

Applied Methodologies, Inc.



***AMILABS
LAB MANUAL***

November 2002

Table of Contents

<u>1.0 WHAT IS AMILABS?</u>	4
<u>1.1 LAB USES</u>	5
<u>2.0 THE LAB</u>	6
<u>2.1 NETWORKING COMPONENTS:</u>	7
Cisco Routers:.....	7
Cisco Switches:.....	8
Communication equipment:.....	8
<u>2.2 THE DMZ SEGMENT</u>	9
<u>2.3 AMILABS DEVICE IP ADDRESS LIST</u>	11
<u>2.4 NAVIGATING THROUGH THE ROUTERS AND SWITCHES</u>	12
2509 Terminal Server 10.1.1.60.....	12
Reverse Telnet into the lab.....	14
Getting to SW3(Catalyst 5505) by a double reverse telnet.....	14
<u>2.5 POWER MANAGEMENT</u>	16
<u>3.0 LAB FILE/APPLICATION SERVERS</u>	18
<u>3.1 WINDOWS SERVER - WIN2KSRV</u>	18
WIN2KSRV DETAILS.....	20
The server directory structure.....	21
<u>3.2 WIN2KSRV APPLICATIONS</u>	22
<u>3.3 LINUX SERVER – LINUXDEV</u>	39
<u>3.4 LINUX ROUTER - LINUXFWTR</u>	40
<u>3.5 A NOTE ABOUT THE LAB SERVERS</u>	41
<u>4.0 PROTOCOL ANALYZERS</u>	42
<u>4.1 AGILENT ADVISOR</u>	42
<u>4.2 LINUX SERVER PROTOCOL ANALYZERS</u>	58
<u>5.0 VOICE OVER IP TESTING</u>	59
<u>5.1 METHOD 1- CSIM FOR JUST IOS CONFIGURATION</u> <u>VALIDATION</u>	59
<u>5.2 METHOD 2 - USING THE PHONE DIALER PRO UTILITY</u>	60

6.0 ACCESSING THE LAB -- VPN INSTALLATION..... 64

7.0 WINDOWS 2000 TERMINAL SERVICES AND VNC..... 65

7.1 WINDOWS TERMINAL SERVICES CLIENT..... 65

7.2 VIRTUAL NETWORK COMPUTING (VNC) SETUP..... 67

8.0 DOCUMENTATION FILES INCLUDED IN THE VPN KIT..... 68

9.0 LAB POLICIES(DO'S AND DON'TS)..... 69

10.0 PRICING AND SCHEDULING..... 70

11.0 TECHNICAL SUPPORT..... 70

11.1 HARDWARE FAILURES..... 71

11.2 SOFTWARE FAILURES..... 71

11.3 RESCHEDULES..... 71

12.0 SPECIAL REQUESTS..... 72

13.0 DISCLAIMERS..... 72

Introduction

Welcome to the Applied Methodologies, Inc. Lab or AMILABS for short. AMILABS is an online network and general Computer Science research resource that is accessible from your office or home. The lab's purpose is to provide you the tools and resources necessary to prepare for industry certifications like Cisco's CCNA through CCIE or test a network/application change before committing such changes on your own production network. The lab can also be used for testing network, application, protocol and security technologies or learning new networking, protocol, server and application technologies. The lab can help you in upgrading your skills or act as a test bed for a solution you have been planning. So, welcome aboard and enjoy your research or training experience. This manual is your roadmap to gaining access to the lab and provides an outline of the lab's components and documentation files.

You should read this manual in its entirety before proceeding with any installation activity or accessing the lab. It is recommended that you get familiar with the lab through this manual as much as possible before going online. Also, you should plan out exactly what you want to test or practice before going online. These approaches ensure that you spend your initial access period achieving what you want out of the lab to save time.

Remember, have fun...

1.0 What is AMILABS?

AMILABS is a data communications and general Computer Science laboratory that is available for students and professionals to study various networking and computer industry technologies. The lab consists of Cisco routers and switches, AT&T CSU/DSUs, Agilent, IBM and other vendors networking products. The lab also contains various servers running Microsoft and Linux operating systems. The lab provides a "**SCRATCH PAD**" environment for a student or professional to learn new or sharpen existing skills plus provide a general research environment. The lab grew out of AMI's Consulting business research arm and Cisco certification requirements and can be used for your CCNA through CCIE preparation. The lab can also help you prepare for Microsoft, Linux, and any other general industry certification such as a the Red Hat Certified Engineer or CISSP security exam. The lab also lends itself for testing hacking exploits on the operating system and protocol levels.

1.1 Lab uses

Stating that this lab's uses are limitless is a little much. However, depending on your imagination and needs, you can use this lab to accomplish many things. Some uses are listed below:

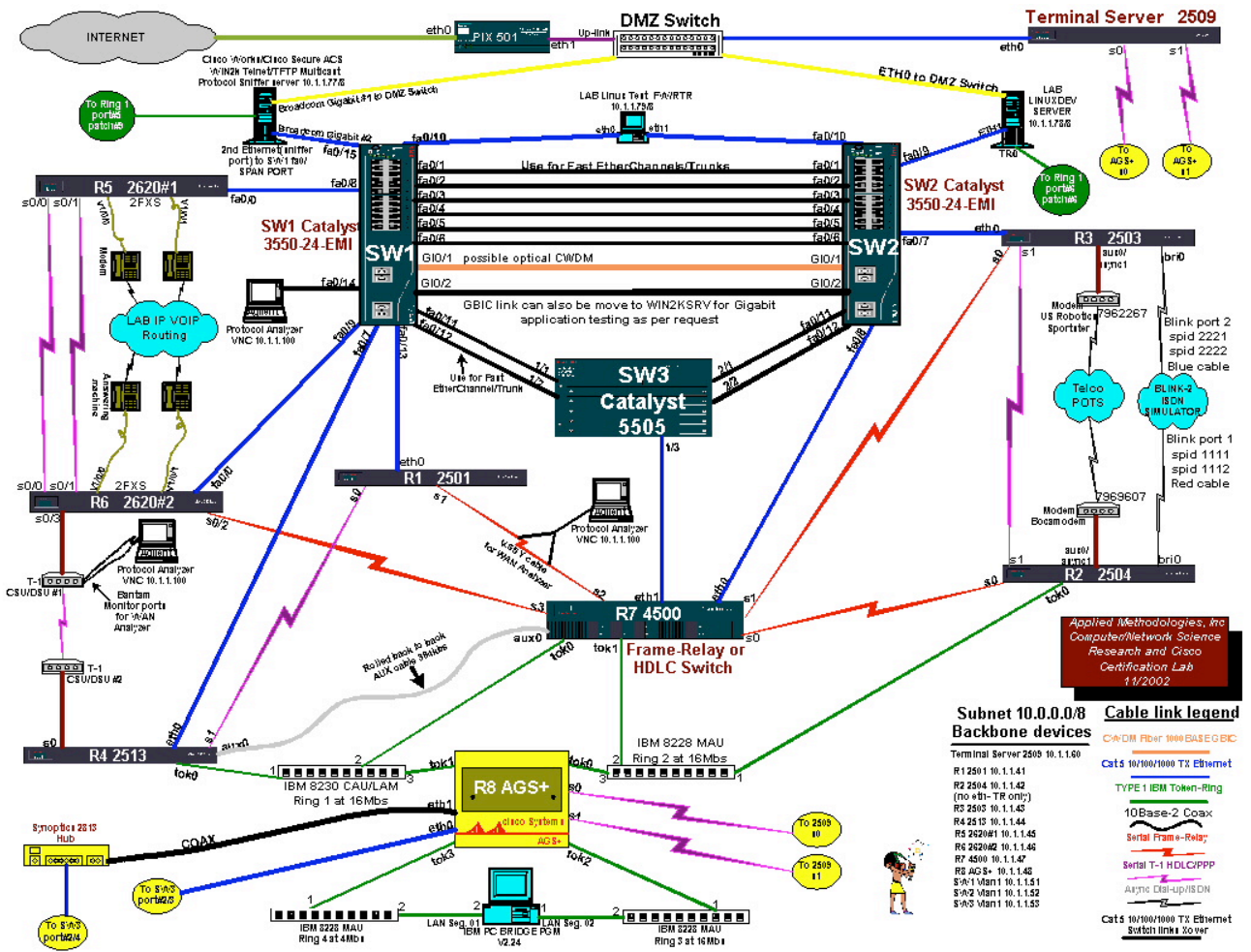
- Cisco certification preparation CCNA through CCIE.
- Testing Cisco based network configuration changes before committing on a production network.
- Researching and testing Cisco based network configuration and IOS options.
- Researching and testing general networking and application protocols.
- Computer and network operating systems research and testing.
- Security and hacking exploit research and testing.
- Application analysis research and testing.
- Application development and testing.
- Stress testing of routers, switches and servers for operational guidance, planning and experimentation with advance networking topics such as QoS, encryption, IPv6, IPSEC, MPLS and Multi-Layer Switching.
- Learning environment for Computer Science and networking subjects for university students.
- Learning environment on tools such as protocol analyzers, compilers, debuggers, traffic generators, network management applications et. al.
- Learn to use the protocol analyzer to analyze VOIP or run a BERT test on a T-1 line.
- Application and traffic analysis and management for technologies such as VOIP and Multicasting.
- Testing new applications, OS or IOS versions.
- By using Cisco routers and protocol analyzers students can really understand the mechanics of how protocols such as BGP, OSPF, Frame-Relay and others really work by not only looking at the Cisco debugging output but also by reviewing real-time packet traces of the protocols in action. This combination of tools helps to enforce your learning or research experience.
- Enhanced VOIP testing and analysis with the combination of Cisco routers and protocol analyzers by Agilent. The student or researcher can initiate a VOIP call from the server and trace it while generating traffic plus analyze the RTP session and QoS capabilities if implemented. This capability is available on LAN and WAN segments.
- For the programmers out there, develop IP based applications using LIBNET, a high level packet creation API. You can create any kind of ICMP, IP, TCP, UDP packet and inject onto the lab network for stimuli analysis. You can also create RIP, OSPF and possibly EIGRP and BGP packets.
- And much more.

For those of you using this lab for any Cisco certification this lab can do just about 95% of all the exercises in the Doyle I/II, Caslow, Halabi, Solie and most of the Cisco Press, Sybex, McGraw-Hill books and CCO examples. This lab has everything you need for the new CCIE changes as of November 4th 2002, except an ATM switch. The Catalyst 5505 and Token-Ring equipment are still available for those who want to learn some of the older equipment or need to test something but cannot do it on their production networks that still may have Token-Ring and or Catalyst 5ks. But remember, this lab can be used for more than just Cisco certification. The protocol analyzers, Windows and Linux servers are also useful for traffic/protocol analysis, application impact analysis, network programming, network modeling and security research and testing.

2.0 The LAB

The AMILABS network consists of a fully meshed LAN and WAN topology utilizing different physical and data link mediums and protocols. The lab network as depicted in **figure (2.1)** is also fully documented in the VISIO diagram named: **AMI NETWORK LAB** included in your VPN kit. The lab network diagram, and all diagrams in this documentation, are also available on the WIN2KSRV server(see [section 3.0 Lab File/Application Servers](#)) so you can make copies for yourself to depict the network in different logical views, you can save your diagrams in your own subdirectory, share them with other students or copy them to your personal computer over the VPN.

Figure (2.1).



The diagram is your map to this scratchpad network. You can reconfigure any device and protocol address in any way. The diagram provides the full PHYSICAL connectivity layout of the lab. All port and interface designations are depicted to simplify your grasp of the network. The layout of the servers and protocol analyzers are also depicted for your ease. The logical configuration of this network is dependent upon your creativity.

2.1 Networking components:

The communications network portion of the lab consists of the following equipment:

Cisco Routers:

- 2501 2 Serials 1 Ethernet
- 2503 1 BRI 2 Serials 1 Ethernet
- 2504 1 BRI 2 Serials 1 Ethernet
- 2513 2 Serials 1 Ethernet 1 Token-Ring
- 2509 2 Serials 1 Ethernet 8 TTY lines
- 2620#1 With 2 VOIP FX interfaces 4 serials 1 Fast Ethernet

- 2620#2 With 2 VOIP FX interfaces 2 Serials 1 Fast Ethernet
- 4500 With 2 Token-Ring, 4 serials 2 Ethernet interfaces
- AGS+ With 2 Ethernet, 4 Token-Ring 14 Serial interfaces*

*The AGS+ is available upon request only

All routers are loaded with the maximum of flash and system memory.

Cisco Switches:

Two Catalyst 3550 24 port Fast Ethernet plus active Gigabit interfaces with EMI software loaded (If demand picks up CWDM modules will be added)

One Catalyst 5505 with a Supervisor III module and NFFC II for MLS and Etherchanneling plus a 24 port 10/100TX Ethernet module

Communication equipment:

Blink2 ISDN emulator

Asynchronous Modems for Async. routing and POTS access for POTS dial routing

AT&T CSU/DSUs (Future access to these units so you can learn how to configure AT&T CSU's for example, from AMI to B8ZS)

IBM 8230 CAU and LAM and 8228 MAUs

Synoptics 2813 10Base-t Hub

IBM Token-Ring Bridge*

***The Token-Ring Bridge is available upon request only**

A Note about Token-Ring: For those of you lab users preparing for the Cisco CCIE exam, Token-Ring is no longer on the lab portion of the lab. However, Token-Ring may still be on the qualifying written portion. So, to help in your studies, Token-Ring technologies are available for your research to understand this protocol.

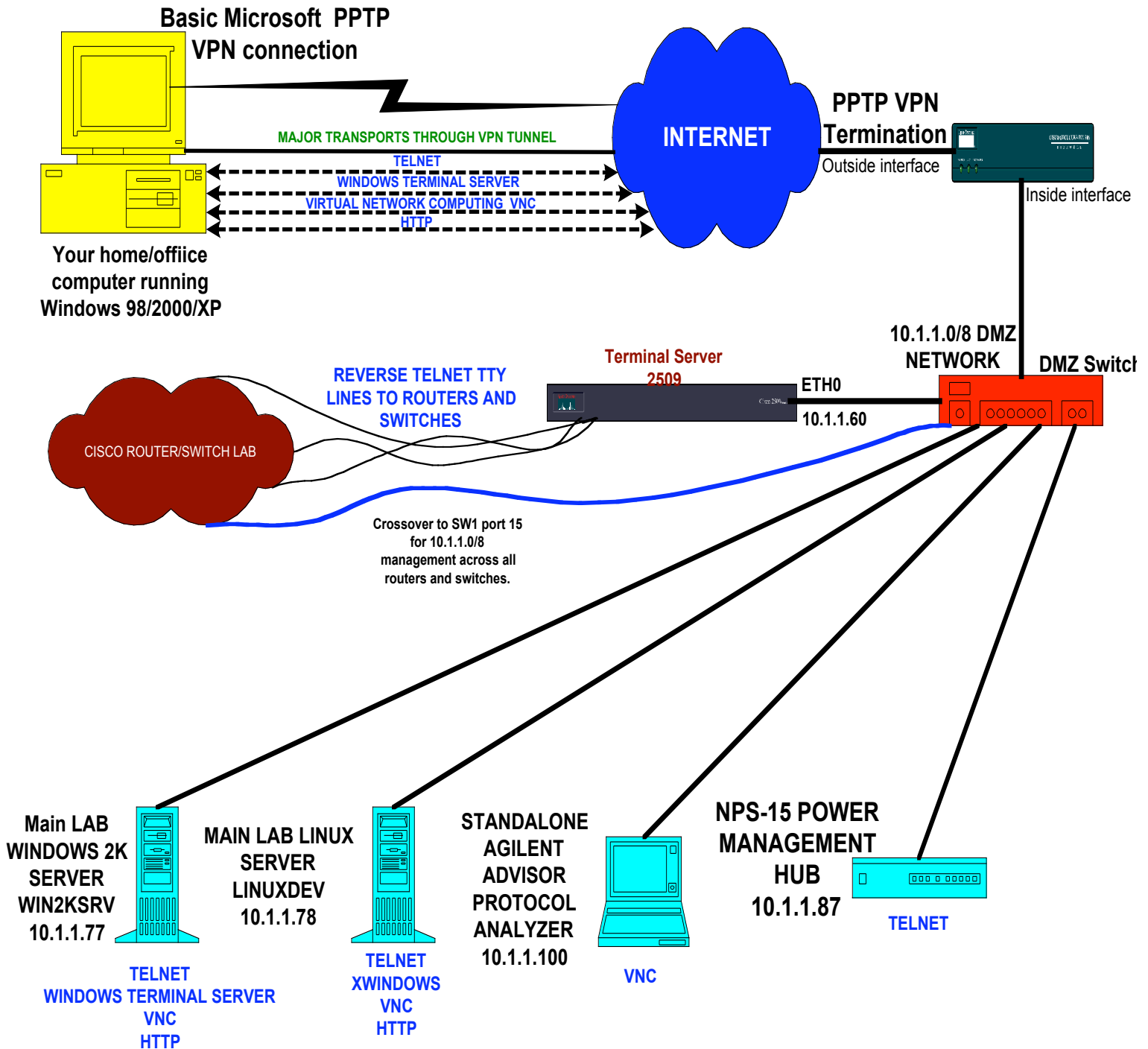
Token-Ring was also left in the lab for many corporations still have a viable amount of Token-Ring technology in their networks. You can use the Token-Ring components of this lab to reproduce a problem that you may be experiencing in the field, test a Token-Ring related change, test a migration approach from Token-Ring or test applications on Token-Ring and obtain a better understanding of Token-Ring for support purposes.

2.2 The DMZ segment

The lab's main user backbone is also a DMZ segment for the VPN connection. The DMZ segment hosts the 2509 Terminal Server and the lab servers outlined in following sections. Refer to **figure (2.2)** for a diagram of how you will be accessing this lab.

Figure (2.2).

AMILABS VPN Diagram



The DMZ segment consists of an unmanaged switch and its major network is 10.1.1.0/8. Please review **figure (2.2)** above or the VISIO diagram named: **VPN LAYOUT**, included in your VPN kit, for an understanding of how you will access the lab. From the unmanaged switch a crossover cable is connected to SW1 for 10.1.1.0/8 connectivity whenever you need it from the lab server's 10.1.1.0/8 interfaces. All lab servers have a second network adapter that is fully addressable for you to use in your lab (any Subnet/VLAN) thus not requiring the crossover cable from the DMZ segment into the lab switches.

All router Ethernet interfaces are currently set to a 10.1.1.0/8 address for default access in the DMZ/BACKBONE. If the Crossover connection to the DMZ is in effect you can telnet from the 2509 terminal server to any 10.1.1.0/8 devices like the AGS+ which is not supported on the terminal server. You can change these interfaces to run on different VLANS since the main connectivity is via the console ports from the 2509 Terminal Server.

You can save your configurations to any of the servers in the lab. You can also load different IOS images from any of the servers. If you need a newer IOS version you can download it from the web via a Windows Terminal Services session to the WIN2KSRV servers then TFTP it to your router or switch.

A full listing of the 10.1.1.0/8 lab device addressing is listed on the lab diagram **figure (2.1)** as well as below:

2.3 AMILABS Device IP address list

Router1	10.1.1.41	used for TFTP and management can be changed
Router2	10.1.1.42	“
Router3	10.1.1.43	“
Router4	10.1.1.44	“
Router5	10.1.1.45	“
Router6	10.1.1.46	“
Router7	10.1.1.47	“
Router8(AGS+)	10.1.1.48	main Ethernet cannot be changed others can
Switch1	10.1.1.51	used for TFTP and management can be changed
Switch2	10.1.1.52	“
Switch3	10.1.1.53	“
2509 Terminal Server	10.1.1.60	cannot be changed
WIN2KSERV	10.1.1.77	cannot be changed, second adapter can be
LINUXDEV	10.1.1.78	cannot be changed, second adapter can be
LINUXFWTR	10.1.1.79	cannot be changed, second adapter can be
WTI Power strip	10.1.1.87	cannot be changed

Standalone Agilent Advisor Protocol Analyzer 10.1.1.100 cannot be changed

Note: Network 10.1.1.0/8 is the lab's Ethernet and DMZ backbone. You cannot change the Ethernet address of the 2509 Terminal Server router from 10.1.1.60. To manage the lab from the 10.1.1.0/8 network just enable the Crossover connection on SW1 port 15 and assign that port to any manageable VLAN of your choice that is in the 10.1.1.0/8 network. Then address you routers and switches to the 10.1.1.0/8 network for manageability. All of the lab servers have one of their Ethernet interfaces on the 10.1.1.0/8 backbone for IOS downloading and SNMP testing from Cisco Works, Cisco Secure and other utilities.

