DJSCOE CSI STUDENT CHAPTER presents

PROTOCOL

(VOLUME 1)

MAY 2010

WIRELESS NETWORK
AND
SECURITY

COMPUTER SOCIETY OF INDIA:

Formed in 1965, the CSI has been instrumental in guiding the Indian IT industry down the right path during its formative years. Today, the CSI has 66 chapters all over India, 381 student branches, and more than 40,000 members, including India's most famous IT industry leaders, brilliant scientists and dedicated academicians. Now, you have the opportunity to be a part of this distinguished fraternity too.

The mission of the CSI is to facilitate research, knowledge sharing, learning and career enhancement for all categories of IT professionals, while simultaneously inspiring and nurturing new entrants into the industry and helping them to integrate into the IT community. The CSI is also working closely with other industry associations, government bodies and academia to ensure that the benefits of IT advancement ultimately percolate down to every single citizen of India.

FACULTY NOTE:

I proudly present to you the latest initiative by CSI - The Protocol Magazine.

The CSI chapter of DJSCOE has been working incessantly to spread technical know-how amongst students. CSI at DJSCOE has shared knowledge about important concepts like .Net Technologies, Linux Operating System, 2G & 3G Technologies, Computer and Mobile Tricks and Tweaks, Innovative Mindset, Professional Web Disigning and Deployment, Middleware and Wireless Technologies, MBA Career Guidance and Vedic Mathematics via various workshops and seminars in the academic year 2009-10.

This magazine aims to continue the good work done in the academic year 2009-10. The concept covered this time is 4G and WiMax along with Career Opportunities in Cisco Wireless Networking Technology. We hope it is of best use to you. Thank you. Best wishes.

CHAIRMAN NOTE:

As a Chairman of DJSCOE CSI Student Chapter I want to thank Prof. Abhijit Joshi CSI branch counsellor for continuous support throughout the year.

I also want to thank my committee member for their support Had some great time while working with all of you.

Magazine committee worked hard to develop this first copy of DJSCOE CSI magazine which is named PROTOCOL after tech fest which DJSCOE CSI used to have till idea of one technical fest came up in 2008.

-Dilkush Patel

MAGAZINE COMMITTEE :

Brijal Gaglani(TE-IT)

Aditya Modi(TE-IT)

Rishabh Shah(TE-IT)

Aishwarya Bhandari(TE-IT)

Harsh Swaminarayan(SE-IT)

Dilkush Patel(TE-IT)

ACTIVITIES DONE BY CSI (DJSCOE) in 2009-2010

Tricks & Tweaks Workshop:

Organized under the banner of DJSCOE_CSI by two students of TE-IT of DJSCOE itself ; **Dilkush Patel and Aditya Modi** , it was a fun filled workshop which included tricks of mobile and computers like how to **crash someone's pc,how to hard reset nokia mobile,getting IMEI no. , how to create virus** etc.
Student liked workshop and gave positive feedback.

Linux Workshop:

Linux is opensource , that means its freely available and no need of piracy.There is not much awareness about opensource among students so this workshop generated much needed awareness about opensource operating systems and platform.Students learned about UBUNTU , an operating system developed by opensource developers.Most amazing part of whole workshop was the lab session.It was stretched over .

.Net Workshop

It was Organized by DJSCOE_CSI and addressed by **professional from TCS.**
Student learned about importance of .net framework and learned how to use .net for building various applications.
Stretched over one day it contained theory as well as practical session also.

Industrial Visit:

The Computer Society of India-DJSCOE chapter 2009-2010 marked one of its biggest events-the Industrial Visit (I.V) on its calendar in the month of January 2010.
The I.V to Kerala and its world famous backwaters was decided. The itinerary included a 9nights/10 Days journey across the Keralian terrain as we started off from the humble metropolitan Cochin, across the fantastical and pristine landscapes of misty Munnar, to the small bustling town of Thekkaddy, the backwaters of Allepy, ending at the laid-back Kovalam with Thiruvananthapuram a quarter of an hour away from it.
There were total 160 students and 5 teachers on I.V.
Industries which were covered in I.V. were Chips Infotech in Cochin, UST Global in Technopark in Trivandrum and Vikram Sarabhai Space Centre in Trivandrum.
We would like to thank the teachers who accompanied us, Prof. Abhijit Joshi (CSI Branch Counselor) for his support and co-operation, Prof. A.C. Daptardar and Prof.
Hari Vasudevan for their well-wishing tips and advice.
-Dilkush Patel
(Chairman –DJSCOE_CSI)

