATM (PPPoA), are used most commonly by Internet Service Providers (ISPs) to establish aDigital Subscriber Line (DSL) Internet service connection with customers.

PPP is commonly used as a data link layer protocol for connection over synchronous and asynchronous circuits, where it has largely superseded the older Serial Line Internet Protocol (SLIP) and telephone company mandated standards (such as Link Access Protocol, Balanced (LAPB) in the X.25 protocol suite). PPP was designed to work with numerous network layer protocols, including Internet Protocol (IP), TRILL, Novell's Internetwork Packet Exchange (IPX), NBF and AppleTalk.

Description

PPP and TCP/IP protocol stack						
Application	FTP	SMTP	HTTP	...	DNS	...
Transport	TCP				UDP	
Internet	IP			IPv6		
Network access	PPP					
	PPPoE		PPPoA		PPP	
	Ethernet		ATM		Serial Modem	

PPP was designed somewhat after the original HDLC specifications. The designers of PPP included many additional features that had been seen only in proprietary data-link protocols up to that time. RFC 2516 describes Point-to-Point Protocol over Ethernet (PPPoE) as a method for transmitting PPP over Ethernet that is sometimes used with DSL. RFC 2364 describes Point-to-Point Protocol over ATM (PPPoA) as a method for transmitting PPP over ATM Adaptation Layer 5 (AAL5), which is also a common alternative to PPPoE used with DSL.

PPP is specified in RFC 1661.

PPP frame

Structure of a PPP frame

The Protocol field indicates the type of payload packet (e.g. LCP, NCP, IP, IPX, AppleTalk, etc.).

The Information field contains the PPP payload; it has a variable length with a negotiated maximum called the Maximum Transmission Unit. By default, the maximum is 1500octets. It might be padded on transmission; if the information for a particular protocol can be padded, that protocol must allow information to be distinguished from padding.

Name	Number of bytes	Description
Protocol	1 or 2	setting of protocol in data field
Information	variable (0 or more)	datagram
Padding	variable (0 or more)	optional padding

Link http://www-ee.uta.edu/online/wang/ppp.pdf

http://technet.microsoft.com/en-us/library/cc768082.aspx

Q5) C) i) EGO CASTING

What ties all these technologies together is the stroking of the ego. When cable television channels began to proliferate in the 1980s, a new type of broadcasting, called “narrowcasting,” emerged — with networks like MTV, CNN, and Court TV catering to specific interests. With the advent of TiVo and iPod, however, we have moved beyond narrowcasting into “egocasting” — a world where we exercise an unparalleled degree of control over what we watch and what we hear. We can consciously avoid ideas, sounds, and images that we don’t agree with or don’t enjoy. As sociologists Walker and Bellamy have noted, “media audiences are seen as frequently selecting material that confirms their beliefs, values, and attitudes, while rejecting media content that conflicts with these cognitions.” Technologies like TiVo and iPod enable unprecedented degrees of selective avoidance. The more control we can exercise over what we see and hear, the less prepared we are to be surprised. It is no coincidence that we impute God-like powers to our technologies of personalization (TiVo, iPod) that we would never impute to gate-keeping technologies. No one ever referred to Caller ID as "Jehovah's Secretary."

TiVo, iPod, and other technologies of personalization are conditioning us to be the kind of consumers who are, as Joseph Wood Krutch warned long ago, "incapable of anything except habit and prejudice," with our needs always preemptively satisfied. But it is worth asking how forceful we want this divining of our tastes to become. Already, you cannot order a book from Amazon.com without a half-dozen DVD, appliance, and CD recommendations fan-dancing before you. And as our technologies become more perceptive about our tastes, the products we are encouraged to consume change as well. A story in the *Wall Street Journal* recently noted that broadcasting companies such as Viacom are branching out into book publishing. A spokesman for Viacom's imprint, which targets 18-34 year olds, told the*Journal*, "Our readers are addicted to at least one reality TV show, they own one iPod, and they are in love with their TiVo." Companies are capitalizing on this knowledge by merging their products.

