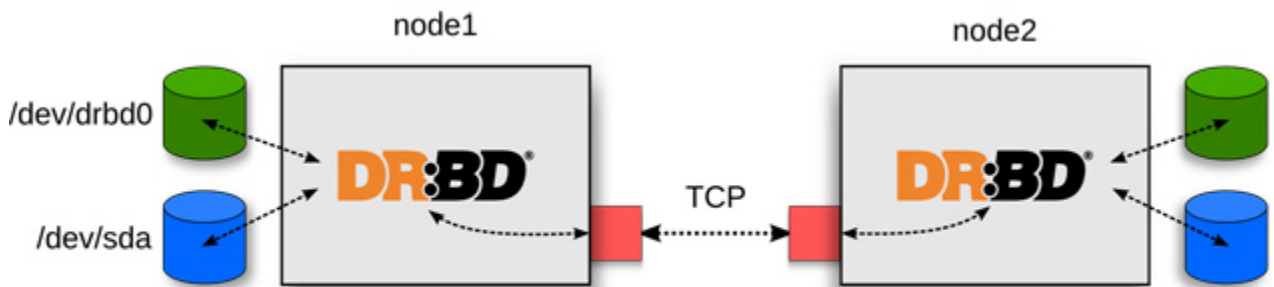


Thiết lập mạng RAID 1 với DRBD trên Ubuntu 11.10

RAID 1 là dạng RAID cơ bản nhất có khả năng đảm bảo an toàn dữ liệu. Cũng giống như RAID 0, RAID 1 đòi hỏi ít nhất hai đĩa cứng để làm việc. Dữ liệu được ghi vào 2 ổ giống hệt nhau (Mirroring). Trong trường hợp một ổ bị trục trặc, ổ còn lại sẽ tiếp tục hoạt động bình thường. Trong khi đó DRBD là viết tắt của **Distributed Replicated Block Device**, là một hệ thống lưu trữ distributed cho các nền tảng GNU/Linux cho phép ngăn chặn các thiết bị mirro trên mạng. Điều này rất hữu ích cho thiết lập có độ sẵn sàng cao (giống như HA NFS server) bởi nếu một nút bị lỗi, toàn bộ dữ liệu vẫn có sẵn từ các nút khác.



Trong bài viết sau chúng tôi sẽ hướng dẫn các bạn thiết lập mạng RAID 1 với sự hỗ trợ của DRBD trên hệ thống Ubuntu 11.10.

Một số lưu ý

Tất cả các lệnh ở hướng dẫn này đều được chạy với quyền root, vì vậy hãy chắc chắn rằng bạn đã trở thành root bằng lệnh:

```
sudo root
```

Ở đây chúng tôi sử dụng hai máy chủ (đều đang chạy Ubuntu 11.10):

- *server1.example.com* (địa chỉ IP 192.168.0.100)
- *server2.example.com* (địa chỉ IP: 192.168.0.101)

Cả hai nút đều có một ổ đĩa unpartitioned thứ hai (*/dev/sdb*) với kích thước giống hệt nhau (trong ví dụ này là 30GB) mà bạn muốn mirro qua mạng (mạng RAID 1) với sự giúp đỡ của DRBD.

Điều quan trọng là cả hai nút đều có thể giải quyết lẫn nhau, hoặc là thông qua DNS hoặc */etc/hosts*. Nếu bạn không tạo những bản ghi DNS cho *server1.example.com* và *server2.example.com*, bạn có thể chỉnh sửa */etc/hosts* trên cả hai nút như sau:

```
server1/server2:
```

```
vi /etc/hosts
```

```
127.0.0.1      localhost.localdomain  localhost
192.168.0.100  server1.example.com    server1
192.168.0.101  server2.example.com    server2

# The following lines are desirable for IPv6 capable
hosts

::1           ip6-localhost ip6-loopback
fe00::0       ip6-localnet
ff00::0       ip6-mcastprefix
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
```

Đồng bộ hóa thời gian

server1/server2:

Việc này rất quan trọng để cả hai nút có cùng một mốc thời gian, chúng ta sẽ cài đặt gói NTP:

```
apt-get install ntp ntpdate
```

Phân vùng */dev/sdb*

server1/server2:

Bây giờ chúng ta phân vùng như sau:

```
fdisk -l
```

```
root@server1:~# fdisk -l
```

```
Disk /dev/sda: 32.2 GB, 32212254720 bytes
255 heads, 63 sectors/track, 3916 cylinders, total 6291
4560 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000712c1
```

Device	Boot	Start	End	Blocks	Id
/dev/sda1	*	2048	499711	248832	83
Linux					
/dev/sda2		501758	62912511	31205377	5
Extended					
/dev/sda5		501760	62912511	31205376	8e
Linux LVM					

```
Disk /dev/sdb: 32.2 GB, 32212254720 bytes
255 heads, 63 sectors/track, 3916 cylinders, total 6291
4560 sectors
Units = sectors of 1 * 512 = 512 bytes
```

Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Disk /dev/sdb doesn't contain a valid partition table

Disk /dev/mapper/server1-
root: 31.4 GB, 31415336960 bytes
255 heads, 63 sectors/track, 3819 cylinders, total 6135
8080 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Disk /dev/mapper/server1-
root doesn't contain a valid partition table

Disk /dev/mapper/server1-
swap_1: 536 MB, 536870912 bytes
255 heads, 63 sectors/track, 65 cylinders, total 104857
6 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Disk /dev/mapper/server1-

```
swap_1 doesn't contain a valid partition table
root@server1:~#
```

Như bạn thấy, `/dev/sdb` không phải phân vùng. Chúng ta thay đổi nó và tạo một phân vùng lớn trên `/dev/sdb1`:

```
fdisk /dev/sdb
```

```
root@server1:~# fdisk /dev/sdb
Device contains neither a valid DOS partition table, no
r Sun, SGI or OSF disklabel
Building a new DOS disklabel with disk identifier 0xf7a
b5969.
Changes will remain in memory only, until you decide to
write them.
After that, of course, the previous content won't be re
coverable.

Warning: invalid flag 0x0000 of partition table 4 will
be corrected by w(rite)

Command (m for help): <-- n
Command action
   e   extended
   p   primary partition (1-4)
<-- p
Partition number (1-4, default 1): <-- 1
First sector (2048-62914559, default 2048): <-- ENTER
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-
62914559, default 62914559): <-- ENTER
```

```
Using default value 62914559
```

```
Command (m for help): <-- t
```

```
Selected partition 1
```

```
Hex code (type L to list codes): <-- 83
```

```
Command (m for help): <-- w
```

```
The partition table has been altered!
```

```
Calling ioctl() to re-read partition table.
```

```
Syncing disks.
```

```
root@server1:~#
```

Bây giờ chạy lại lệnh:

```
fdisk -l
```

và bạn sẽ tìm thấy `/dev/sdb1` trong đầu ra:

```
root@server1:~# fdisk -l
```

```
Disk /dev/sda: 32.2 GB, 32212254720 bytes
```

```
255 heads, 63 sectors/track, 3916 cylinders, total 62914560 sectors
```

```
Units = sectors of 1 * 512 = 512 bytes
```

```
Sector size (logical/physical): 512 bytes / 512 bytes
```

```
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

```
Disk identifier: 0x000712c1
```

Device	Boot	Start	End	Blocks	Id
/dev/sda1	*	2048	499711	248832	83

```
Linux
/dev/sda2          501758      62912511    31205377     5
Extended
/dev/sda5          501760      62912511    31205376    8e
Linux LVM
```

```
Disk /dev/sdb: 32.2 GB, 32212254720 bytes
64 heads, 51 sectors/track, 19275 cylinders, total 6291
4560 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xf7ab5969
```

Device	Boot	Start	End	Blocks	Id
/dev/sdb1		2048	62914559	31456256	83

Linux

```
Disk /dev/mapper/server1-
root: 31.4 GB, 31415336960 bytes
255 heads, 63 sectors/track, 3819 cylinders, total 6135
8080 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```

```
Disk /dev/mapper/server1-
```



```
root doesn't contain a valid partition table

Disk /dev/mapper/server1-
swap_1: 536 MB, 536870912 bytes
255 heads, 63 sectors/track, 65 cylinders, total 104857
6 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

Disk /dev/mapper/server1-
swap_1 doesn't contain a valid partition table
root@server1:~#
```

Cài đặt và cấu hình DRBD

server1/server2:

Tiếp theo chúng ta cài đặt DRBD trên cả hai nút như sau:

```
apt-get install drbd8-utils
```

Tải các module hạt nhân của DRBD:

```
modprobe drbd
```

Kiểm tra nếu nó đã được tải:

```
lsmod | grep drbd
```

Kết quả đầu ra sẽ tương tự như thế này:

```
root@server1:~# lsmod | grep drbd
drbd                273002  0
```

```
lru_cache          14896  1 drbd
root@server1:~#
```

Bây giờ chúng ta trở lại tập tin gốc `/etc/drbd.conf` và tạo một cái mới cho cả hai nodes:

```
cp /etc/drbd.conf /etc/drbd.conf_orig
cat /dev/null > /etc/drbd.conf
vi /etc/drbd.conf

global { usage-count no; }

common { syncer { rate 100M; } }

resource r0 {

    protocol C;

    startup {

        wfc-timeout 15;

        degr-wfc-timeout 60;

    }

    net {

        cram-hmac-alg sha1;

        shared-secret "secret";

    }

    on server1.example.com {

        device /dev/drbd0;

        disk /dev/sdb1;

        address 192.168.0.100:7788;

        meta-disk internal;
```

```
    }  
    on server2.example.com {  
        device /dev/drbd0;  
        disk /dev/sdb1;  
        address 192.168.0.101:7788;  
        meta-disk internal;  
    }  
}
```

Hãy chắc chắn rằng bạn sử dụng chính xác tên nút trong tập tin (thay vì *server1.example.com* và *server2.example.com*), chạy lệnh:

```
uname -n
```

Ngoài ra cũng cần đảm bảo rằng bạn điền chính xác địa chỉ IP trong dòng address và ổ đĩa tại dòng disk (nếu không sử dụng */dev/sdb1*).

Bây giờ khởi tạo lưu trữ dữ liệu meta trên cả hai nodes:

```
drbdadm create-md r0
```

```
root@server1:~# drbdadm create-md r0  
Writing meta data...  
initializing activity log  
NOT initialized bitmap  
New drbd meta data block successfully created.  
root@server1:~#
```

Sau đó khởi động DRBD trên cả hai nodes:

```
/etc/init.d/drbd start
```

```
root@server1:~# /etc/init.d/drbd start
* Starting DRBD resources [ d(r0) s(r0) n(r0) ] [ OK ]
root@server1:~#
```

Trên server1 thực hiện các node chính:

```
drbdadm -- --overwrite-data-of-peer primary all
```

Sau đó dữ liệu sẽ bắt đầu đồng bộ hóa giữa server1 và server2.

Trên server2 chạy lệnh:

```
cat /proc/drbd
```

để thấy tiến trình đồng bộ hóa:

```
root@server2:~# cat /proc/drbd
version: 8.3.11 (api:88/proto:86-96)
srcversion: DA5A13F16DE6553FC7CE9B2
 0: cs:SyncTarget ro:Secondary/Primary ds:Inconsistent/
UpToDate C r-----
      ns:0 nr:10166400 dw:10166400 dr:0 al:0 bm:620 lo:1
pe:7407 ua:0 ap:0 ep:1 wo:f oos:21288860
      [=====>.....] sync'ed: 32.4% (20788/30
716)Mfinish: 0:03:53 speed: 91,180 (86,152) want: 102,4
00 K/sec
root@server2:~#
```

(Bạn có thể chạy:

```
watch cat /proc/drbd
```

để xem những gì đang diễn ra của quá trình này. Nhấn *CTRL+C* nếu muốn thoát.)

Chờ cho đến khi đồng bộ hóa hoàn thành, kết quả hiển thị như sau:

```
root@server2:~# cat /proc/drbd
version: 8.3.11 (api:88/proto:86-96)
```

```
srcversion: DA5A13F16DE6553FC7CE9B2
 0: cs:Connected ro:Secondary/Primary ds:UpToDate/UpToD
ate C r-----
      ns:0 nr:31455260 dw:31455260 dr:0 al:0 bm:1909 lo:0
pe:0 ua:0 ap:0 ep:1 wo:f oos:0
root@server2:~#
```

Đoạn **ro:Secondary/Primary** cho chúng ta biết đây là node thứ cấp.

Trên server1 có đầu ra của

```
cat /proc/drbd
```

như sau (sau khi đồng bộ hóa thành công):

```
root@server1:~# cat /proc/drbd
version: 8.3.11 (api:88/proto:86-96)
srcversion: DA5A13F16DE6553FC7CE9B2
 0: cs:Connected ro:Primary/Secondary ds:UpToDate/UpToD
ate C r-----
      ns:31455260 nr:0 dw:0 dr:31455924 al:0 bm:1920 lo:0
pe:0 ua:0 ap:0 ep:1 wo:f oos:0
root@server1:~#
```

Đoạn **ro:Primary/Secondary** cho chúng ta biết đây là node thứ cấp.

Bây giờ chúng ta đã có mạng RAID 1 ngăn chặn thiết bị `/dev/drbd0` (bao gồm `/dev/sdb1` từ server1 và server2). Chúng ta hãy tạo một hệ thống tập tin ext4 trên đó và mount tới thư mục `/data`. Điều này chỉ thực hiện trên server1.

```
mkfs.ext4 /dev/drbd0
mkdir /data
mount /dev/drbd0 /data
```

Sau đó xem kết quả tại `/dev/drbd0`:

mount

```
root@server1:~# mount
/dev/mapper/server1-root on / type ext4
(rw,errors=remount-ro)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
fusectl on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
udev on /dev type devtmpfs (rw,mode=0755)
devpts on /dev/pts type devpts
(rw,noexec,nosuid,gid=5,mode=0620)
tmpfs on /run type tmpfs
(rw,noexec,nosuid,size=10%,mode=0755)
none on /run/lock type tmpfs
(rw,noexec,nosuid,nodev,size=5242880)
none on /run/shm type tmpfs (rw,nosuid,nodev)
/dev/sda1 on /boot type ext2 (rw)
/dev/drbd0 on /data type ext4 (rw)
root@server1:~#
```

và

df -h

```
root@server1:~# df -h
Filesystem              Size  Used Avail Use% Mounted on
/dev/mapper/server1-root
                        29G 1017M   27G   4% /
udev                    238M   4.0K  238M   1% /dev
tmpfs                    99M   228K   99M   1% /run
```

```
none          5.0M  4.0K  5.0M   1% /run/lock
none          247M    0  247M   0% /run/shm
/dev/sda1     228M   24M  193M  11% /boot
/dev/drbd0    30G   172M   28G   1% /data
root@server1:~#
```

Thử nghiệm

Bây giờ chúng ta tạo một số tập tin hoặc thư mục trong /data tại server1 và kiểm tra xem chúng có được tái tạo trên server2 hay không.

```
touch /data/test1.txt
```

```
touch /data/test2.txt
```

```
ls -l /data/
```

```
root@server1:~# ls -l /data/
total 16
drwx----- 2 root root 16384 2011-10-28 14:12 lost+found
-rw-r--r-- 1 root root    0 2011-10-28 14:13 test1.txt
-rw-r--r-- 1 root root    0 2011-10-28 14:13 test2.txt
root@server1:~#
```

Tiếp theo gỡ liên kết thư mục /data trên server1:

```
umount /data
```

Sau đó gán secondary cho server1:

```
drbdadm secondary r0
```

Vào server2 và kiểm tra xem chúng ta có thể nhìn thấy tập tin/thư mục đã tạo trên server1 trong thư mục /data.

Đầu tiên gán primary cho server2:

```
drbdadm primary r0
```

Kiểm tra đầu ra của

```
cat /proc/drbd
```

bạn sẽ thấy server2 là nút chính:

```
root@server2:~# cat /proc/drbd
version: 8.3.11 (api:88/proto:86-96)
srcversion: DA5A13F16DE6553FC7CE9B2
 0: cs:Connected ro:Primary/Secondary ds:UpToDate/UpToD
ate C r-----
      ns:0 nr:31691444 dw:31691444 dr:664 al:0 bm:1909 lo
:0 pe:0 ua:0 ap:0 ep:1 wo:f oos:0
root@server2:~#
```

Tạo thư mục /data và mount tới /dev/drbd0:

```
mkdir /data
```

```
mount /dev/drbd0 /data
```

Kiểm tra nội dung của thư mục /data:

```
ls -l /data/
```

Nếu mọi thứ diễn ra tốt đẹp, bạn sẽ thấy nội dung của tập tin/thư mục đã tạo trên server1:

```
root@server2:~# ls -l /data/
total 16
drwx----- 2 root root 16384 2011-10-
28 14:12 lost+found
-rw-r--r-- 1 root root      0 2011-10-28 14:13 test1.txt
-rw-r--r-- 1 root root      0 2011-10-28 14:13 test2.txt
root@server2:~#
```

Bây giờ trên server1 chúng ta đã chuyển đổi vai trò cho nó, vì vậy mà đầu ra của


```
cat /proc/drbd
```

sẽ trông như sau:

```
root@server1:~# cat /proc/drbd
version: 8.3.11 (api:88/proto:86-96)
srcversion: DA5A13F16DE6553FC7CE9B2
 0: cs:Connected ro:Secondary/Primary ds:UpToDate/UpToD
ate C r-----
      ns:31691444 nr:185568 dw:421752 dr:31457005 al:83 b
m:1920 lo:1 pe:0 ua:0 ap:0 ep:1 wo:f oos:0
root@server1:~#
```

Bài 3

Cài đặt và thiết lập mạng ngang hàng

1. Mục tiêu:

Trang bị cho học sinh các kiến thức cơ bản về thiết lập và cài đặt mạng ngang hàng. Sau bài học này, học sinh cần phải nắm được các bước cài đặt và thiết lập mạng, nguyên tắc hoạt động của mạng ngang hàng, phương pháp kiểm tra thông tin và ghi nhận cấu hình hệ thống.