3G and 4G: Mobile and Wireless Networks

ARTICLE BY: **Prof. S. M. Chaware**

Today's world of globalization, mobile and wireless networks plays an important role. There are wide areas of applications and services; where without these networks human can be handicapped. These may include from home such as controlling appliances such as speed of fans, fridge, TV etc., accessing of web on mobile, pay or transfer the payments on a single click and so on. In this article, focus has been given on basic services and its perspective in our country.

Mobile networks will include mobile phone i.e. mobile station (MS), base station (BS), BSC (base station controller), MSC (Message switching center) etc as an infrastructure. Some of these will work on wireless or wired medias. Mobile stations will have wireless interface with base station to transmit or receive the signals. The signals are generated by trans-receivers as electromagnetic waves and propagated into the air. The signals travel along the earth's surface due to gravitational force of an earth. There are two types of channels being used by the either side, logical or physical. Logical channels are used as handshake signals among the MS and BS and physical channels are being used for actual voice or data transmission. Paging will be used by the BS in order to locate MS in his area. MSC will maintain a database in his register, such as HLR and VLR to identify the home user or visitors.

The First generation wireless mobile communication systems were introduced in early eighties and second generations systems in the late 1980s were intended primarily for transmission of voice. The initial systems used analog frequency modulation where as the second as well as the subsequent mobile systems use digital communication techniques with time division multiplexing (TDM), frequency division multiplexing (FDM) or the code division multiple access (CDMA). The third generation wireless systems which are just getting introduced in the world markets offer considerably higher data rates, and allow significant improvements over the 2G systems. The 3G Wireless systems were proposed to provide voice and paging services to provide interactive multimedia including teleconferencing and internet access and variety of other services. However, these systems offer wide area network (WAN) coverage of 384 kbps peak rate and limited coverage for 2 Mbps. Hence providing broadband services would be one of the major goals of the 4G Wireless systems.

3G Wireless System

Essential qualities and characteristics of a 3G wireless system:

- Bit rates are growing up to 2 Mbps.
- Variable bit rate generating bandwidth on demand.
- Multiplexing of services with various quality requirements on a single connection, e.g. speech, video, and packet data.
- Delay requirements from delay-sensitive real-time traffic to flexible best-effort packet data.
- Quality requirements from 10% frame error to 10-6 bit error rate
- Coexistence of second and third generation systems handovers for coverage enhancements and load balancing.
- Support of asymmetric uplink traffic, e.g. web browsing causes more loading to downlink and uplink.
- High spectrum efficiency.
- Coexistence of FDD and TDD models.

Features of 4G Wireless Systems

The following are some possible features of the 4G systems:

- Support interactive multimedia, voice, video, wireless internet and other broadband services.
- High speed, high capacity and low cost per bit.
- Global mobility, service portability, scalable mobile networks.
- Seamless switching, variety of services based on Quality of Service (QoS) requirements.
- Better scheduling and call admission control techniques.
- Ad hoc networks and multi-hop networks.

3G Vs 4G

The following table shows comparisons between some key parameters of 3G Vs possible 4G systems.

	3G	4G
Frequency Band	1.8 - 2.5 GHz	2 - 8 GHz

Bandwidth	5-20 MHz	5-20 MHz
Data rate	Up to 2Mbps (384 kbps WAN)	Up to 20 Mbps or more
Access	Wideband CDMA	Multi-carrier - CDMA or OFDM(TDMA)
FEC	Turbo-codes	Concatenated codes
Switching	Circuit/Packet	Packet
Mobile top speeds	200 kmph	200 kmph

WiMAX Technology

ARTICLE BY: Aditya Modi

Why Not WiMAX ??

Who doesn't want High Speed Broadband Internet on the go ?

We have good broadband connections but they are wired What if we are travelling at a speed of 100 kmph on the highway and still want high speed internet access ?