University of Chicago law professor Cass Sunstein engaged this dilemma in his book, *Republic.com*. Sunstein argues that our technologies — especially the Internet — are encouraging group polarization: "As the customization of our communications universe increases, society is in danger of fragmenting, shared communities in danger of dissolving." Borrowing the idea of "the daily me" from M.I.T. technologist Nicholas Negroponte, Sunstein describes a world where "you need not come across topics and views that you have not sought out. Without any difficulty, you are able to see exactly what you want to see, no more and no less." Sunstein is concerned about the possible negative effects this will have on deliberative democratic discourse, and he urges websites to include links to sites that carry alternative views. Although his solutions bear a trace of impractical ivory tower earnestness — you can lead a rabid partisan to water, after all, but you can't make him drink — his diagnosis of the problem is compelling. "People should be exposed to materials that they would not have chosen in advance," he notes. "Unplanned, unanticipated encounters are central to democracy itself." Sunstein's insights have lessons beyond politics. If these technologies facilitate polarization in politics, what influence are they exerting over art, literature, and music? In our haste to find the quickest, most convenient, and most easily individualized way of getting what we want, are we creating eclectic personal theaters or sophisticated echo chambers? Are we promoting a creative individualism or a narrow individualism? An expansion of choices or a deadening of taste?

Source - http://www.thenewatlantis.com/publications/the-age-of-egocasting

Q5) C) ii) BROADCASTING:

Broadcasting is the distribution of audio and video content to a dispersed audience via any audio or visual mass communications medium, but usually one using electromagnetic radiation (radio waves). The receiving parties may include the general public or a relatively large subset thereof. Broadcasting has been used for purposes of private recreation, non-commercial exchange of messages, experimentation, self-training, and emergency communication such as amateur (ham) radio and amateur television (ATV) in addition to commercial purposes like popular radio or TV stations with advertisements.

History

The term broadcast was first adopted by early radio engineers from the Midwestern United States, treating broadcast sowing as a metaphor for the dispersal inherent in omnidirectional radio signals.Broadcasting is a very large and significant segment of the mass media. Originally all broadcasting was composed of analog signals using analog transmission techniques and more recently broadcasters have switched to digital signals using digital transmission.

- Analog audio vs. HD Radio
- Analog television vs. Digital television
- Wireless

The world's technological capacity to receive information through one-way broadcast networks more than quadrupled during the two decades from 1986 to 2007, from 432 exabytesof (optimally compressed) information, to 1.9 zettabytes.[2] This is the information equivalent of 55 newspapers per person per day in 1986, and 175 newspapers per person per day by 2007.[3]

Types of electronic broadcasting

Historically, there have been several types of electronic media broadcasting:

- Telephone broadcasting (1881–1932): the earliest form of electronic broadcasting (not counting data services offered by stock telegraph companies from 1867, if ticker-tapes are excluded from the definition). Telephone broadcasting began with the advent of Théâtrophone ("Theatre Phone") systems, which were telephone-based distribution systems allowing subscribers to listen to live opera and theatre performances over telephone lines, created by French inventor Clément Ader in 1881. Telephone broadcasting also grew to include telephone newspaper services for news and entertainment programming which were introduced in the 1890s, primarily located in large European cities. These telephone-based subscription services were the first examples of electrical/electronic broadcasting and offered a wide variety of programming.
- Radio broadcasting (experimentally from 1906, commercially from 1920): radio broadcasting is an audio (sound) broadcasting service, broadcast through the air as radio wavesfrom a

transmitter to a radio antenna and, thus, to a receiver. Stations can be linked in radio networks to broadcast common radio programs, either in broadcast syndication,simulcast or subchannels.

- History of television broadcasting (telecast), experimentally from 1925, commercial television from the 1930s: this television programming medium was long-awaited by the general public and rapidly rose to compete with its older radio-broadcasting sibling.
- Cable radio (also called "cable FM", from 1928) and cable television (from 1932): both via coaxial cable, serving principally as transmission mediums for programming produced at either radio or television stations, with limited production of cable-dedicated programming.
- Direct-broadcast satellite (DBS) (from circa 1974) and satellite radio (from circa 1990): meant for direct-to-home broadcast programming (as opposed to studio network uplinks and downlinks), provides a mix of traditional radio or television broadcast programming, or both, with dedicated satellite radio programming. (See also: Satellite television)
- Webcasting of video/television (from circa 1993) and audio/radio (from circa 1994) streams: offers a mix of traditional radio and television station broadcast programming with dedicated internet radio-webcast programming.