Be careful of your VLAN and Spanning Tree testing if you cause a loop on the VLAN while connected via the crossover cable to the DMZ 10.1.1.0/8 network you may lose connectivity to the terminal server and will not be able to get it back. Remember, you have second adapters on the servers to test applications and management functions so the only real use of the crossover cable is if you wanted to store configs. etc. directly to any 10.1.1.0/8 lab device or to any lab sever to save time. If you do run into problems using the crossover link and servers between the DMZ and your VLAN configurations follow the procedures in section 11.0 Technical Support.

All router Ethernet interfaces are currently set to a 10.0.0.0/8 address for default access in the DMZ/BACKBONE. If the Crossover connection to the DMZ is in effect you can telnet from your PC over the VPN to additional 10.1.1.0/8 devices like the AGS+ or the power strip to reboot devices. You can change the interfaces(as listed in section 2.3) to run on different VLANS since the main connectivity is via the console ports from the terminal server.

The **default** setting for the entire lab of routers and switches is everything connected to **VLAN1** in the **10.1.1.0/8** network.

2.4 Navigating through the routers and switches

2509 Terminal Server 10.1.1.60

To access the 2509 Terminal Server from you PC open a telnet connection over the VPN to address **10.1.1.60**. This will be your main access to the routers and switches in the lab. 10.1.1.60 is a 2509 router terminal server. Shown below in **figure (2.3)** is the login banner you will see when you log into the 2509 Terminal Server via a Telnet connection from your PC to 10.1.1.60. The banner contains with instructions on how to perform a reverse telnet:

Figure (2.3).

```

*****
*****
*****
*****
*****
*****
*****
*****
*****
*****
*****
*****
*****
*****
*****
*****
*****
*****
*****
*****
*****
*****
*****
*****

Welcome to the Applied Methodologies, Inc.
Computer Science LAB and Network

*****
*
*   Unauthorized access is prohibited
*
*   Offenders will be prosecuted to the full extent of the LAW!
*
*   We are currently watching your steps!
*
*****

User Access Verification
Username: amilab
Password: C

*** Welcome to the AMI Network ***

AMI LABS provides you access to its data network communications lab for research
and educational uses only. AMI is not responsible for any malicious code created
or launched from this lab that results in any activities deemed criminal or
resulting in another user's or business's Internet site or internal computer
systems to be compromised, destroyed or denied access to any internal network or
the Internet.

This lab consists of the following Cisco routers and switches as well as other
data communications equipment for your research and training activities. There
are also several Servers that are accessible for storage of configuration files
and notes. These servers can also be used for testing operating system
applications and protocol exploits.

The main entry point into the lab is via the 2509 router(Terminal Server).
There is a series of IP HOSTS defined to access all of the other routers and
switches via reverse telnet.(ctrl+shift+6 key sequence then press X) This 2509
is not fully configurable. You can change the configuration on the serial ports
as per request. This is your DMZ connection. All other routers and switches are
fully configurable. There are other devices accessible in this lab for you to
use so please see the README file included in your VPN kit.

The following is the layout of host access to each lab device. To access a
device just type it's name, i.e. type r1 to access a 2620 router. Type WIN2KSRV
to telnet to a Windows 2k server et al.

ROUTERS
R1 is a 2501
R2 is a 2504
R3 is a 2503
R4 is a 2513
R5 is a 2620#1
R6 is a 2620#2
R7 is a 4500
R8 is a AGS+ (this is a telnet connection)

SWITCHES
SW1 is a 3550
SW2 is a 5505(this is a reverse telnet via the Aux port on the 2509)
SW3 is a 2924C-XL-EN
(this is a DOUBLE reverse telnet via the Aux port on ROUTER#1)
SW4 is a 2924XL
(this is a DOUBLE reverse telnet via the Aux port on ROUTER#7)

A DOUBLE reverse telnet is(ctrl+shift+6+6 key sequence then press X)

SERVERS
WIN2KSRV (this is a telnet connection)
LINUXDEV (this is a telnet connection)
LinuxFWRTR (this is a telnet connection)

WIN2KSRV is a windows 2k server running various applications as well as a TFTP
server. you have full access to this server via Telnet and Terminal Server
client included in your VPN kit.

LINUXDEV is a Linux scratch pad server for application development and Linux
training you have full super user access on this box to play around
and research. Access to this server is via Telnet and/or VNC Viewer
included in your VPN kit.

LinuxFWRTR is a Linux configured Firewall and Router to test Firewall
technologies such as IPTABLES and Linux Routing. Access to this server is via
Telnet and/or VNC Viewer included in your VPN kit.

Type MENU at the 2509# prompt for help...

*****
2509#

```

Reverse Telnet into the lab

A note about accessing routers and switches via reverse telnet: There are more devices than there are terminal lines on the 2509 Terminal Server router. So the first 8 devices, routers 1 through 7, SW1 are handled by the 8 terminal lines in a traditional manner. To get to SW2(the second 3550) you have to clear the aux port before typing SW2 on the terminal server You have to clear the AUX line by using the command:

CLEAR LINE AUX 0 or type in **CLA** (this is an alias of the previous command)

Then type in **SW2** to access SW2 – The second 3550.

Since the 2509 Terminal server only has 8 terminal lines, 1-8 are for the routers and the first switch(3550) line 9(AUX 0) on the 2509 Terminal Server goes to the SW2(second 3550) console's port. To get to switches SW3 you can either telnet to it if the crossover cable in SW1 is active by typing SW3 from the 2509 Terminal Server or use a double reverse telnet.

Getting to SW3(Catalyst 5505) by a double reverse telnet

Since this switch may not be used as often its ports are turned off but you can use them with SW1 and SW2 to create complex Trunking, Etherchannels and Spanning Tree configurations.

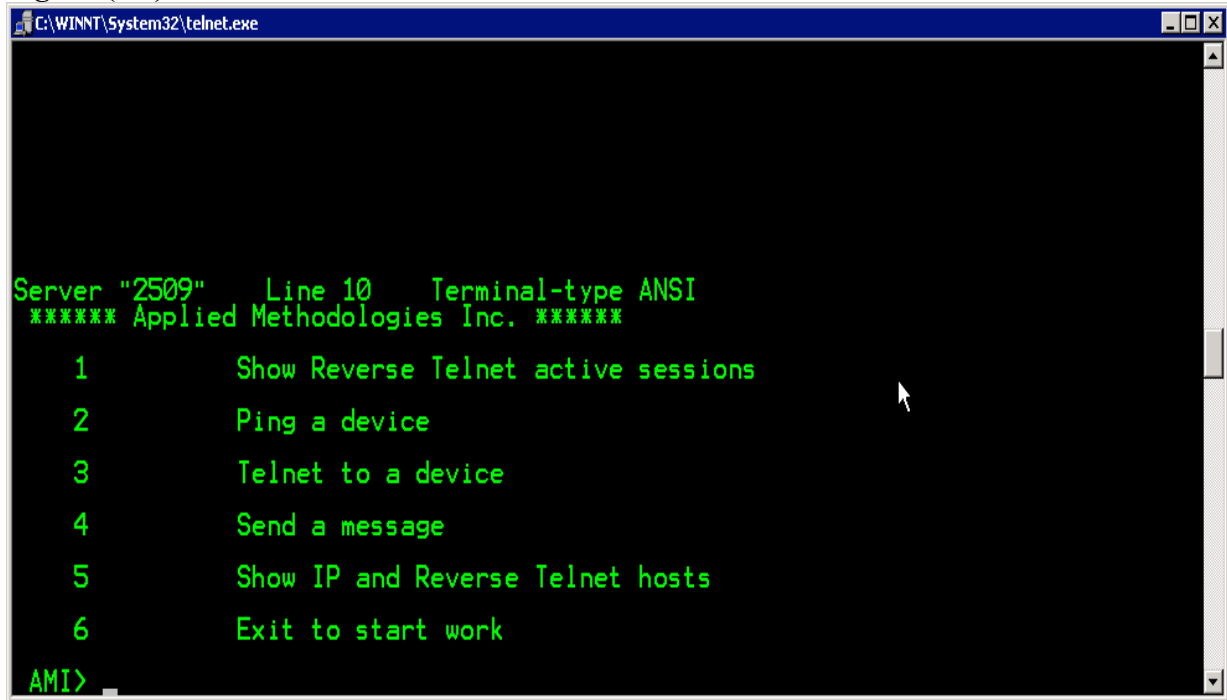
To get to **SW3(5505)** reverse telnet to **Router1** from the 2509 Terminal Server and then at the **Router1** prompt type in **SW3**. This will put you into SW3 via the Router1's AUX port. You may need to clear the AUX port(**use the CLA command**) just like on the 2509 Terminal Server. To get back to the 2509 Terminal Server just execute a typical reverse telnet. To just jump back one level to Router1 execute a **ctrl-shift-6-6 then X**

The information above about reverse telnet is also displayed again during your login into the 2509 terminal server. Just scroll back to see the instructions again.

It is recommended that you use the 2509 Terminal Server to access all Cisco routers and switches. All routers and switches with the exception of the 2509 Terminal Server and the AGS+ do not have login and enable passwords set. This makes jumping around these devices and jumping between user and privilege(enable) exec modes easier from the 2509 Terminal Server. You will have to add enable passwords to these devices(any telnet only device like the AGS+) if you wish to use privilege(enable) modes via Telnet to any of these devices once you set or use the existing IP address on them. All passwords for the routers and switches are listed in a file called Lab Passwords included in your VPN kit.

The 2509 Terminal server also has a help menu for your use to get a quick look at your terminal sessions and connections. At the **2509#** prompt type **menu** to get the following help menu as depicted in **figure (2.4)**.

Figure (2.4).

A screenshot of a Windows telnet window. The title bar reads 'C:\WINNT\System32\telnet.exe'. The window content shows a green text prompt 'Server "2509" Line 10 Terminal-type ANSI' followed by a separator line '***** Applied Methodologies Inc. *****'. Below this is a numbered list of six menu options: 1 Show Reverse Telnet active sessions, 2 Ping a device, 3 Telnet to a device, 4 Send a message, 5 Show IP and Reverse Telnet hosts, and 6 Exit to start work. At the bottom left, the prompt 'AMI>' is visible. A mouse cursor is positioned over the text of the menu options.

```
C:\WINNT\System32\telnet.exe

Server "2509"   Line 10   Terminal-type ANSI
***** Applied Methodologies Inc. *****

 1      Show Reverse Telnet active sessions
 2      Ping a device
 3      Telnet to a device
 4      Send a message
 5      Show IP and Reverse Telnet hosts
 6      Exit to start work

AMI>
```

2.5 Power Management

WTI NPS-15 Power Management hub for router and server remote reboot capabilities. WTI 10.1.1.87

You can Telnet into this unit to reboot a router, switch or server. Refer back to **section 2.3 AMILABS Device IP address list** for the IP address to use to telnet to. Refer to the file included in you VPN kit named: **LAB PASSWORDS** for the password to use. You can also access this unit from the 2509 Terminal Server by typing **WTI** at the **2509#** prompt. Once you logged into this unit you will be presented with a screen as depicted in **figure (2.5)**

Figure(2.5).

```

C:\WINNT\System32\telnet.exe
Network Power Switch v3.00          Site: AMI LABS...

Plug | Name | Status | Boot Delay | Password | Default |
-----|-----|-----|-----|-----|-----|
2 | ROUTERS_5_6 | OFF | 5 sec | (defined) | ON |
3 | ROUTERS_1_2_3_4 | OFF | 5 sec | (defined) | ON |
4 | SWITCHES_1_2 | OFF | 5 sec | (defined) | ON |
5 | ROUTER7_SW3_SW4 | OFF | 5 sec | (defined) | ON |
6 | CAU/HUB/CSU/MODE | OFF | 5 sec | (defined) | ON |
7 | AMI_LAB_SERVERS | ON | 5 sec | (defined) | ON |
8 | Terminal_Server | ON | 5 sec | (defined) | ON |

Communication Settings: 9600,N,8,1
Modem Init. String: ATEM0M0Q1&C1&D2S0=1
Modem Disc. String: (undefined)
Disconnect Timeout: 15 Min
Command Echo: 0n
Command Confirmation: 0n

"/H" for help.
NPS>

```

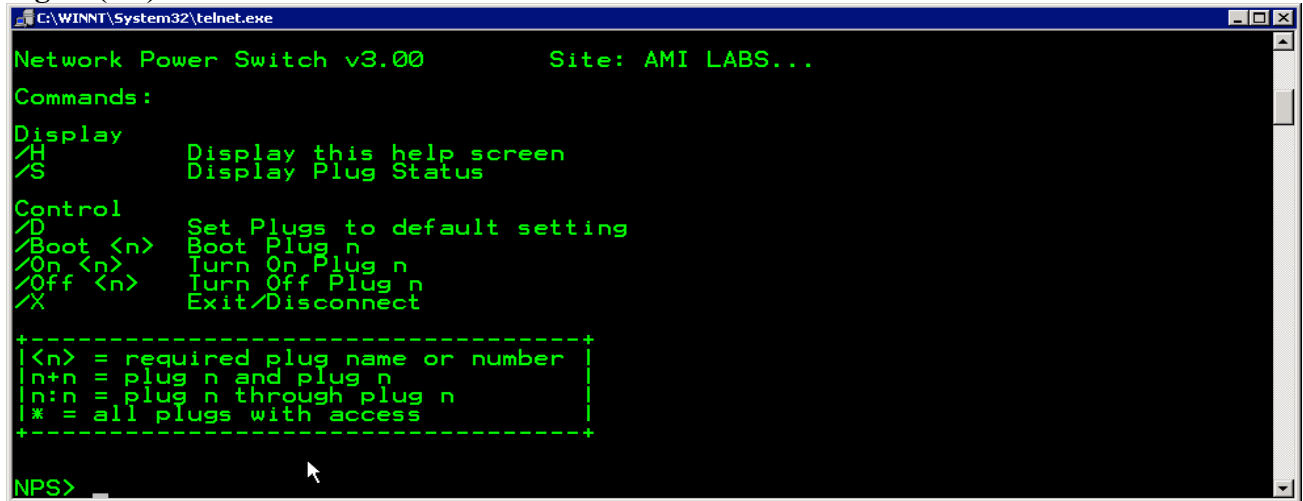
To turn off a plug with the appropriate devices on it at the **NPS>** prompt type **/off 3** for example to turn off the power to routers 1 through 4

To turn on a plug with the appropriate devices on it at the **NPS>** prompt type **/on 3** for example to turn on the power to routers 1 through 4

To reboot a plug with the appropriate devices on it at the **NPS>** prompt type **/boot 3** to reboot routers 1 through 4 with a 5 second boot delay.

To obtain online help, at the **NPS>** prompt, type **/h** for a list of commands and shortcuts as shown below in **figure (2.6)**.

Figure(2.6)



```
C:\WINNT\System32\telnet.exe
Network Power Switch v3.00      Site: AMI LABS...
Commands:
Display
/H      Display this help screen
/S      Display Plug Status

Control
/D      Set Plugs to default setting
/Boot <n>  Boot Plug n
/On <n>   Turn On Plug n
/Off <n>  Turn Off Plug n
/X      Exit/Disconnect

-----
<n> = required plug name or number
n+n = plug n and plug n
n:n = plug n through plug n
* = all plugs with access
-----

NPS>
```

The complete manual on how to use the WTI power switch is located on the WIN2KSRV server's desktop.



3.0 Lab File/Application Servers

The routers and switches are very easy to access and do not require any additional instruction. If your main use of this lab is for Cisco certification preparation then you already are familiar with navigating around a terminal sever for router and switch access. The lab servers are different and require a considerable amount more instruction so you can use them efficiently. You should use these servers even for your Cisco studies to save configs, generate traffic, download and swap IOS images and capture packet traces.

It is recommended that you read the server section in its entirety and become familiar with the servers before you access the lab...

The lab has three servers available for your research and training needs. There is a main Windows 2000 server and two Red Hat Linux servers. You can Telnet into these servers over the VPN to run command line utilities and console based applications as well as develop console based applications. The servers are also accessible via a Windows Terminal Sever(A Windows Terminal Services kit is included with the VPN kit) or Virtual Network Computing(VNC) so you can access the GUI based applications(protocol analyzers etc.) and utilities for your research and studies. Each server has two 10/100 Ethernet, interfaces installed for IP, IPX, Netbui/Netbios, DLC and other protocols. The server can act as a client or server for various applications. One such use is Multicast testing. Token-Ring server interfaces will be added shortly. The second adapter can also be your sniffer adapter to a switch SPAN port.

Server Hardware:

IBM eSeries X305 Server - Pentium IV 1.8Ghz 40Gb HD with 512 Mb ram running Windows 2000 Server. This server has 2 10/100/1000Mbs Ethernet interfaces installed.

IBM Netvista server - Pentium III 500 Mhz 20Gb with 296Mb ram running Red Hat Linux 7.2 Server. This server has 2 10/100Mbs Ethernet interfaces installed.

IBM PC350 running Red Hat Linux 7.0 operating as a Linux Router and firewall. This server has 2 10Mbs Ethernet interfaces installed.

3.1 Windows Server - WIN2KSRV

10.1.1.77

A Windows 2000 server running DNS, DHCP, WINS, Media Services, TFTP, FTP, Telnet, IIS and all of the other Windows services available under a standard Windows 2000 server.

Applications on the servers

- Adobe Acrobat reader
- AG groups EtherPeek
- Agilent Advisor protocol analyzer
- Agilent Advisor CBTs
- Analyzer shareware protocol analyzer
- Astricom BLINK-2 ISDN simulator management application - (The student can run ISDN traces from the Blink application)
- CiscoSecure ACS 2.6
- CiscoWorks 2000 3.2
- Cisco CD ROM documentation April 2002
- Cisco TFTP server
- Hummingbird Exceed software suite
- Libnet packet development APIs
- Mathsoft MathCAD
- Mcaster Multicast shareware utility
- Microsoft Office 2000
- Microsoft Visio 2000
- Microsoft SQL Server 2000
- Microsoft Visual C++
- Microsoft Visual Basic
- Microsoft Visual J++
- Modem test utility
- Modern Age Books Encyclopedia of Networking
- Full access to the internet to download any patches or updates to the applications and OS
- Nantech BGP traffic generator (trial version)
- NetScan tools
- NetSnoop utility
- Netscape communicator
- Network Toolbox 2.1
- Norton AntiVirus Corporate edition
- Phone Dialer Pro(for VOIP testing)
- PingPlus utility
- Pine Mountain Group PMG tools
- Pine Mountain Group documentation resources
- Protocols Come Alive protocol simulator from RADCOMM
- Real Player
- SnagIT
- Sybex Cisco exam book practice tests
- Tardis 2000 NTP server
- Virtual Network Computing VNC server and viewer
- Windows 2000 resource kit
- Windows Media Server
- Windows Media Player
- WinZip
- WS_FTP server
- Various CBTs, tutorials, documentation and standards references
- Packetyzer Protocol Analyzer
- LinkFerret Protocol Analyzer
- And much more...

WIN2KSRV DETAILS

The windows server WIN2KSRV is your main resource of tools, tutorials and utilities in the lab. Getting familiar with the server is important so you can get the most out of your lab experience. This section will cover instructions on how to access the server and the more popular applications that you will most likely use. Remember, there is plenty of “good stuff” on this server, like RFC indexes, protocol tutorials and so forth, so take advantage of all this information that is located at one source.

You can access this server in two ways. If your needs are simple like copying router configuration files and command line based, then you can Telnet to the server from your PC over the VPN by telnetting to the **10.1.1.77** address. You will be presented with a login and banner screen. Please reference the **LAB PASSWORDS** file included in your VPN kit for you access IDs. All users will share the same user ID and password. Since only one user at a time is in the lab there will be no overlap of resources.

You will have full administrator level access to this server so be careful in what you do. AMILABS has provided full access to the servers in the spirit of open access and knowledge sharing. Please refer to *section 9.0 Lab Policies/Do's and Don'ts* of this manual on server etiquette.

The second and more preferred method of accessing the server is via a Windows Terminal Services client, included in your VPN kit, or VNC also included in your VPN kit.

Since most of the applications, tools, and tutorials require a GUI this method will probably be your main method of using the server.