The solution to the above mentioned questions is WiMAX

WiMAX is the next-generation of wireless technology designed to enable pervasive, high-speed mobile Internet access to the widest array of devices including notebook PCs, handsets, smartphones, and consumer electronics such as gaming devices, cameras, camcorders, music players, and more. As the fourth generation (4G) of wireless technology, WiMAX delivers low-cost, open networks and is the first all IP mobile Internet solution enabling efficient and scalable networks for data, video, and voice. As a major driver in the support and development of WiMAX, Intel has designed embedded WiMAX solutions for a variety of mobile devices supporting the future of high-speed broadband on-the-go

WiMAX has the potential to do to broadband Internet access what cell phones have done to phone access. In the same way that many people have given up their "land lines" in favor of cell phones, WiMAX could replace cable and DSL services, providing universal Internet access just about anywhere you go. WiMAX will also be as painless as WiFi – turning your computer on will automatically connect you to the closest available WiMAX antenna.

WiMax (802.16e) is a newer standard of wireless networking designed to provide the last mile of high speed internet access to the end user. Some people would call Wimax WiFi on steroids but this would be to broad of an assessment. Wifi was and still will be used in LAN environments for the foreseeable future. WiMax was designed to provide (MAN) Metropolitan Area Access, to homes and businesses.

Engineers are stating that WiMax has the capability of reaching 30 Miles but real world testing has shown 4-8 mile working radius.

How WiMax works

WiMax (MAN) deployments are similar to a WiFi network. First the ISP would have their T3 or higher access. The ISP would then use line of sight antennas (Bridges) to connect to towers that would distribute the non line of sight signal to (MAN) residential/business clients.

WiMax line of sight antennas operate at a higher Frequency up to 66mhz. Distribution antennas do not have to be in the line of sight with their clients. Non – line of sight towers operate on a range similar to WiFi . WiMax can operate right next to cell phone towers with no interference.

Problem associated with WiMAX

QOS (Quality of Service) is an major issue with WiMax because of the number of people accessing a tower at once. Some would think that a tower could be easily overloaded with a lot of people accessing it at once.

Solution

Built into the WiMax standard is an algorithm that when the tower/base station is nearing capacity then it automatically will transfer the user to another WiMax tower or cell. Unlike a Wifi clients who have to kind of fight to stay associated with a given access point; WiMax will only have to perform this hand shake at the MAC level the first time they access the network.

Where is WiMax suitable to use

WiMax is designed for building a network infrastructure when the environment or distance is not favorable to a wired network. Also, WiMax is a cheaper and quicker alternative than having to lay wire. Third world countries will greatly benefit from deploying WiMax networks. African countries are now going to start deploying WiMax networks instead of cell phone networks. Disaster zones can also utilize WiMax giving them the ability to distribute crisis information quickly and cheaply.

Militaries are already using wireless technology to connect remote sites. Logistics will be simplified with the ease of tracking with RF technologies. WiMax can also handle Webcams and streaming video which would give commanders eyes on target capability. Just imagine if

planes were able to drop preconfigured self deploying WiMax antennas in strategic areas giving troops real time battlefield intel. Armed with wireless cameras, drones and a GPS one soldier would truly be an Army of One.

Wireless Network Security

ARTICLE BY: Rishabh Shah

There are many of us who make use of a WiFi network for internet access . But is the network that we are using secured enough to guarantee the confidentiality and privacy of the data sent over the WiFi Network.

Lets have a look at the **THREATS** and then their **SOLUTIONS**

1.SSId's (SSID are the name of the wireless routers) are useless:-

The 802.11 standard specifies the SSID (service set identifier) as a form of password for a user's radio NIC to join a particular wireless LAN. 802.11 requires that the user's radio NIC have the same SSID as the access point have to enable association and communications with other devices.

The use of SSIDs is a fairly weak form of security, however, because most access points broadcast the SSID multiple times per second within the body of each beacon frame.

Some network administrators turn off SSID broadcasting ,but a hacker can still sniff the SSID from frames that stations use when associating with an access point. They just have to wait until someone associates or re-assoicates (e.g when roaming) with the network.

Many administrators use default SSId's set by the vendors,like Cisco uses tsunami and most other vendors use the name of their company as the default SSID.