Economic models

Economically there are a few ways in which stations are able to broadcast continually. Each differs in the method by which stations are funded:

- in-kind donations of time and skills by volunteers (common with community radio broadcasters)
- direct government payments or operation of public broadcasters
- indirect government payments, such as radio and television licenses
- grants from foundations or business entities
- selling advertising or sponsorships
- public subscription or membership

Broadcasters may rely on a combination of these business models. For example, National Public Radio (NPR), a non-commercial educational (NCE) public radio media organization within the U.S., receives grants from the Corporation for Public Broadcasting (CPB) (which, in turn, receives funding from the U.S. government), by public membership and by selling "extended credits" to corporations.

Q 5) E) BLUETOOTH PROTOCOLS

Wireless data exchange standard Bluetooth uses a variety of protocols. Core protocols are defined by the trade organization Bluetooth SIG. Additional protocols have been adopted from other standards bodies. This article gives an overview of the core protocols and those adopted protocols that are widely used.

The Bluetooth protocol stack is split in two parts: a "controller stack" containing the timing critical radio interface, and a "host stack" dealing with high level data. The controller stack is generally implemented in a low cost silicon device containing the bluetooth radio and a microprocessor. The host stack is generally implemented as part of an operating system, or as an installable package on top of an operating system. For integrated devices such as bluetooth headsets, the host stack and controller stack can be run on the same microprocessor to reduce mass production costs; this is known as a hostless system.

Controller stack

i) Asynchronous Connection-oriented [logical transport] (ACL)

The normal type of radio link used for general data packets using a polling TDMA scheme to arbitrate access. It can carry packets of several types, which are distinguished by:

- length (1, 3, or 5 time slots depending on required payload size)
- forward error correction (optionally reducing the data rate in favour of reliability)
- modulation (EDR - enhanced data rate - packets allow up to triple data rate by using a different RF modulation for the payload)

A connection must be explicitly set up and accepted between two devices before packets can be transferred. ACL packets are retransmitted automatically if unacknowledged, allowing for correction of a radio link that is subject to interference. For isochronous data, the number of retransmissions can be limited by a flush timeout; but without using L2PLAY retransmission and flow control mode or EL2CAP, a higher layer must handle the packet loss.

ACL links are disconnected if there is nothing received for the supervision timeout period; the default timeout is 20 seconds, but this may be modified by the master.

ii) Synchronous connection-oriented (SCO) link

The type of radio link used for voice data. An SCO link is a set of reserved timeslots on an existing ACL link. Each device transmits encoded voice data in the reserved timeslot. There are no retransmissions, but forward error correction can be optionally applied. SCO packets may be sent every 1, 2 or 3 timeslots. Enhanced SCO (eSCO) links allow greater flexibility in setting up links: they may use retransmissions to achieve reliability, allow a wider variety of packet types, and greater intervals between packets than SCO, thus increasing radio availability for other links.

iii) Link management protocol (LMP)

Used for control of the radio link between two devices, handling matters such as link establishment, querying device abilities and power control. Implemented on the controller.

iv) Host/controller interface (HCI)

Standardised communication between the host stack (e.g., a PC or mobile phone OS) and the controller (the Bluetooth IC). This standard allows the host stack or controller IC to be swapped with minimal adaptation.

There are several HCI transport layer standards, each using a different hardware interface to transfer the same command, event and data packets. The most commonly used areUSB (in PCs) and UART (in mobile phones and PDAs).

In Bluetooth devices with simple functionality (e.g., headsets), the host stack and controller can be implemented on the same microprocessor. In this case the HCI is optional, although often implemented as an internal software interface.

v) Low Energy Link Layer (LE LL)

This is the LMP equivalent for Bluetooth Low Energy (LE), but is simpler. It is implemented on the controller and manages advertisement, scanning, connection and security from a low-level, close to the hardware point of view.

Host stack

i) Logical link control and adaptation protocol (L2CAP)

L2CAP is used within the Bluetooth protocol stack. It passes packets to either the Host Controller Interface (HCI) or on a hostless system, directly to the Link Manager/ACL link.