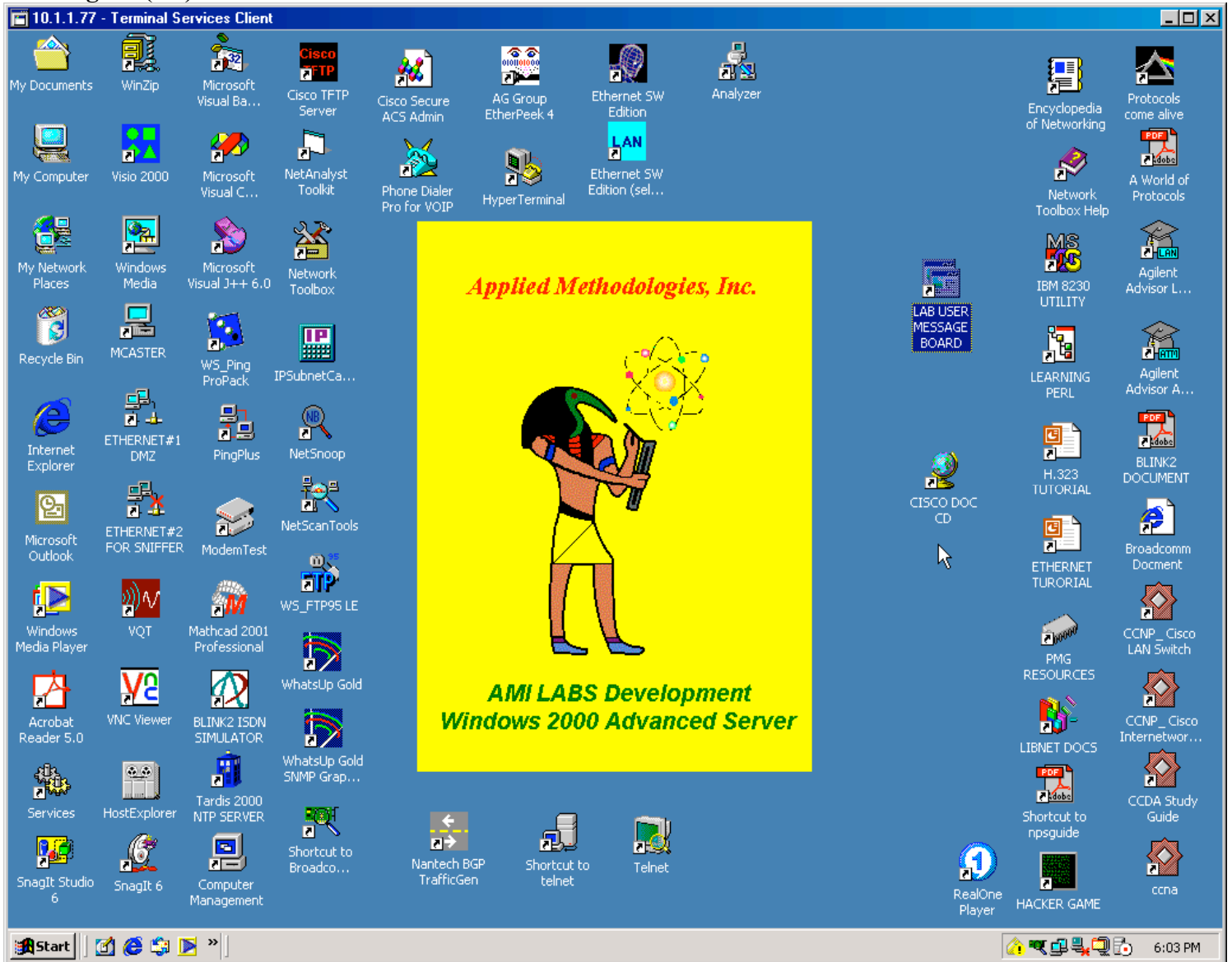
Windows Terminal Services is the recommend method to access the WIN2KSRV desktop for it functions more efficiently than VNC in terms of display control and crispness. VNC is available as a backup and is also used to access the NDIS adapters for the Software edition of Agilent Advisor protocol analyzer software. (Windows Terminal Services blocks the use of the NDIS adapters but VNC does not).

Section 6.0 describes the installation of Windows Terminal Services and VNC.

The left side of the desktop contains most of the application, tools and utilities icons you will use. The right side contains most of the icons for documentation, CBTs and other training links.

After you have installed the terminal server and logged in you will be presented with a desktop as depicted in **figure (3.0)**.

Figure (3.0).



The server directory structure

When you Telnet or use Windows Terminal Services client to gain access into the server you will have a default directory of labuser.

From within the labuser directory you should create you own personalized directory to store your Cisco configurations and any other research documents. Since these directories are seen by all users you can share your documents amongst them.

Directory structure on the server:

ANALYZER	A public domain protocol analyzer(desktop icon in place)
ASFRoot	Windows Media server files
CISCO	Cisco CD execution files
CISCO CERT	Various config. examples from cert. books
CISCO IOS	A directory hierarchy of different IOS Images for lab routes/switches
DOCUMENTS AND SETTINGS	Default OS document repository
DOWNLOADS	A directory where you can download utilities to from the Web
EDGETEST	Cisco Cert test directory (desktop icon in place)
HACKERGAME	Directory where hacker game is stored
IBM8230 UTILS	Directory where IBM 82330 CAU/LAM utilities are stored
INETPUB	IIS directory
LAB DOCUMENTATION	This is an important directory to consult for the documentation of many of the LAB applications, utilities and tutorials. Any tool or utility you download and install in the lab for your use and others should have a directory and documentation file here. This is also a general repository of reference documents.
LAB VPN DOCUMENTATION	A directory containing all of the files in your VPN kit for easy reference including the VISIO diagrams for your editing purposes.
LABUSER	This is your main directory to put shared documents and create subfolders for your specific files
LIBNET	C packet development API files
MCMASTER	Shareware Multicast utility(desktop icon in place)
PMG TOOLS	Pine Mountain Tools **Very Good** (desktop icon in place)
PROGRAM FILES	Where most of the applications are stored
SAMPLE PACKET TRACE	I have included some of my packet traces for your studies or research.
TEMP	A temporary directory to unzip apps. Please clean up when you are done.
WINNT	Main OS directory. Please be careful in here.

3.2 WIN2KSRV applications

If you are studying for a Cisco certification you will find many tools and reference links on the desktop to aid in your studies.

Cisco TFTP Server



You can use this tool or Windows TFTP to up/download configuration files and IOS images to the lab routers and switches. This tool is a little easier than the windows version. Just point the root directory to your directory under the LABUSER directory to store your configuration files.

Telnet



There are two telnet icons for your use in the lab. You can telnet from your PC over the VPN as discussed in the previous section to access the 2509 Terminal Server or to save on traffic depending on your links performance just use the Windows Terminal Services telnet desktop programs to access the 2509 Terminal Server or other lab devices like the Linux servers.

These are here for your ease of opening additional connections. One Telnet program is the standard Microsoft Telnet program the other is Exceed’s Telnet application. Each application has different benefits of use so depending on your needs they are both available.

Server network adapters. The server has two network adapters. These adapters can be managed with the following desktop icons:



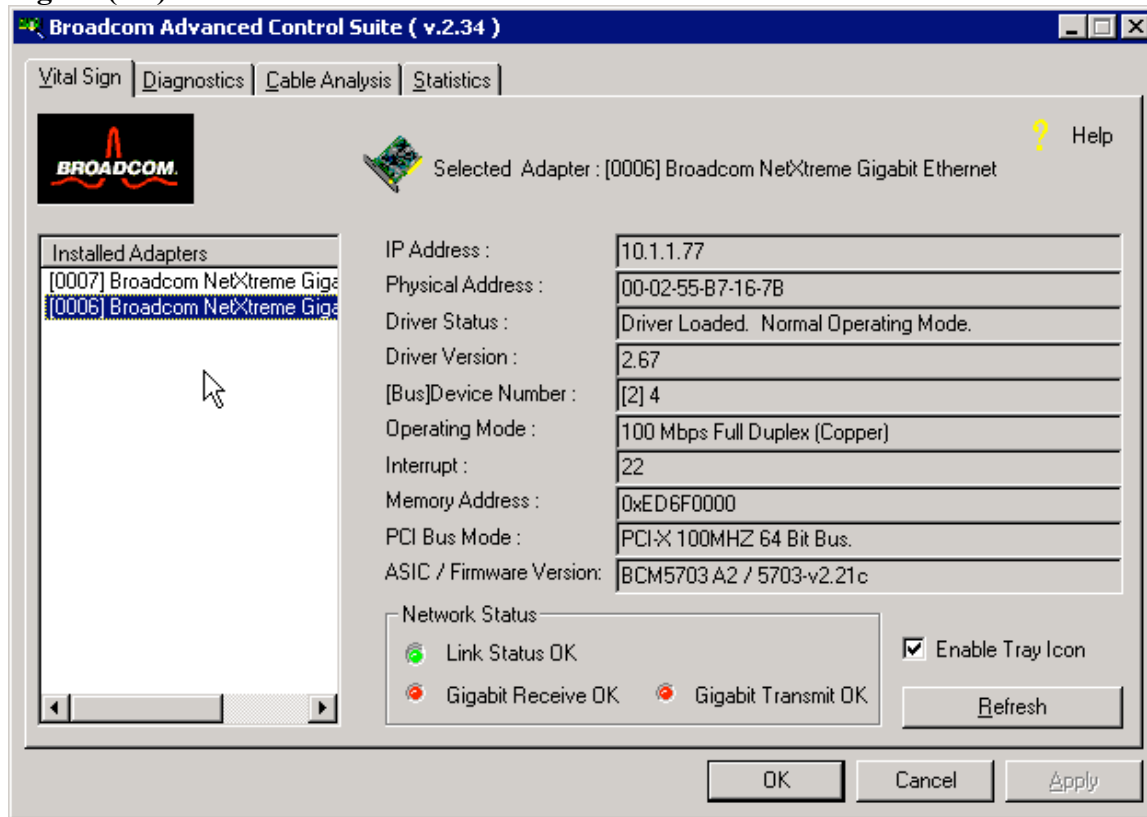
A note of caution about the adapters: They are represented differently in the various protocol analyzer software loaded on the server. You can use the adapter that has 10.1.1.77 assigned to it to “sniff” your DMZ(VLAN 1) segment but be careful on the mode of sniffing used. You may knock yourself off your Windows Terminal Services connection. If this happens please follow the directions in *section 10 Technical Support*.

A second broadcom adapter is available for addressing and sniffing. This adapter can have any address and belong in any VLAN of your choice. You can run server applications like Cisco Secure and multicasting server from this adapter and sniff at the same time. Any problems or conflicts in this adapter will not affect your Windows Terminal Services session. Please refer to *section 4.0 Protocol Analyzers* for details about adapter selection. To check to see which Broadcom adapter is assigned what MAC address and IP address easily you can click on the following icon on the desktop:



You will get the following screen as depicted in **figure (3.1)**.

Figure (3.1).



You can check adapter status and run diagnostics from this utility.

WIN2KSRV Services



The Services Icon is available to start and stop services and applications. For example DNS, DHCP, WINS and other services are currently stopped by default. If your testing/research requires such services, just configure the service, start the service, and perform your testing. When you are completed with such testing please remember to turn off the service for the next user.

Windows Media



This is an actual Windows Media Multicasting server. You can learn how to produce multicasting content and send it out over the lab network. You can learn how to use Windows Media sever. You can combine learning the Windows Media server application with your Cisco multicasting research and certification studies. One example is to create or add your own media files, you can download these from the web, multicast them out of the main interface 10.1.1.77 side, over the crossover cable into your lab then have your Cisco configured multicasting setup direct the multicast back onto the second interface where you can have Windows Media player receive it. All of this is happening in the lab, remember you can sniff this too, and only the screen shots are crossing the VPN.

MCASTER



MCASTER is a quick and dirty multicasting server utility to test your Cisco Multicasting configurations. Use of this utility is primarily for Cisco configuration testing without the need of multicasting receivers and so forth.

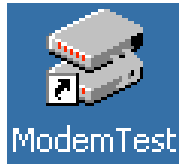
Phone Dialer Pro



This application is used for your Cisco VOIP testing.

The Phone Dialer Pro or HyperTerminal utilities are used to access the COMM ports on the server. The COM. ports are connected to modems that connect to the VOIP routers. You can initiate calls from WIN2KSRV, run debug on your Cisco router, and trace it either from the stand-alone protocol analyzer or one of the protocol analyzers on WIN2KSRV. This is much more flexible than using CSIM on the router which locks up your current session. An answering machine is provided on another VOIP router so you can have 2 minutes of traffic to trace and test your QOS options. You can use HyperTerminal and AT commands as a quick and dirty tool to initiate VOIP calls or use in conjunction with Phone Dialer pro to have two different calls initiate at once, on different COM. ports and monitor, sniff and debug your configurations. Please refer to [section 5.0 VOIP Testing](#) for more details on how to test VOIP in this lab.

Modem test



Modem test is a quick little utility to check the status of the modems attached off the server. You can use this tool to initiate VOIP calls but the others mentioned above are easier to use.

BLINK2 ISDN Simulator



The lab contains a BLINK2 ISDN simulator. Most other rental racks use the BLINK2 but your only control is from the Cisco Router. From the WIN2KSRV you can console into the BLINK2 and run in-depth traces and change ISDN parameters such as SPIDS, Carrier Switch types et al. You can then save and load these configurations at your convenience. Below are some screen shots of the BLINK2 administration tool.

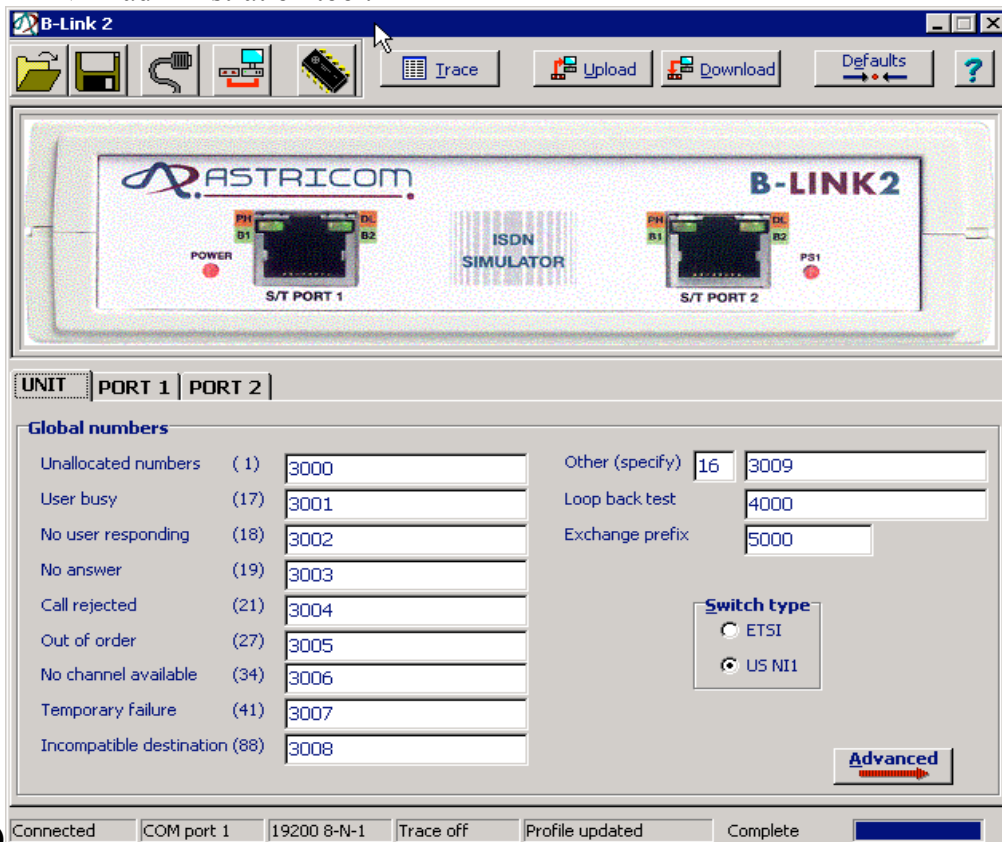
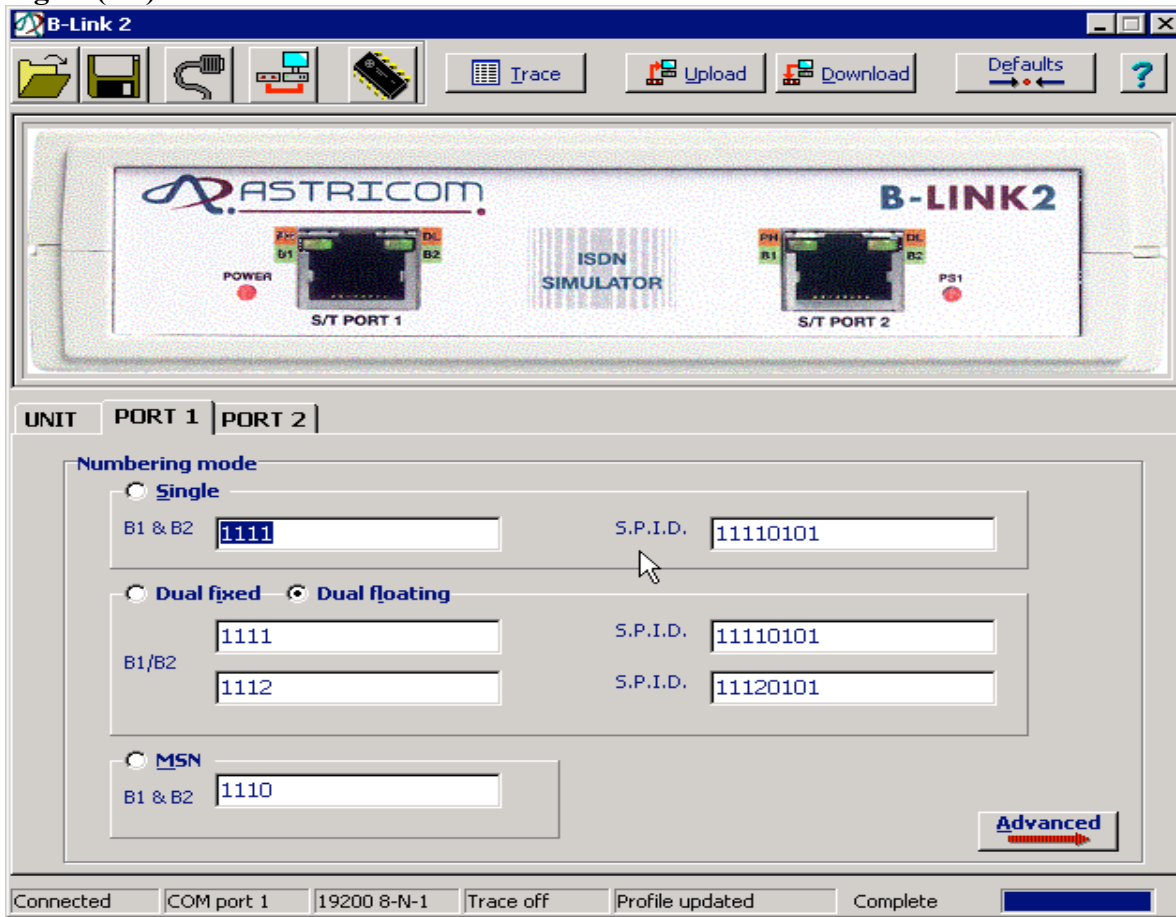


Figure (3.3)

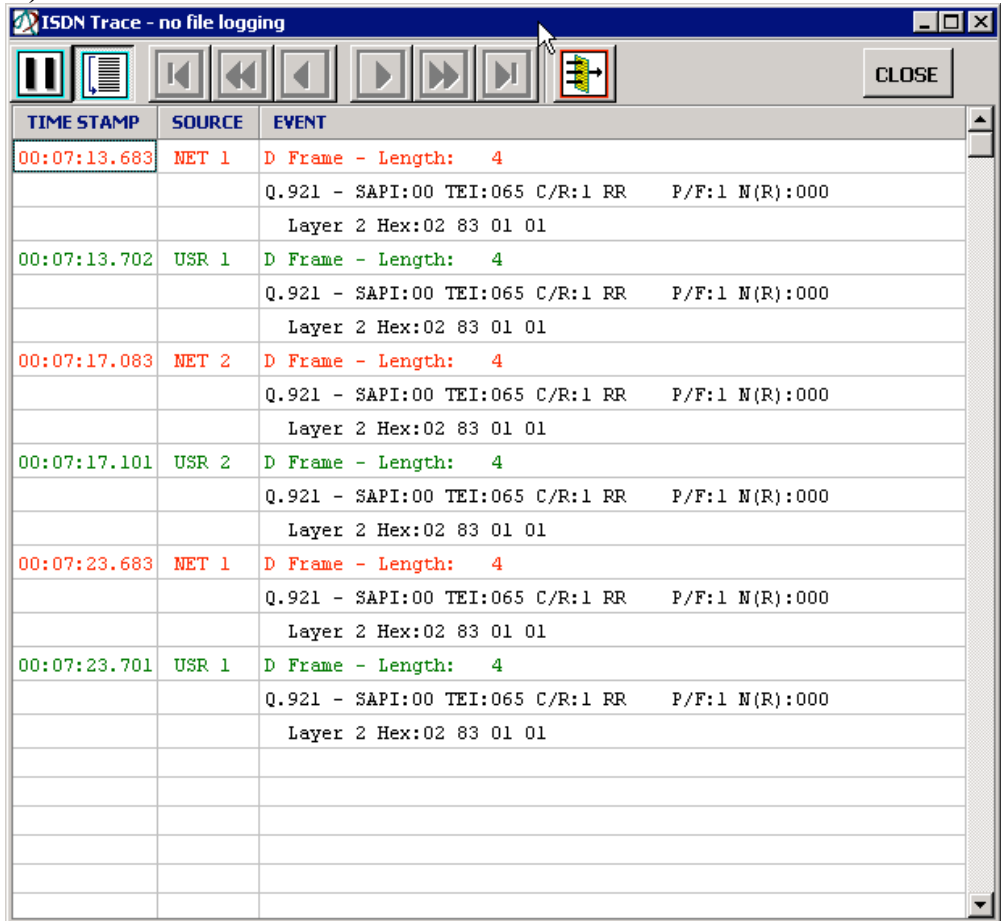
Select Port 1 or Port 2 to change SPID parameters:

Figure(3.4).