2.DHCP (DHCP assigns a dynamic IP address) weakens the security:-

wi-fi users are automatically assigned IP address when they connect.Thus even a hacker gets a legitimate IP address with which he can drill down into other users computer and access their confidential information!.This is a serious problem that many end users overlook, especially when operating from home and public networks.

3.Denial of service attacks

Another form of security attack is denial of service. In this case, the hacker might not steal any information. They just keep users from accessing services, either to gain some sort of competitive advantage or just have some devious "fun."

A mischievous person can use a wireless client to insert bogus packets into the wireless LAN with the intent of keeping users from getting access to services. A brute force way of doing this is to setup a relatively high power signal generator to produce enough RF interference to block other radio NICs from accessing the medium. The 802.11 MAC Layer is fairly polite and avoids transmitting when it senses other RF activity. This gives the intruder enough control to keep users from accessing network services for an indefinite period of time.

Since there is not a specific method by which we can provide security we have to use combination of the methods mentioned below

1.Make Your Wireless Network Invisible:-

Wireless access points can announce their presence to wireless-enabled computers. This is referred to as "identifier broadcasting." In certain situations, identifier broadcasting is desirable. For instance, an internet cafe.However, you're the only one who needs to know you have a wireless network in your home. To make your network invisible to others, see your access point's user manual for instructions on disabling identifier broadcasting.

2.Rename Your Wireless Network:-

Many wireless access point devices come with a default name. This name is referred to as the "service set identifier" (SSIS) or "extended service set identifier" (ESSID). The default names used by various manufacturers are widely known and can be used to gain unauthorized access to your network.

3.Encrypt Your Network Traffic:-

Your wireless access point device should allow you to encrypt traffic passing between the device and your computers. By encrypting wireless traffic, you are converting it to a code that can only be understood by computers with the correct key to that code.

The original encryption method, WEP (wired equivalent privacy), was found to be fundamentally flawed. WEP relies on a shared key, or password, to restrict access.Anyone who knows that key can enter the network.

The next generation of encryption, WPA (Wi-Fi Protect Access), is designed to leverage an 802.1X-compliant authentication server, but it can also be run similar to WEP in PSK (Pre-Shared Key) mode. The main improvement from WEP to WPA is the use of TKIP (Temporal Key Integrity Protocol), which dynamically changes the key to prevent the sort of cracking techniques used to break WEP encryption.

The most current form of encryption is WPA2. The WPA2 encryption provides even more complex and secure mechanisms including CCMP, which is based on the AES

4.Connect Using a VPN:-

Many companies and organizations have a virtual private network (VPN). VPNs allow employees to connect securely to their network when away from the office. VPNs encrypt connections at the sending and receiving ends, and keep out traffic that is not properly encrypted.

CAREERS IN WIRELESS

ARTICLE BY: Harsh Swaminarayan

The growing use of wireless and mobile technologies such as smart-phones and laptops is driving an increased need for qualified wireless network professionals. Businesses need to make sure these wireless devices are used effectively and securely within the company's network. As Cisco is the leader in Wireless LAN (WLAN) technology, a Cisco wireless certification will improve a network professional's standing with employers looking for these skills.

Cisco Wireless Certifications Available

Cisco Certified Networking Associate Wireless (CCNA Wireless) – This certification validates associate level knowledge needed to configure, implement and support wireless Cisco LANs in small to medium businesses and enterprise networks.

Cisco Certified Networking Professional Wireless (CCNP Wireless) – This professional level certification focuses on wireless networking principles and theory and the ability to create technical specifications based on network business requirements that result in successful installations.

Cisco Certified Internetworking Expert Wireless (CCIE Wireless) – Cisco's expert level wireless certification ensures the certificate-holder has broad theoretical knowledge of wireless networking as well as an advanced understanding of Cisco Wireless LAN technologies.

Preparing for Cisco Wireless Exams

To prepare for a Cisco Wireless exam, a network professional should take an appropriate training course from a reputable school. Many community colleges, technical training centers and career schools provide courses to prepare for these exams. Course options may include traditional classrooms, online courses, boot-camp style courses and self-study videos. Prices for training will vary depending on the course and style but may range from several hundred dollars for a self-study video to many thousands of dollars for a boot-camp course.