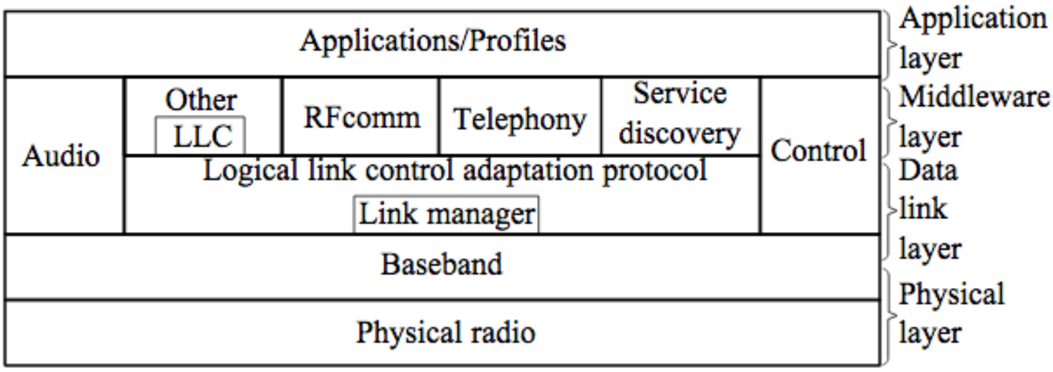
L2CAP's functions include:

- Multiplexing data between different higher layer protocols.
- Segmentation and reassembly of packets.
- Providing one-way transmission management of multicast data to a group of other Bluetooth devices.
- Quality of service (QoS) management for higher layer protocols.

L2CAP is used to communicate over the host ACL link. Its connection is established after the ACL link has been set up.

ii) Bluetooth network encapsulation protocol (BNEP)

BNEP is used for delivering network packets on top of L2CAP. This protocol is used by the personal area networking (PAN) profile. BNEP performs a similar function to Subnetwork Access Protocol (SNAP) in Wireless LAN. In the protocol stack, BNEP is bound to L2CAP.



iii) Radio frequency communication (RFCOMM)

The Bluetooth protocol RFCOMM is a simple set of transport protocols, made on top of the L2CAP protocol, providing emulated RS-232 serial ports (up to sixty simultaneous connections to a Bluetooth device at a time). The protocol is based on the ETSI standard TS 07.10. RFCOMM is sometimes called serial port emulation. The Bluetooth serial port profile is based on this protocol.

RFCOMM provides a simple reliable data stream to the user, similar to TCP. It is used directly by many telephony related profiles as a carrier for AT commands, as well as being a transport layer for OBEX over Bluetooth. Many Bluetooth applications use RFCOMM because of its widespread support and publicly available API on most operating systems. Additionally, applications that used a serial port to communicate can be quickly ported to use RFCOMM. In the protocol stack, RFCOMM is bound to L2CAP.

iv) Service discovery protocol (SDP)

Used to allow devices to discover what services each other support, and what parameters to use to connect to them. For example, when connecting a mobile phone to a Bluetooth headset, SDP will be used to determine which Bluetooth profiles are supported by the headset (headset profile, hands free profile, advanced audio distribution profile, etc.) and the protocol multiplexer settings needed to connect to each of them. Each service is identified by a Universally Unique Identifier (UUID), with official services (Bluetooth profiles) assigned a short form UUID (16 bits rather than the full 128). In the protocol stack, SDP is bound to L2CAP.

v) Telephony control protocol (TCP)

Also referred to as telephony control protocol specification binary (TCS binary). Used to set up and control speech and data calls between Bluetooth devices. The protocol is based on the ITU-T standard Q.931, with the provisions of Annex D applied, making only the minimum changes necessary for Bluetooth. TCP is used by the intercom (ICP) and cordless telephony (CTP) profiles.

vi) Audio/video control transport protocol (AVCTP)

Used by the remote control profile to transfer AV/C commands over an L2CAP channel. The music control buttons on a stereo headset use this protocol to control the music player

In the protocol stack, AVCTP is bound to L2CAP.

vii) Audio/video data transport protocol (AVDTP)

Used by the advanced audio distribution profile to stream music to stereo headsets over an L2CAP channel. Intended to be used by video distribution profile. In the protocol stack, AVDTP is bound to L2CAP.

viii) Object exchange (OBEX)