2. Yêu cầu thiết bị:

- Máy tính
- Đĩa cài đặt hệ điều hành
- Driver thiết bị
- Card mạng
- Switch
- Cáp mạng
- Đầu nối
- Kim bấm

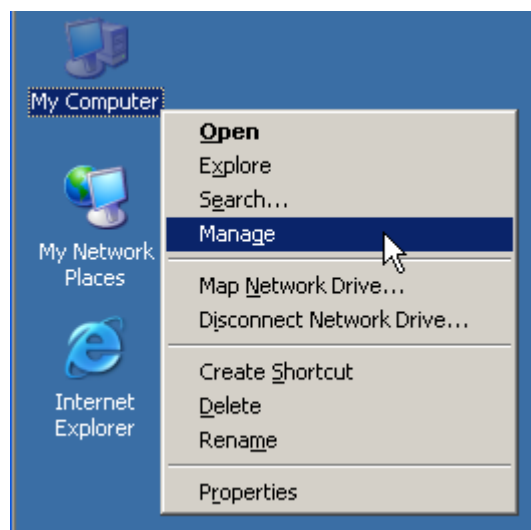
3. Nội dung thực hành:

- Lắp đặt thiết bị phần cứng (card mạng + cáp)
- Cài đặt Card mạng
- Cài đặt giao thức mạng
- Cài đặt dịch vụ mạng
- Thiết lập tên máy, tên vùng
- Đăng nhập mạng
- Kiểm tra kết quả đăng nhập
- Ghi nhận thông tin về cấu hình mạng

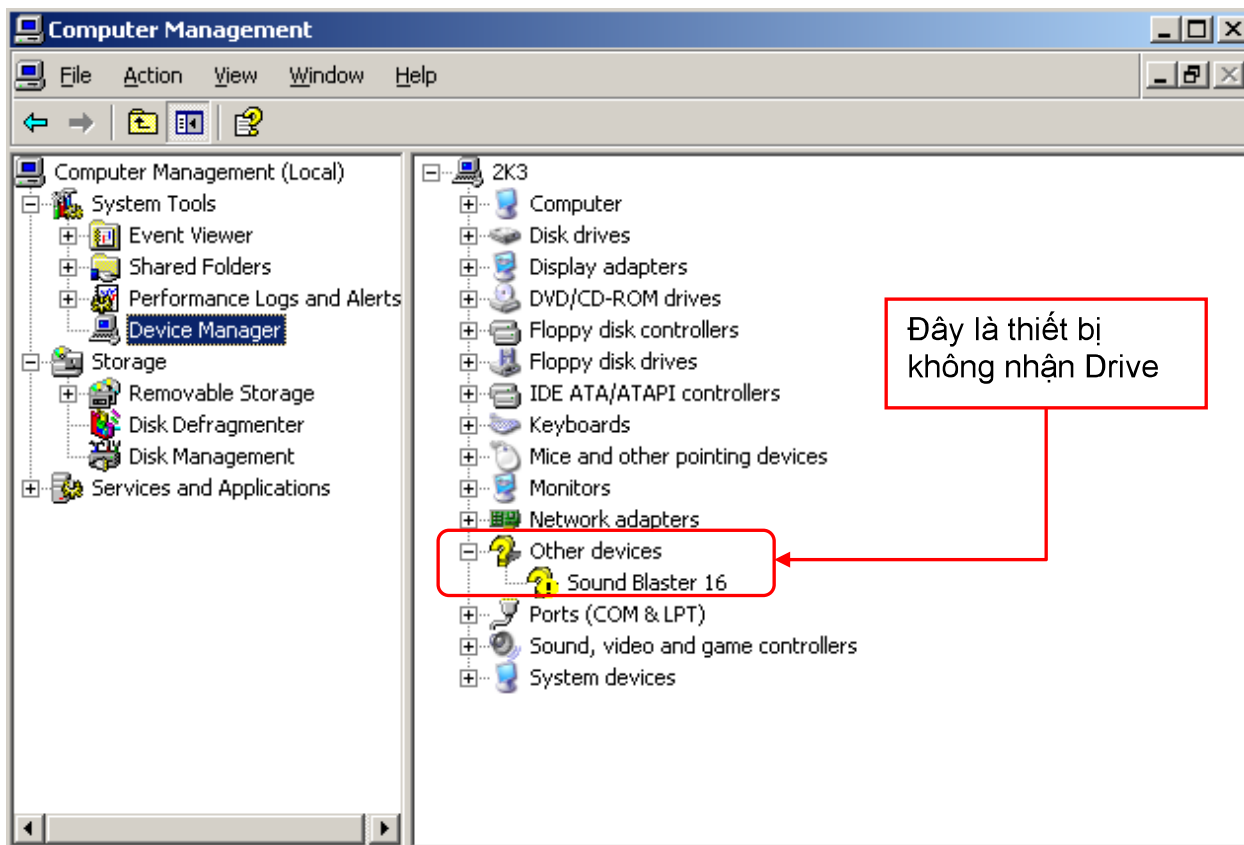
4. Nội dung chi tiết

4.1. - Cài đặt Card mạng

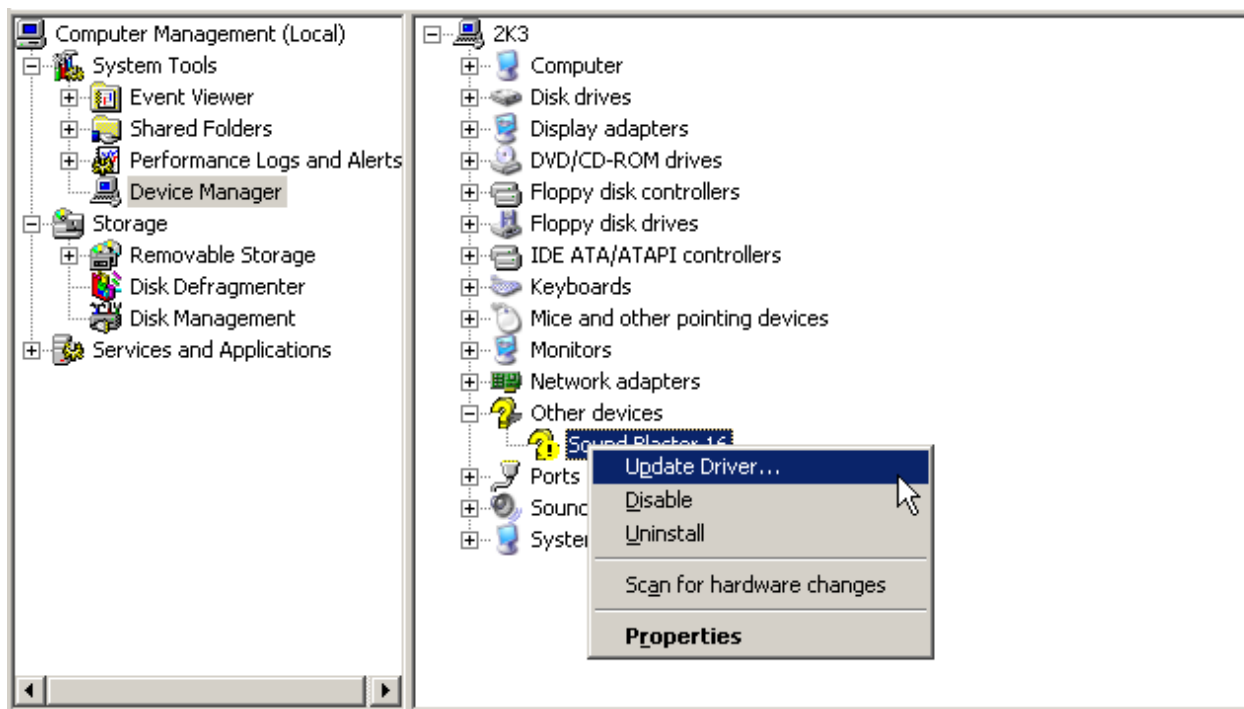
- Mở nắp thùng máy và gắn Card mạng vào khe cắm PCI
- Bật công tắc nguồn – hầu hết các máy tính đời mới hiện nay đều tự động nhận Driver mà không cần phải cài đặt. Nếu trường hợp máy tính không nhận Driver ta tiến hành cài đặt Driver như sau:
 - Nhấp phải chuột vào My Computer – Manage



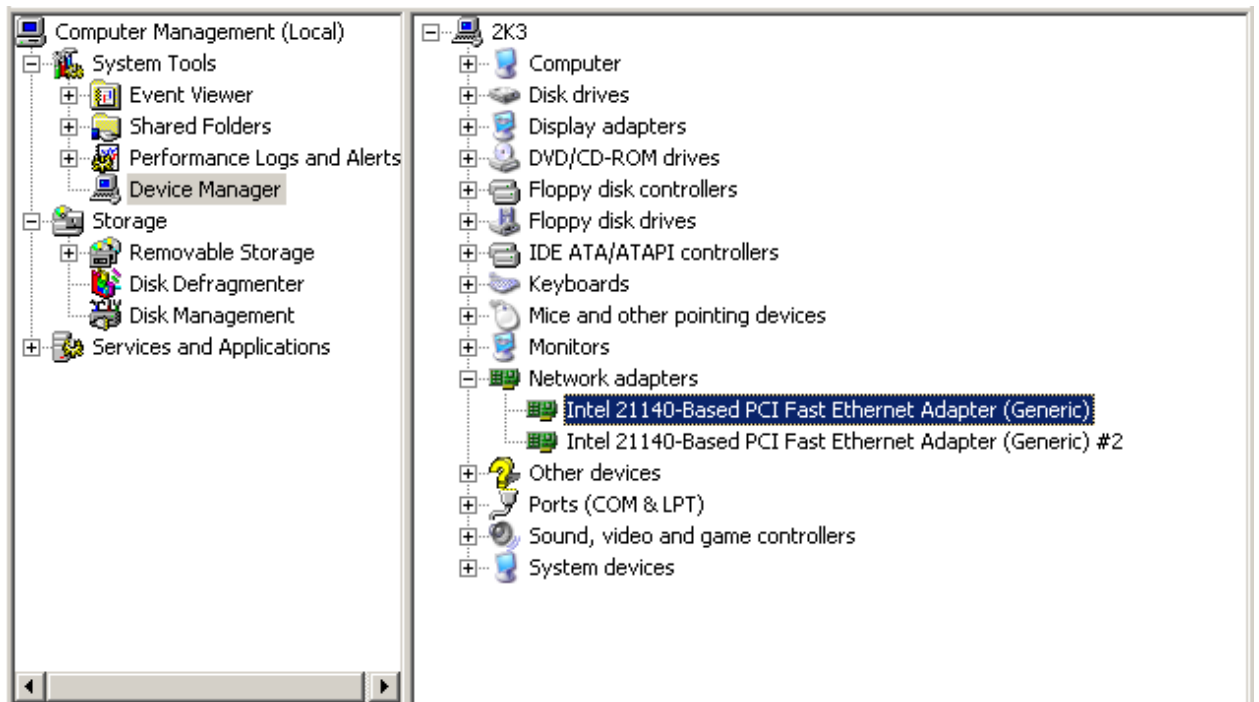
- Trên màn hình Computer Management – nhấp chọn Device Manage



- Trên màn hình bên phải nhấp phải chuột vào thiết bị không nhận Drive – chọn Update Drive

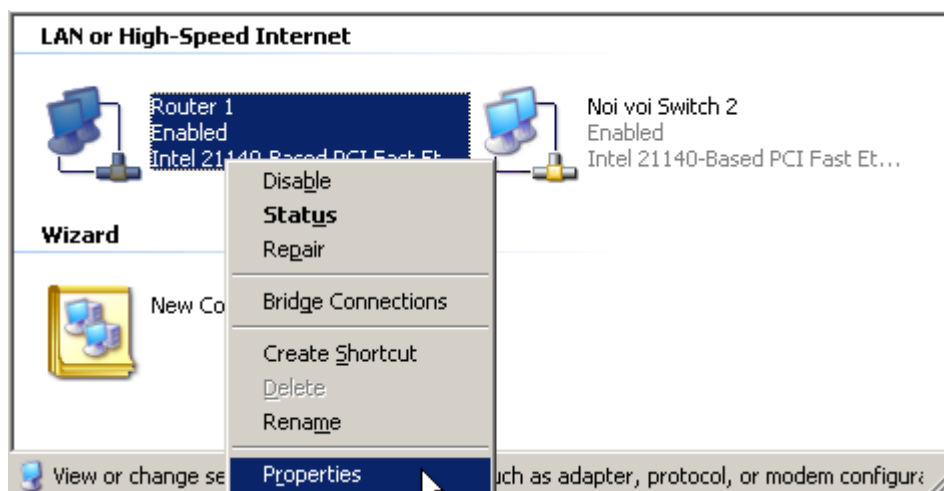


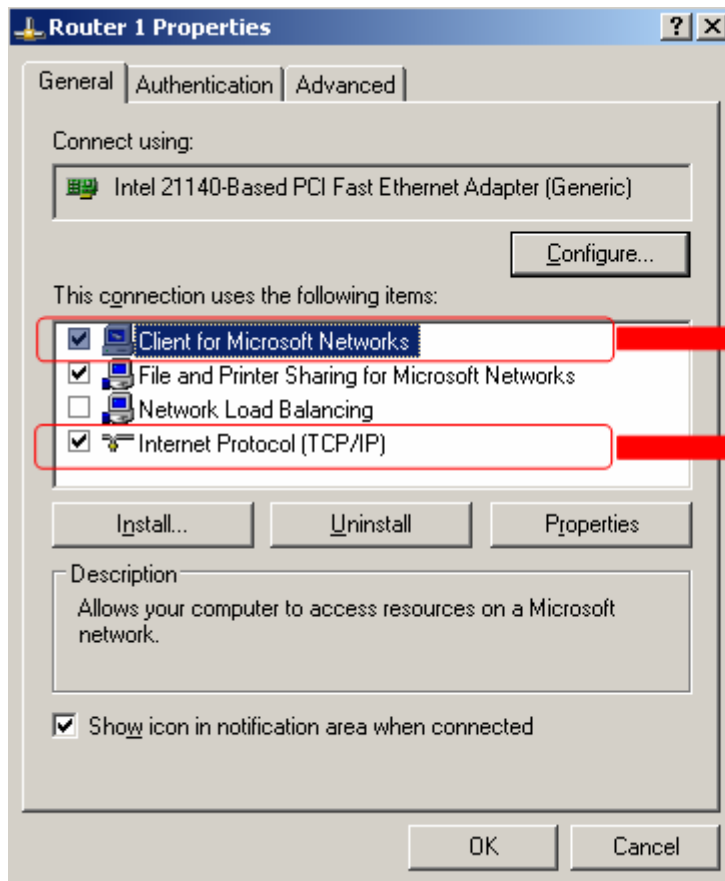
- Đưa đĩa Driver vào ổ CD chọn đúng Driver của Card mạng và nhấp OK
- Card mạng sau khi cài đúng cách trong Device Manager sẽ có dạng như trong hình sau:



4.2- Cài đặt giao thức mạng

- Để các máy tính có thể kết nối được với nhau ta cần phải cài đặt các giao thức sau:
- Kiểm tra các giao thức bằng cách : nhấp phải chuột vào My Network Places – chọn Properties. Trên màn hình Network Connection nhấp phải chuột vào một biểu tượng kết nối và chọn Properties



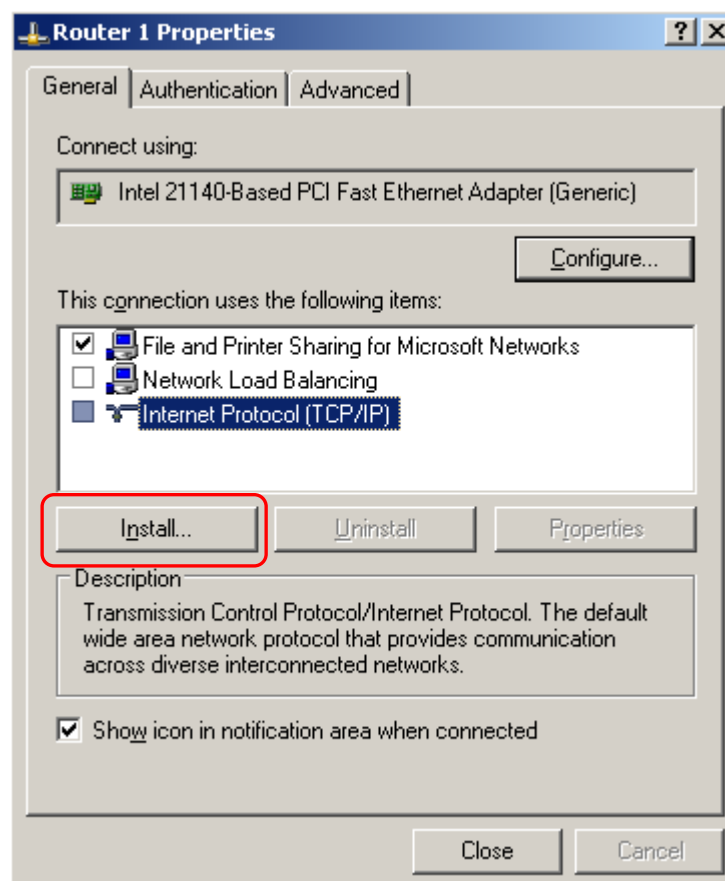


Mặc định sau khi Card mạng được cài đặt đúng cách thì các giao thức này được tự động cài đặt

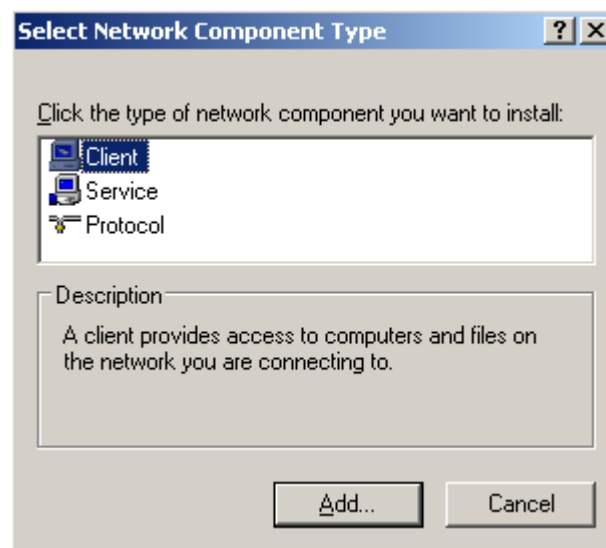
Nếu kiểm tra chưa có các giao thức này ta tiến hành cài đặt như sau:

