

Installing RADIUS in Windows 2003 SP1, using the WRT54G V4 AP

This is the first document of three to be used in this lab activity. The other two documents are: Domain Controller and WAP Enterprise.

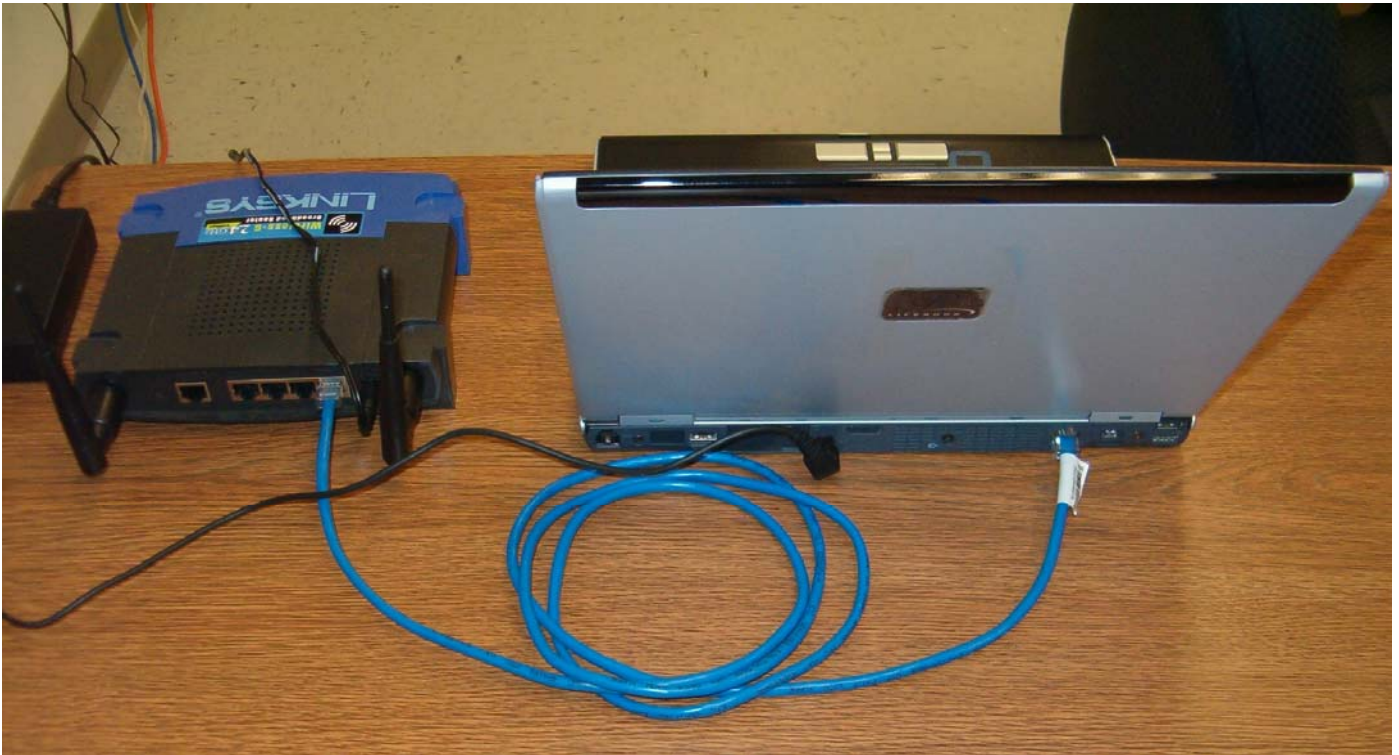
The lab setup is oriented towards using the least amount of equipment, and a quick setup, using the options to assure a quick connection. By no means can this setup be used in a production environment.

With additional equipment along with the proper security measures it can be scaled:

- A standalone CA server or purchase a certificate. Microsoft recommends transferring certificates via floppies or other channels, as long as the CA authority is physically isolated, from unauthorized users and disconnected from the network.
- A secured advanced server installation. Only needed services are to be running, proper firewalls and of course up to the latest service level. Utilities such as Nessus can be used to test the security of the server.
- A secured AP. Proper password schemes, change default passwords, disable WEB management, etc.