Exam Content

Cisco Certified Networking Associate Wireless (CCNA Wireless)- There is one exam required for this certification: "Implementing Cisco Unified Wireless Networking Essentials". It validates the test-takers knowledge of installing, configuring, operating and troubleshooting small to medium-sized WLANs. Topics include WLAN fundamentals, installation of a basic Cisco WLAN, installation of wireless clients, implementing security, operate basic Wireless Control System(WCS), and basic WLAN maintenance and troubleshooting.

Cisco Certified Networking Professional Wireless (CCNP Wireless) – There are four exams required for this certification as described below:

Conducting Cisco Unified Wireless Site Survey - This exam validates a test-taker's ability to plan and conduct a wireless site survey, to design an RF network and to conduct a post installation assessment to ensure compliancy.

Implementing Cisco Unified Wireless Voice Networks – This exam assesses the candidate's ability to integrate Voice over Wireless LAN (VoWLAN) services into the WLAN and to implement Quality of Service, MPLS networks, and high bandwidth applications into the wireless network.

Implementing Cisco Unified Wireless Mobility Services – This exam validates the candidate's ability to integrate mobility services into the WLAN, to tune and troubleshoot the WLAN, and to implement indoor enterprise mesh networks.

Implementing Advanced Cisco Unified Wireless Security – This exam assesses the test-takers ability to secure the wireless network from security threats via appropriate security policies and best practices, to properly implement security standards, and to properly configure wireless security components.

Cisco Certified Internetworking Expert Wireless(CCIE Wireless) - A two-hour written exam and an eight-hour lab exam must both be passed to earn this prestigious certificate. The written exam covers expert knowledge and skills required to plan, design, implement, operate and troubleshoot Wireless LANs in an enterprise environment. The lab exam requires the candidate to configure a series of networks to given specifications. The exam focuses on implementation of Autonomous Infrastructure, Unified Infrastructure, Unified Controllers and AP's, Unified WCS and Location and Voice over WLAN.

Cost

The cost of taking a written or computer-based exam will range from $80 to $350, depending on the exam. The CCIE Wireless lab exam can only be taken at a few locations around the world and will likely require travel. The cost to take the lab exam is $1400.

TRICKS N TRADES

Wireless Router (WiFi) Buying Guide

Almost every broadband router destined for the home market these days has Wi-Fi capability. In fact, it's been ages since we reviewed a router that *didn't* include radios for wireless networking.

One way *not* to choose is to go by the makers' advertised speeds, which seldom have much to do with reality. Some vendors go as far as using the "300" megabits-per-second speed in the names of routers that can't achieve anywhere near that throughput in the real world. Fortunately, the market is flooded with Wi-Fi routers, so finding a good one could be simpler than you might think, if you know what you're looking for.

We have put together a list of the nine key points you should consider when choosing a Wi-Fi router:

Is 802.11n (N) really that much better than 802.11g (G)?

Yup. Believe it or not, the 802.11g Wi-Fi router, which uses a technology that has been around for seven years, is still popular. Small businesses buy G routers because they are cheaper and perform adequately. Some 802.11g routers include specialized functions that are essential in business, such as powerful policy-based firewalls and threat-management features. In the home, however, speed is far more important, and there the 802.11n Wi-Fi router is king. Some N routers, such as the TrendNet Gigabit, can deliver upwards of 200 Mbps. 802.11n routers often deliver as much as five times as much throughput as G routers in real-world testing.

Are dual-band routers better than single-band routers?
802.11n routers come in two flavors—single-band and dual-band. Single-band routers use the 2.4-GHz band, the same frequency used by G routers. Dual-band N routers support 2.4-GHz and 5-GHz bands. Even at 2.4 GHz, 802.11n routers are faster than G routers because they make better use of the frequency range in the band, and they're better at bouncing signals off surrounding surfaces such as furniture and walls. Switching a dual-band N router from 2.4 GHz to 5 GHz is like trading a Toyota for a Maserati. The answer is, therefore, an overwhelming yes: Dual-band band routers, though generally more expensive, outperform single-band (2.4-GHz) routers.