4.2.1. Cài đặt giao thức Client For Microsoft Network.

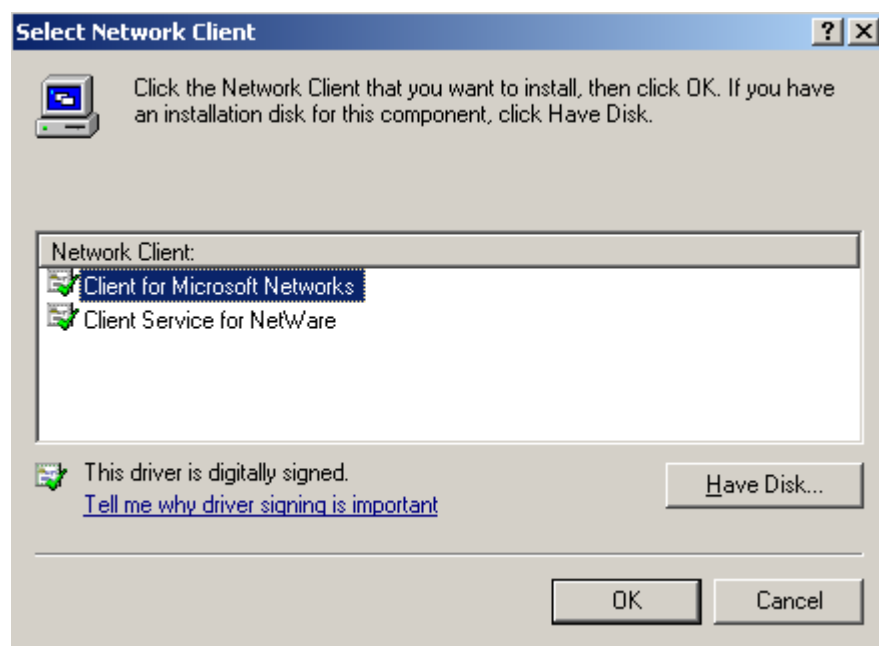
- Trên màn thuộc tính nhấn nút Install



- Trên màn hình Select Network Component Type chọn Client và nhấp Add

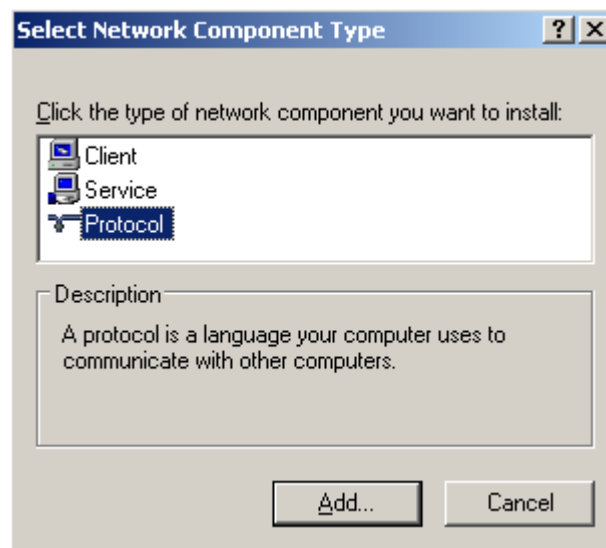


- Trong màn hình Select Network Client chọn Client for Microsoft Network nhấp OK

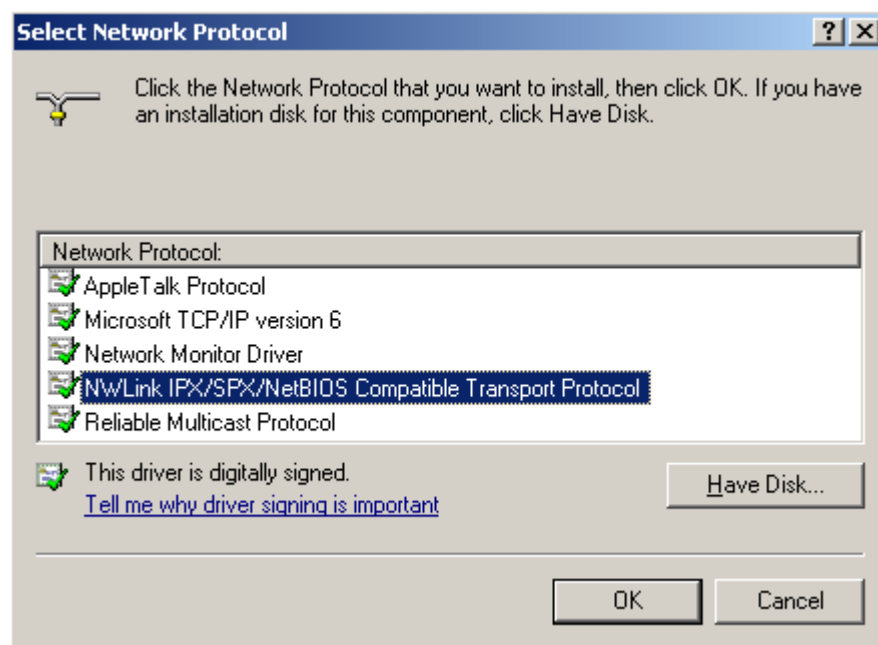


4.2.2. Cài đặt giao thức IPX/SPX hoặc TCP/IP

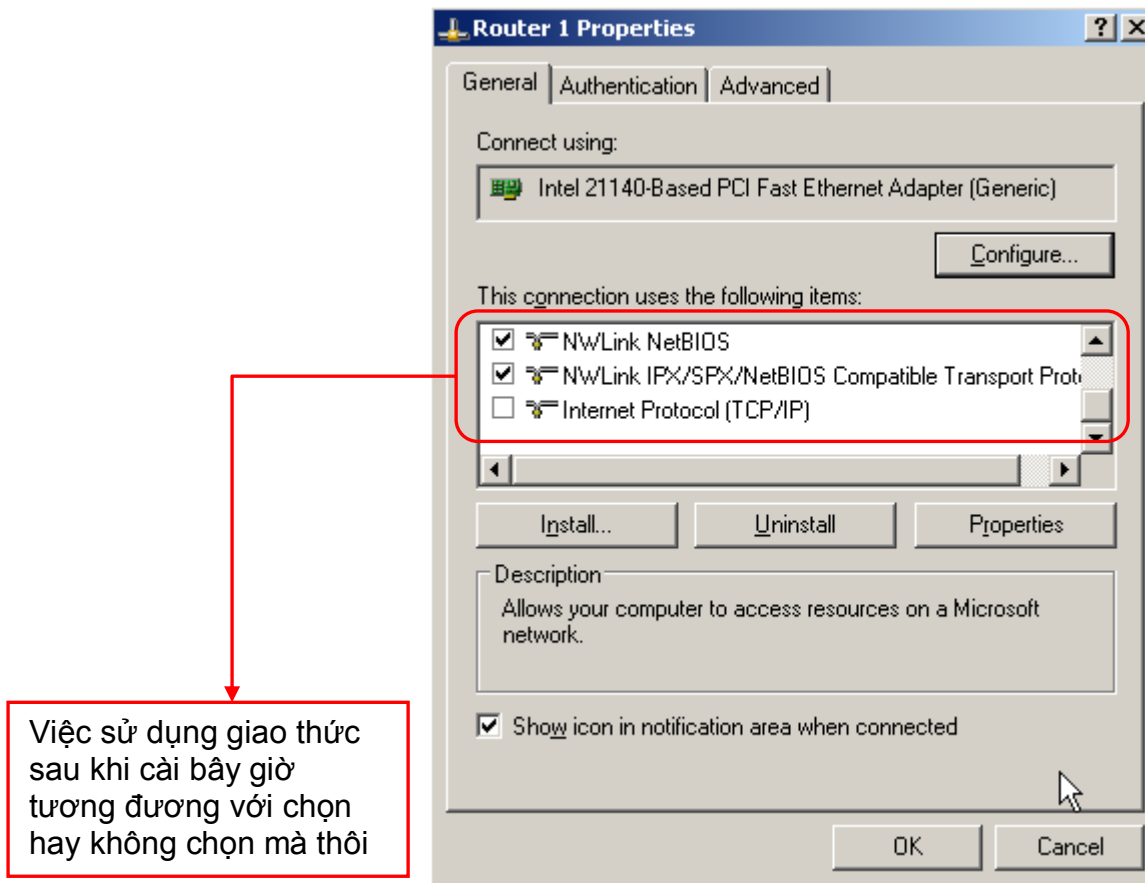
- Làm tương tự phần cài đặt giao thức Client for Microsoft Network nhưng tại màn hình Select Network Component Type chọn Protocol và nhấp Add



- Trên màn hình Select Network Protocol chọn giao thức IPX/SPX và nhấp OK

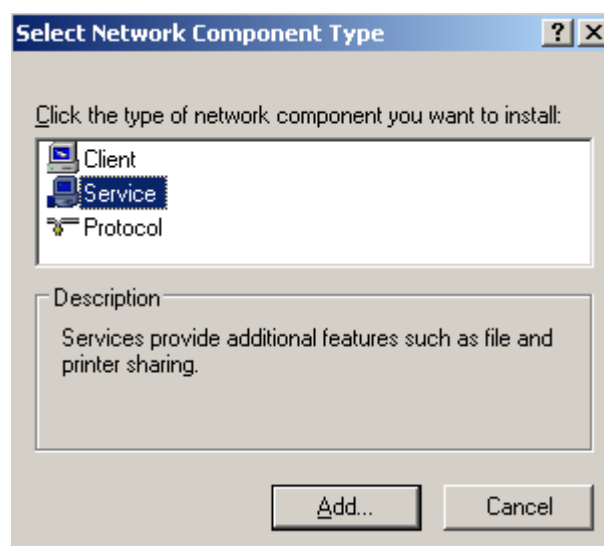


- Sau khi cài các giao thức xuất hiện như sau:

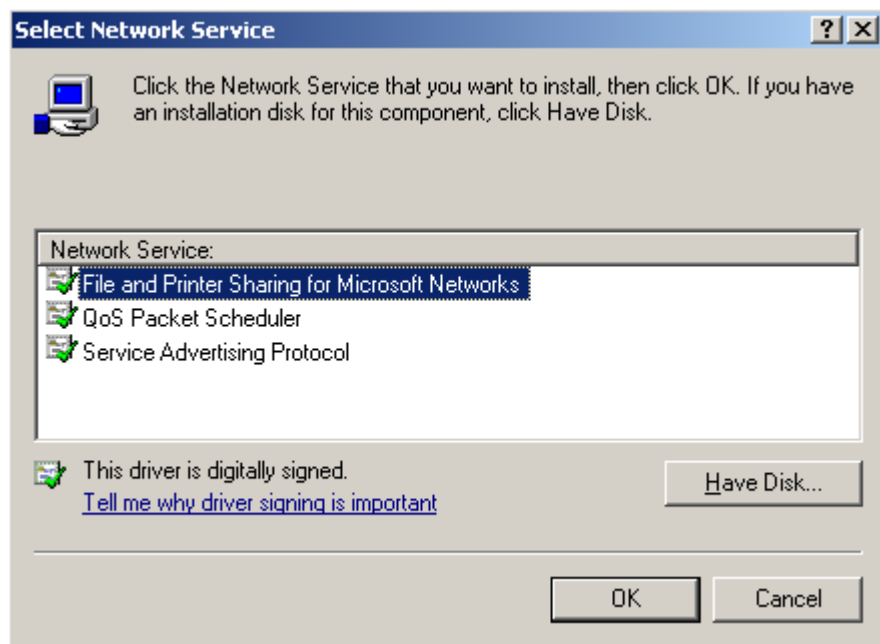


4.3 - Cài đặt dịch vụ mạng

Trên màn hình Select Network component Type chọn Service và nhấp Add



- Trên màn hình Select Network Service chọn File And Printer Sharing for Microsoft Networks và nhấp OK



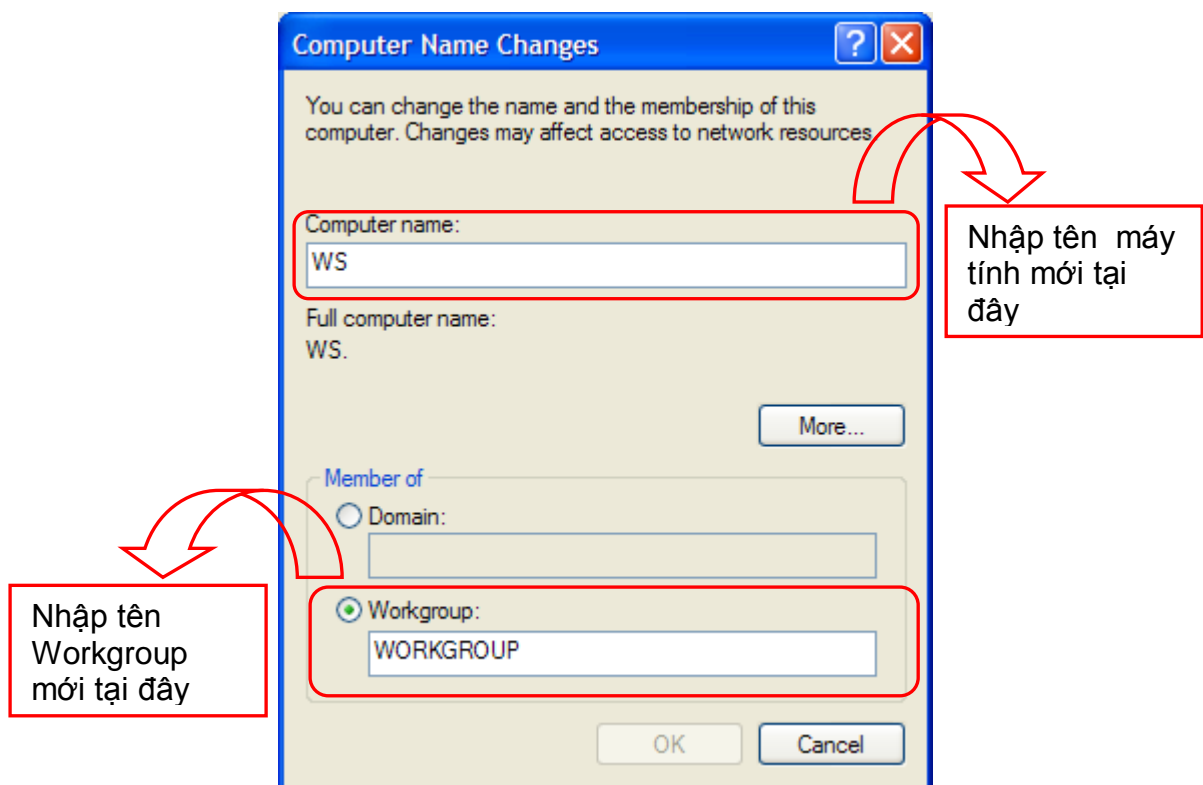
4.4 - Đặt tên máy, tên workgroup

Các máy tính trong cùng mạng phải có:

- Giao thức giống nhau
- Workgroup: giống nhau
- Tên máy tính: phải khác nhau

Đặt lại tên máy trạm và đặt lại tên nhóm:

- Nhấp phải chuột vào My Computer chọn Properties trên màn hình System properties nhấp Tab Computer name và nhấp nút Change



Nhấp OK (*Máy tính yêu cầu khởi động lại để đăng nhập mạng*)

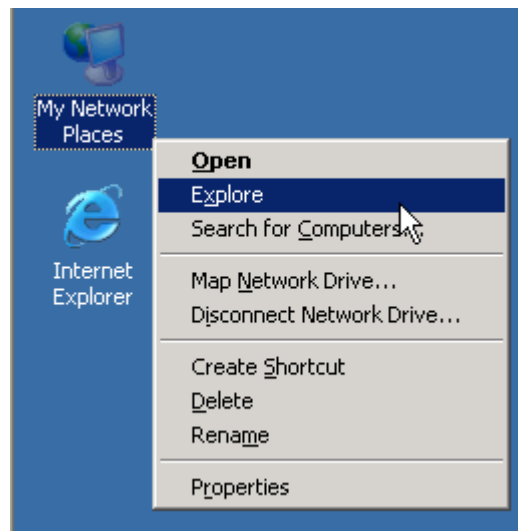
4.5 - Đăng nhập mạng

Đăng nhập lần đầu

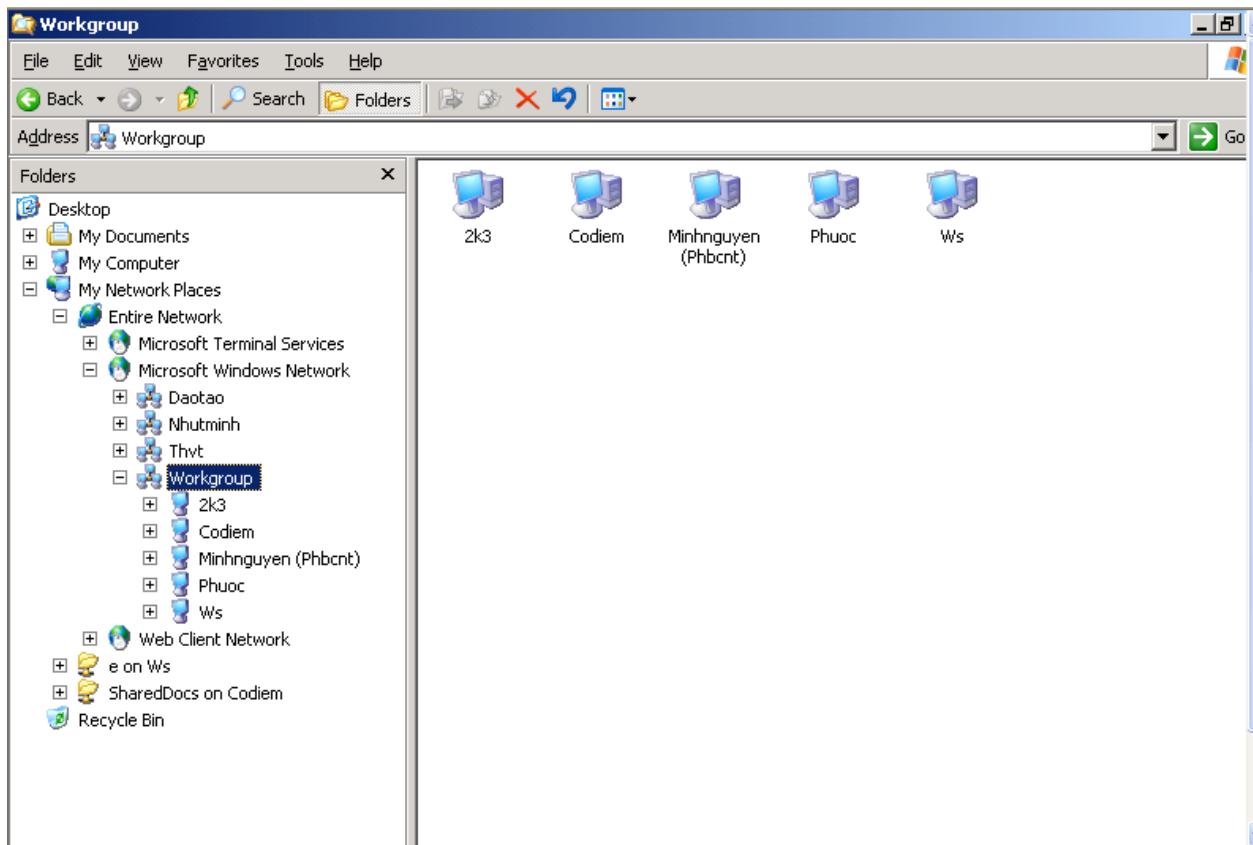
Khởi động máy trạm

Nhập User Name, password và bấm Enter

Nhấp phải Network Places chọn Explore



- Trên màn hình bên trái mở theo đường dẫn sau: My Network Places – Entries Network – Microsoft Windows Network – nhấp chọn Workgroup trên màn hình bên phải là toàn bộ các máy tính có trong nhóm Workgroup

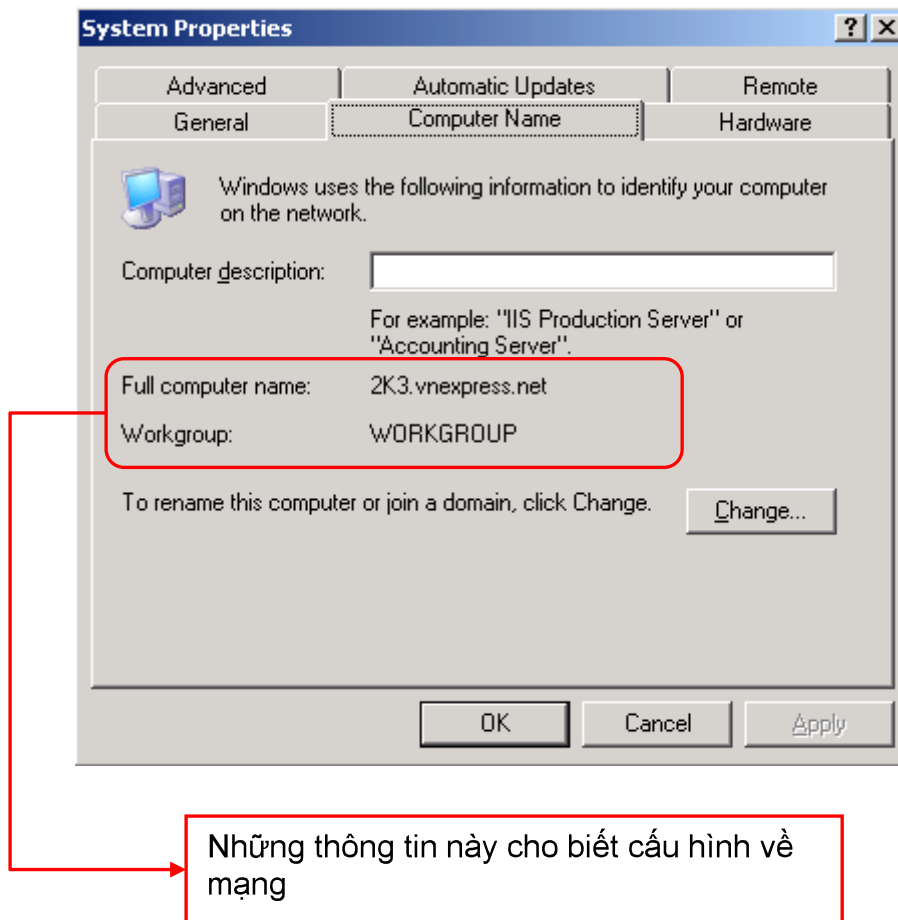


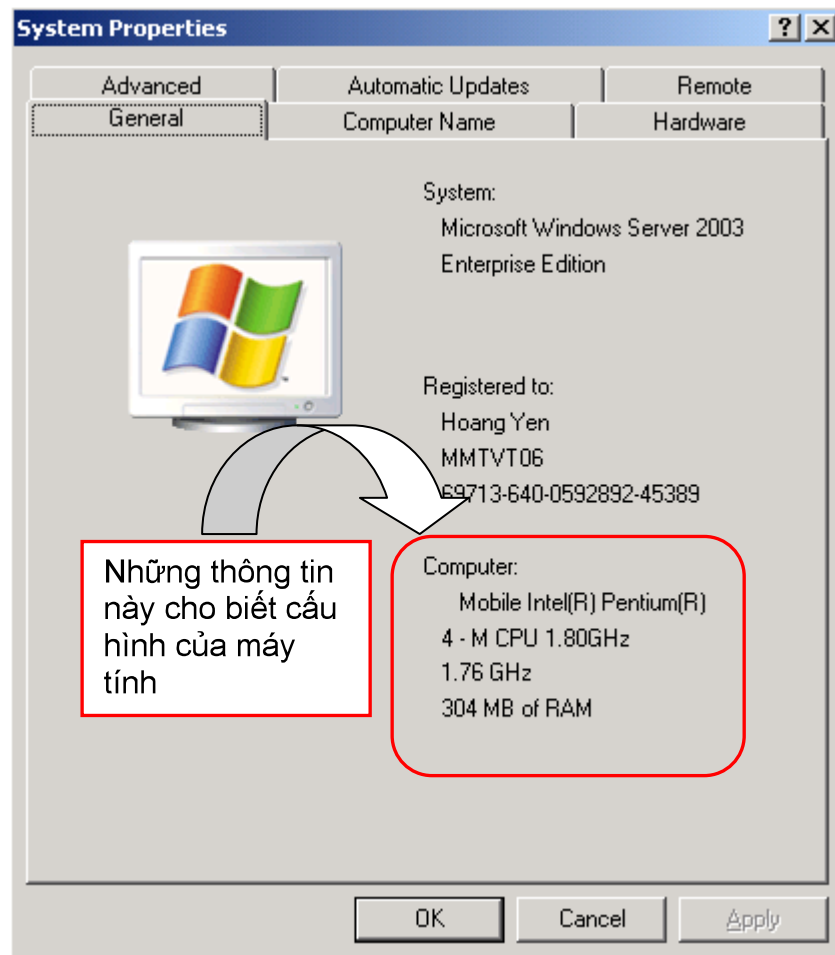
(Nếu xuất hiện biểu tượng các máy khách thì quá trình đăng nhập thành công, nếu không cần phải đăng nhập lại)

4.6 - Ghi nhận thông tin về cấu hình mạng

Muốn biết thông tin cấu hình mạng: nhấp phải chuột vào My Computer chọn Properties và nhấp Tab Computer Name.