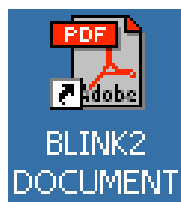


You can even run an in-depth ISDN trace to fully help your understanding of how the ISDN protocol suite works.

Figure (3.5).



BLINK2 Documentation



BLINK2 Documentation icon is located on the right side of you desktop. It is the PDF documentation on how to use the BLINK2 ISDN Simulator. Please reference before using the BLINK2 utility mentioned earlier.

Nanotech BGP trafficGen



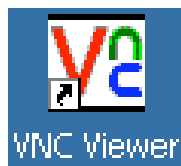
Nanotech BGP TrafficGen is a shareware utility that you can use to Generate BGP route traffic into the lab. This tool is great for your Cisco Certification studies. You can generate traffic on any of the WIN2KSRV interfaces, debug it on your routers and sniff the packets as well... This utility also generates regular traffic and you can set QoS levels for each generated stream to test various QoS configurations. This is a trial version so if demand picks up on its use a licensed copy will be added.

Tardis NTP 2000 Server



Tardis NTP 2000 Server is a shareware NTP server you can use on any of the WIN2KSRV interfaces for Cisco NTP testing. You can make WIN2KSRV the master server and have lab routers peer with this server. The server can obtain accurate times via the web. Another non-managed Tardis server is available on the 10.1.1.0/8 segment if you want to peer with that one. It is located at 10.1.1.254. However you will need the crossover connection into the 10.1.1.0/8 network to synchronize you lab routers and switches.

VNC Viewer



VNC Viewer is also available from the desktop. You can use this viewer to access the Linux servers and or the stand-alone Agilent Advisor protocol analyzer in the lab instead of running the view from your PC over the VPN. Your use either local on the WIN2KSRV or over the VPN is your choice based on performance or ease of accessibility(all apps running from the server). Refer to [section 6.0 Terminal Services and VNC](#) on how to use this application.

CISCO DOC CD



CISCO DOC CD contains the April CD of the Cisco Documentation in the Server's CDROM Drive, Drive D:

This is available for Cisco Certification students and general Cisco testing and research usages. You can also access the CCO web site by just initiating an Internet Explorer session.

Internet Explorer. Favorites are very good.



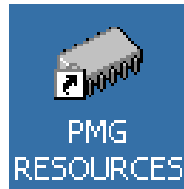
Internet Explorer is the default browser installed on this server. You can access the web from this server to reach other research sites, download configs, utilities or IOS images(if you have a CCO account), directly to the server. No need to use your PC's Internet connection do download such items and then transfer them over the VPN to the server. This step has been removed for your ease. The Favorites already includes a Computer Science folder with a plethora of networking and general computer science links. Some of the more popular Cisco topic links are included. You can rearrange these for your studying purposes. Other topics like Wireless and Network Security are available. Check them out or copy them to view from your own PC when you are not online in the lab.

NetAnalyst Toolkit ***VERY COOL***



Netanalyst Toolkit is a very good network tool that is highly recommended you use to solve problems and learn networking topics.

PMG Resources ***VERY GOOD***



PMG Resources is an excellent source of RFC, OUI, IEN and general protocol indexes. All of this information is on your desktop so if you need a quick reference to some protocol information it is available.

IP Subnet Calculator



IP Subnet Calculator is a quick little utility to aid you in your subnetting exercises.

Encyclopedia of Networking



Encyclopedia of Networking is a useful indexed Encyclopedia of network technologies from LAN TIMES. A very good reference and study tool.

Protocols Come Alive ***AWESOME***



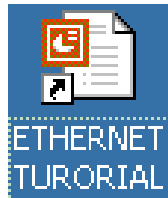
Protocols Come alive is a protocol packet simulator from RADCOM that lets you select any kind of LAN or WAN interface and layer 1 through 5 protocol and it generates traffic in simulation mode(not on any interface) plus displays the decodes for you. You can simulate and look at ATM, OC3, SONET, FRAME-RELAY traffic and packet headers. A great learning tool for understanding protocols.

A World of Protocols ***VERY GOOD***



A World of Protocols is the accompanying documentation and protocols reference guide for the Protocols Come Alive application. In the preface there is a section titled “**About this Book**” just click on the **Protocols** or **Technologies** links to get a comprehensive reference about just about every protocol in use. The Technologies link covers WAN technologies and pin outs for most interfaces.

Ethernet Tutorial ***VERY GOOD***



Ethernet Tutorial is a very good Power Point based tutorial on Ethernet and Fast Ethernet. This tutorial covers the lower level electrical and mechanical aspects of Ethernet technologies. A must read.

H.323 Tutorial *** VERY GOOD***

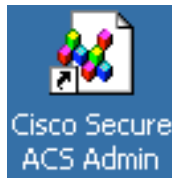


This is a very good Power Point based H.323 and VOIP tutorial that covers the in-depth mechanics of the protocols involved a great reference to you VOIP testing and protocol analysis.

Learning Perl



Learning Perl is a local Web based tutorial on Perl programming.
Cisco Secure ACS



Cisco Secure ACS is the Cisco Secure ACS version 2.6 server running on this server. The services are already started. To stop the Cisco Secure ACS service just go into the **Services** application(mentioned earlier) and stop the following services that start with a **CS**. You can use the DMZ 10.1.1.66 or the free interface to experiment, test and manage all of the security options on the Cisco Routers and Switches.

To access Cisco Secure you can use the WIN2KSRV desktop shortcut Icon or from your workstation over the VPN just open a web browser window and point to the following URL
<http://10.1.1.77:2002>

Cisco Works coming soon.

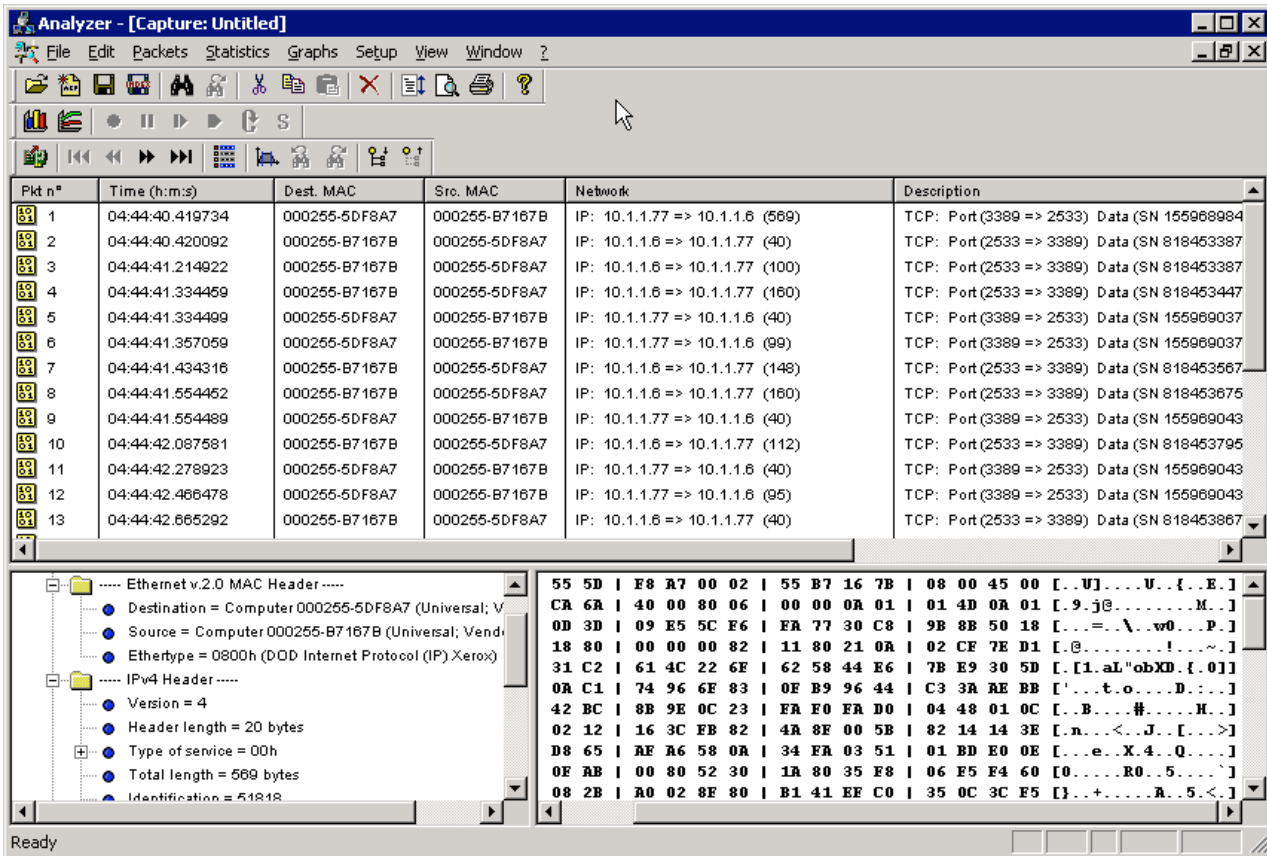
AMILABS in house version is available upon request. – See *section 11.0 Special Requests*.

Analyzer ***Pretty GOOD***



Analyzer(see **figure (3.6)**) is a shareware public domain protocol analyzer and is very good for quick and dirty traces. It can natively use the NDIS adapters while you are in your Windows Terminal Services session, so no need to have a separate VNC session just to use this protocol analyzer. The web site for this analyzer is <http://analyzer.polito.it/> if you wish to get your own copy and check out the documentation.

Figure (3.6).



The Analyzer, Packetyzer, Ethereal and Agilent Advisor protocol Analyzers Icons will be covered in more detail [section 4.0 Protocol Analyzers](#).

VQT



VQT is an Agilent’s Telegra Voice Quality testing tool. With this product, you can evaluate the quality and characteristics of voice signals carried on both analog and digital links. The VQT is particularly useful when evaluating voice signals carried on packet networks. VQT Application Software. This intuitive and easy-to-use software leads you through the necessary steps to test voice quality, calculates and displays measurement results in both graphical and spreadsheet formats, and provides procedural and interpretive information via a multi-mode embedded Help system. In addition, you can customize the application for your unique testing situations in the form of user-configurable Task Lists and automated test scripts. The software provides for both local and remotely controlled testing involving single or multiple VQT test devices. The demo scenario is a great resource to learn how to use such a tool. See **figure (3.7)** below for a screen shot.

Figure (3.7).

The screenshot shows the Agilent Technologies Telegra VQT (Analog) software interface in Demo Mode. The main window displays the configuration for a Clarity (PSQM) measurement. The Audio Configuration section shows the Audio Source set to Port A (FXO) and Audio Destination set to Port B (FXO). The Audio Reference File is Data\wav\ldr1-mjeb1-Si837.wav and the Received Audio File is Data\wav\psqmsave.wav. The Start button is highlighted in green, indicating the test is running. The Clarity graph shows the PSQM Score and Amplitude (dBm) over time. The results table below the graph provides the following data:

Average PSQM	0.67	Maximum PSQM	4.70
Avg PSQM Threshold	3.00	Max PSQM Thresh	6.00
Outliers (%)	0.00	PSQM Std. Deviation	0.4458
Outliers Threshold (%)	5.0	Estimated MOS Equiv.	4.57
Loss/Gain (dB)	-4.74	Estimated Delay (ms)	58.625
Correlation Timeout	No	Sync. Timeout	No

Additional information includes a 'To run this measurement' section with four steps: (1) Make sure you have done these things, (2) Configure the Clarity parameters above, (3) Start the test (Start button above), and (4) See the primary results (white background in the spreadsheet) to quickly interpret the measurement. There are also links for 'More Info' and 'Interpreting Clarity (PSQM) Results'.

Agilent Advisor LAN CBT *VERY GOOD*****



Agilent Advisor LAN CBT - this icon is on the right side of your desktop and is a full CBT on how to use the Stand Alone advisor unit in the lab and the software edition on this server. You should go through this CBT before using the analyzers. AMILABS can provide a quick online demonstration and tutorial to get you going on the protocol analyzers. The lab administrator can step you through the process of starting a trace, generating traffic, editing packets, using the VOIP RTP functions and saving your traces. This can be done in VNC.

LAB USER MESSAGE BOARD



LAB USER MESSAGE BOARD is just a basic MS-WORD document that lab users can use to post messages, tips, requests to use one another's files and so forth. It is just a basic communication method among visiting users. The users, if they feel comfortable, can leave their email address for others to use to communicate directly. If demand picks up a web based board or IRC type of application may be added in the future. Remember this is an open system so postings should only be relative to lab issues.

Other applications

Other Icons on the desktop such as Netsnoop or Ipscan are general utilities you can use in your network testing and security research. Most of the other Icons on the desktop are self-explanatory. The development Icons for Visual C, Basic and Java are also available. There are additional applications that were listed at the beginning of section 3.0 that are not present on the desktop for space reasons but are available in the START - PROGRAMS menu and a full list of the remaining applications will appear. See **figure (3.8)** below.

Figure (3.8).

Accessories	Tardis
Administrative Tools	The Edge Tests
Agilent Advisor	VNC
Agilent Advisor ATM CBT	WhatsUp
Agilent Advisor LAN CBT	Windows 2000 Resource Kit
Astricom	Windows Media
Cisco CD-ROM Products	WinZip
CiscoSecure ACS v2.6	WS_FTP
Exceed	WS_Ping ProPack
Exceed Tools	Acrobat Reader 5.0
Hayes V.92 Modem	AG Group EtherPeek 4
Hummingbird Accessories	Cisco TFTP Server
Hummingbird System Administration	Internet Explorer
Hummingbird Host Access	Microsoft Access
LiveUpdate Administration Utility	Microsoft Excel
Mathsoft Apps	Microsoft FrontPage
Microsoft Developer Network	Microsoft Outlook
Microsoft Office Tools	Microsoft PowerPoint
Microsoft SQL Server	Microsoft Word
Microsoft SQL Server - Switch	NetSnoop
Microsoft Visual J++ 6.0	Outlook Express
Microsoft Visual Studio 6.0	RealOne Player
Microsoft Web Publishing	Visio 2000
ModemTest	Windows Media Player
Modern Age Books	Microsoft Exchange Chat Service
NetScanTools	Line Monitor
Netscape Communicator Professional Edition	
Network Toolbox 2.1	
Norton AntiVirus Corporate Edition	
Phone Dialer Pro	
PingPlus	
PMG Tools	
Protocols come alive	
Real	
RealVNC	
SnagIt 6	
Startup	
Sybex CCDP SG	

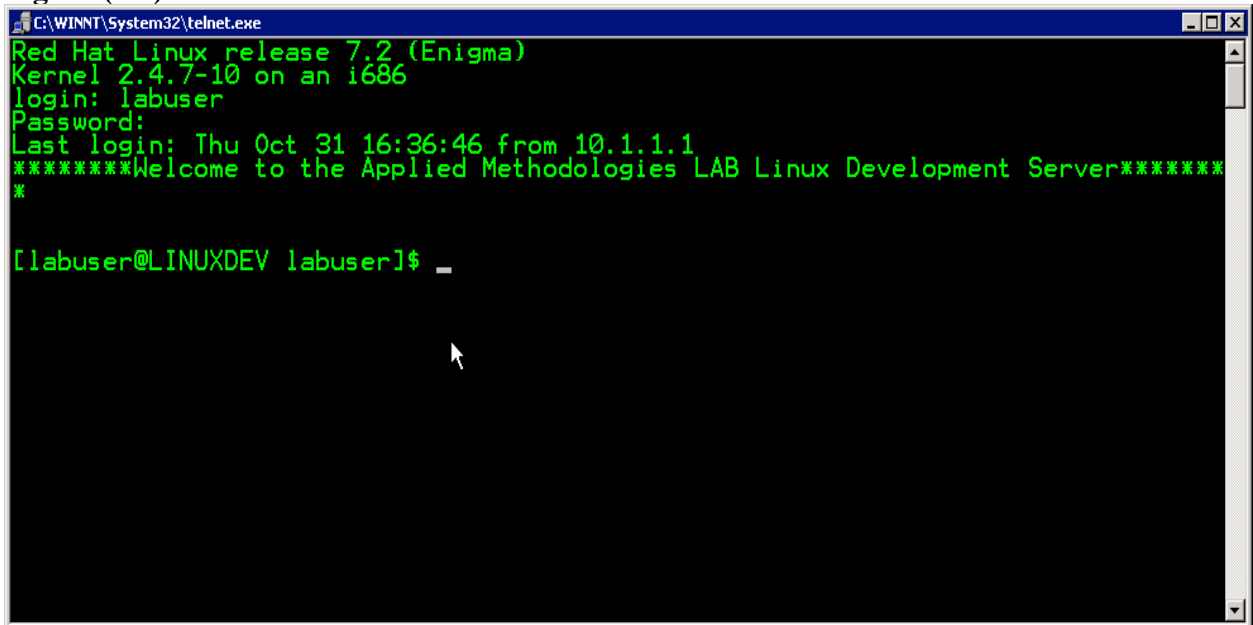
3.3 Linux Server – LINUXDEV

10.1.1.78

This is a full Red Hat 7.2 installation with GNOME, KDE environments, all packages and RPMs installed. This server is a fully blown **RED HAT LINUX 7.2 Server** containing all of the Linux desktop and server application suites included in Red Hat Linux server. You can Telnet to this server see **figure (3.9)** and access all resources at **Super User level**. The server has two 10/100Mbs Ethernet and one 16Mbs Token-Ring interface. You can access this server via Telnet, VNC and X Windows if you have X client software or run the Exceed client on the WIN2KSRV server. This server can also be used for DNS, TFTP, FTP, Multicasting, WEB and other services.

- Full console and X Windows development with KDD 2.0
- LIBNET and LIBCAP packet development API libraries
- APACHE server
- NFS server
- DNS server
- SQL server
- All application Daemons available
- XServer
- TCPDUMP sniffer daemon
- Oracle (9i coming soon)
- All Linux administration tools and applications that come standard with Red Hat Sever 7.2
- Full access to the Internet to download any patches or updates to the applications and OS

Figure (3.9).