Object exchange (OBEX; also termed IrOBEX) is a communications protocol that facilitates the exchange of binary objects between devices. It is maintained by the Infrared Data Association but has also been adopted by the Bluetooth Special Interest Group and the SyncML wing of the Open Mobile Alliance (OMA). In Bluetooth, OBEX is used for many profiles that require simple data exchange (e.g., object push, file transfer, basic imaging, basic printing, phonebook access, etc.).

ix) Low Energy Attribute Protocol (ATT)

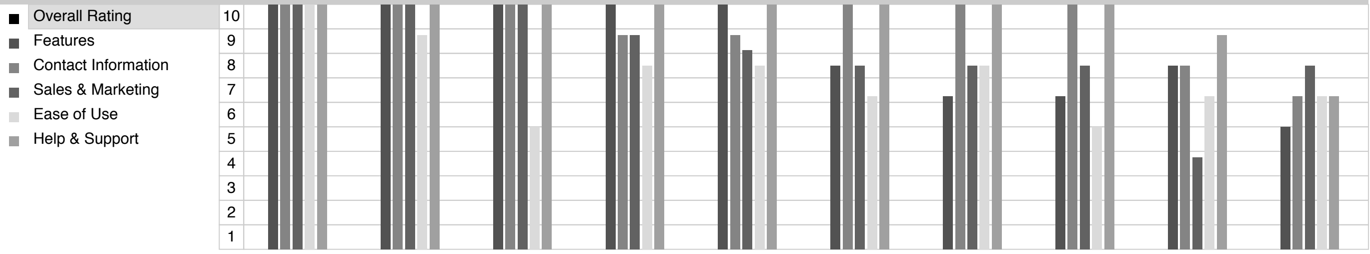
Similar in scope to SDP, but specially adapted and simplified for Low Energy Bluetooth. It allows a client to read and/or write certain attributes exposed by the server in a non-complex, low-power friendly manner. In the protocol stack, ATT is bound to L2CAP.

x) Low Energy Security Manager Protocol (SMP)

This is used by Bluetooth Low Energy Implementations for pairing and transport specific key distribution. In the protocol stack, SMP is bound to L2CAP.

2013 Compare Best CRM Software

Rank	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
10-9 Excellent **8-6** Good **5-4** Average **3-2** Poor **1-0** Bad	Sales Force	Oncontact	Sage ACT! Premium	Prophet	AIMcrm	Relenta	webAsyst	Maximizer CRM	TeamWox	Chaos Intellect
Ratings	**10.00**	**9.80**	**9.20**	**9.05**	**8.90**	**8.28**	**8.20**	**7.80**	**6.68**	**6.25**



Pricing Information										
Number of Users	Unlimited	Unlimited	10	Unlimited	Unlimited	5	✓	✓	5	Unlimited
Hosted Cost	$65/user	$59.95/user	-	$45/user	$55/user	$75/five users	$29.95	$199/user	$75/5 users	$59.95/user
Hosted Payment Frequency	Monthly	Monthly	-	Monthly	Monthly	Monthly	Monthly	One-time	Monthly	Monthly
On-Premise Solution	-	$995/user	$199.99/first $139.95/each additional	$500/user	-	-	$799/user	$699/user	$3,400/25 users	-
On-Premise Payment Frequency	-	One-time Fee	One-time	One-time	-	-	One-time	One-time	One-time	-
On-Premise Maintenance	-	$250	-	-	-	-	-	Included	-	-
Features										
Email Integration	✓	✓	✓	✓	✓		✓	✓	✓	✓
Web Hosted Solution	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Daily Schedule/To-Do	✓	✓	✓	✓	✓	✓		✓	✓	✓
Contact/Account Notes	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mobile Access	✓	✓	✓	✓	✓	✓		✓	✓	✓
Calendar Integration	✓	✓	✓	✓	✓			✓	✓	✓
Remote Synchronization	✓	✓	✓	✓		✓	✓	✓	✓	✓
Dialing Capabilities	✓	✓		✓	✓				✓	✓
On-Premise Solution		✓		✓				✓	✓	✓
Contact Information										
Company Websites	✓	✓	✓	✓	✓		✓	✓	✓	
Contact History	✓	✓	✓	✓	✓	✓		✓	✓	✓
Contact Information Pages	✓	✓	✓	✓	✓	✓	✓		✓	✓
Social Networking Pages	✓	✓	✓	✓	✓		✓	✓		
Organize Into Groups	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Map With Travel Instruction	✓	✓	✓	✓	✓		✓	✓		
Link Contacts	✓	✓	✓	✓	✓			✓	✓	✓
Sales & Marketing Tools										
Reporting Options	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Letterheads	✓	✓	✓	✓	✓	✓	✓	✓		✓
Mailing Labels	✓	✓	✓	✓	✓	✓	✓	✓		✓
Automated E-mail Campaigns	✓	✓	✓	✓	✓	✓	✓	✓		✓
Real-Time Alerts	✓	✓	✓	✓	✓			✓	✓	✓
Help & Support										
Tutorials	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Help Section/FAQs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Automatic Updates	✓	✓	✓	✓	✓			✓	✓	✓
Telephone Customer Support	✓	✓	✓	✓	✓			✓	✓	✓
Online Customer Support	✓	✓	✓	✓		✓	✓	✓	✓	✓