Muốn biết thông tin cấu hình máy tính: nhấp phải chuột My Computer – Properties và nhấp Tab General





Hướng dẫn thiết lập mạng không dây

Kết nối mạng không dây đang dần trở thành một xu thế hiện đại, thời thượng bên cạnh các loại hình kết nối mạng truyền thống dùng dây cáp. Chất lượng tin cậy, hoạt động ổn định, thủ tục cài đặt đơn giản, giá cả phải chăng là những yếu tố đặc trưng chứng tỏ kết nối không dây đã sẵn sàng đáp ứng mọi nhu cầu trao đổi thông tin khác nhau từ sản xuất, kinh doanh đến nhu cầu giải trí... Bài viết này sẽ cung cấp cho bạn thông tin cần thiết để xây dựng một mạng máy tính không dây.

Chuẩn công nghệ không dây

Công nghệ mạng không dây do tổ chức IEEE xây dựng và được tổ chức Wi-Fi Alliance chính thức đưa vào sử dụng thống nhất trên toàn thế giới. Có 3 tiêu chuẩn: Chuẩn 802.11a, tốc độ truyền dẫn tối đa 54Mbps; Chuẩn 802.11b, tốc độ truyền dẫn tối đa 11Mbps; Chuẩn 802.11g, tốc độ truyền dẫn tối đa 54Mbps (xem thêm bảng chỉ tiêu kỹ thuật kèm theo). Đặc tính chung của từng công nghệ như sau:

Chuẩn 802.11b có tốc độ truyền dẫn thấp nhất (11Mbps) nhưng lại được dùng phổ biến trong các môi trường sản xuất, kinh doanh, dịch vụ do chi phí mua sắm thiết bị thấp, tốc độ truyền dẫn đủ đáp ứng các nhu cầu trao đổi thông tin trên internet như duyệt web, e-mail, chat, nhắn tin...

Chuẩn 802.11g có tốc độ truyền dẫn cao (54Mbps), thích hợp cho hệ thống mạng có lưu lượng trao đổi dữ liệu cao, dữ liệu luân chuyển trong hệ thống là những tập tin đồ họa, âm thanh, phim ảnh có dung lượng lớn. Tần số phát sóng vô tuyến của chuẩn 802.11g cùng tần số với chuẩn 802.11b (2,4GHz) nên hệ thống mạng chuẩn 802.11g giao tiếp tốt với các mạng máy tính đang sử dụng chuẩn 802.11b. Tuy nhiên theo thời giá hiện nay, chi phí trang bị một hệ thống kết nối không dây theo chuẩn 802.11g cao hơn 30% so với chi phí cho một hệ không dây theo chuẩn 802.11b.

Chuẩn 802.11a tuy có cùng tốc độ truyền dẫn như chuẩn 802.11g nhưng tần số hoạt động cao nhất, 5GHz, băng thông lớn nên chứa được nhiều kênh thông tin hơn so với hai chuẩn trên. Và cũng do có tần số hoạt động cao hơn tần số hoạt động của các thiết bị viễn thông dân dụng như điện thoại 'mẹ bồng con', Bluetooth... nên hệ thống mạng không dây sử dụng chuẩn 802.11a ít bị ảnh hưởng do nhiễu sóng. Nhưng đây cũng chính là nguyên nhân làm cho hệ thống

dùng chuẩn này không tương thích với các hệ thống sử dụng 2 chuẩn không dây còn lại.

Cách chọn mua thiết bị không dây

Thiết bị cho mạng không dây gồm 2 loại: card mạng không dây và bộ tiếp sóng/điểm truy cập (Access Point - AP). Card mạng không dây có 2 loại: loại lắp ngoài (USB) và loại lắp trong (PCI). Chọn mua loại nào tùy thuộc vào cấu hình phần cứng (khe cắm, cổng giao tiếp) của PC. Loại lắp trong giao tiếp với máy tính qua khe cắm PCI trên bo mạch chủ nên thủ tục lắp ráp, cài đặt phần mềm cũng tương tự như khi chúng ta lắp card âm thanh, card mạng, card điều khiển đĩa cứng... Loại lắp ngoài nối với máy tính thông qua cổng USB nên tháo ráp rất thuận tiện, thích hợp với nhiều loại máy tính khác nhau từ máy tính để bàn đến máy xách tay, lại tránh được hiện tượng nhiễu điện từ do các thiết bị lắp trong máy tính gây ra. Cần lưu ý nếu PC dùng cổng USB 1.0 (tốc độ truyền dữ liệu 12Mbps) thì chỉ thích hợp với chuẩn 802.11b, nếu dùng với 2 chuẩn còn lại thì sẽ làm chậm tốc độ truyền dữ liệu.

Thủ tục để xây dựng một mạng ngang hàng (peer-to-peer) không dây rất đơn giản. Chỉ cần trang bị cho mỗi máy tính một card mạng không dây, bổ sung

phần mềm điều khiển của thiết bị là các máy tính trong mạng đã có thể trao đổi dữ liệu với nhau. Nhưng nếu muốn truy xuất được vào hệ thống mạng LAN/WAN sẵn có hay truy xuất internet thì phải trang bị thêm thiết bị tiếp sóng Access Point. Chức năng chính của thiết bị này gồm tiếp nhận, trung chuyển tín hiệu giữa các card mạng trong vùng phủ sóng và là thiết bị chuyên tiếp trung gian giúp card mạng không dây giao tiếp với hệ thống mạng LAN/WAN (cũng có khi là modem) và internet. Tuy nhiên tùy theo quan điểm của nhà sản xuất, yêu cầu sử dụng và tạo thuận tiện cho người quản trị mạng, một số thiết bị Access Point có thêm một vài chức năng mạng khác như: cổng truy nhập (gateway), bộ dẫn đường... TGVN A số tháng 4/2003, 5/2003, 8/2003 và 11/2003, có bài viết giới thiệu một số loại Access Point cùng các tính năng của thiết bị.

Xây dựng mạng không dây

Hình 1: Kiểm tra chất lượng phát sóng của kết

Thiết lập một mạng không dây không tốn kém thời gian, công sức và phức tạp như các hệ thống mạng truyền thống khác, đôi khi không quá một giờ đồng hồ lao động là có thể hình thành một hệ thống mạng không dây. Thực tế cho thấy, đa số các sự cố, trục trặc xảy ra trong hệ thống mạng không dây là do phần mềm điều khiển thiết bị có lỗi nên cần ưu tiên sử dụng các trình điều khiển thiết bị mới nhất do nhà sản xuất thiết bị cung cấp, cập nhật hay tải về từ internet. Nếu hệ thống đang sử dụng hệ điều hành Windows XP thì cũng nên cài đặt bản Service Pack mới nhất do Microsoft phát hành.

Khi lắp đặt thiết bị, nên bố trí các bộ tiếp sóng (AP) ở những vị trí trên cao, tránh bị che khuất bởi các vật cản càng nhiều càng tốt. Các loại vật liệu xây dựng, trang trí nội thất như: giấy dán tường phủ kim loại, hệ thống dây dẫn điện chiếu sáng, cây cảnh... cũng có thể làm suy giảm tín hiệu của AP. Nhớ dựng các cần anten của AP thẳng góc 90°. Nếu sử dụng chuẩn không dây 802.11b và 802.11g thì cần chú ý bố trí các AP nằm xa các thiết bị phát sóng điện từ có khoảng tần số trùng với tần số của AP (2,4GHz) như lò vi ba, điện thoại 'mẹ bồng con', đầu thu phát Bluetooth... Khi thi công mạng nên di chuyển, bố trí AP tại nhiều vị trí lắp đặt khác nhau nhằm tìm ra vị trí lắp đặt

thiết bị sẽ cho chất lượng tín hiệu tốt nhất.

Khoảng cách giữa card mạng không dây với AP cũng ảnh hưởng rất nhiều đến tốc độ truyền dẫn, càng xa AP thì tốc độ truyền dẫn càng giảm dần. Ví dụ đối với các mạng không dây chuẩn 802.11b thì tốc độ suy giảm dần từng mức, mức sau bằng $\frac{1}{2}$ so với mức trước (11Mbps xuống 5,5Mbps xuống 2Mbps...). Đa số các phần mềm tiện ích đi kèm card mạng không dây và AP có chức năng hiển thị tốc độ truyền dẫn của mạng.

Nếu không gian làm việc vượt quá bán kính phủ sóng của AP hiện có thì chúng ta phải mua thêm bộ khuếch đại (repeater) để nâng công suất phát sóng cũng như bán kính vùng phủ sóng của AP.

Sau đó tiến hành thủ tục cấu hình phần mềm cho hệ thống mạng, cụ thể là:

Sử dụng địa chỉ IP cố định hay tự động: Nếu hệ thống mạng không dây đang xây dựng có truy cập internet thì cần liên hệ với nhà cung cấp kết nối internet (ISP) để được cung cấp địa chỉ IP và hướng dẫn cách cài đặt cho card mạng không dây.

Sử dụng dịch vụ DHCP: Cũng như với mạng máy tính thông thường, nên sử dụng dịch vụ DHCP để hệ thống tự động cung cấp địa chỉ IP cho tất cả các thiết bị mạng tham gia trong mạng. Làm như vậy sẽ tiết kiệm rất nhiều công sức cho người quản trị mạng.

SSID: Tương tự như khái niệm tên miền trong internet, SSID (Service Set Identifier) là chuỗi ký tự đại diện cho một hệ thống mạng không dây. Tất cả các thiết bị mạng (Access Point, card mạng không dây...) của một hệ thống mạng không dây phải được khai báo chung một số SSID thì mới làm việc được với nhau. Thường thì người quản trị mạng sẽ khai báo cho toàn bộ hệ thống một tên mạng, nhưng chính chuỗi SSID này là kẽ hở giúp các hacker phán đoán loại thiết bị mạng đang sử dụng trong hệ thống để tìm cách truy cập vào đó bất hợp pháp.

Hình 2: Tìm mạng hiện diện trong
vùng phủ sóng bằng công cụ Wireless
Zero của Windows XP

Kênh thông tin: Băng thông của chuẩn 802.11b và 802.11g cho phép xây dựng 14 kênh khác nhau để truyền dẫn thông tin nhưng hiện nay người ta thường dùng một trong các kênh đánh số từ 1 đến 11, và tránh dùng lẫn lộn các kênh 1, 6 và 11 để nâng chất lượng sóng tín hiệu.

Tiếp đến tiến hành cài đặt và cấu hình phần mềm điều khiển card mạng không dây. Có 2 chế độ cài đặt: Chế độ Infrastructure nếu dùng thiết bị tiếp sóng (Access Point), bộ dẫn đường (router), nhớ khai báo SSID và kênh thông tin; Chế độ Ad hoc dành cho chế độ mạng ngang hàng. Sau khi bổ sung phần mềm điều khiển, nếu máy tính chạy hệ điều hành Windows XP thì chức năng quản trị mạng không dây có tên Wireless Zero Configuration (WZC) sẽ được kích hoạt, thông qua chức năng này (biểu tượng nằm trong khay hệ thống) chúng ta sẽ biết được danh sách các mạng không dây đang hiện diện xung quanh máy tính (có card mạng không dây). Nhấn kép chọn vào một mạng không dây trong danh sách để thực hiện thủ tục kết nối vào mạng đó.

Theo quy định chung, danh sách các mạng không dây hiện diện xung quanh máy tính sẽ được phân thành 2 loại: Available networks chứa danh sách tất cả các mạng không dây máy tính có thể kết nối được; Preferred networks là danh

sách tất cả các mạng không dây mà WZC của Windows XP, xếp thứ tự ưu tiên từ cao xuống thấp, sẽ tự động thực hiện thủ tục kết nối mạng. Hai danh sách này nằm trong cửa sổ Properties của tiện ích cấu hình card mạng không dây, thủ tục khởi động cửa sổ này như sau: Nhấn chuột phải vào biểu tượng có nhãn My Network Places, chọn menu Properties rồi menu Wireless Networks.

Bảo mật hệ thống: ngăn ngừa sự tò mò không cần thiết

Để hệ thống hoạt động an toàn và bảo mật thông tin trong hệ thống nội bộ, bạn nên tuân thủ một số quy định sau:

Sử dụng mật khẩu: Không nên dùng mật khẩu truy cập

hệ thống chỉ là khoảng trắng hay do phần mềm thiết bị tự động tạo ra.

Hình 3: Cửa sổ cấu

hình card mạng không
dây

Không cung cấp số định danh SSID: Theo mặc định, AP tự động cung cấp thông tin số định danh SSID của hệ thống mạng cho tất cả các thiết bị nằm trong bán kính phủ sóng của nó khi có yêu cầu. Điều này giúp cho người sử dụng máy tính có đầy đủ thông tin để tham gia vào mạng, nhưng lại là nhược

điểm bị các hacker lợi dụng để thâm nhập bất hợp pháp, vì vậy đối với các mạng cục bộ cần vô hiệu hóa chức năng này để mạng hoạt động an toàn hơn.

Chỉ cho phép các thiết bị có địa chỉ MAC nhất định được tham gia vào hệ thống: Tất cả các thiết bị nối mạng đều có một chuỗi 12 ký tự duy nhất dùng làm số định danh cho từng thiết bị, từ chuyên môn gọi là địa chỉ MAC (Media Access Control). Để hệ thống hoạt động an toàn hơn, chỉ những thiết bị nối mạng có số đăng ký MAC nhất định mới được quyền truy cập vào hệ thống. Danh sách địa chỉ MAC các thiết bị nối mạng không dây sử dụng trong hệ thống mạng được khai báo thông qua phần mềm quản trị Access Point. Trong Windows XP hay 2000, thủ tục xác định địa chỉ MAC của thiết bị mạng như sau: Nhấn chuột vào Start->Run, nhập vào dòng lệnh cmd rồi nhấn phím OK. Trong cửa sổ DOS của tiện ích cmd, nhập vào dòng lệnh ipconfig /all (lưu ý giữa ipconfig và /all có khoảng trống phân cách) rồi nhấn phím Enter. Sau dấu ':' của dòng thông báo Physical Address chính là địa chỉ MAC của thiết bị mạng. Với Windows 98/Me chỉ cần nhập câu lệnh winipconfig vào trong cửa sổ của lệnh Run, địa chỉ MAC sẽ nằm trên dòng thông báo có nhãn 'Adapter Address'.

Áp dụng tiêu chuẩn bảo mật WPA hoặc WEP cho hệ thống: WEP (Wireless

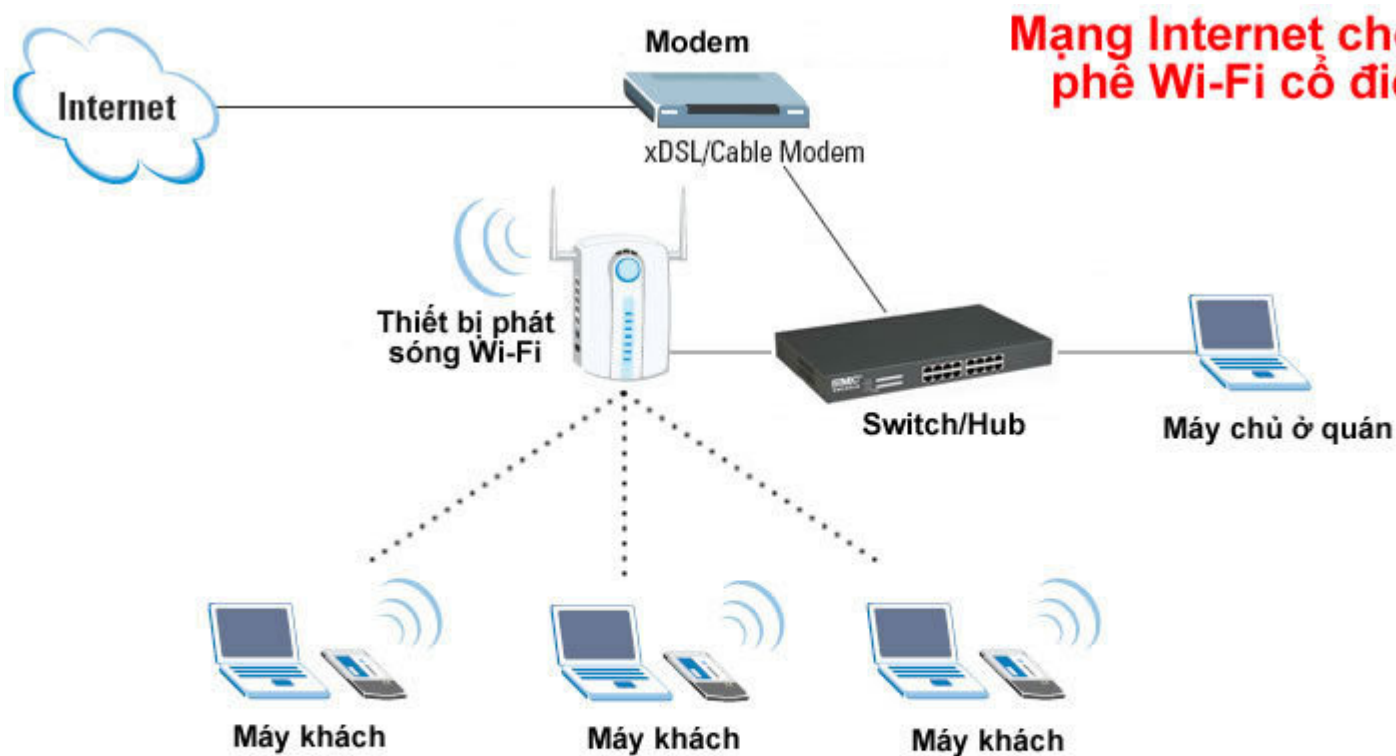
Encryption Protocol) và WPA (Wi-Fi Protected Access) là các công nghệ bảo mật hệ thống mạng không dây. Tuy nhiên hiện nay các hacker đã tìm ra cách thức vô hiệu hóa chế độ bảo mật WEP nên cần ưu tiên sử dụng chuẩn WPA để bảo mật cho hệ thống. Nếu hệ thống của bạn hiện đang áp dụng chuẩn WEP thì nên liên hệ với nhà sản xuất để được hướng dẫn chuyển sang sử dụng chuẩn WPA.