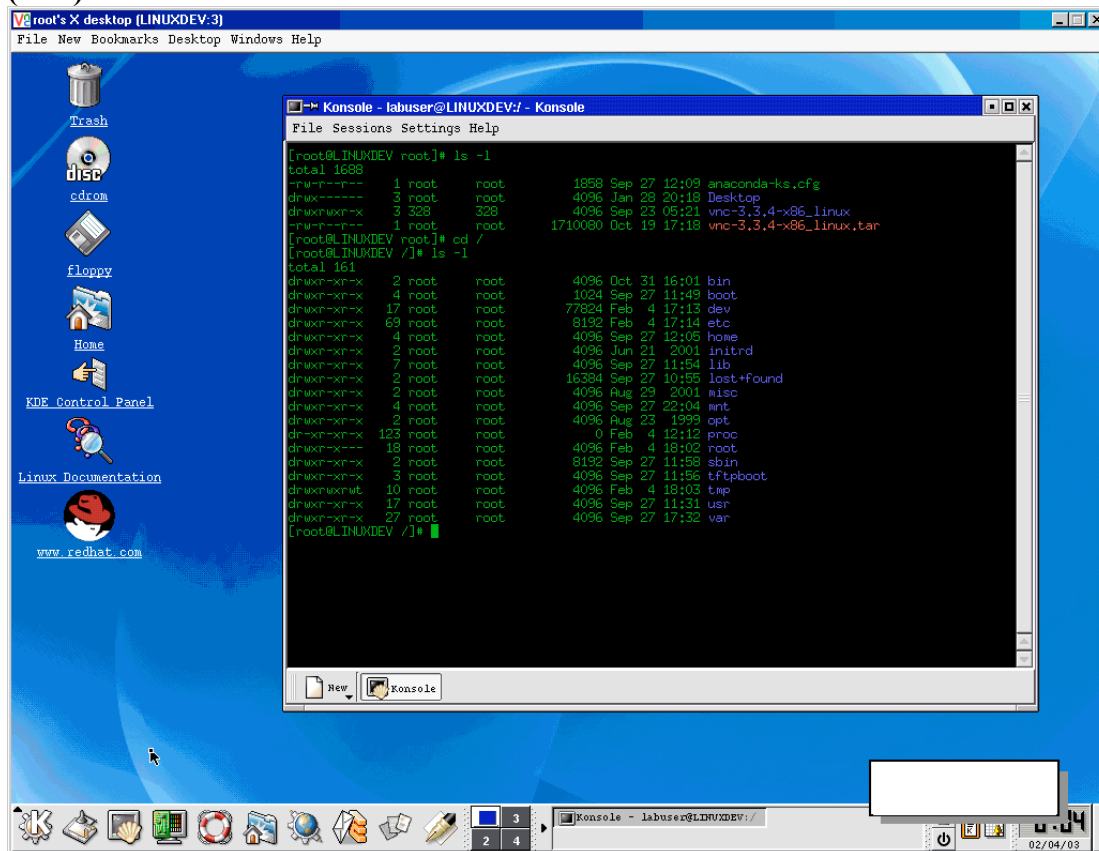
```
C:\WINNT\System32\telnet.exe
Red Hat Linux release 7.2 (Enigma)
Kernel 2.4.7-10 on an i686
login: labuser
Password:
Last login: Thu Oct 31 16:36:46 from 10.1.1.1
*****Welcome to the Applied Methodologies LAB Linux Development Server*****
*

[labuser@LINUXDEV labuser]$ _
```

VNC to this server – see figure (3.10)

The server has a basic VNC configuration. You can use your VNC viewer from your desktop over the VPN or from the WIN2KSRV server in Windows Terminal Services. If you are familiar with tuning VNC on the Linux Server you can reconfigure it to support the GNOME or KDE desktops.

**Figure
(3.10).**



A copy of Exceed is also available on the WIN2KSRV server for your use as an Xwindow client to the LINUXDEV server.

3.4 Linux Router - LINUXFWRTR

10.1.1.79

This is a Red Hat Linux 7.0 Firewall and Router. This server is stripped down in terms of applications and run level daemons available but provides an excellent environment to learn and test Linux routing and firewall capabilities with IPChains/Tables and Tripwire. The server has two 10Mbs Ethernet adapters to be configured any which way you wish. One example is to configure adapters on different VLANS so you can run TCPDUMP or any shareware Linux protocol analyzer on different segments thus turning this box into a “distributed sniffer”. You can perform the same action on all the other servers mentioned previously as well. You can access this server by Telnet or VNC. See **figure (3.11)**.

Note: you may have to fiddle around with some Windows/Linux settings to get some of the applications to work properly. Sorry, but that is the nature of an open system with various commercial, demo and beta applications installed.

4.0 Protocol Analyzers

The lab contains several protocols analyzers for your use to help in understanding how network protocols work, generate traffic for stimuli tests against routers, switches, servers, plus perform application impact analysis, test and validate your network configurations, analyze VOIP traffic and for learning how to use a LAN/WAN protocol analyzer. Various protocol analyzers are available to enhance your understanding of using such tools, compare differences between analyzer products and to assist you in expanding your skill base by using different protocol analyzers.

4.1 Agilent Advisor

Agilent Advisor Stand-alone J2300E *** THE GREATEST***

The Agilent Advisor is a fully functional standalone Agilent Advisor LAN/WAN protocol analyzer model J2300E with Fast Ethernet, Token-Ring, T-1 bantam, DDS, ISDN, V.35, RS232, and RS449 interfaces. You can access this protocol analyzer as if you were in front of it by using VNC either from your computer over the VPN or from the WIN2KSRV server. You can run traces on WAN and LAN segments separately or simultaneously to follow your packets from LAN to WAN media, generate traffic and monitor/analyze VOIP calls.

The main network diagram **AMI NETWORK LAB** shown in section 2.0 and included in your VPN kit) shows the three points in the lab network where the unit is physically connected and the interfaces used. The Agilent Advisor software is GUI based and is easy to figure out if you have used protocol analyzers(sniffers) before. However, it is recommended that before you use this unit you go through the CBT on the WIN2KSRV server. The Advisor currently has the Fast Ethernet interface undercradle and the T-1 network module installed. If you want to use the combined Token-Ring and 10Mbps Ethernet under cradle please send a request to the lab administrator before your session starts. See [section 12.0 Special Requests](#) for more details.



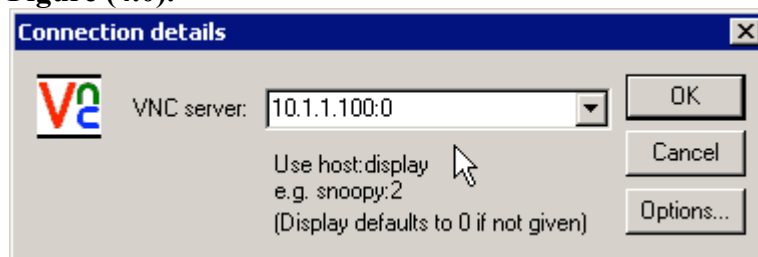
To use the standalone J2300E Agilent Advisor follow these steps:

Establish a VNC session to the protocol analyzer either from your VNC viewer over the VPN or from the WIN2KSRV server. See [section 7.2 Virtual Network Computing \(VNC\) setup for](#) instructions on how to setup VNC.

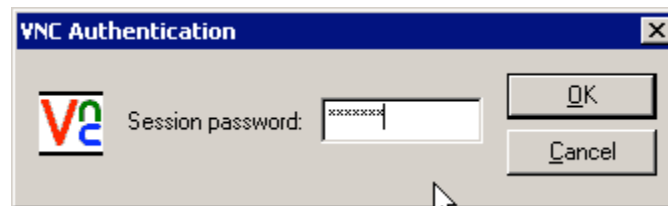


Then type in **10.1.1.100:0** in the VNC viewer window: the **10.1.1.100** is the address of the standalone Advisor the **0** is the VNC display number. This is the default to use on this unit. See **figure (4.0)** below:

Figure (4.0).



You will be prompted for a password just use the password listed in the **LAB PASSWORD** file included in your VPN kit.



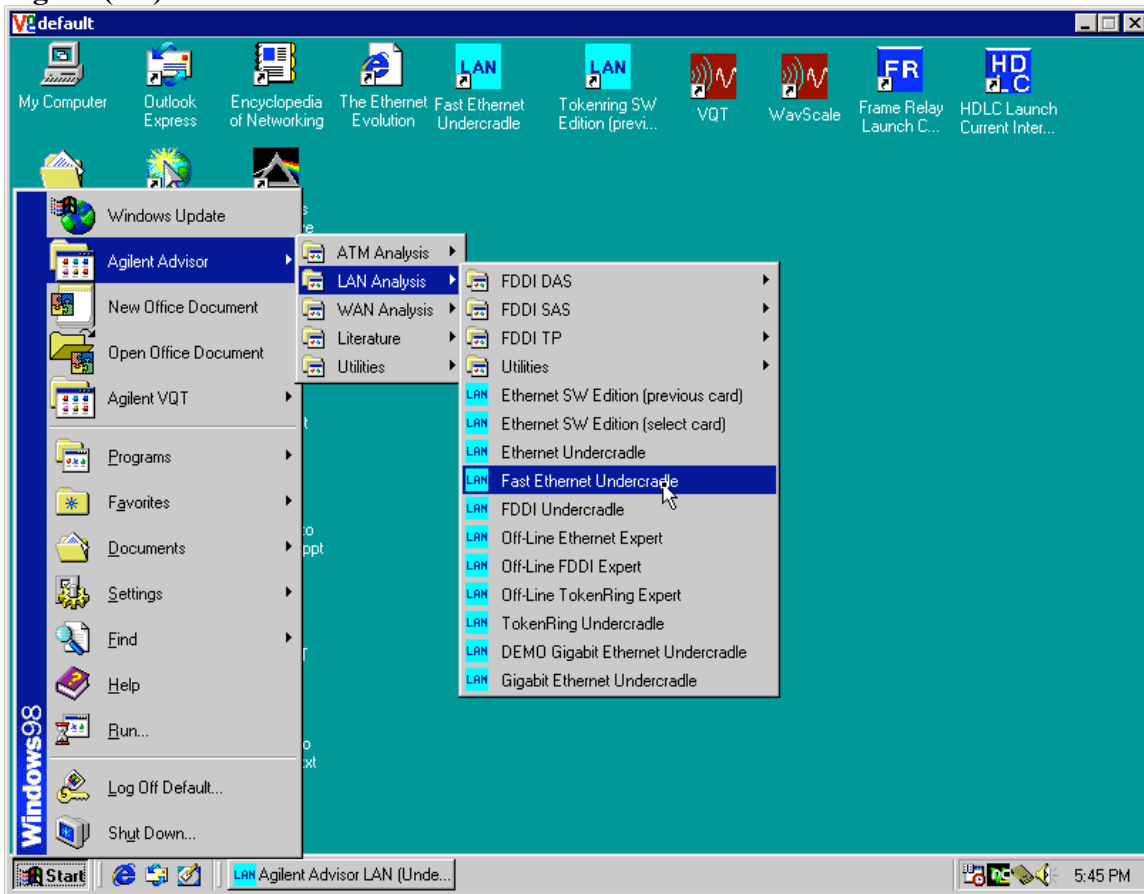
Then you will get the stand alone units desktop as shown if **figure (4.1)** below:

Figure (4.1).



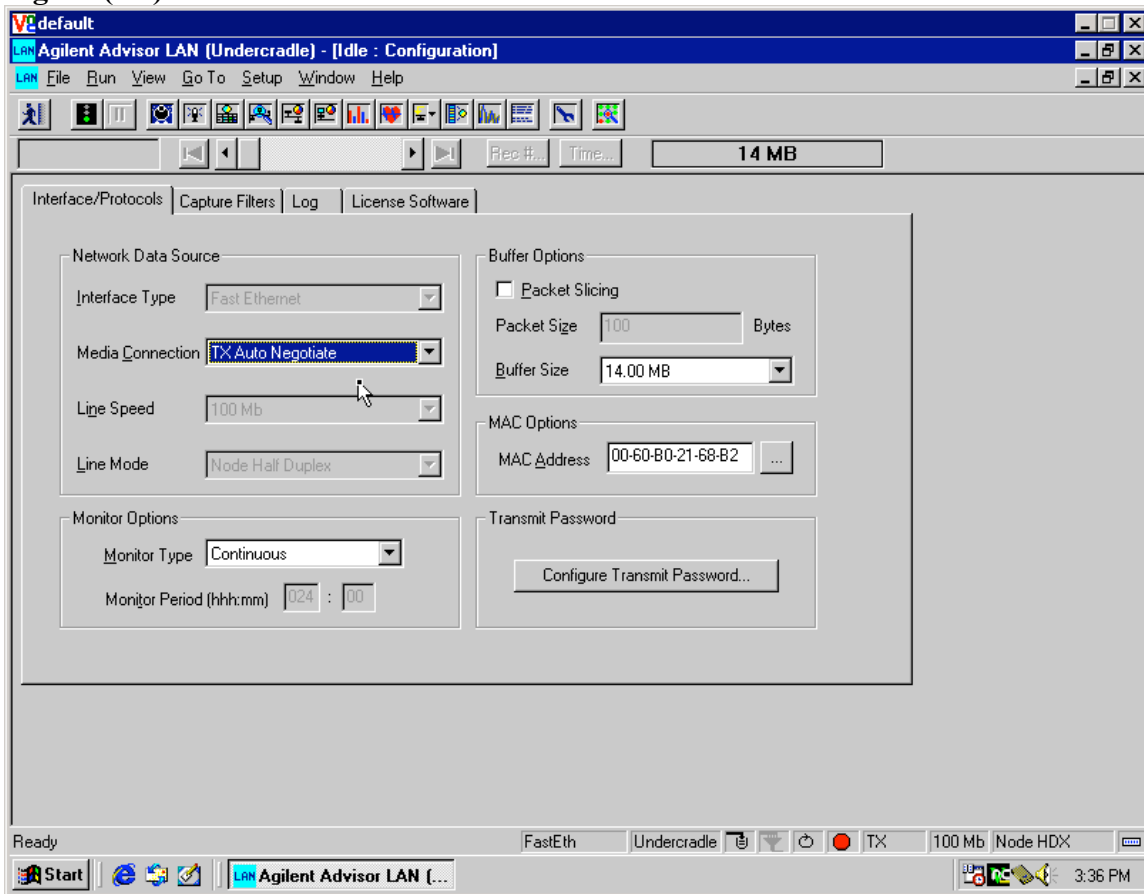
You can select the desktop Icons or use the Start Menu as shown in **figure (4.2)**.

Figure (4.2).



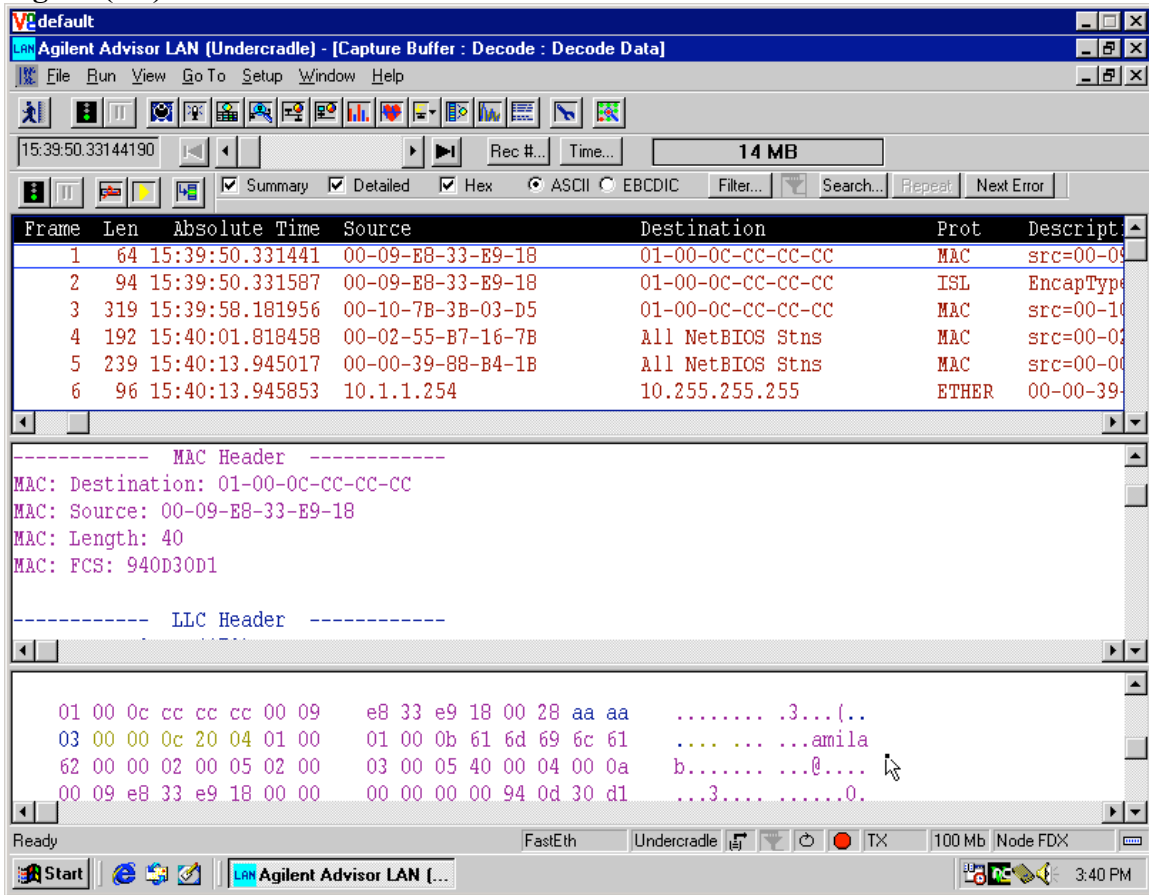
Then select your adapter to **AUTO-NEGEOIATE** if not already set. See **figure (4.3)**.

Figure (4.3).



Then select the tool you want to use in this case **DECODES** and press the traffic light to change from **GREEN** to **RED** to start and stop your traces. See figure (4.4).

Figure (4.4).



Agilent Advisor Software Edition model J1955A on the WIN2KSRV server.

The Best



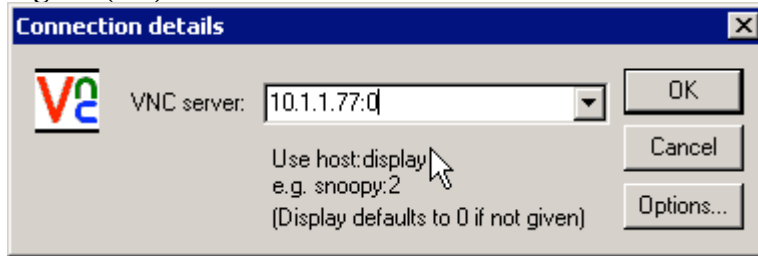
This software is functionally equivalent on the standalone unit discussed above with the exceptions of the WAN and Token-Ring interfaces. There is currently an issue using this software under Windows Terminal Services for the NDIS adapters do not show up.

To use this software just open a VNC connection as discussed earlier to the WIN2KSRV server and run the application. A window titled “Quickstart Expert” mode window may pop up to assist you. If you know what you are doing you can close this window and go directly into the application. It is recommended that you do not change the **LINE MODE** option in the configuration panel of the adapters from “MONITOR” to “NODE” if it is allowed.

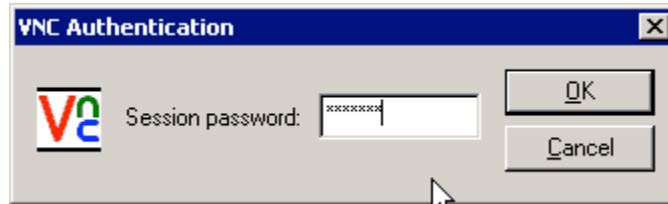
In **NODE** mode you may lose connectivity to the server if you are using the **10.1.1.77** adapter. In **MONITOR** mode you can capture and generate traffic while still connected to the server from that single interface. Of course you should be using the second interface for you “sniffing” needs. You can adjust the capture buffer from 0.50Mb to 64Mb.

To use the Agilent Advisor on the WIN2KSRV server VNC from your PC over the VPN to the server using the address of **10.1.1.77:0**. See **figure (4.5)**.

Figure (4.5).



You will be prompted for a password just use the password in the **LAB PASSWORD** file included in your VPN kit.