Do I need two, three, or four antennas, or hidden ones?
Because the speed in N routers depends heavily on signal bouncing and multiple transmitters and receiver antennas, the ideal antenna configuration is 4-by-4. Generally, however, most high-end N routers come with a 3-by-2 or 3-by-3 antenna configuration.While antennas come in all shapes and sizes, most are visible, tubular antennas.

Should I get a portable router?
If you want or need to take your Wi-Fi on the road, a new breed of router making its mark is the portable. It can travel with you because it uses a 3G signal from a cellular carrier for backhaul, AKA the connection back to the Internet. This means it won't be as fast as hooking it up to your cable modem, but what you lose in throughput you gain in movement. Because they're not as fast, most of them only support 802.11g instead of the faster 802.11n, which also keeps the cost down. However, keep in mind that while the Wi-Fi side is free, you have to pay a carrier for the 3G.

What is guest access?
Guest access is one of the most useful, and most underrated, features of a wireless router. Routers with guest access, such as the Belkin N+ Wireless Router (F5D8235-4), can separate one Wi-Fi network into two. This allows friends to use your broadband access without knowing the password for your main network, so they can't get to your files. You can achieve a similar configuration with routers that support virtual LANs (VLANs), but the steps in setting up multiple VLANs are more difficult. We highly recommend this feature.

Tightening access to your router with MAC access control

If you are still not convinced that your wireless network is secure after encrypting your Wi-Fi router with Wi-Fi Protected Access 2 (WPA2)don't worry because this step ensures that only your computers can access your Wi-Fi network. MAC filtering allows or prevents computers with certain MAC addresses to access your network. Like a fingerprint, no two network adapters can have the same MAC address, so snooping neighbours are out of luck when you enable that MAC filter.

How many wired ports do I want?
The more the merrier. While most Wi-Fi N routers come with a standard five-port block, you'll be surprise how many don't—the Apple AirPort Xtreme and Apple Time Capsule, for example, have only four ports apiece. Adding a NAS device, an Xbox 360, a VoIP phone, and a PC will max out a five-port router. If your router has only three free LAN ports, you'll have to buy an extra Ethernet switch to accommodate extra network devices.

Turning your router into a gaming powerhouse
No one wants their Internet games to interfere with YouTube videos, Skype calls and Web surfing, or vice versa. The answer lies in the QoS feature in your router. A router with QoS can separate network packets and prioritize your network traffic, allowing your most important applications (i.e. games) to get the largest bandwidth chunk. Luckily, games don't take up a lot of bandwidth, but they can slow your network down when you are sharing the connection with the family.

Is a router with a strong firewall important? Luckily, most routers include a firewall, and many use the SPI (stateful packet inspection) firewall, which is better than the older NAT firewall alone. A few routers, such as the SMC Barricade N Wireless Broadband Router (SMCWBR14S-N2), provide a range of manual settings on a firewall. Are these routers better? Not really. Typically, manual firewall settings are designed for specific usage needs and not for enhancing the overall capability of a firewall. As long as a Wi-Fi router has a SPI firewall, that's enough for most us.

Can home routers meet the needs of small businesses?
For the most part, yes . However, sometimes businesses need extra security or technologies that are not available in some home routers.

What's the best way to access your router remotely?
Routers like the Netgear WNR3500, which support dynamic DNS—as in the Dyndns.org or TZO.com services—are the best to buy if you want to access your network remotely. With dynamic DNS, you can gain access by using a domain name like myhomenetwork.net instead of using the IP address provided to you by your ISP.

How to hack wireless network :

http://www.youtube.com/watch?v=TiPWUykw3uU

BLUETOOTH

ARTICLE BY: Dilkush Patel

Bluetooth one of the most exciting technogy that young generation uses every now n then without havin slightest of knowledge of how that works. Bluetooth is really a very exciting technology to learn.

Bluetooth exists in many products, such as telephones, the Wii, PlayStation 3, PSP Go, Lego Mindstorms NXT and in some high definition watches, modems and headsets. The technology is useful when transferring information between two or more devices that are near each other in low-bandwidth situations. Bluetooth is commonly used to transfer sound data with telephones (i.e., with a Bluetooth headset) or byte data with hand-held computers (transferring files).