Tắt chế độ dùng chung tập tin của Windows: Khởi động phần mềm Windows Explorer. Nhấn chuột phải vào từng biểu tượng đại diện cho các ổ đĩa trong máy tính của bạn rồi chọn menu có nhãn Sharing and Security (Windows XP) hoặc Sharing (các phiên bản Windows 9x, NT). Bỏ đánh dấu chọn tại mục có nhãn 'Sharing this folder on the network'.

Theo PCWorld Vietnam

Lập mạng Wifi cho cà phê

Nếu ai từng làm Wifi cà phê, thì có lẽ cũng biết người ta sẽ chạy mô hình này nhiều hơn:



Tự thiết lập 1 mô hình wifi để cung cấp cho quán cà phê vừa và nhỏ
Sử dụng máy chủ để quản lý

Yêu cầu:

Đường truyền tốt để có thể cung cấp ổn định cho nhiều máy (ở đây LAPPY)
Modem/Router, Acces Point

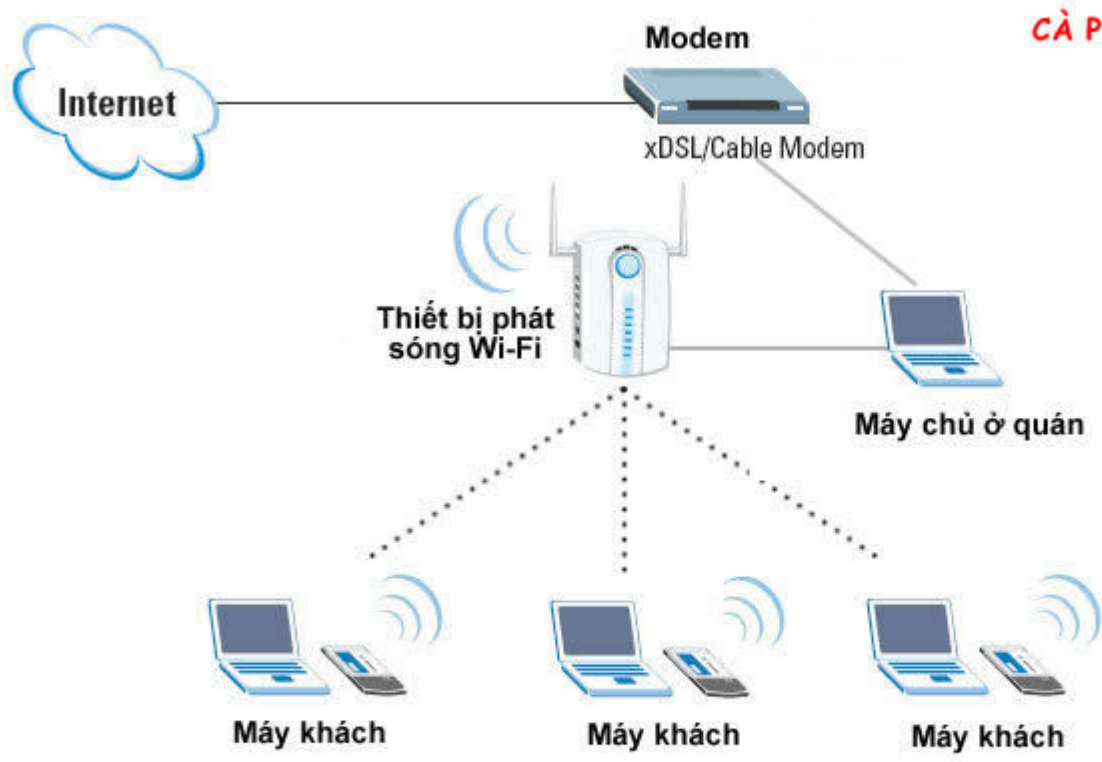
Một Server chạy Windows Server 2003 (PC này sẽ cần 2 cạc mạng LAN)

_1 cạc nối vào Modem đặt tên NET

_1 cạc nối vào Access Point đặt tên LAN).



Mô hình sẽ chạy theo kiểu



CÀ PHÊ & SÓNG WI-FI
SERVER PHÁT

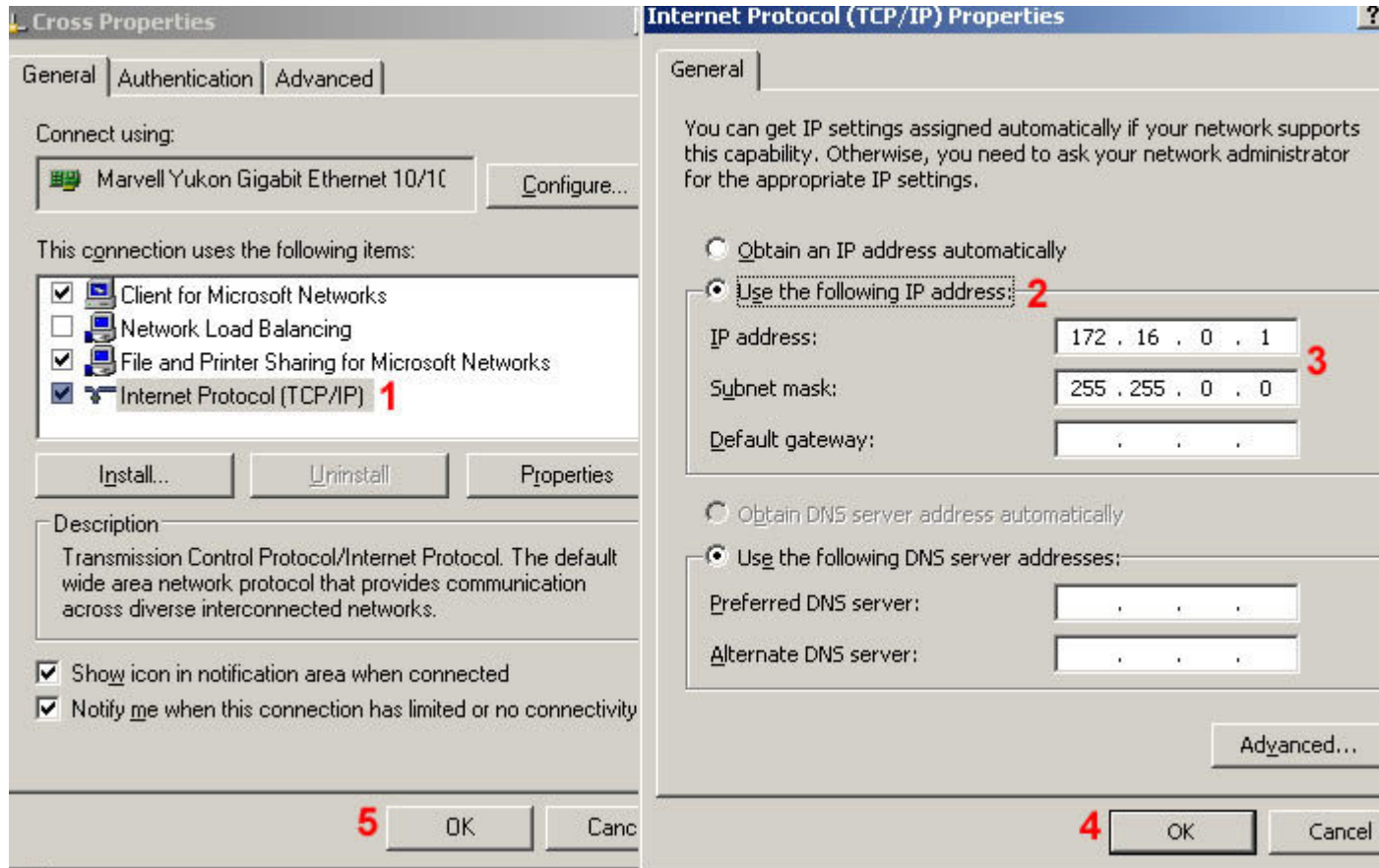
=====Cách thực hiện=====

1.1/Máy PC cài Windows Server 2003:

Việc cài đặt này diễn ra bình thường tương tự như WinXP.
Cài tất cả các Driver cần thiết cho hệ thống để hoạt động ổn định

1.2/Cấu hình các mạng cho Windows Server 2003:

Mở Properties của các LAN rồi thiết đặt như hình



Trong đó, con số 172.16.0.1 là số IP Address nội bộ mà bạn tự đặt, Subnet Mask thì nó tự nhận diện cho bạn. Bạn có thể đặt là bất kỳ, nhưng buộc phải theo 4 dãy số sau

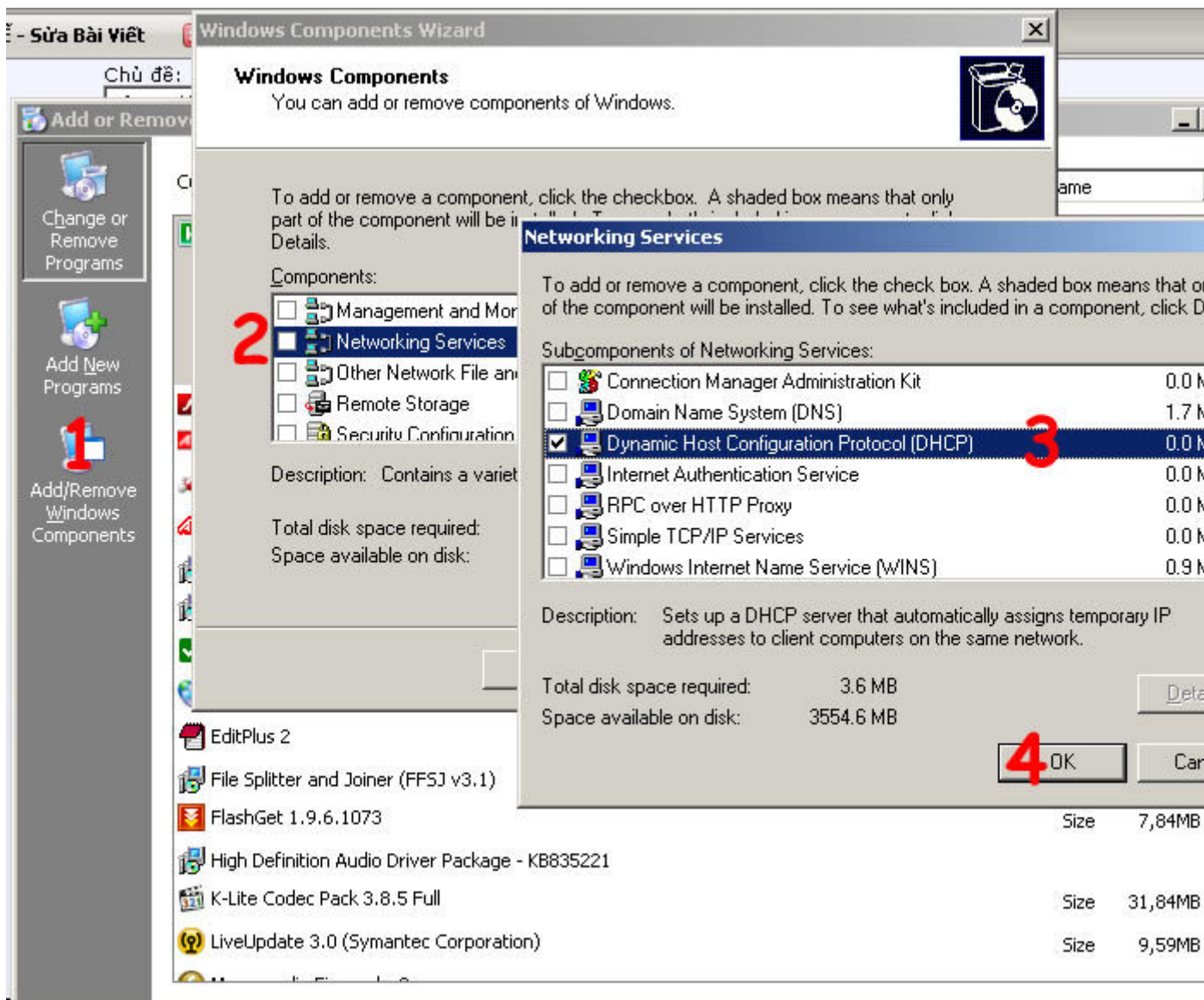
_172.16.x.x - 255.255.0.0

_172.31.x.x - 255.255.0.0

_10.x.x.x - 255.0.0.0

_192.168.x.x - 255.255.255.0

Con số bạn có thể lấy là từ 0 đến 254

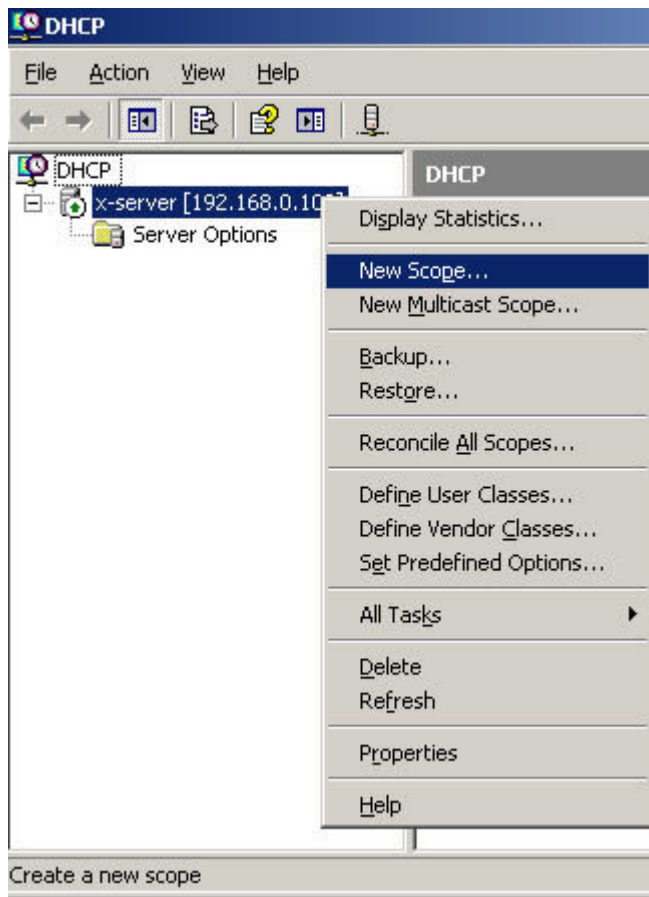


Nếu cài, nó đòi đĩa, hãy bỏ đĩa Windows Server 2003 vào rồi tiếp tục. Nên khởi động lại cho ổn định.

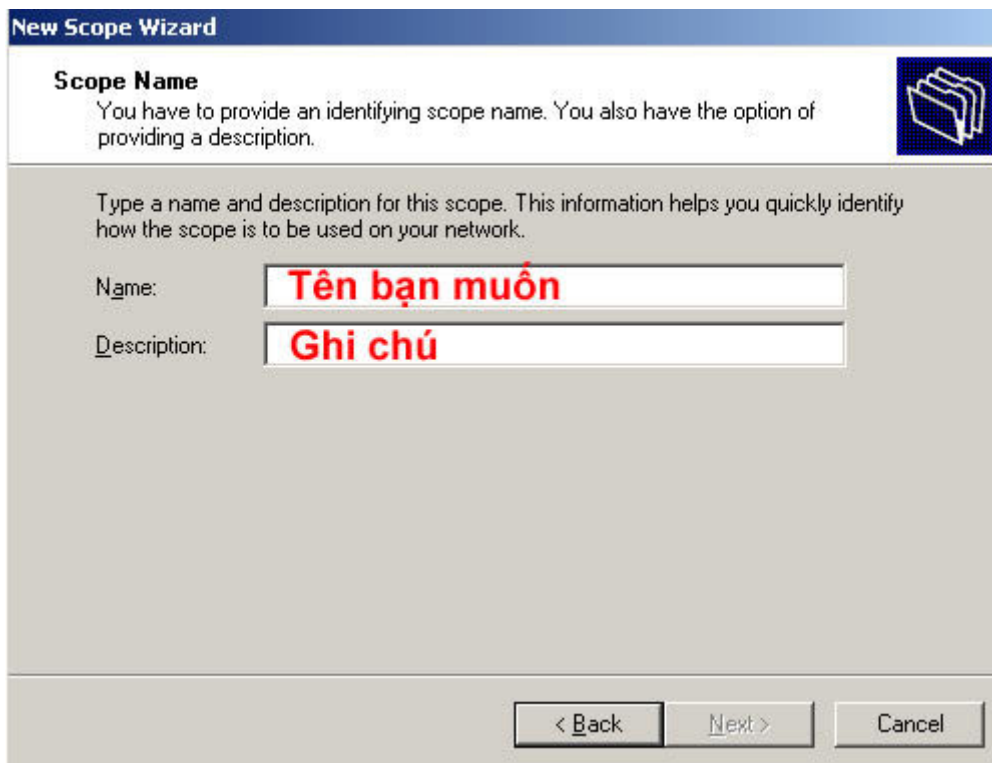
2.2/Cấu hình DHCP để chia lớp mạng:

Vào Start > Settings > Control Panel (cái này có nhiều cách mở) > Administrative Tools > DHCP

Nhấn chuột phải vào tên Server chọn New Scope.



Một bảng hiện ra Next > Đặt tên bất kỳ, vd: Scope1



New Scope Wizard

Scope Name
You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

< Back Next > Cancel

Tiếp tục, đặt theo lớp mạng bạn muốn các laptop của khách hàng khi kết nối phải dùng. Phải có thông số tương đương các LAN bạn đang dùng nối vào Access Point (là các mạng chia sẻ internet).

Trong VD này, lấy:

_Start IP Address: 172.16.0.10 <= địa chỉ IP sẽ bắt đầu, khách hàng nào kết nối đầu tiên sẽ có số IP này

_End IP Address: 172.16.0.254 <= địa chỉ IP kết thúc, khách hàng vào trễ nhất sẽ có số IP này

_Subnet Mask: điền y như lúc thiết đặt các LAN. VD này thiết đặt là 255.255.0.0

_Leqht: bạn xem, nó sẽ tự tăng (giới hạn bài này bạn không cần quan tâm)

New Scope Wizard

IP Address Range
 You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address: 172 . 16 . 0 . 10

End IP address: 172 . 16 . 0 . 254

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 16

Subnet mask: 255 . 255 . 0 . 0

< Back Next > Cancel

Next > Add Exclusions > Next > Lease Duration > Next > Configure DHCP Options > No, I will configure these options later > Next > Finish

New Scope Wizard

Configure DHCP Options
 You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

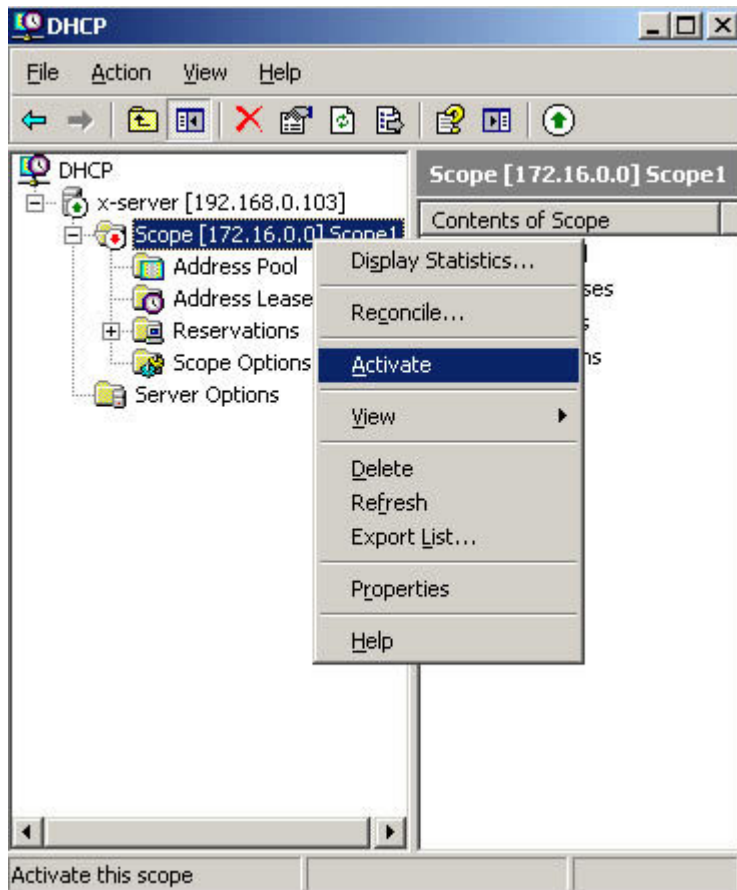
Do you want to configure the DHCP options for this scope now?