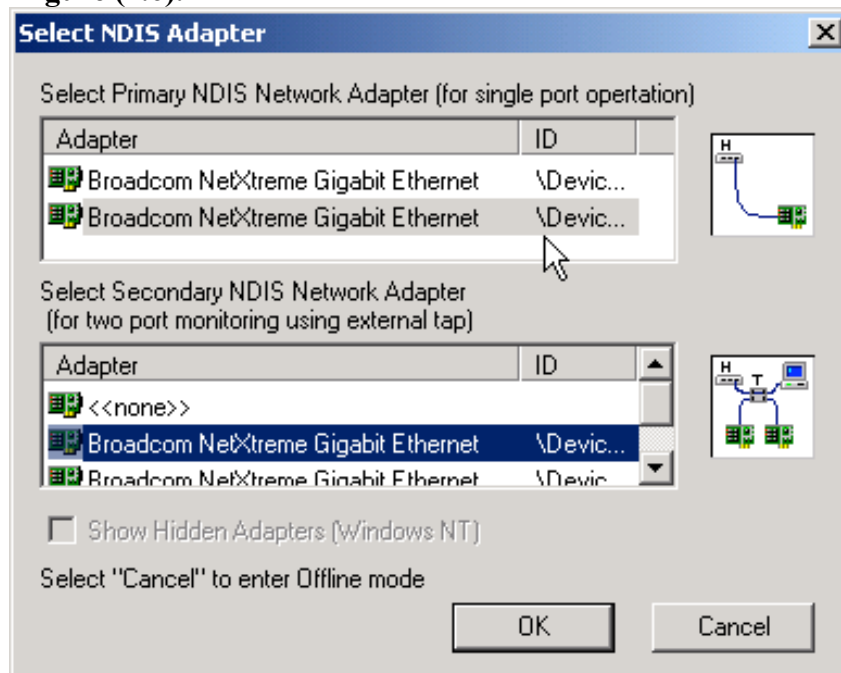


To use the Agilent Advisor on the WIN2KSRV to use both Broadcom 10/100/1000 Ethernet adapters select the following Icon to select one or both Broadcom adapters:



You will get the following screen as shown in **figure (4.6)**.

Figure (4.6).



A note about the WIN2KSRV server NDIS Broadcom Gigabit Ethernet adapters and the protocol analyzers used: The **bottom NDIS adapter** in **figure (4.6)** and all such displays is the adapter you have your Windows Terminal Services session through (10.1.1.77). The **top NDIS adapter** is the **free NDIS adapter** in your lab for use. You can select both to be used, a primary and secondary. The proper configuration to use your **second** Broadcom adapter is to have the **primary NDIS adapter set to the bottom adapter** and the **secondary NDIS adaptor set to the top adaptor** as depicted above in **figure (4.6)**.

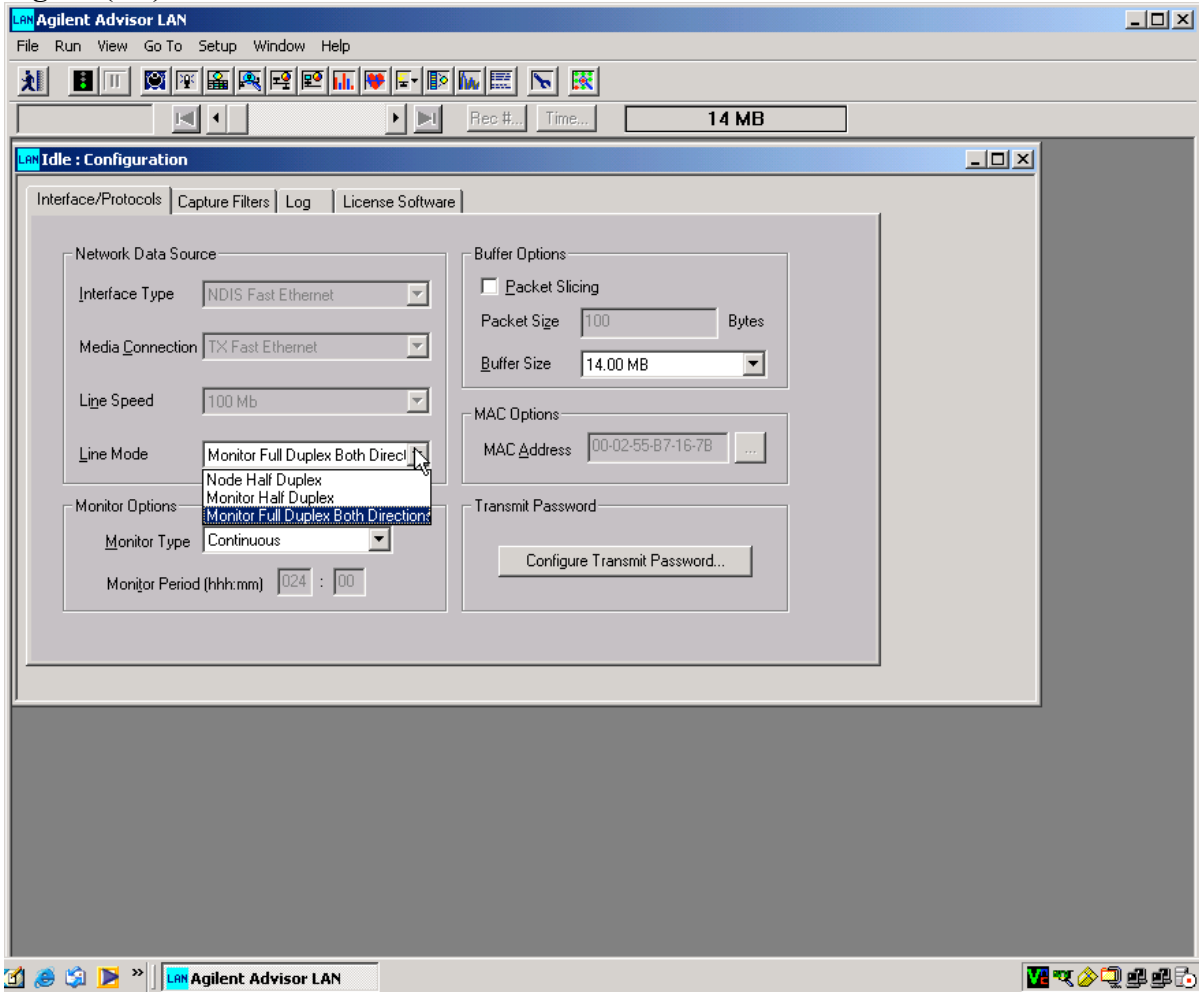
And the icon to use that remembers the last adapter selected and does not provide a choice is:



The adapters have already been setup for you so you just use the icon above to start the Advisor session.

You will get the same screens and **START MENU** options as shown previously in the stand alone Agilent Advisor J2300E section however, instead of the of **AUTO NEGEOATE** setting for the line mode, in the WIN2KSRV Software edition via VNC make sure your line mode is configured **MONITOR FULL DUPLEX BOTH DIRECTIONS**, as per **figure (4.7)**.

Figure (4.7).



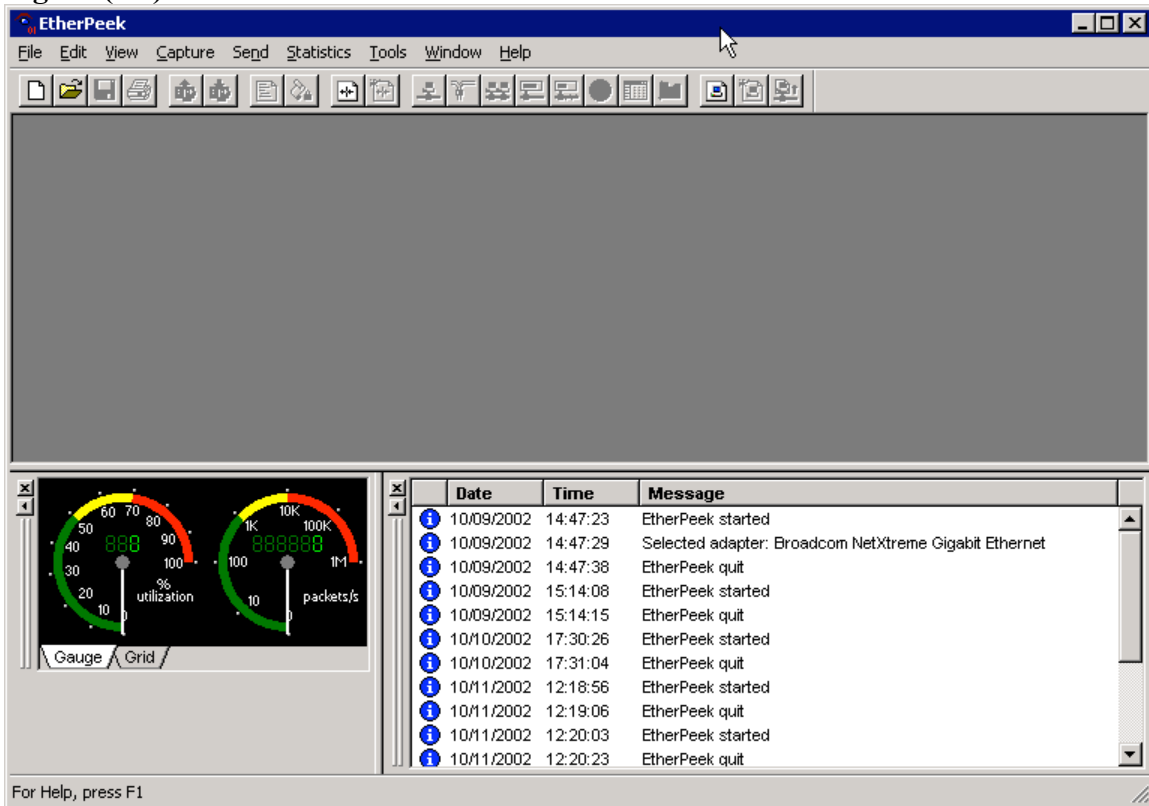
You can then proceed to trace and run tests as mentioned earlier in this section.

AG Group Etherpeek4 on the WIN2KSRV server.



To run Etherpeek the same issue regarding the Windows Terminal Services and NDIS adapters that were present for the Agilent software are present for the Etherpeek software. The solution is the same as the Agilent, just use VNC to connect to the server to run the Etherpeek software and select an adapter to use.

Figure (4.8).

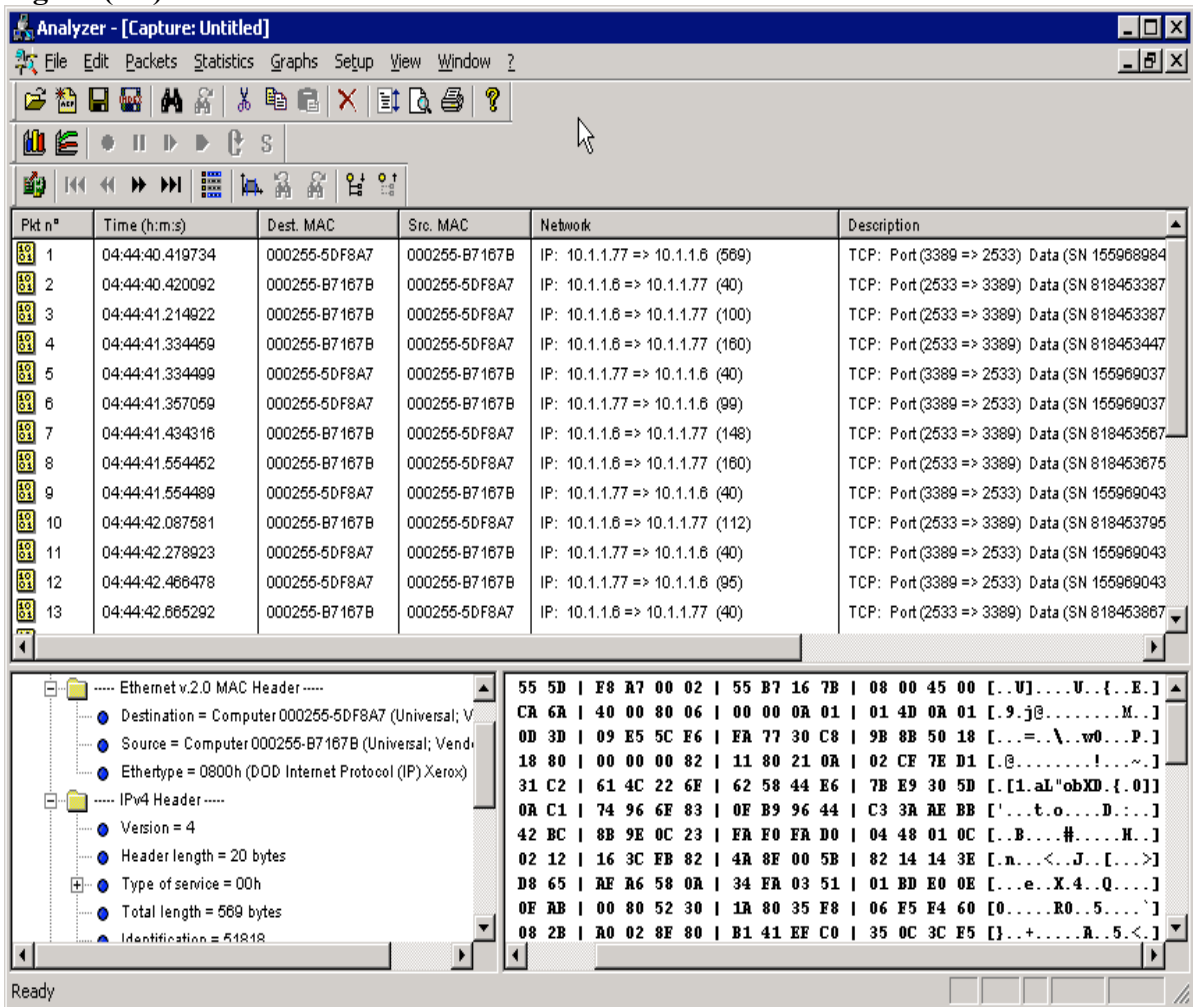


Analyzer on the WIN2KSRV server *Pretty Good*****



Analyzer is a shareware protocol analyzer on the WIN2KSRV server from Politecnico Analyzer. There is no NDIS and Windows Terminal Services issue with this software so it can be run within you normal Windows Terminal Services session. So, no VNC session is required. This software is a quick and easy to use protocol analyzer for that quick “trace”. The documentation and links to obtain you own copy are found at <http://analyzer.polito.it/>. **Figure (4.9)** below is a screenshot of Analyzer’s post capture screen.

Figure (4.9).



Wireless 802.11b Protocol Analysis**Packetyzer and the WSP100 on the WIN2KSRV server ***VERY GOOD*****

Packetyzer is a shareware protocol analyzer on the WIN2KSRV server. With Packetyzer there are no NDIS and Windows Terminal Services issue with this software so it can be run within your normal Windows Terminal Services session. So, no VNC session is required. This software is a quick and easy to use protocol analyzer for that quick “trace”. It is also a real time analyzer meaning that you will see the packets cross your display in real time like the Agilent’s but without the RTP and extensive tool/decodes. The documentation and links to obtain your own copy are found at <http://www.packetyzer.com>.

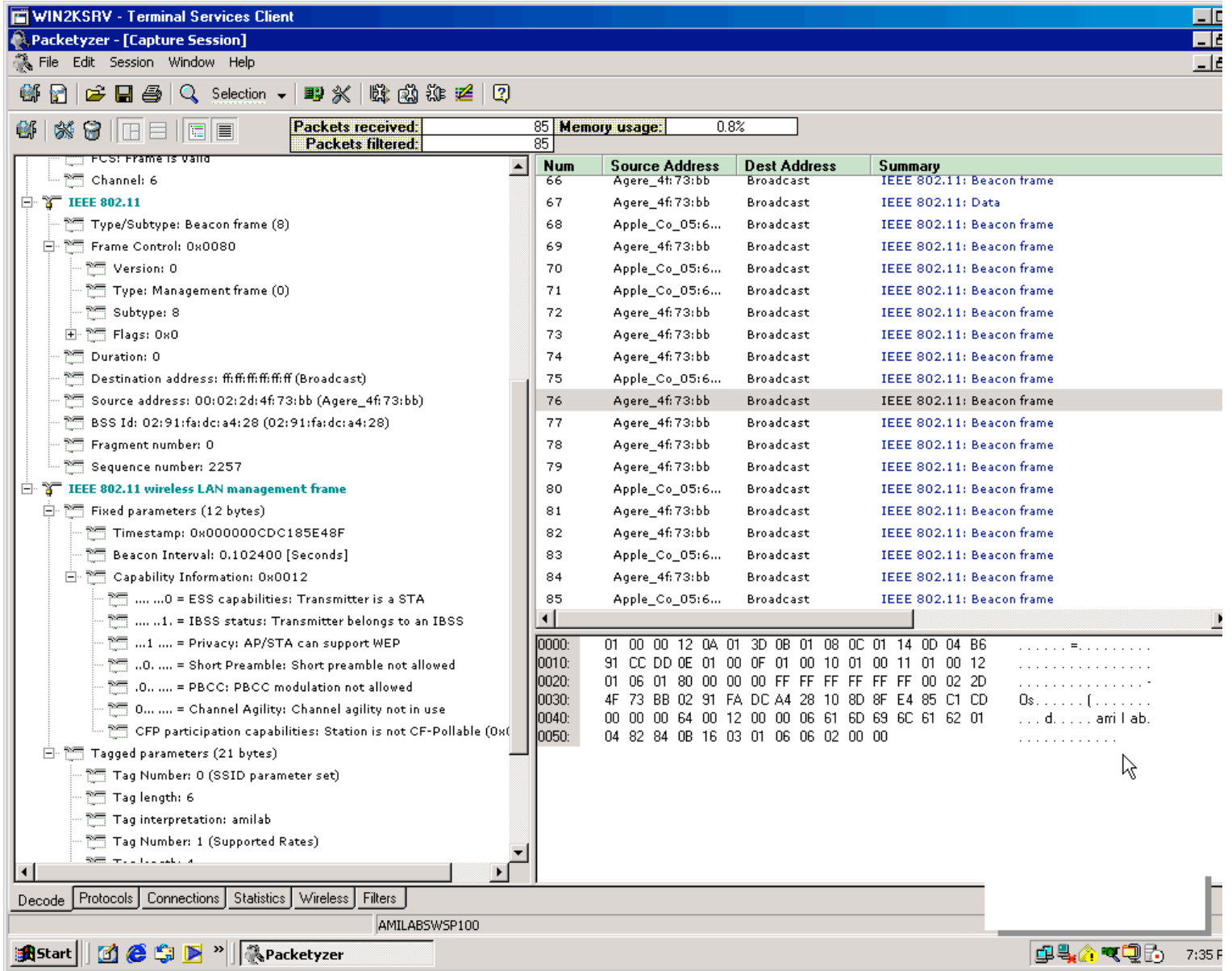
Packetyzer also runs in conjunction with the WSP100 a remote 802.11b receiver so the student can learn about 802.11b MAC protocol and trace wireless lab activity. Packetyzer uses the WSP100 as another adapter but it is a remote wireless receiver. The WSP100 sends packets over the lab Ethernet DMZ network to the Packetyzer application running on the WIN2KSRV.

Figure (4.10) below shows the conceptual layout of the WSP100 in action.

Figure(4.10).