The list above is just a starting point; the attached documents provide more information. The RADIUS server can manage a large number of AP's, although in such cases, Microsoft recommends to have two RADIUS servers for redundancy, half of the devices is setup in one, the other half in the other one, and both RADIUS servers are pointing at each other as backup. The additional documentation provides more info.

To start, configure the equipment following the sequence given by the pages below.



List of equipment:

1. Laptop and software
 - We used a Fujitsu S-6230 with 512MB RAM
 - Windows 2000 Professional SP4
 - VMWare version 5.5.1
 - 1 Ethernet adapter
 - 1 Wireless G adaptor (Client)
2. Windows 2003 Server SP1 installed in VMWare
 - Default settings used (240MB RAM, 1 Ethernet adapter).
 - See VNP Setup 2.doc for more info. (Server)
3. LINKSYS WRT54G V4 (Firmware version 4.30.05)

Go ahead and connect everything.

Access Point

1. Reset the AP
 - Set the LAN IP to 172.16.1.1/24

The screenshot shows the Linksys WRT54GL router configuration interface. The page is titled "Setup" and includes a navigation menu with options like "Wireless", "Security", "Access Restrictions", "Applications & Gaming", "Administration", and "Status". The "Internet Setup" section is active, showing "Automatic Configuration - DHCP" selected. The "Router IP" section is also visible, showing the Local IP Address set to 172.16.1.1 and Subnet Mask set to 255.255.255.0. The DHCP Server is enabled, with a Starting IP Address of 172.16.1.100, Maximum Number of DHCP Users set to 50, and Client Lease Time set to 0 minutes. A help sidebar on the right provides additional information about the settings.

LINKSYS
A Division of Cisco Systems, Inc. Firmware Version: v4.30.5

Wireless-G Broadband Router **WRT54GL**

Setup | **Wireless** | **Security** | **Access Restrictions** | **Applications & Gaming** | **Administration** | **Status**

Basic Setup | DDNS | MAC Address Clone | Advanced Routing

Internet Setup

Internet Connection Type Automatic Configuration - DHCP

Optional Settings (required by some ISPs)

Router Name: WRT54GL
Host Name:
Domain Name:
MTU: Auto
Size: 1500

Network Setup

Router IP

Local IP Address: 172 . 16 . 1 . 1
Subnet Mask: 255 . 255 . 255 . 0

DHCP Server: Enable Disable

Starting IP Address: 172.16.1.100
Maximum Number of DHCP Users: 50
Client Lease Time: 0 minutes (0 means one day)
Static DNS 1: 0 . 0 . 0 . 0

Automatic Configuration - DHCP : This setting is most commonly used by Cable operators.

Host Name : Enter the host name provided by your ISP.

Domain Name : Enter the domain name provided by your ISP.

More...

Local IP Address : This is the address of the router.

Subnet Mask : This is the subnet mask of the router.

DHCP Server : Allows the router to manage your IP addresses.

Starting IP Address : The address you would like to start

2. Nothing else needs to be changed in the laptop.
 - The laptop will connect to AP
3. Type the default IP of 172.16.1.1.
 - The username is left blank,
 - Password is admin.
4. You might have to renew the IP on the laptop.