Yes, I want to configure these options now

No, I will configure these options later

< Back Next > Cancel

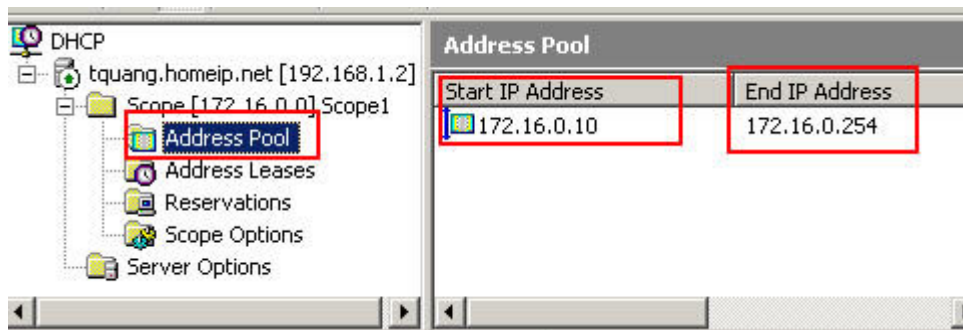
Sau khi thiết đặt xong phần trên, quay lại bảng chính của DHCP rồi chọn như hình sau để kích hoạt dịch vụ DHCP



Khi đã được kích hoạt, chọn Address Pool. Bạn sẽ thấy thông số mình đã thiết đặt IP như hình dưới bao gồm

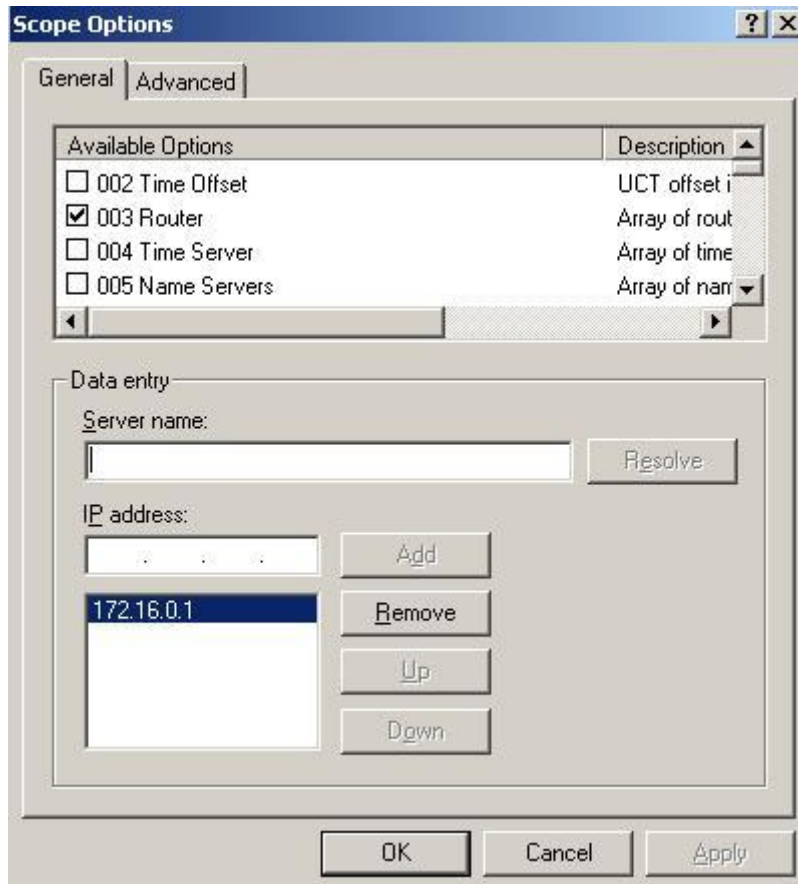
_Start IP: 172.16.0.10

_End IP: 172.16.0.254

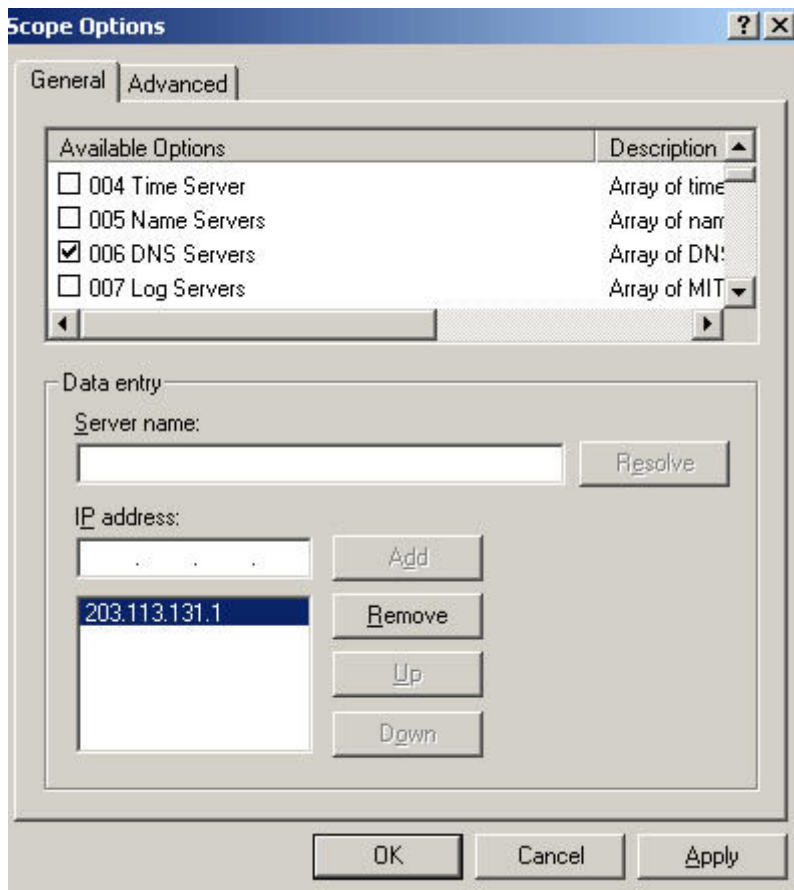


Chuyển xuống phần Scope Options để thiết đặt việc cho phép kết nối Internet: nhấn chuột phải > Configure Options...

_Check vào 003 Router rồi nhập thông số IP của các LAN (tức các ở Server nối đến Access Point), nhập xong nhấn Add



_Check tiếp vào 006 DNS Server rồi nhập số DNS mà nhà cung cấp dịch vụ Internet họ cấp. Trong ví dụ minh họa là số DNS của Viettel.



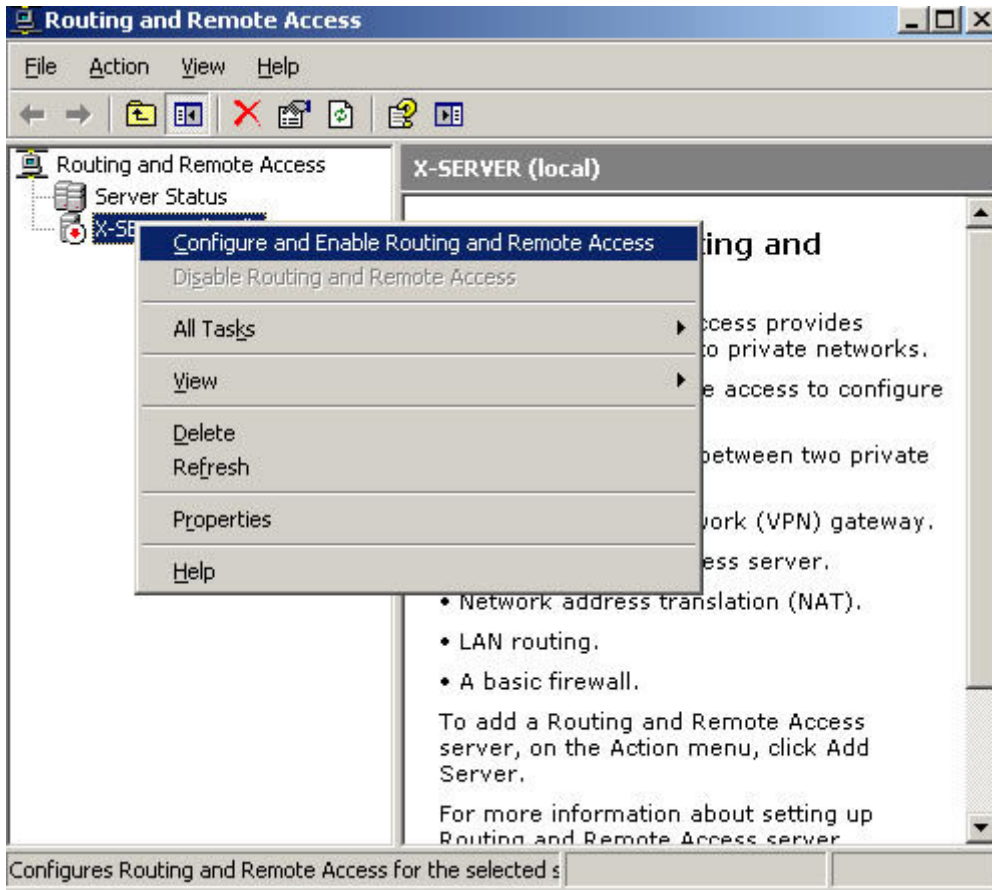
Chọn Ok để hoàn tất thiết đặt DHCP, đóng phần thiết đặt DHCP lại.

Những bước trên, ta đã cấu hình để cho Server cấp phát các IP tự động cho các Laptop mỗi khi kết nối rồi. Tuy nhiên, nếu chỉ làm như vậy thì máy lappy (client) vẫn chưa thể kết nối Internet được. Ta cần cấu hình thêm. Việc cấu hình này gọi là NAT.

3/Cấu hình NAT cho Server để máy con truy cập mạng:

Control Panel > Administrative Tools > Routing and Remote Access

Thiết lập bước đầu, nhấn chuột phải vào tên của Server > Configure and Enable Routing and Remote Access



Next > Custom Configuration > Next

Routing and Remote Access Server Setup Wizard

Configuration

You can enable any of the following combinations of services, or you can customize this server.



- R**emote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure Virtual Private Network (VPN) Internet connection.
- N**etwork address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.
- V**irtual Private Network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.
- S**ecure connection between two private networks
Connect this network to a remote network, such as a branch office.
- C**ustom configuration
Select any combination of the features available in Routing and Remote Access.

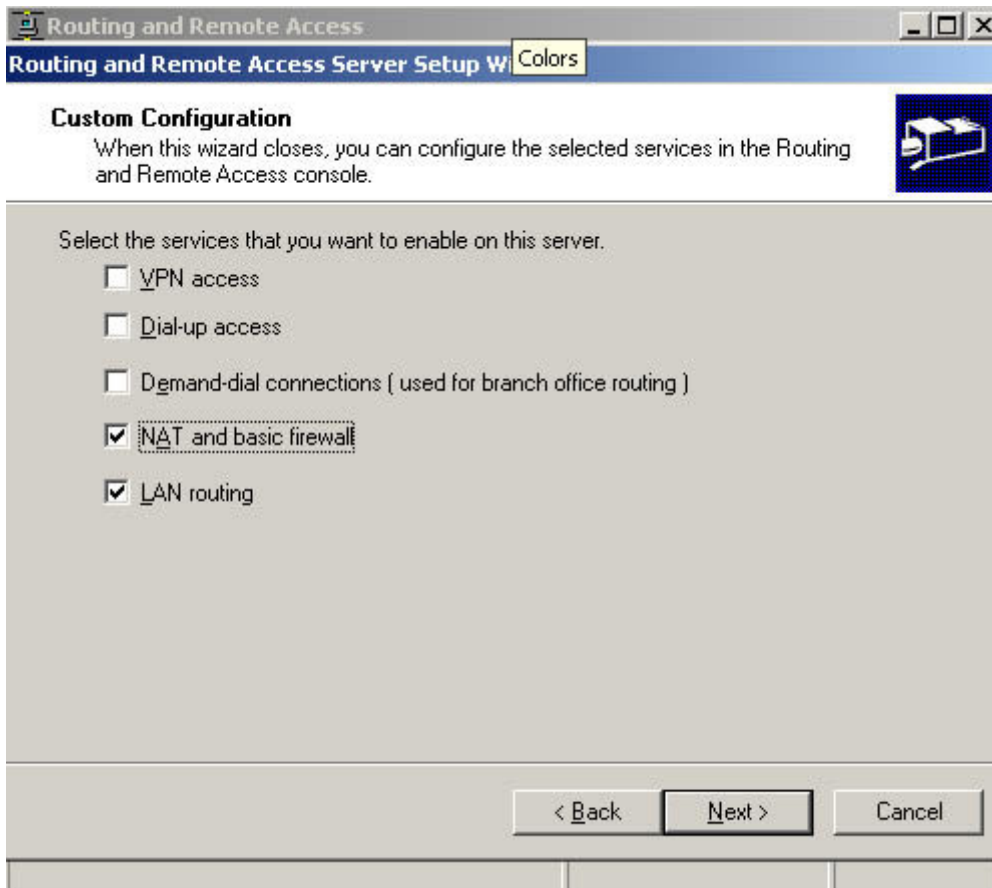
For more information about these options, see [Routing and Remote Access Help](#).

< Back

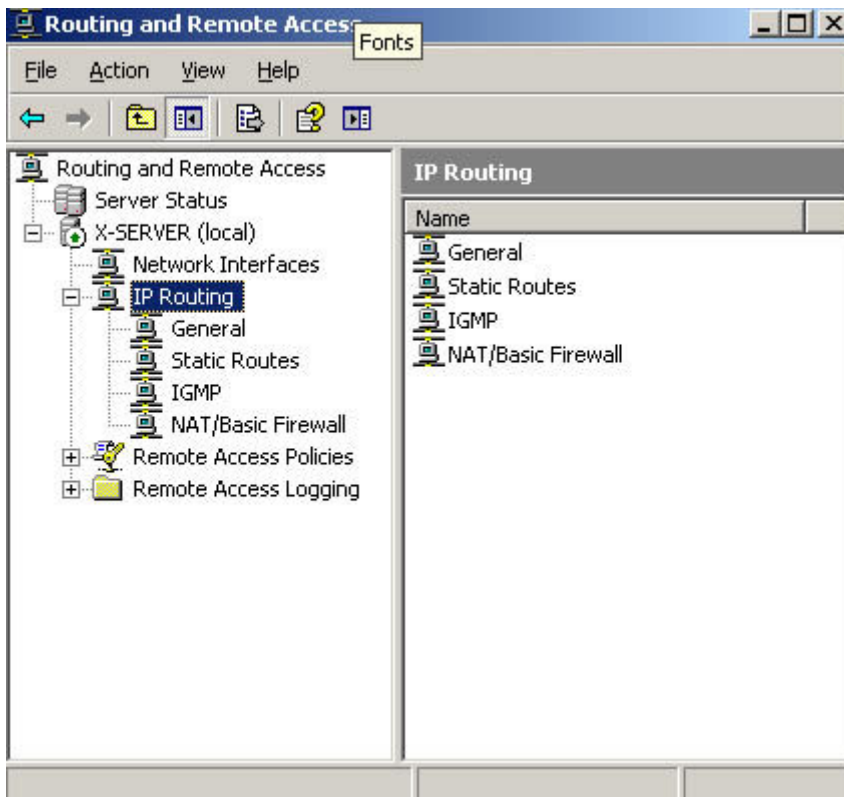
Next >

Cancel

Chọn NAT và LAN > Next > Finish > Yes



Bung dấu cộng (+) ở IP Routing ra để cho dễ nhìn



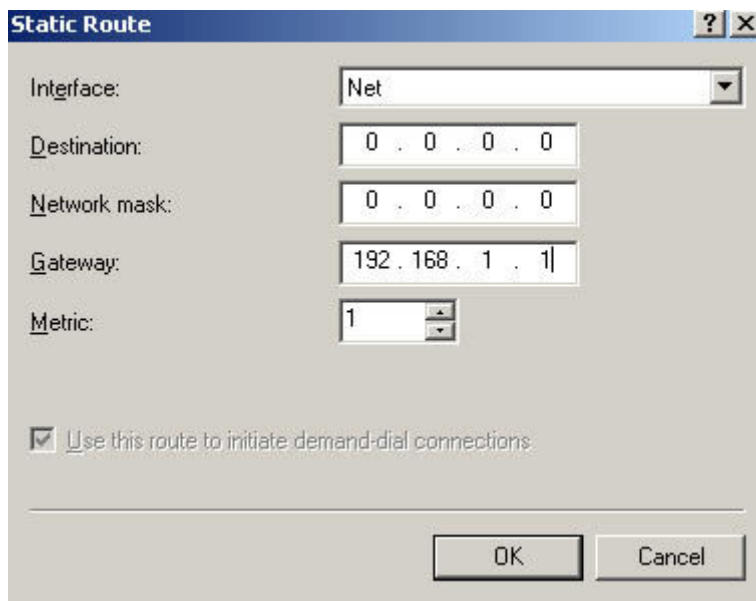
Nhấn phải chuột vào Static Routes > New Static Route..., kể đến thiết đặt thông số như sau:

_Interface: Net (Net là tên của cạc kết nối trực tiếp đến modem)

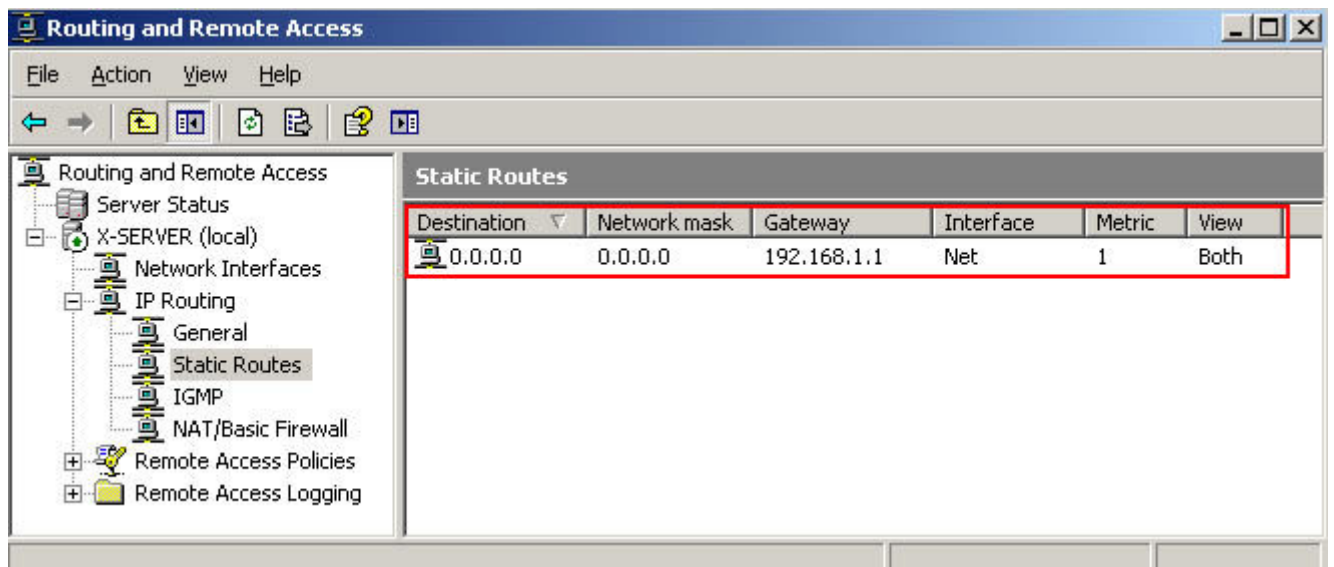
_Destination: 0.0.0.0

_Network Mask: 0.0.0.0

_Gateway: 192.168.1.1 (Đây là số IP của modem)

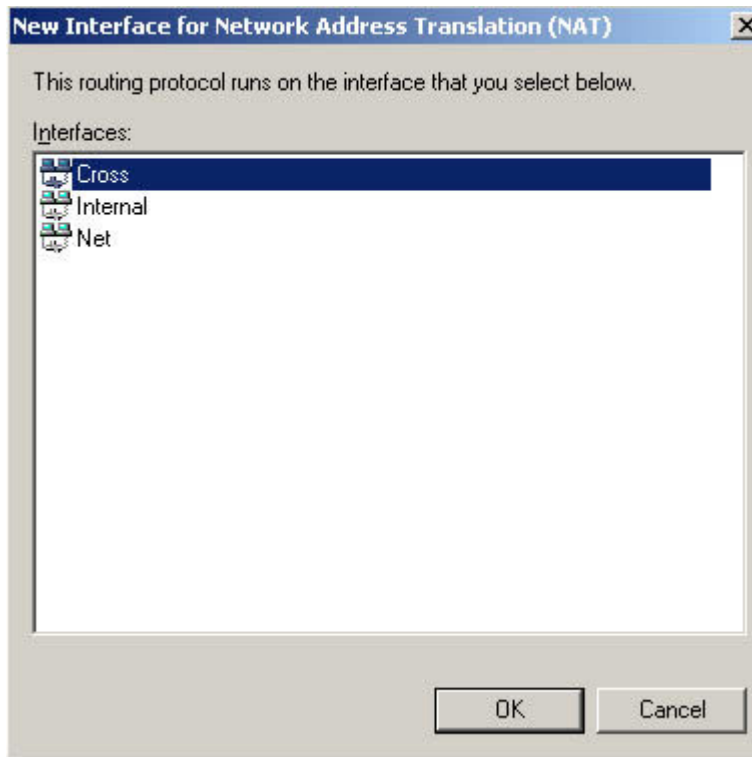


au khi thiết đặt như vậy, bạn thấy như hình sau là đã được.