Figure (4.10) shows the Packetyzer in action:



For more information and documentation about the Packetyzer and WS100 802.11b wireless sniffer please visit the site

<http://www.networkchemistry.com/products/wsp100/index.html>

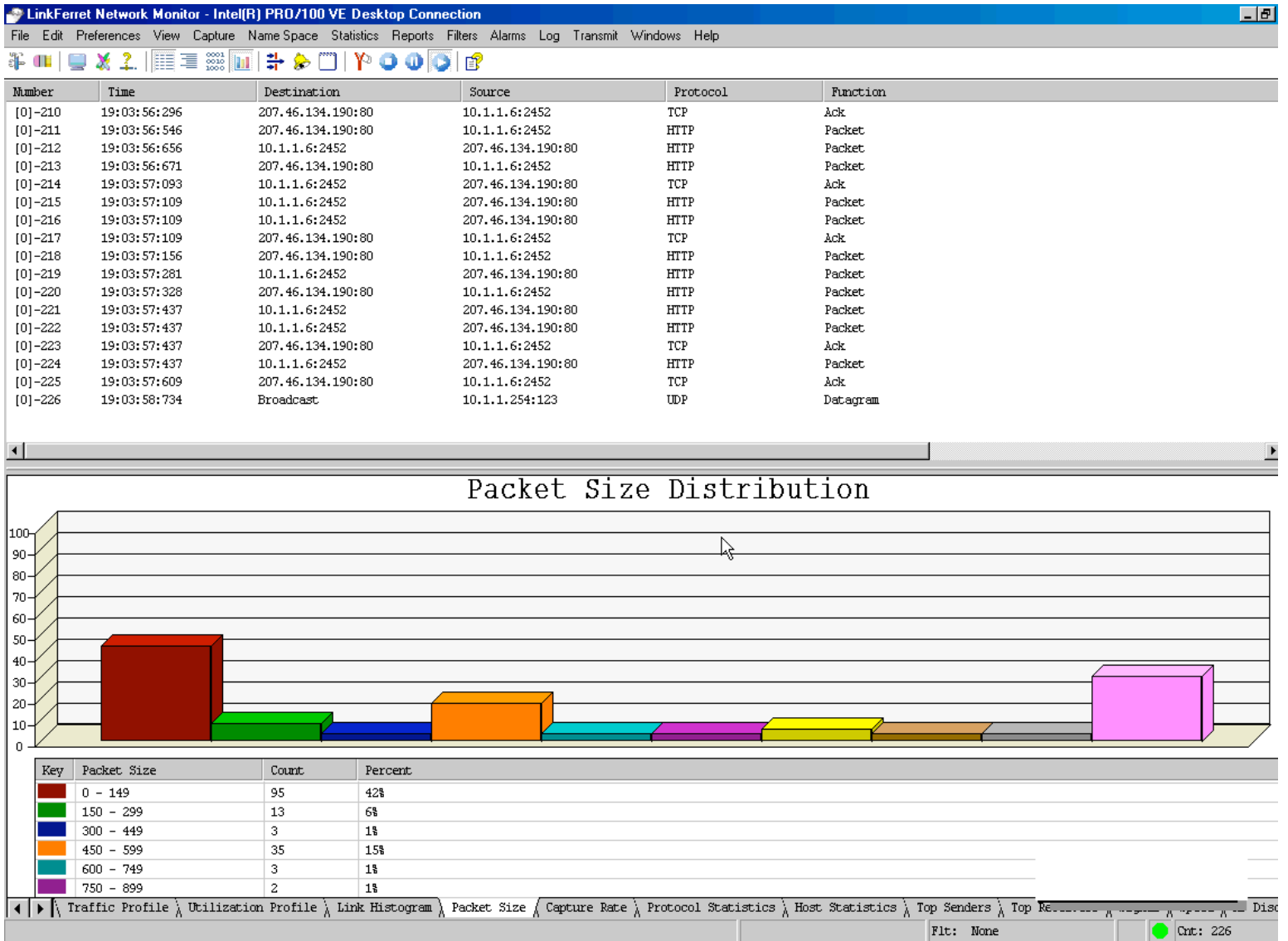
LinkFerret ***VERY GOOD***

LinkFerret is also a very good commercial wire line real time based protocol analyze available on the Windows server.

LinkFerret network monitoring products for LAN and wireless topologies provide you with a comprehensive set of monitoring utilities and packet sniffers for capture, statistical analysis, and protocol decoding. LinkFerret brings you newly optimized tools that have been in use in the conformance test lab at Baseband Technologies for 10 years. With their enhanced user interface and new features, LinkFerret products are the best tools at the best price. With LinkFerret, you have a competitive edge. A screenshot of LinkFerret in action is below.

For more information about LinkFerret please go directly to the website for details.
WWW.LINKFERRET.WS

Figure(4.11).



The best protocol analyzers to use in this lab are the ones from **Agilent, LinkFerret and Packetyzer** for the display shows you the real time packets on the screen. You can watch trace packet behavior unfold in front you while your test is conducted. You can note particular packets such as requests or broadcasts in real time. Also you can generate and watch you traffic and the impact it has on the network or to an application in real time.

The other two protocol analyzers, **Etherpeek** and **Analyzer** are capture and post capture review types of analyzer. This means that you do not see the actual packets “going by” as you are tracing. You have to stop the trace to review the packets.

Note: Screen update performance will vary using Windows Terminal Services or VNC and the type of connection you are using for your VPN.

As soon as the NDIS to Windows Terminal Services adapter locking issue is resolved you will not need to run VNC for the Agilent and Etherpeek protocol analyzers on the WIN2KSRV server.

Approaches for using the protocol analyzer from the WIN2KSRV server.

You can use your Windows Terminal Services session to launch applications and generate traffic and in another window on your PC, over the VPN, have a VNC session to a protocol analyzer on the WIN2KSRV using a different adapter and/or another VNC session to the standalone Agilent Advisor protocol analyzer. This gives you the ability to have several “sniffing or trace” points throughout the lab for your research. Remember the Agilent software and standalone unit can simultaneously trace and generate traffic on both the WAN and LAN segments at the same time. Remember to have your SPAN ports configured properly on SW1. You can also use LinkFerret or Packetyzer for your general trace needs locally on the WIN2KSRV and stay in your Windows Terminal Server without the need to open additional VNC sessions for the Agilent Advisor analyzer.

4.2 Linux Server protocol analyzers

Ethereal

If you are connected to the LINUXDEV server via VNC or Exceed and have the full GNOME or KDE desktop you can use the GUI version of Ethereal on this sever. Just select the second adapter (Eth1) and you are ready to trace.

TCPdump

If you just want a quick and dirty trace from any of the LINUX servers just execute the command **TCPDUMP** at the command line. See **figure (4.11)**. You can run **TCPDUMP -h** for help or run a MAN page on TCPDUMP for the documentation about this program. You have to be **Super User** to run TCPDUMP please refer to the **LAB PASSWORDS** file included in your VPN kit for the password.

Figure (4.11).

```

C:\WINNT\System32\telnet.exe
21:14:02.625024 0:40:f4:11:21:11 > Broadcast null I (s=0,r=0,C) len=42
21:14:02.655024 10.1.1.77.4911 > 10.1.1.78.telnet: . ack 1183 win 63889 (DF)
21:14:02.655024 10.1.1.78.telnet > 10.1.1.77.4911: P 1183:1434(251) ack 0 win 58
40 (DF) [tos 0x10]
21:14:02.785024 802.1d config 6001.00:09:e8:33:e9:00.800f root 6001.00:09:e8:33:
e9:00 pathcost 0 age 0 max 20 hello 2 fdelay 15
21:14:02.875024 10.1.1.77.4911 > 10.1.1.78.telnet: . ack 1434 win 63638 (DF)
21:14:02.875024 10.1.1.78.telnet > 10.1.1.77.4911: P 1434:1743(309) ack 0 win 58
40 (DF) [tos 0x10]
21:14:03.095024 10.1.1.77.4911 > 10.1.1.78.telnet: . ack 1743 win 63329 (DF)
21:14:03.095024 10.1.1.78.telnet > 10.1.1.77.4911: P 1743:1922(179) ack 0 win 58
40 (DF) [tos 0x10]
21:14:03.155024 CDP v2, ttl=180s
      DevID 'SW1'
      Addr (1): IPv4 10.1.1.51
      PortID 'FastEthernet0/15'
      CAP 0x28
      [!cdp]
21:14:03.315024 10.1.1.77.4911 > 10.1.1.78.telnet: . ack 1922 win 63150 (DF)
21:14:03.315024 10.1.1.78.telnet > 10.1.1.77.4911: P 1922:2231(309) ack 0 win 58
40 (DF) [tos 0x10]

25 packets received by filter
0 packets dropped by kernel
[root@LINUXDEV labuser]#

```

You can also run **TCPDUMP** in several terminal sessions in one VNC window on the **LINUXDEV** server for added flexibility.

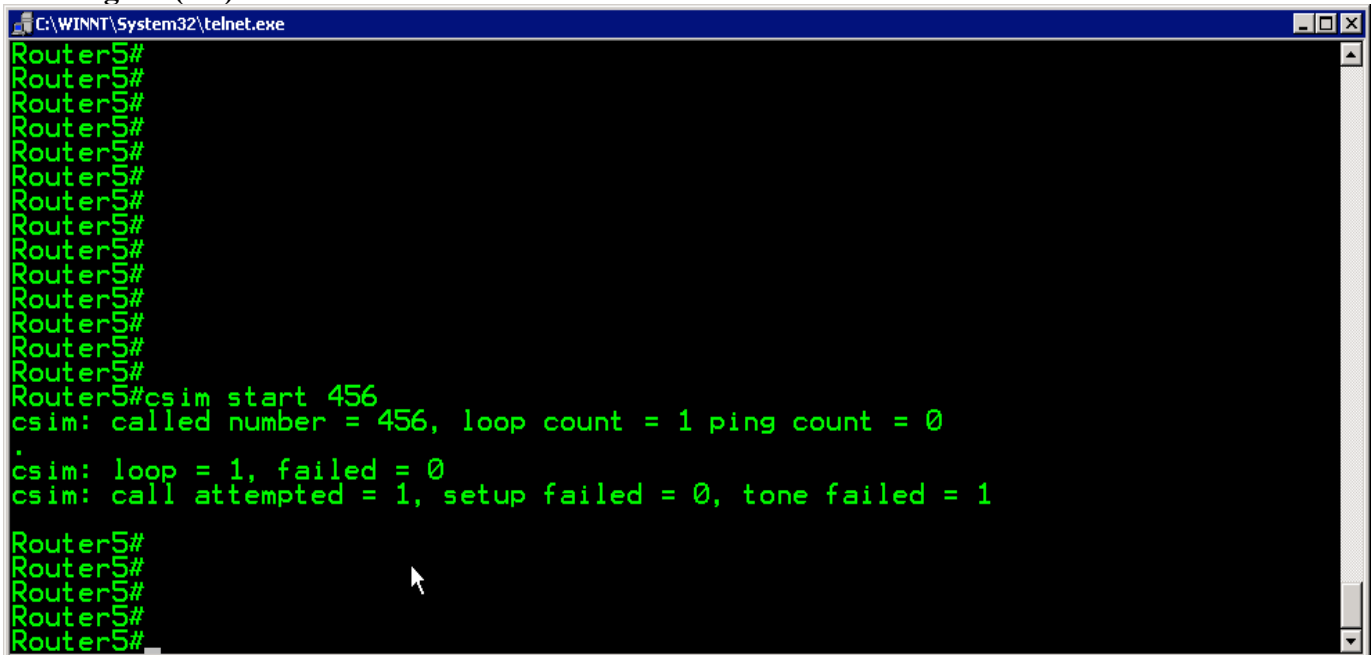
5.0 Voice Over IP Testing

To test Cisco IOS router based VOIP technologies and configurations or to learn the mechanics of how VOIP works AMILABS provides two methods and tools to assist you in your research. Please to the Visio diagram named **VOIP MECHANICS** included in your VPN kit for an understanding of how the lab's VOIP environment is configured.

5.1 Method 1- CSIM for just IOS configuration validation

You can use the **CSIM** undocumented command to make a call from one router to another and use the debug output or the analyzers to validate operation. **Figure (5.0)** below shows a basic use of CSIM.

Figure (5.0).

A screenshot of a telnet session window titled 'C:\WINNT\System32\telnet.exe'. The window shows a series of 'Router5#' prompts. The user enters the command 'csim start 456'. The output shows 'csim: called number = 456, loop count = 1 ping count = 0', followed by a period, then 'csim: loop = 1, failed = 0' and 'csim: call attempted = 1, setup failed = 0, tone failed = 1'. The session continues with several more 'Router5#' prompts.

```
C:\WINNT\System32\telnet.exe
Router5#
Router5#
Router5#
Router5#
Router5#
Router5#
Router5#
Router5#
Router5#
Router5#
Router5#
Router5#
Router5#
Router5#
Router5#
Router5#csim start 456
csim: called number = 456, loop count = 1 ping count = 0
.
csim: loop = 1, failed = 0
csim: call attempted = 1, setup failed = 0, tone failed = 1

Router5#
Router5#
Router5#
Router5#
Router5#
```

CSIM is a simple and quick undocumented command to test VOIP configurations. It does lock up your router session while it is executing so it is not very flexible beyond its quick use.

5.2 Method 2 - Using the Phone Dialer Pro utility

The second method involves using the Phone Dialer Pro dialer utility, modems and answer machines so you can really simulate a voice call, debug it on the routers and trace it using the Agilent or other protocol analyzers in the lab.

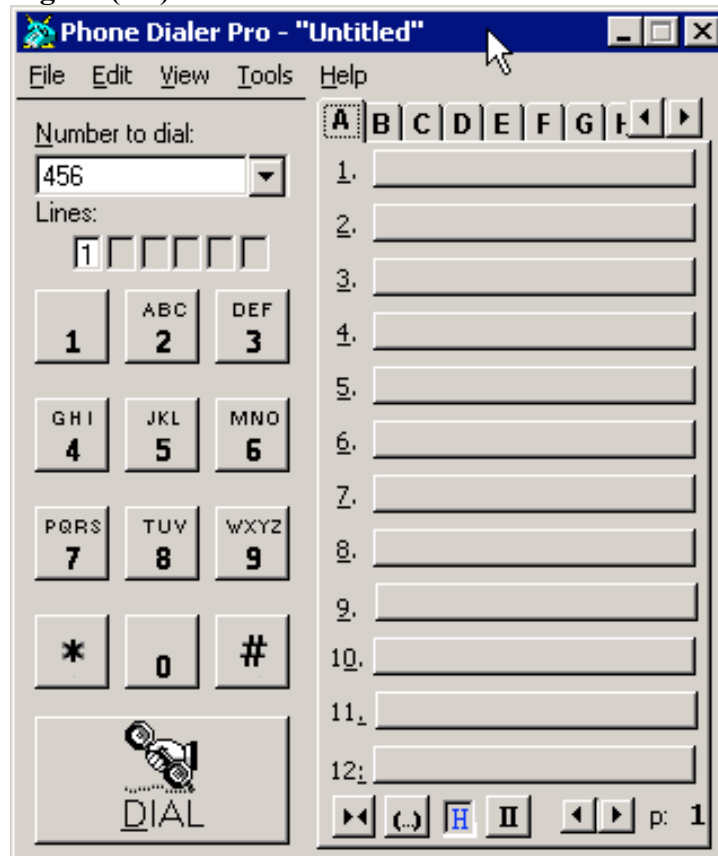
The first step is to have your IOS VOIP configuration in place.

Next on the WIN2KSRV server execute the Phone Dialer Pro application by clicking on the icon below:



Now enter the number of the dial-peer you would like to call as shown in **figure (5.1)**. You can customize this utility and create profiles of phone numbers to use for repeated testing of different Cisco VOIP configurations.

Figure (5.1).



Remember to select the correct modem COM. port to the router you want to use.

COM3 connects to ROUTER5 (default)

A second modem and answering machine may be added to COM 4 in the future.

Press the **DIAL** button and watch the call status as per **figure (5.2)**.

Figure (5.2).



When your call is connected you will see the following screen as per **figure(5.3)**.

Figure (5.3).



To cancel the call just press the **OK** button

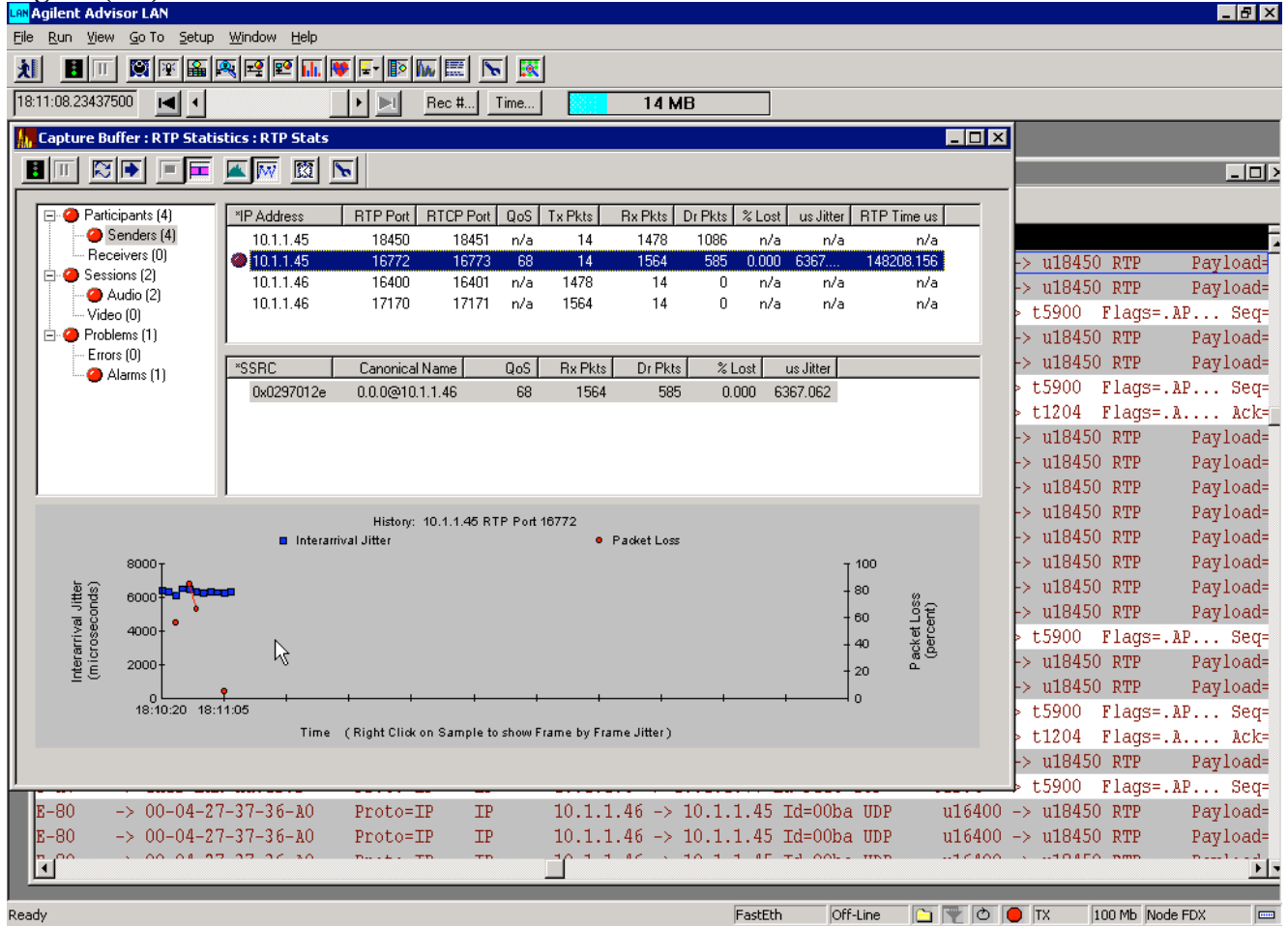
You can validate you call by debugging your VOIP configuration on the Cisco routers as per **figure (5.4)**.

```

C:\WINNT\System32\telnet.exe
000048: *Mar 1 04:51:11.130: dsp_soutput: [1/0/0]
000049: *Mar 1 04:51:11.130: dsp_digit_collect_on: [1/0/0] packet_len=20 channe
l_id=128 packet_id=35 min_inter_delay=240 max_inter_delay=9760 mim_make_time=10
max_make_time=100 min_brake_time=10 max_brake_time=100
000050: *Mar 1 04:51:11.130: dsp_soutput: [1/0/0]
000051: *Mar 1 04:51:11.134: htsp_process_event: [1/0/0, FXSLS_WAIT_SETUP_ACK,
E_HTSP_SETUP_ACK]
000052: *Mar 1 04:51:12.578: dsp_digit_collect_off: [1/0/0] packet_len=8 channe
l_id=128 packet_id=36
000053: *Mar 1 04:51:12.582: dsp_soutput: [1/0/0]
000054: *Mar 1 04:51:12.582: htsp_process_event: [1/0/0, FXSLS_OFFHOOK, E_HTSP_
PROCEEDING]htsp_alert_notify
000055: *Mar 1 04:51:12.602: htsp_process_event: [1/0/0, FXSLS_OFFHOOK, E_HTSP_
VOICE_CUT_THROUGH]
000056: *Mar 1 04:51:22.618: htsp_dsp_message: SEND/RESP_SIG_STATUS: state=0x4
timestamp=34871 systime=1748262
000057: *Mar 1 04:51:22.618: htsp_process_event: [1/0/0, FXSLS_OFFHOOK, E_DSP_S
IG_0100]fxspls_offhook_onhook, HF duration=500
000058: *Mar 1 04:51:22.622: htsp_timer - 500 msec
000059: *Mar 1 04:51:23.122: htsp_process_event: [1/0/0, FXSLS_OFFHOOK, E_HTSP_
EVENT_TIMER]fxspls_offhook_timerhtsp_release_req: cause 16, no_onhook 0
000060: *Mar 1 04:51:23.126: htsp_process_event: [1/0/0, FXSLS_ONHOOK, E_HTSP_R
ELEASE_REQ]fxspls_onhook_release
000061: *Mar 1 04:51:23.126: htsp_timer_stop
000062: *Mar 1 04:51:23.130: hdspfm_close_cleanup
    
```


Also while this call was going on the Agilent Advisor Software edition's RTP analyzer running off the WIN2KSRV second Broadcom adaptor was analyzing Jitter, packet loss and any QoS options present as per **figure (5.6)**.