5. On Wireless Security page configure the options as shown below.

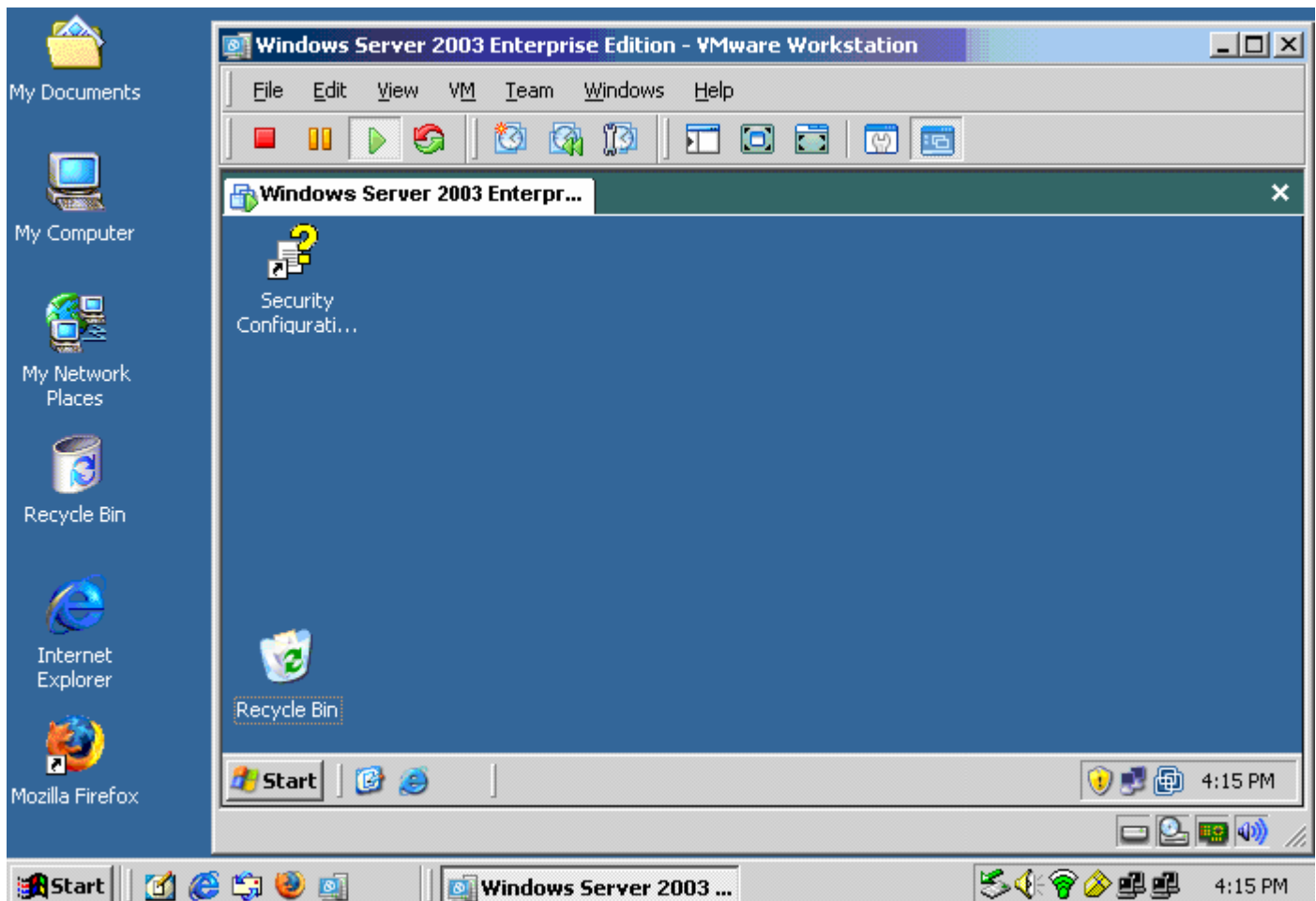
The screenshot displays the Linksys WRT54GL configuration interface. The top navigation bar includes 'Wireless', 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications & Gaming', 'Administration', and 'Status'. The 'Wireless Security' page is active, showing the following configuration fields:

| | |
|------------------------|-------------------|
| Security Mode: | WPA Enterprise |
| WPA Algorithms: | AES |
| RADIUS Server Address: | 172 . 16 . 1 . 10 |
| RADIUS Port: | 1812 |
| Shared Key: | qaz123 |
| Key Renewal Timeout: | 3600 seconds |

At the bottom of the page, there are 'Save Settings' and 'Cancel Changes' buttons. A 'Security Mode' warning box on the right states: 'Security Mode : You may choose from Disable, WEP, WPA Pre-Shared Key, WPA RADIUS, or RADIUS. All devices on your network must use the same security mode in order to communicate. More...'