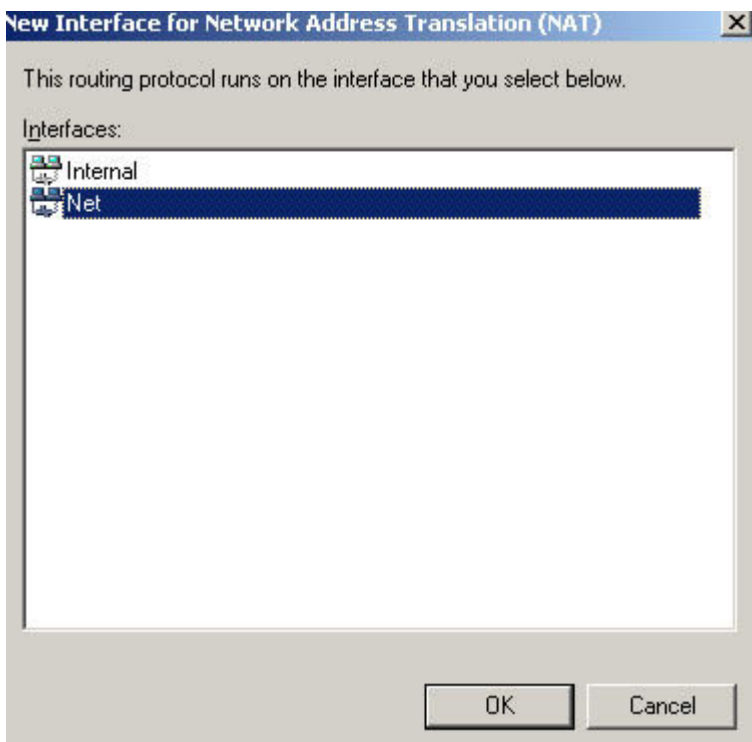


Giờ đây, ta cần phải cầu hình làm sao cho Routing có thể nhận biết đâu là các nối mạng, đâu là các chia sẻ mạng

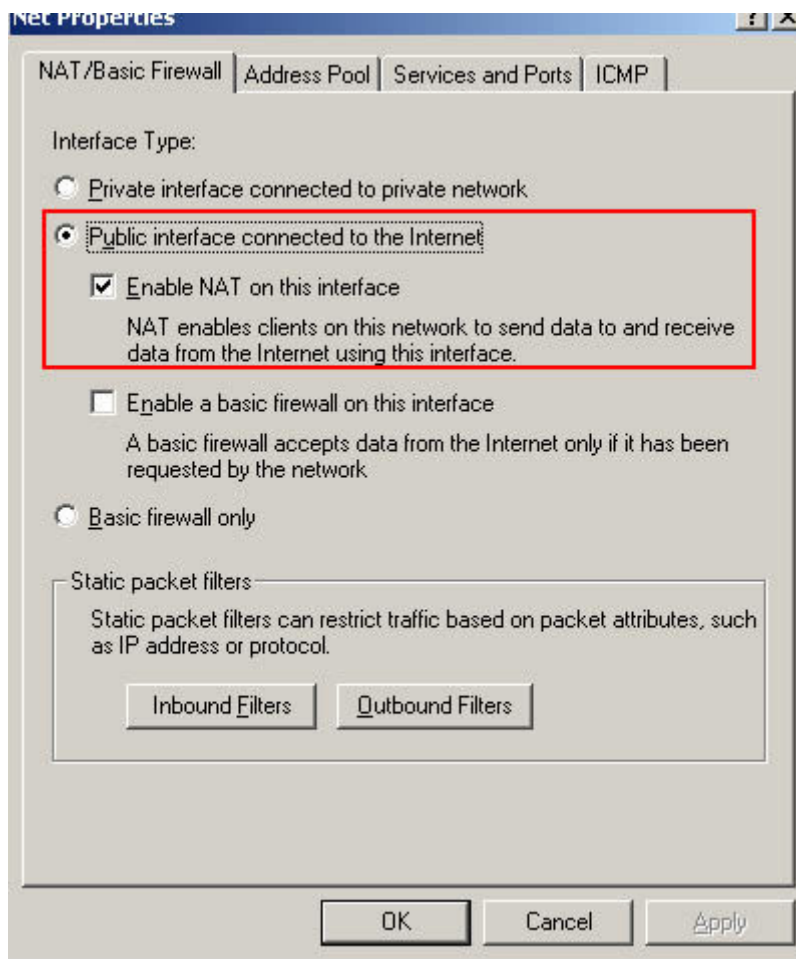
Phải chuột vào NAT/Basic Firewall > New Interface ... > LAN (trong hình minh họa, tui đặt tên là Cross) > OK. Một bảng khác hiện ra, chọn OK



Tiếp đến, cũng làm tương tự với các NET: Phải chuột vào NAT/Basic Firewall > New Interface ... > NET > OK



Một bảng khác hiện lên, chọn Public interface connected to the Internet, check vào Enable NAT on this interface > OK



Như vậy, ta đã hoàn tất việc cấu hình cho Server rồi. Thế còn cấu hình cho Access Point thì làm sao? Mình sẽ không thực hiện bước này. Bước này sẽ để cho bạn tự ngẫm cứu nhé . Có 1 gợi ý nhỏ là: Tắt chức năng DHCP trong Access Point

Gợi ý: nếu bạn kết hợp mô hình 1 và mô hình 2, bạn sẽ có khả năng tận dụng nhiều Server cho nhiều mục đích khác nhau nhằm dàn trải đến sự tiện lợi cho khách hàng

I. GIỚI THIỆU

Ngày nay, Internet đã phát triển mạnh về mặt mô hình cho đến công nghệ, đáp ứng các nhu cầu của người sử dụng. Internet đã được thiết kế để kết nối nhiều mạng khác nhau và cho phép thông tin chuyển đến người sử dụng một cách tự do mà không xem xét đến máy và mạng mà người sử dụng đó đang dùng. Để làm được điều này người ta sử dụng một máy tính đặc biệt gọi là router để kết nối các LAN và WAN với nhau. Các máy tính kết nối vào Internet thông qua nhà cung cấp dịch vụ (ISP-Internet Service Provider), cần một giao thức chung là TCP/IP. Điều mà kỹ thuật còn tiếp tục phải giải quyết là năng lực truyền thông của các mạng viễn thông công cộng. Với Internet, những dịch vụ như giáo dục từ xa, mua hàng trực tuyến, tư vấn y tế, và rất nhiều điều khác đã trở thành hiện thực.

Tuy nhiên, do Internet có phạm vi toàn cầu và không một tổ chức, chính phủ cụ thể nào quản lý nên rất khó khăn trong việc bảo mật và an toàn dữ liệu cũng như trong việc quản lý các dịch vụ. Từ đó người ta đã đưa ra một mô hình mạng mới nhằm thoả mãn những yêu cầu trên mà vẫn có thể tận dụng lại những cơ sở hạ tầng hiện có của Internet, đó chính là mô hình mạng riêng ảo (Virtual Private Network - VPN). Với mô hình mới này, người ta không phải đầu tư thêm nhiều về cơ sở hạ tầng mà các tính năng như bảo mật, độ tin cậy vẫn đảm bảo, đồng thời có thể quản lý riêng được sự hoạt động của mạng này. VPN cho phép người sử dụng làm việc tại nhà, trên đường đi hay các văn phòng chi nhánh có thể kết nối an toàn đến máy chủ của tổ chức mình bằng cơ sở hạ tầng được cung cấp bởi mạng công cộng.[5] Nó có thể đảm bảo an toàn thông tin giữa các đại lý, người cung cấp, và các đối tác kinh doanh với nhau trong môi trường truyền thông rộng lớn. Trong nhiều trường hợp VPN cũng giống như WAN (Wide Area Network), tuy nhiên đặc tính quyết định của VPN là chúng có thể dùng mạng công cộng như Internet mà đảm bảo tính riêng tư và tiết kiệm hơn nhiều.

VPN có ba loại chính: truy nhập VPN, intranet VPN và extranet VPN.

+ Truy nhập VPN: cung cấp khả năng truy nhập từ xa đến intranet hay extranet của tổ chức qua cơ sở hạ tầng chung. Truy nhập VPN sử dụng kỹ thuật tương tự, quay số, ISDN, DSL, mobile IP và cáp để thực hiện kết nối an toàn cho người dùng lưu động, người dùng truyền thông và các văn phòng chi nhánh.

+ Intranet VPN: liên kết các văn phòng trung tâm, các chi nhánh tới mạng intranet thông qua cơ sở hạ tầng dùng chung bằng các kết nối chuyên biệt.

+ Extranet VPN: Liên kết khách hàng, nhà cung cấp, đối tác hay các cộng đồng quyền lợi tới mạng tổ chức thông qua cơ sở hạ tầng dùng chung bằng các kết nối chuyên biệt. Extranet VPN khác với intranet VPN là chúng cho phép truy nhập tới người dùng bên ngoài tổ chức.[4]

II. MẠNG RIÊNG ẢO

Một VPN có thể được cài đặt theo nhiều cách, có thể được xây dựng qua ATM, frame relay hay công nghệ X.25. Tuy nhiên, phương pháp chung nhất là triển khai VPN dựa trên IP, phương pháp này cho phép kết nối linh hoạt và dễ dàng hơn. Hầu hết các mạng Intranet đều dùng công nghệ IP và Web, IP-VPN có thể dễ dàng mở rộng tính năng này thông qua mạng diện rộng. Một liên kết IP-VPN có thể được thiết lập tại bất cứ đâu trên thế giới giữa hai điểm cuối, và mạng IP tự động quản lý quá trình lưu thông này.

Riêng tư và bảo mật dữ liệu là điểm quan trọng nhất khi triển khai dịch vụ này trên Internet. Khả năng an toàn của IP-VPN được thực hiện thông qua các quá trình mã

hoá (encryption) và chứng thực (authentication), đồng thời phân lớp trên mạng IP có sẵn. Nhằm đáp ứng vấn đề bảo mật, tổ chức Internet Engineering Task Force (ietf.org) đã phát triển bộ giao thức IP Security (IPSec), đây là bộ giao thức mở rộng của IP nhằm chú trọng đến chứng thực và bảo mật dữ liệu.

Mặc dù VPN của các nhà cung cấp khác nhau có những điểm riêng nhưng vẫn là mạng riêng dựa trên IP backbone, mã hoá dữ liệu, proxy chứng thực, bức tường lửa (firewall) và lọc spam.

Các hệ thống VPN thường rơi vào ba loại: hệ thống dựa trên phần cứng, hệ thống dựa trên bức tường lửa và gói ứng dụng chạy độc lập. Phần lớn VPN dựa trên phần cứng là các router có khả năng mã hoá, đây là loại dễ dùng và đơn giản trong cài đặt, nó giống như thiết bị "cắm và chạy" (plug and play). Tuy nhiên chúng lại không mềm dẻo hơn hệ thống dựa trên phần mềm, khi mà hai điểm kết nối VPN không cùng một tổ chức, loại này thường thích hợp cho các đối tác kinh doanh hay các máy con ở xa. Loại VPN dựa trên bức tường lửa được chú trọng vào bảo mật, tuy nhiên một khi bức tường lửa được dựng lên thì nhiều vấn đề sẽ nảy sinh bất ngờ.

Hình 1: Mô hình mạng riêng ảo.

1. Hoạt động của VPN

Một giải pháp VPN là sự kết hợp của các công nghệ:

- Tạo kết nối đường ống.
- Mã hoá dữ liệu.
- Khả năng chứng thực.
- Điều khiển truy cập.

VPN được truyền tải trên Internet, được mạng IP hay các nhà cung cấp backbone quản lý. Để sự truyền tải hoạt động, các backbone này kết hợp bất kỳ một công nghệ truy cập nào, bao gồm T1, frame relay, ISDN, ATM hay đơn giản là quay số. Khi một máy khách gửi một luồng các gói tin Point-to-Point Protocol (PPP) đã được mã hoá đến máy chủ hay router, thay vì sử dụng một đường truyền riêng biệt (giống như WAN), nó được truyền qua một đường ống trên mạng chia sẻ. [1]

Phương pháp tạo ra đường ống chung được chấp nhận là đóng gói một giao thức mạng (như là IPX, NetBEUI, AppleTalk, hay các loại khác) bên trong PPP, và rồi đóng gói toàn bộ gói (package) trong một giao thức đường ống, thường là IP nhưng cũng có thể là ATM hay frame relay. Phương pháp này gọi là đường ống tầng 2 (Layer-2) và giao thức gọi là giao thức đường ống tầng hai (Layer-2 Tunneling Protocol - L2TP). Với mô hình này, các gói tin có ghi thông tin điều khiển ở phần đầu hướng đến các mạng ở xa sẽ đi đến thiết bị khởi tạo đường ống, thiết bị này có nhiệm vụ chuyển mọi thứ từ một router đến một PC có sử dụng phần mềm cho phép quay số vào VPN. Từ thiết bị khởi tạo đường ống cho đến thiết bị VPN đầu cuối hay một bộ chuyển mạch đường ống đều thống nhất một mẫu mã hoá để có thể giao tiếp với nhau. Thiết bị khởi tạo đường ống mã hoá các gói tin nhằm đảm bảo an toàn trước khi truyền đến cho thiết bị đầu cuối, sau đó thiết bị đầu cuối sẽ giải mã các gói tin và phân tán chúng đến đích trong mạng.

Có hai loại kết nối VPN: kết nối VPN truy cập từ xa (remote access VPN connection) và kết nối VPN từ router đến router (router-to-router VPN connection).

Loại kết nối VPN truy cập từ xa được tạo ra bởi một người dùng ở xa, người dùng truy nhập theo một mã nhất định vào điểm truy nhập gần nhất (POP) của nhà cung cấp dịch vụ (thiết lập kết nối vào Internet), sau đó truy nhập vào mạng VPN thông

qua hệ thống chứng thực VPN, khách hàng cung cấp tên thuê bao và mật khẩu, hoặc số nhận dạng cá nhân PIN (Personal Identification Number)... Sau khi cung cấp các thông tin đầy đủ, VN server sẽ cung cấp khả năng tạo kênh kết nối ảo và mã hoá dữ liệu trong quá trình tương tác. Trường hợp khách hàng sử dụng kênh kết nối trực tiếp thì quá trình truy nhập vào Internet là không cần thiết.

Hình 2: Mô hình kết nối VPN truy cập từ xa.

Loại kết nối VPN từ router đến router được tạo ra do sự kết nối của hai mạng riêng. VPN server cung cấp khả năng kết nối đến một mạng riêng khác mà tại đó cũng có sự hoạt động của VPN server. Với loại kết nối này, các gói tin được bắt đầu gửi đi từ mỗi router, sau đó router nhận sẽ phân phối các gói tin đến các thành viên trong mạng tùy theo đích đến của mỗi gói tin.

Hình 3: Mô hình kết nối VPN từ router đến router.



lele_2612

[View Public Profile](#)

[Send a private message to lele_2612](#)

[Find all posts by lele_2612](#)

#2
11-05-2006

[lele_2612](#) 
Senior Member
Senior Member

Join Date: Mar 2006
Posts: 113



2. Giao thức

Các giao thức được dùng chủ yếu cho VPN gồm có PPTP, L2TP, IPSEC và IP-IP. Các giao thức này có thể được dùng với nhau hay độc lập. [6]

PPTP Point-to-Point Tunneling Protocol (PPTP) là một mở rộng của PPP, nó đóng gói các khung PPP vào gói tin IP (IP datagram) để truyền đi trên mạng công cộng như là Internet. PPTP có thể sử dụng trong mạng riêng LAN-LAN.

PPTP sử dụng một kết nối TCP nhằm duy trì đường ống đồng thời sử dụng một biến dạng của GRE (Generic Routing Encapsulation) để đóng gói các frame PPP là dữ liệu truyền trong đường ống. Khối dữ liệu chứa các frame PPP đóng gói có thể được mã hoá hay nén lại hoặc là cả hai. PPTP hoạt động như là đã có sẵn một mạng IP giữa máy khách PPTP (máy khách VPN có sử dụng giao thức đường ống PPTP) và máy chủ PPTP (máy chủ VPN có sử dụng giao thức đường ống). Tức là máy khách PPTP có thể đã tham gia vào mạng IP để đến được máy chủ PPTP, hay máy khách PPTP có thể là dạng quay số đến một máy chủ của mạng truy cập (NAS) nhằm thiết lập một kết nối IP trong trường hợp người dùng quay số.

Các đường ống PPTP được thiết lập phải thông qua giai đoạn chứng thực bằng các kỹ thuật chứng thực giống như của các kết nối PPP, như là PAP (Password Authentication Protocol), SPAP (Shiva Password Authentication Protocol), MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol), CHAP và EAP (Extensible Authentication Protocol). PPTP kế thừa kỹ thuật mã hoá và nén khối dữ liệu chứa frame PPP từ PPP. PPTP điều khiển kết nối giữa địa chỉ IP của máy khách PPTP và địa chỉ của máy chủ PPTP bằng cổng TCP. Sau đây là khuôn dạng gói dữ liệu PPTP (hình 4):

Hình 4: Gói dữ liệu PPTP truyền trên đường ống.