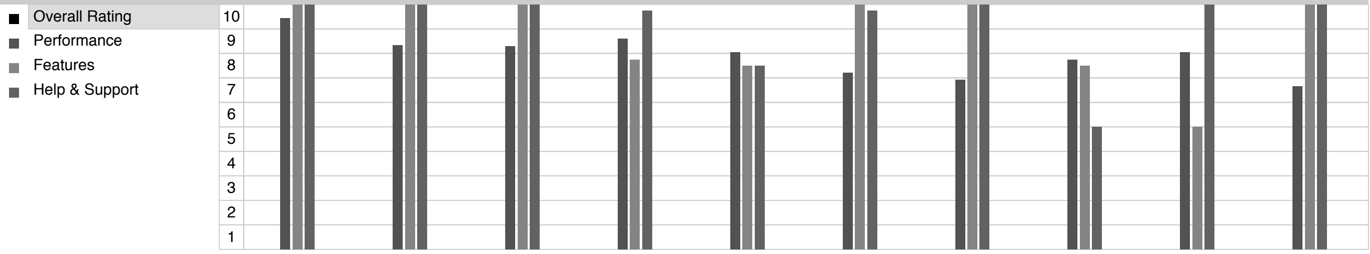
TopTenREVIEWS™

2013 Compare The Best Antivirus Software Products

Rank	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
	Bitdefender Antivirus Plus	Kaspersky Anti-Virus	Norton AntiVirus	F-Secure Anti-Virus	G Data AntiVirus	BullGuard Antivirus	AVG Anti-Virus	Avast! Pro Antivirus	Trend Micro Titanium Antivirus +	VIPRE Antivirus

10-9	Excellent
8-6	Good
5-4	Average
3-2	Poor
1-0	Bad

Ratings	9.58	8.75	8.73	8.50	7.93	7.90	7.70	7.58	7.55	7.50



	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
Windows 7 Performance										
Protection Score	100%	92%	92%	100%	100%	83%	75%	83%	100%	58%
Repair Score	100%	75%	75%	83%	67%	58%	58%	67%	67%	75%
Usability Score	83%	83%	83%	75%	75%	75%	75%	83%	75%	67%
Features										
Anti-Malware	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Browser Exploits	✓	✓	✓	✓	✓	✓	✓	✓		✓
Anti-Virus	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Trojan	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Spyware	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Worm	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Rootkit	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Phishing	✓	✓	✓		✓	✓	✓	✓	✓	✓
Secure Network	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Email scans	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Bootable Rescue CD	✓	✓	✓	✓	✓	✓	✓	✓		✓
On-demand Scanning	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Auto-clean Infected Files	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Scan compressed Files	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Infected File Quarantine	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Instant Messaging Protection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Registry Startup Protection	✓	✓	✓	✓	✓		✓	✓	✓	✓
Gamer Mode	✓	✓	✓			✓	✓	✓		
Auto USB Detect	✓	✓	✓			✓	✓		✓	✓
Supported Configurations										
Windows 8	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Windows 7	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Windows Vista	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Windows XP	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Help & Support										
Live Chat	✓	✓	✓	✓		✓	✓		✓	✓
Email	✓	✓	✓	✓	✓	✓	✓		✓	✓
Phone Support	✓	✓	✓	✓	✓	✓		✓	✓	✓