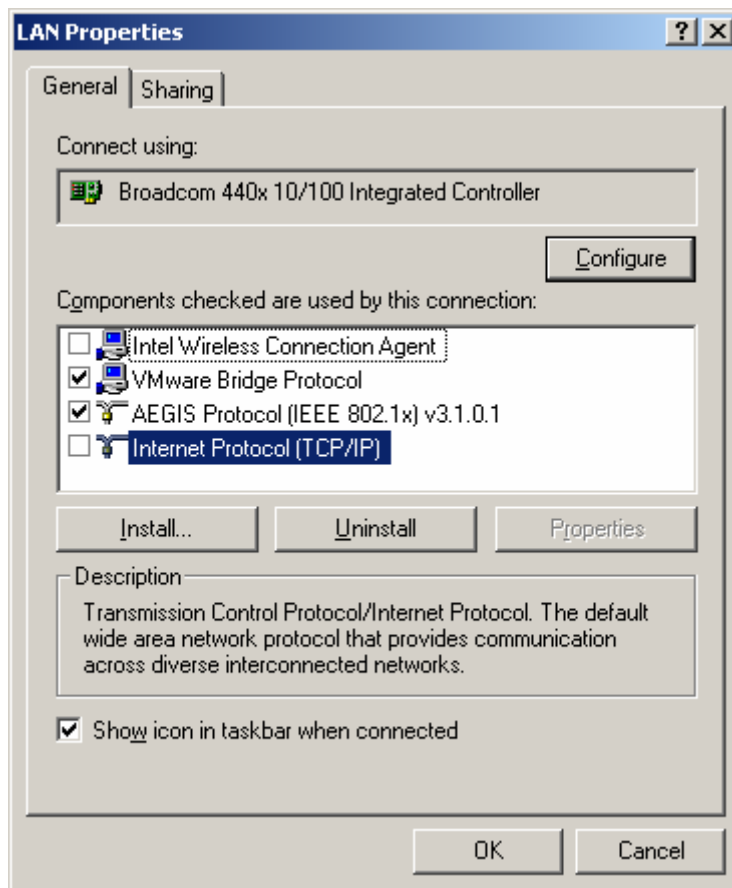
- The shared key only has the purpose of encrypting the traffic between the AP and the RADIUS server. They must match.
- If needed, change the wireless channel to the least used one. The wireless client on the laptop will show the one with least use.

Screen shot of Windows 2000, running Windows 2003 inside VMWare.



6. Go ahead and install Windows 2003 Advanced Server in VMWare
 - The assumption is that the WLAN adaptor will not be associated to an AP, therefore VMWARE will attach itself to the running “copper” adaptor of the laptop.
 - It will remain associated to the Ethernet adaptor for the rest of the lab.
 - The Ethernet adaptor will be used by the virtual adaptor in Windows 2003 to send and receive messages from the RADIUS server to the AP.

Screen shot for the Laptop Ethernet adapter properties.



7. After you have installed the certificate on the wireless client (the laptop), you can come back and disable TCP/IP from the laptop adapter.
 - This will not affect in any way the operation of VMWARE.
 - This will simply avoid a possible problem with Windows 2000 having two IP addresses belonging to the same network segment when the WLAN associated with the AP.

The initial conditions are as follows:

- The WLAN adaptor of the laptop is not attached (associated) to any network.
 - The Ethernet or copper adaptor of the laptop has the IP Protocol enabled
 - The AP is now configured with the IP and the WAP-AES settings ready.
 - The IE version installed on the laptop does not matter, Active X controls will be configured by the server when they are needed, simply accept them; and we do not intend to surf the Internet.
8. Start Windows 2003 and follow the instructions on the Domain Controller document.

Troubleshooting:

Two basic items can go wrong with any setup:

1. Improper credentials are being submitted and
2. Improper encryption protocol setup.

Event Viewer/System will show most of these mistakes. Once you get it to work, play with the settings on the laptop WLAN adaptor, and see the recorded error messages. This last item is a great source of information to gain a better understanding of the logs.

Another source of information are the RADIUS server logs, stored in the system32 folder of Windows Advanced Server, under the name of IN*.LOG, where the wildcard takes the place of characters used to describe the date of the log. If there is no activity in the logs, the most likely problem lies in an erroneous configuration of the encryption protocols. If you have activity in the logs, but the WLAN still does not associate, you are 50% there. Check usernames and other credentials, including the issued certificate to the client. The logs will give you ideas of which set of credentials is wrong.

Items that depend on BIOS settings:

Power saving features, such as standby and processor stepping according to demands can make it very hard to spot problems. These power saving feature settings are very common in laptops. The system will connect, work well, and then stop working suddenly.

The bottom line: Experiment!!!