Figure (5.6).



For a full understanding on how the VOIP router to modem to answering machine connectivity is configured please refer to the VISIO diagram named **VOIP MECHANICS** included in your VPN kit and on the WIN2KSRV server.

The routers FXS ports to modem and answering machine is already depicted in the VISIO diagram named **AMI NETWORK LAB** included in your VPN kit and on the WIN2KSRV server. The FXS port to handset table is included below for your convenience.

<u>Router</u>	<u>FXS port</u>	<u>Device attached</u>
Router5	V1/0/0	Modem from WIN2KSRV COM3 port
Router5	V1/0/1	Regular POTS handset for CSIM use
Router6	V1/0/0	Answering machine with a one minute message
Router6	V1/0/1	Regular POTS handset for CSIM use

VOIP testing approach:

You can run several tests simultaneously by using CSIM and Phone Dialer Pro all the while generation traffic with one protocol analyzer and monitoring with another.

6.0 Accessing the LAB -- VPN Installation

The instructions to install your VPN is in the file named: **VPN CONFIGURATION** that is included in your VPN kit.

Please follow the instructions in the document step by step. The instructions and applications outlined in this document were tested on POTS dial-up 46kbs-56kbs v.90 and ISDN 128kbs links. Cable Modem, open Wireless access and DSL have also been tested. Once completed with the configuration and you can Telnet to the Terminal Server 2509 router you can also access the servers listed earlier in section 3.0 via Telnet, Windows Terminal Services, VNC or HTTP.

Recommended OS platforms for the VPN are Windows 2000 (any version) and Windows 98 second edition. VPN access has not been tested on Linux, Solaris or Apple platforms.

To access the lab over the VPN follow the instructions in the file named: **VPN CONFIGURATION**

Once your VPN is running you can Telnet to the following devices from your workstation:

- 10.1.1.60** **2509 Terminal Server**
- 10.1.1.77** **WIN2KSRV Windows server**
- 10.1.1.78** **LINUXDEV Linux server**
- 10.1.1.79** **LINUXFWRTR Linux firewall/router**
- 10.1.1.87** **WTI Power Management strip**
- 10.1.1.53** **SW3 if crossover cable is enabled**
- 10.1.1.48** **Router8 AGS+ if available**

You can use Windows Terminal Services client to the following systems from your workstation:

- 10.1.1.77** **WIN2KSRV Windows server**

You can VNC to access the following systems from your workstation:

- 10.1.1.77** **WIN2KSRV Windows server**
- 10.1.1.78** **LINUXDEV Linux server**
- 10.1.1.100** **Standalone Agilent Advisor protocol analyzer**

The IP addresses listed earlier are the only addresses you are allowed to connect to thru the VPN for the Firewall is blocking all others. To access any other address or subnet just Telnet to any of the above devices in the DMZ/Backbone to gain access to the rest of the lab devices.

7.0 Windows 2000 Terminal Services and VNC

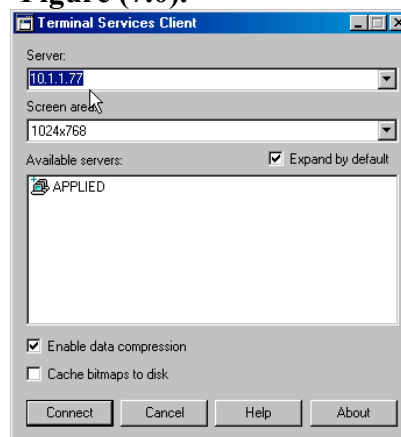
7.1 Windows Terminal Services Client

To access the GUI desktop of the **WIN2KSERV** server you must install the Terminal Server client software on your workstation. The software is included in two zip files named:

TSDISK1.ZIP
TSDISK2.ZIP

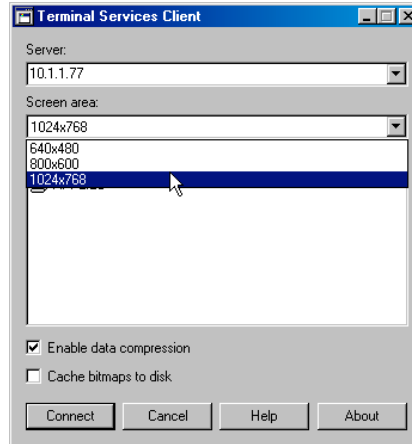
Unzip each of these files to a formatted floppy diskette. Then run the setup program on **disk#1** to install the Terminal Server client. You will be prompted to insert **disk#2** to complete the installation. Once completed run the Terminal Services Client application and input the IP address of the **WIN2KSERV** server(**10.1.1.77**). See **figure (7.0)**

Figure (7.0).



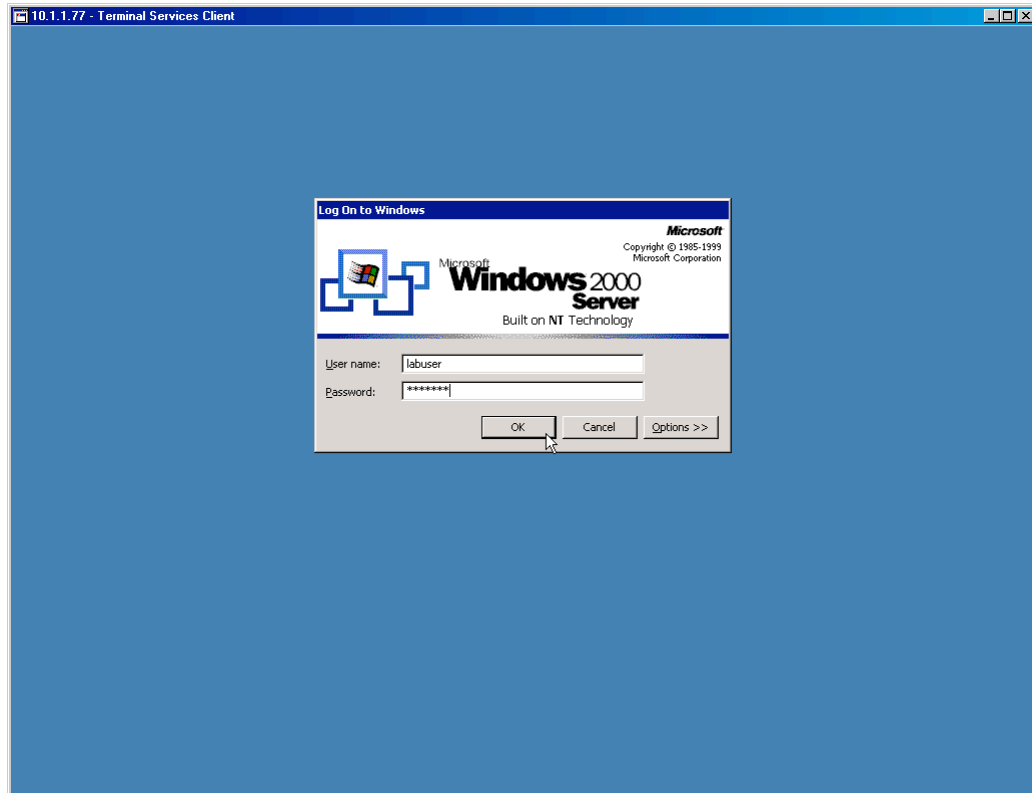
Remember to select what display size you want as per **figure (7.1)**.

Figure (7.1).



Press the connect button and you will see the following screen **figure (7.3)**.

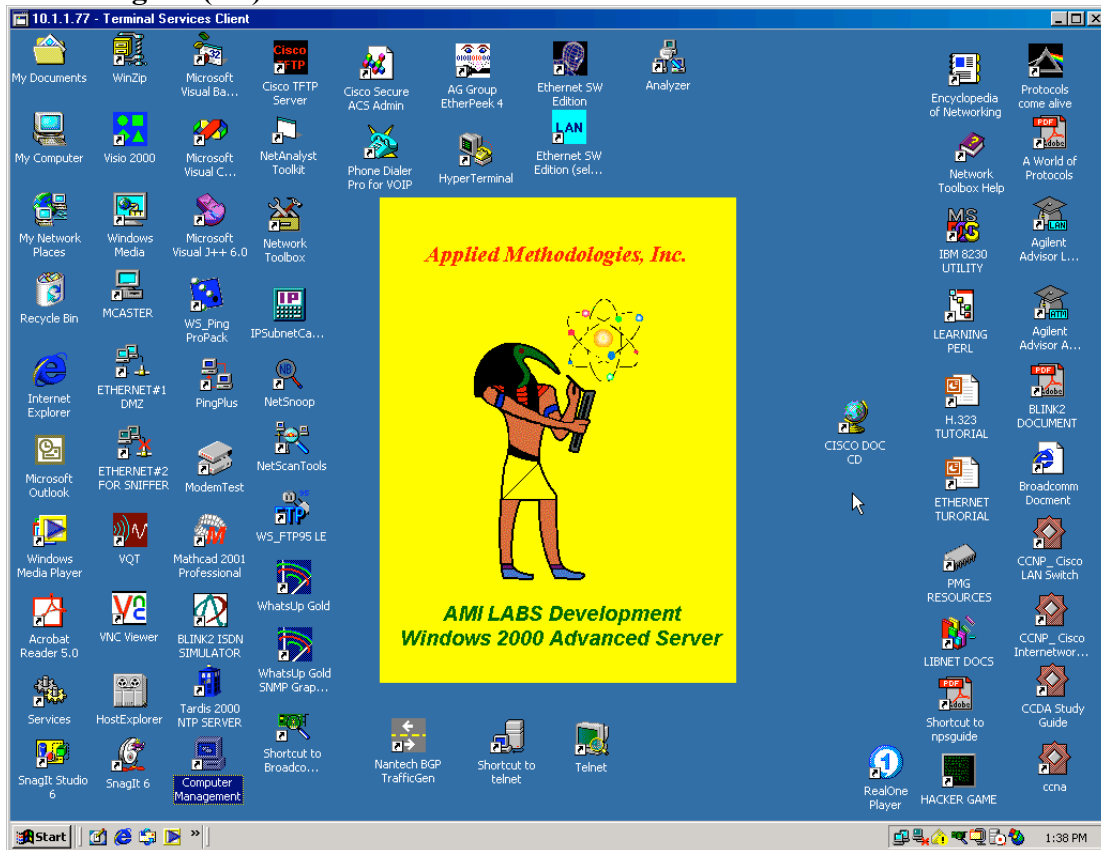
Figure (7.3).



Then login passwords are supplied in file named **LAB PASSWORDS** included in the VPN kit.

You will now have the desktop of the server in a separate window via the VPN for you to access the applications of your choice as shown in **figure (7.4)**.

Figure (7.4).



7.2 Virtual Network Computing (VNC) setup

Virtual Networking Computing or VNC gives you a similar method to remotely access the GUI desktop and have complete remote control of a lab server. VNC is not as robust as Windows Terminal Services but runs on many platforms such as Linux, Win98, MacOS, BSD UNIX and many more. VNC is required to use the protocol analyzers on the WIN2KSRV and the standalone Agilent Advisor. You can also use VNC to access LINUXDEV for a GUI terminal.

Please refer to the file named: **VNC SETUP MANUAL** included in your VPN kit.

Please refer to the VNC web site for additional documentation about VNC and how to install and use VNC options. The link is: <http://www.uk.research.att.com/vnc/index.html>.

8.0 Documentation files included in the VPN kit

<u>File name</u>	<u>Description</u>
LAB PASSWORDS	Text document with all the user ids and passwords
AMI NETWORK LAB	Visio diagram of lab
VOIP MECHANICS	Visio diagram of how VOIP testing is executed
VPN CONFIGURATION	VPN configuration document
VPN LAYOUT	Visio VPN diagram depicting how lab access works
TSDISK1.ZIP	Terminal Server installation disk#1
TSDISK2.ZIP	Terminal Server installation disk#2
vnc-3.3.4-x86_win32.exe	VNC installation file
VNC SETUP MANUAL	VNC setup and use instructions
LAB Manual	This document

9.0 Lab Policies(Do's and Don'ts)

This lab is an open lab for your certification studies, general Computer Science and network technologies research. Please be cognizant of others using this lab. The following policies are a set of general use guidelines to prevent problems from occurring and to ensure that your lab experience is as positive as possible.

- Save your router/switch configurations in your own directory.
- Do not go into other users directories without their permission. Do not delete files or directories that were not your own. You can post your request to share files on the lab message board.
- You can start and stop any service or daemon on the servers but please set the service and daemon back to its original state it was in when your lab session started.
- You can add applications to the servers for your use in the lab but please inform the lab administrator of this.
- Any applications, utilities or tools downloaded to the server should reside in the DOWNLOAD directory.
- Do not remove any applications from any of the lab servers.
- Do not change any of the registry entries or daemon processes in any of the servers unless you know what you are doing, notify the lab administrator if you need to do this for a utility you are installing.
- If you ordered only one session and another user follows you after your session, your router/switch configs will be reset for the next user. (save your configs)
- If you ordered consecutive sessions back to back or across some open time slots your router configs will be preserved. If another user orders a slot in-between your sessions your configs. will NOT be backed up to your directories. Please try to order consecutive time slots to reduce any administration mishaps.
- Any hacking or denial of service attacks launched from this lab to outside Internet systems is strictly prohibited.
- You can launch Denial of Service, worms and other security related exploits in this lab but please be careful. Do not launch any virus or exploit that will damage any lab equipment or hard disk.
- Do not change any of the lab servers boot parameters.
- Do not change any of the lab server's disk partition configurations.
- Do not change or flip any of the lab servers primary network interface IP address you may lose connectivity to the server.
- Please do not change any of the operating system and program files on the stand alone Agilent Advisor.
- Damage to any equipment hardware or software based resulting in any components of the lab becoming unusable that was not the result of testing the last user on the lab may be responsible, held accountable, and removed from any further use.
- Any equipment or software failures that prevented you the use of accessing a lab device, that was not caused by testing or changes, will be credited to your session

block of time. If you lost an hour due to a hardware problem you can just use that hour at another time or lump it into another session.

- AMILABS is not responsible for files left on the server in user directories. Please backup your experiment documentation and configuration files over the VPN to your PC.
- AMILABS is not responsible for poor performance due to a slow connection to the Internet or Internet traffic impacting access to the lab. Slow VPN performance is not considered a hardware or software problem.

10.0 Pricing and Scheduling

The cost to rent online lab time is \$45 per 7 hour block. There will be three seven-hour blocks available per day. A seven-hour session seemed to be just the right amount of time on average for someone to spend on such a rack. Since 8 to over 12 hours for even a lower cost rack is just not efficient. This is the case for those studying for any certification, for a 12 or 24 hour block is almost useless because during your sleep time you are just throwing money away. Lower cost blocks of time, but with fewer routers and switches for CCNA/DA type students, is available upon request. The 7 hours is enough to have a day of testing or experimenting. The AGS+ is not included in this price. It is available upon request at \$3.00 extra per session.

For Cisco CCIE candidates using this lab:

So for the CCIE rule of thumb of 300 hours of rack time, the total cost to you here could be \$1,935.00. This is 43 x 7 hour block sessions at \$45.00 per 7hr block. You do not have to use all 43 blocks and just use what and when you need to of course. As you can see \$1,935.00 is less than the cost of just one Catalyst 3550 switch. So instead of purchasing a lab just use AMI's. The 7-hour blocks will be scheduled on a first come first serve basis. AMILABS will try to keep the availability according to your needs however, if demand increases a fixed three session per day schedule may be implemented. Since most study material and practice labs are already available in abundance on the Internet AMILABS will not offer any practice labs or scenarios. Students can of course store their practice configurations under their own directory and share them with other students.

To request access to AMILABS please send a request email to ADMIN@AMILABS.COM and include in CAPS "**LAB REQUEST**" in the subject field. Also, include the date and the seven-hour time span you would like to have your access available.

Payment for lab time will initially be accepted by PAYPAL, check, money or orders only. Details on where to send payment, refunds, schedule changes, technical support and access after payment is made will be provided in a response email. The lab documentation, passwords and VPN kit will follow your response email.

11.0 Technical support

Although this lab has been tested thoroughly sometimes issues do occur. If you happen to encounter a problem please follow the procedures below.

11.1 Hardware failures

Please report any equipment failures such as Windows hardware message, system freezing, router/switch hardware messages or you just cannot access a device.

To report hardware failures send an email to SUPPORT@AMILABS.COM. In the email message please state, and if you can, cut and paste the error message, the time it happened, and session block you were in.

Remember you have remote reboot capability for all devices. So if a router, or server freezes during a configuration change or test, (especially any spanning tree or debugging testing) you can reboot your device back to the operational state it was in before the change as long as you did not commit any changes to the router or switches.

11.2 Software failures

Please report any software failures such as Windows system messages, Linux messages, router/switch IOS messages that cause a freeze up or complete inoperability of a lab device. Any VPN setup or login issues should also be reported.

To report software failures send an email to SUPPORT@AMILABS.COM in the email state and if you can, cut and past the error message, the time it happened, and session block you were in.

You can also contact the lab administrator at (516)796-9607 press 2 for AMILABS and leave your message.

11.3 Reschedules

If your lab does not work on the onset of access or you had many issues that were identified locally(AMILABS side) as the problem, AMILABS will reschedule your entire session on a case-by-case basis. AMILABS will provide an immediate reschedule to get you going as soon as possible. If the lab is experiencing problems or issue occur that are beyond AMILABS's control you will be immediately notified and rescheduled.

User initiated reschedules

If you booked lab time and are unable to attend AMILABS will try to reschedule your session to meet your convenience depending on other user's schedules. To reschedule your lab please send an email to ADMIN@AMILABS.COM and request a reschedule and the 7 hour slot you would like one full day in advance of your lab session start time. AMILABS does understand, especially if you work in IT and even more if you support a network that you might be detained at work and could miss you scheduled lab slot. If this happens please send an email as soon as possible to the email address listed earlier stating your issue and the 7-hour session you would like. Also, call **(516)796-9607 press 2** and leave a message stating information about your session's reschedule.

AMILABS understands the urgency of lab use, especially if you are preparing for a Cisco exam. We will do everything to get you up and running and try not to impact your study schedule. AMILABS will provide rescheduled access in the event of lab problems.

12.0 Special Requests

During your research or Cisco studies you may want something changed on the physical layout of your lab for your next study session. Please send your request one day in advance to the email address ADMIN@AMILABS.COM and state specifically what you want moved or added. AMILABS can accommodate changes however, the changes allowed are outlined below:

- Moving a WAN, Token-Ring or Ethernet cable to different ports changing the physical layout of the lab can be accommodated within reason. (Just a couple of cables for a test but not a complete lab physical change)
- Requesting the AGS+ and IBM Token-Ring Bridge to become activated
- Moving a server's second interface to another physical port
- Changing LAN/WAN modules on the stand alone Agilent Advisor (switching from fast Ethernet to Ethernet/Token-Ring LAN module)
- Activating POTS modem to test POTS routing
- Requesting use of the Standalone Agilent Advisor
- Request use of in-house version of CiscoWorks 2000
- Change of kernel or registry entry for an application use

13.0 Disclaimers

AMI is not responsible for any pirated/duplicated applications found on their servers and prohibits these activities to the best of its abilities. Any duplicated, unlicensed or stolen applications, excluding freeware, shareware and the applications originally provided on the servers, shall be removed.

AMI LABS provides you access to its data network communications lab for research and educational uses only. AMI is not responsible for any malicious code created or launched from this lab that results in any activities deemed criminal or resulting in another user's or business's internet site or internal computer systems to be compromised, destroyed or denied access to any internal network or the internet.

This online lab system is not affiliated with nor endorsed by Cisco Systems Inc.c.. Cisco, Cisco Systems, Cisco Systems logo, CCNA, CCNP, CCDA, CCDP, CCIE, Cisco Certified Network Associate, Cisco Certified Network Professional, Cisco Certified Design Associate, Cisco Certified Design Professional, and Cisco Certified Internetwork Expert are registered trademarks of Cisco Systems Inc. This manual is not associated with nor endorsed by Cisco Systems, Inc.

All manufactures hardware, software and technology concepts mentioned in this documentation are registered trademarked and copyrighted by their respective corporations.

All applications in this lab have been purchased or donated for use.

Have fun and enjoy your research...

Applied Methodologies, Inc.