Bluetooth is a proprietary open wireless technology standard for exchanging data over short distances (using short length radio waves) from fixed and mobile devices, creating personal area networks (PANs) with high levels of security.

Bluetooth uses a radio technology called frequency-hopping spread spectrum, which chops up the data being sent and transmits chunks of it on up to 79 bands of 1 MHz width in the range 2402-2480 MHz. This is in the globally unlicensed Industrial, Scientific and Medical (ISM) 2.4 GHz short-range radio frequency band.

Bluetooth provides a secure way to connect and exchange information between devices such as faxes, mobile phones, telephones, laptops,personal computers, printers, Global Positioning System (GPS) receivers, digital cameras, and video game consoles.

The Bluetooth specifications are developed and licensed by the Bluetooth Special Interest Group (SIG). The Bluetooth SIG consists of more than 13,000 companies in the areas of telecommunication, computing, networking, and consumer electronics

To be marketed as a Bluetooth device, it must be qualified to standards defined by the SIG.

Some of the advantages of Bluetooth

Universally accepted - Bluetooth technology is accepted world wide, with it gaining so much popularity, you can rely on it for years to come with an advent of more and more devices started to use Bluetooth technology.

Automatic – setting up Bluetooth connectivity is automatic Bluetooth and doesn't need professionals. When two or more devices enter a range of up to 30 feet of each other the communication automatically begins between them.

Upgradeable - Upgradeable Bluetooth standard versions of Bluetooth in the offer various new advantages and backward compatibility with older versions.

Low power consumption - Bluetooth with the help of low power signals technology requires very less energy reducing the battery consumption or electrical power.

Best alternative to data transfer - in case of corrupt flash/pen drives or DVD/CD ROM. It has helped a lot of times when I forgot my pen drive.

List of applications of Bluetooth

- Wireless control of and communication between a mobile phone and a hands-free headset. This was one of the earliest applications to become popular.
- Wireless networking between PCs in a confined space and where little bandwidth is required.
- Wireless communication with PC input and output devices, the most common being themouse, keyboard and printer.
- Transfer of files, contact details, calendar appointments, and reminders between devices with OBEX.
- Replacement of traditional wired serial communications in test equipment, GPS receivers, medical equipment, bar code scanners, and traffic control devices.
- For controls where infrared was traditionally used.
- For low bandwidth applications where higher USB bandwidth is not required and cable-free connection desired.
- Sending small advertisements from Bluetooth-enabled advertising hoardings to other, discoverable, Bluetooth devices.
- Wireless bridge between two Industrial Ethernet (e.g., PROFINET) networks.
- Three seventh-generation game consoles, Nintendo's Wii and Sony's PlayStation 3 and PSP Go, use Bluetooth for their respective wireless controllers.
- Dial-up internet access on personal computers or PDAs using a data-capable mobile phone as a wireless modem like Novatel mifi.

- Short range transmission of health sensor data from medical devices to mobile phone, set-top box or dedicated telehealth devices.

A personal computer that does not have embedded Bluetooth can be used with a Bluetooth adapter or "dongle" that will enable the PC to communicate with other Bluetooth devices (such as mobile phones, mice and keyboards). While some desktop computers and most recentlaptops come with a built-in Bluetooth radio, others will require an external one in the form of adongle.

Unlike its predecessor, IrDA, which requires a separate adapter for each device, Bluetooth allows multiple devices to communicate with a computer over a single adapter.

Bluetooth v4.0 is the latest specification in world of Bluetooth. On April 21, 2010, the Bluetooth SIG completed the Bluetooth Core Specification version 4.0, which includes Classic Bluetooth, Bluetooth high speed and *Bluetooth low energy* protocols. Bluetooth high speed is based on Wi-Fi, and Classic Bluetooth consists of legacy Bluetooth protocols.

This is the end of Bluetooth for now will talk more about Bluetooth when we will talk about mobile technologies.

MBAcrackers.com
Live your dream

presents

Road to 100 percentile in CAT

Rs. 5515/- only

Test Series – 20 Full Length Online Mock CATs

Rs. 2206/- only

Join www.mbacrackers.com and avail exciting offers!

For more details, call us on:
(022) 3221 5553, (022) 3221 5554