L2TP Layer 2 Tunneling Protocol (L2TP) là sự kết hợp của PPTP và Layer 2 Forwarding (L2F) được Cisco đề xuất. L2TP gộp nhặt những đặc tính tốt nhất của hai giao thức này. L2TP là giao thức mạng đóng gói các frame PPP để gửi đi thông qua mạng IP, X.25, Frame Relay hay ATM. L2TP có thể được sử dụng như là một giao thức đường ống qua Internet. L2TP cũng được dùng cho mạng riêng LAN-LAN.

L2TP sử dụng UDP (User Datagram Protocol) với một chuỗi các thông điệp nhằm duy trì đường ống. L2TP cũng sử dụng UDP để gửi khối dữ liệu đóng gói các frame PPP và khối dữ liệu này được mã hoá rồi nén lại. L2TP có thể sử dụng kỹ thuật chứng thực là PPP hay là IPSec. L2TP tạo ra đường ống giống như PPTP, thông qua kết nối có sẵn giữa người dùng với máy chủ. L2TP kế thừa kỹ thuật nén của PPP còn kỹ thuật mã hoá thì sử dụng IPSec vì kỹ thuật PPP không cung cấp khả năng chứng thực cũng như tính toàn vẹn cho mỗi gói tin.

Đường ống L2TP được thiết lập cũng phải thông qua quá trình chứng thực với các kỹ thuật chứng thực giống như PPTP. Không giống như PPTP, L2TP duy trì đường ống bằng một kết nối TCP riêng biệt. L2TP điều khiển và quản lý lưu thông bằng việc gửi các thông điệp UDP giữa máy khách và máy chủ L2TP. Sơ đồ khuôn dạng gói dữ liệu L2TP như sau (hình 5):

Hình 5: Gói dữ liệu L2TP truyền trên đường ống.

Như vậy cả PPTP và L2TP đều sử dụng PPP cho kết nối WAN "điểm - điểm" nhằm gói dữ liệu và gắn vào phần đầu để truyền tải trên mạng. Tuy nhiên vẫn có sự khác nhau giữa PPTP và L2TP:

- PPTP đòi hỏi mạng nó đi qua phải là mạng IP thì L2TP chỉ yêu cầu phương tiện đường ống cung cấp khả năng tạo kết nối "điểm-điểm". L2TP có thể chạy trên IP (dùng UDP), Frame Relay PVC, X.25 VC hay ATM PVC.

- L2TP cung cấp khả năng nén dữ liệu phần đầu, do vậy L2TP chỉ sử dụng 4 byte cho phần đầu so với 6 byte của PPTP.

IPSec

IP Security (IPSec) là giao thức tầng hầm lớp 3 (tầng mạng), gồm một chuỗi các tiêu chuẩn hỗ trợ truyền dữ liệu một cách an toàn trên mạng IP. Mô hình đường ống ESP (IPSec Encapsulating Security Payload) có thể đóng gói và mã hóa toàn bộ IP datagram để có thể truyền tải an toàn trên mạng công cộng.

Với mô hình đường ống IPSec ESP, một IP datagram hoàn chỉnh được đóng gói và mã hóa với ESP. Dựa trên công thức mã hóa datagram, máy chủ sẽ phân tích phần đầu các gói tin, quá trình xử lý các gói tin diễn ra một cách tuần tự: mã hóa, định tuyến rồi giải mã.

IP-IP

IP-IP, hay IP trong IP, là một kỹ thuật đường ống đơn giản dựa trên lớp 3 OSI. Một mạng ảo được tạo bằng cách đóng gói một gói tin IP cộng thêm một phần đầu IP. IP-IP được sử dụng chính cho việc truyền tải trên một vùng mạng mà không hỗ trợ cho việc định tuyến. Cấu trúc của gói tin IP-IP bao gồm vùng ngoài của phần đầu IP, phần đầu của đường ống, vùng trong của phần đầu IP và khối dữ liệu tải IP.

Khối dữ liệu tải IP chứa mọi thứ về IP, nó có thể là TCP, UDP hay phần đầu ICMP và dữ liệu. Việc duy trì đường ống được thực hiện bởi các thông điệp ICMP, các thông điệp này cho phép đường ống có thể kiểm soát và xác định lỗi khi xảy ra tắc nghẽn và định tuyến.

3. Bảo mật trong VPN

Tất cả các VPN đều cần phải cấu hình trên một thiết bị truy nhập, có thể là phần mềm hay phần cứng, nhằm tạo ra một kênh an toàn. Một người dùng nào đó không dễ gì có thể đăng nhập vào hệ thống VPN nếu không cung cấp một số thông tin cần thiết. Khi sử dụng một kỹ thuật chứng thực mạnh, VPN có thể ngăn chặn sự xâm nhập trái phép ngay cả khi bằng cách nào đó chúng có thể bắt được một phiên làm việc của VPN.

Hầu hết các VPN đều dùng công nghệ IPSec, do tương thích với hầu hết các phần mềm và phần cứng VPN khác nhau. IPSec không yêu cầu người dùng hiểu biết nhiều, bởi vì sự chứng thực không dựa trên người sử dụng, thay vào đó nó sử dụng địa chỉ IP của máy trạm hay các chứng nhận nhằm thiết lập định danh cho người sử dụng. Một đường ống IPSec bảo vệ tất cả các gói tin đi qua nó, kể cả ứng dụng. Các mã khoá được thay đổi cho từng gói tin (như trong PPTP) hay mỗi khoảng thời gian nhất định (như trong L2TP) tùy theo độ dài của mã khoá và quá trình giải mã mỗi gói tin không phụ thuộc vào gói tin trước.

Gói lọc (Packet Filtering)

Để truyền dẫn giữa hai giao diện vật lý (interface), như là router, trên mạng chia sẻ và intranet, VPN server cần phải lọc những địa chỉ không thuộc hệ thống VPN nhằm bảo vệ intranet khỏi những truy cập không phải là VPN.

Cả PPTP và L2TP đều có sử dụng gói lọc này và chúng có thể được cấu hình trên VPN server hay trực tiếp trên bức tường lửa.

4. Cách đánh địa chỉ và định tuyến trong VPN

Cách đánh địa chỉ và định tuyến trong VPN phụ thuộc vào loại kết nối VPN. Một kết nối VPN tạo ra một giao diện ảo, với một địa chỉ IP, và router phải định tuyến được dữ liệu từ địa chỉ ảo này đến đích một cách an toàn theo đường ống chứ không phải là mạng chia sẻ.

Khi một máy tính được kết nối, VPN server sẽ gán một địa chỉ IP cho máy tính đồng thời thay đổi định tuyến mặc định để có thể truyền thông trên giao diện ảo.

Với người dùng quay số, trước đó đã kết nối vào Internet nên đồng thời tồn tại hai địa chỉ IP:

- Khi tạo kết nối PPP, IPCP (IP Control Protocol) sẽ dàn xếp với NAS (Network Access Server) của ISP một địa chỉ IP công cộng.

- Khi tạo kết nối VPN, IPCP dàn xếp với VPN server để gán một địa chỉ IP Intranet. Địa chỉ này có thể là một địa chỉ công cộng hay một địa chỉ riêng phụ thuộc vào mạng

Intranet đó đánh địa chỉ công cộng hay địa chỉ riêng.

Trong cả hai trường hợp, địa chỉ IP đều phải cho phép VPN client với đến tất cả các máy trong Intranet. VPN server điều chỉnh bảng định tuyến để VPN client đến được các máy khác trong Intranet và Router phải điều chỉnh bảng định tuyến để có thể đến được VPN client. Router chuyển dữ liệu đến VPN server bằng địa chỉ IP công cộng của server, còn VPN client sử dụng địa chỉ IP do ISP cung cấp để giao tiếp với VPN server.

Hình 6: Địa chỉ công cộng và địa chỉ riêng trong kết nối VPN.

Phân Tích Và Thiết Lập Mạng Riêng Ảo (tt)

III. CÀI ĐẶT VÀ KHAI THÁC ỨNG DỤNG

1. Mạng máy tính Đại Học Huế

Do đặc điểm các trường đại học thành viên nằm rải rác trong thành phố, nên mỗi trường đều có một mạng LAN riêng. Trong đó, trường ĐHKH với nhiệm vụ chính là kết nối với Internet thông qua đường leased line (đường truyền thuê bao) sẽ là mạng LAN trung tâm. Hiện tại, các trường đại học thành viên có thể quay số đến mạng Intranet của ĐHKH để có thể truy cập Internet và cơ quan Đại Học Huế đã kết nối WAN với mạng trung tâm.

Mạng trung tâm được xây dựng trên mạng LAN, hình thành bởi mỗi liên kết giữa ba toà nhà. Do các toà nhà nằm cách xa nhau nên ngoài những thiết bị thông thường còn có các thiết bị hỗ trợ để truyền dữ liệu đến các trạm ở xa như router, repeater, hub, switch,... Các dịch vụ trên mạng trung tâm gồm có : WWW, E-mail, FTP và TELNET. [2]

Hình 7: Sơ đồ hệ thống mạng Đại học Huế.

2. Triển khai ứng dụng

Với mục đích thử nghiệm, chúng tôi đã tiến hành thiết kế xây dựng hệ thống mạng riêng ảo phục vụ cho việc truyền số liệu đảm bảo an toàn trên giao thức đường ống của mạng riêng ảo. Với mô hình này, giúp hiểu được cơ chế hoạt động của hệ thống mạng riêng ảo, phân tích khả năng chứng thực, mã hoá và an toàn dữ liệu.

Mô hình này bao gồm các thành phần như sau:

- Yêu cầu về thiết bị phần cứng:

o Đối với đường truyền quay số: modem, đường điện thoại thuê bao, máy tính.

o Đối với mạng LAN: máy tính có kết nối đến mạng LAN.

- Yêu cầu về phần mềm:

o Đối với máy chủ: hệ điều hành có dịch vụ VPN.

o Đối với máy trạm: có phần mềm cho phép truy nhập vào mạng VPN.

Các thủ tục chính:

- Tại máy chủ: cài đặt dịch vụ Routing and Remote Access (RRA).

Hình 8: Dịch vụ RRA sau khi cài đặt VPN.

Tạo chương trình kết nối cho máy trạm từ xa, trong Windows 9x hay Windows NT, nó là một biểu tượng thể hiện kết nối dial-up để đăng nhập vào mạng. Để có thể quản lý các user một cách hợp lý ta cần phải có Connection Manager Administration Kit.

- Tại máy trạm: Tại máy trạm lấy file cpvpn.exe từ máy chủ. Người dùng cần chạy file cpvpn.exe. Nó sẽ cài đặt VPN Connector lên máy trạm (có thể tìm thấy VPN connector trong My Network Properties trên desktop).

3. Thực Hiện Kết Nối

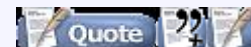
Tại máy trạm, nếu là trạm từ xa thì trước tiên phải thực hiện kết nối vào mạng internet thông qua ISP, người dùng chạy VPN connector, chương trình yêu cầu nhập user name và password. Sau khi kết nối thành công, trên khay hệ thống (system tray) xuất hiện biểu tượng của kết nối VPN:

Hình 9: Các biểu tượng sau khi kết nối đối với Client 9x và 2000.

Để theo dõi quá trình định tuyến, từ dấu nhắc hệ thống, ta thực hiện lệnh netstat-rn:

Hình 10: Trạng thái sau khi kết nối VPN.

Qua bảng, ta nhận được địa chỉ IP thật và ảo của Client và địa chỉ IP thật của Server đang tồn tại kết nối trên hệ thống mạng. Đồng thời một cổng TCP được thiết lập để duy trì đường ống giữa Server và Client.




lele_2612


[View Public Profile](#)

[Send a private message to lele_2612](#)

[Find all posts by lele_2612](#)

[Add lele_2612 to Your Contacts](#)

#2 
14-05-2006

[lele_2612](#) 
Senior Member
Senior Member

Join Date: Mar 2006
Posts: 113



4. Khai thác dịch vụ trên mạng riêng ảo

Với hệ thống mạng riêng ảo xây dựng được, ta có thể triển khai các dịch vụ giống như trên Internet. Để minh họa, chúng tôi đã thử nghiệm với hai dịch vụ là FTP và WWW.

Dịch vụ FTP

Tại máy chủ VPN, thiết lập địa chỉ IP của FTP server là địa chỉ ảo của VPN server, chẳng hạn như 100.0.0.1, đây là địa chỉ mà FTP server sẽ hoạt động trong mạng VPN. Tại máy trạm, người dùng bây giờ có thể sử dụng dịch vụ FTP với địa chỉ <ftp://100.0.0.1>.

Hình 11: Sử dụng dịch vụ ftp.

Dịch vụ World Wide Web trên VPN

Chúng tôi xây dựng ứng dụng quản lý và phát triển phần mềm cho một đơn vị sản xuất. Với ứng dụng này, lập trình viên làm việc tại các điểm khác nhau có thể cùng phát triển và trao đổi các module sản phẩm thông qua trang web chạy trên VPN mà vẫn đảm bảo an toàn. Người dùng cần đăng nhập vào mạng VPN sau khi truy nhập vào Internet. Trang web được thể hiện qua hình sau:

Hình 12: Trang Web trao đổi dữ liệu giữa các nhóm lập trình trên môi trường VPN.

IV. KẾT LUẬN

Sau khi thử nghiệm trên mô hình ĐH-Huế, với tư cách của người quản trị mạng Internet thông thường dựa trên giao thức TCP/IP, không thể nhìn thấy quá trình trao đổi thông tin của VPN trên các trình điều khiển hệ thống mạng. Từ đó mọi thông tin trao đổi trên VPN trên mô hình ĐH-Huế được bảo mật và trong suốt.

Đây là một mô hình đảm bảo tính riêng tư và an toàn dựa trên nền tảng Internet nên lợi dụng được cơ sở hạ tầng hiện có. Như vậy, qua bài này chúng tôi đã tiến hành nghiên cứu một cách đầy đủ từ lý thuyết sâu sắc của kỹ thuật đường ống, cơ chế hoạt động, mô hình hệ thống cho đến cài đặt và triển khai ứng dụng trên VPN.

Hầu hết các VPN đều dựa vào kỹ thuật gọi là Tunneling để tạo ra một mạng riêng trên nền Internet. Về bản chất, đây là quá trình đặt toàn bộ gói tin vào trong một lớp header (tiêu đề) chứa thông tin định tuyến có thể truyền qua hệ thống mạng trung gian theo những "đường ống" riêng (tunnel).

Khi gói tin được truyền đến đích, chúng được tách lớp header và chuyển đến các máy trạm cuối cùng cần nhận dữ liệu. Để thiết lập kết nối Tunnel, máy khách và máy chủ phải sử dụng chung một giao thức (tunnel protocol).

Giao thức của gói tin bọc ngoài được cả mạng và hai điểm đầu cuối nhận biết. Hai điểm đầu cuối này được gọi là giao diện Tunnel (tunnel interface), nơi gói tin đi vào và đi ra trong mạng.

Kỹ thuật Tunneling yêu cầu 3 giao thức khác nhau:

- Giao thức truyền tải (Carrier Protocol) là giao thức được sử dụng bởi mạng có thông tin đang đi qua.
- Giao thức mã hóa dữ liệu (Encapsulating Protocol) là giao thức (như GRE, IPSec, L2F, PPTP, L2TP) được bọc quanh gói dữ liệu gốc.
- Giao thức gói tin (Passenger Protocol) là giao thức của dữ liệu gốc được truyền đi (như IPX, NetBeui, IP).

Người dùng có thể đặt một gói tin sử dụng giao thức không được hỗ trợ trên Internet (như NetBeui) bên trong một gói IP và gửi nó an toàn qua Internet. Hoặc, họ có thể đặt một gói tin dùng địa chỉ IP riêng (không định tuyến) bên trong một gói khác dùng địa chỉ IP chung (định tuyến) để mở rộng một mạng riêng trên Internet.

Kỹ thuật Tunneling trong mạng VPN điểm-nội điểm

Trong VPN loại này, giao thức mã hóa định tuyến GRE (Generic Routing Encapsulation) cung cấp cơ cấu "đóng gói" giao thức gói tin (Passenger Protocol) để truyền đi trên giao thức truyền tải (Carrier Protocol). Nó bao gồm thông tin về loại gói tin mà bạn đang mã hóa và thông tin về kết nối giữa máy chủ với máy khách. Nhưng IPSec trong cơ chế Tunnel, thay vì dùng GRE, đôi khi lại đóng vai trò là giao thức mã hóa. IPSec hoạt động tốt trên cả hai loại mạng VPN truy cập từ xa và điểm- nối-điểm. Tất nhiên, nó phải được hỗ trợ ở cả hai giao diện Tunnel.



Trong mô hình này, gói tin được chuyển từ một máy tính ở văn phòng chính qua máy chủ truy cập, tới router (tại đây giao thức mã hóa GRE diễn ra), qua Tunnel để tới máy tính của văn phòng từ xa.

Kỹ thuật Tunneling trong mạng VPN truy cập từ xa

Với loại VPN này, Tunneling thường dùng giao thức điểm-nối-điểm PPP (Point-to-Point Protocol). Là một phần của TCP/IP, PPP đóng vai trò truyền tải cho các giao thức IP khác khi liên hệ trên mạng giữa máy chủ và máy truy cập từ xa. Nói tóm lại, kỹ thuật Tunneling cho mạng VPN truy cập từ xa phụ thuộc vào PPP.

Các giao thức dưới đây được thiết lập dựa trên cấu trúc cơ bản của PPP và dùng trong mạng VPN truy cập từ xa.

L2F (Layer 2 Forwarding) được Cisco phát triển. L2 F dùng bất kỳ cơ chế thẩm định quyền truy cập nào được PPP hỗ trợ.

PPTP (Point-to-Point Tunneling Protocol) được tập đoàn PPTP Forum phát triển. Giao thức này hỗ trợ mã hóa 40 bit và 128 bit, dùng bất kỳ cơ chế thẩm định quyền truy cập nào được PPP hỗ trợ.

L2TP (Layer 2 Tunneling Protocol) là sản phẩm của sự hợp tác giữa các thành viên PPTP Forum, Cisco và IETF. Kết hợp các tính năng của cả PPTP và L2F, L2TP cũng hỗ trợ đầy đủ IPSec. L2TP có thể được sử dụng làm giao thức Tunneling cho mạng VPN điểm-nối-điểm và VPN truy cập từ xa. Trên thực tế, L2TP có thể tạo ra một tunnel giữa máy khách và router, NAS và router, router và router. So với PPTP thì L2TP có nhiều đặc tính mạnh và an toàn hơn.

Quá trình thiết lập một mạng không dây

Cập nhật lúc 16h23' ngày 04/03/2009

 **Bản in**

 **Gửi cho bạn bè**

 **Phản hồi**

Xem thêm: *mạng không dây, lan, wan*

Brien M. Posey

Quản trị mạng - Lúc này chắc hẳn nhiều bạn trong số chúng ta hẳn đều biết rằng, chỉ cần một laptop có hỗ trợ truy cập mạng không dây là bạn có thể ngồi bất cứ ở đâu đó trong địa điểm phủ sóng của một điểm truy cập không dây để truy cập vào mạng. Quả thực mạng không dây đã mang lại cho chúng ta rất nhiều sự lựa chọn trong sơ sở hạ tầng mạng của một công ty nào đó. Quá trình thiết lập một mạng không dây về căn bản sẽ như thế nào? Đó chính là chủ đề trong bài mà chúng tôi sẽ giới thiệu cho các bạn về quá trình thiết lập một mạng không dây.

Phần cứng mạng không dây

Việc thiết lập một mạng không dây cũng tương tự như việc thiết lập một mạng chạy dây. Tuy nhiên điểm khác biệt lớn nhất nằm ở phần cứng. Trong phần này, chúng tôi sẽ giới thiệu cho các bạn một số các thiết bị thường được sử dụng nhất và giải thích những chức năng thực hiện của chúng.

Điểm truy cập không dây

Thành phần trung tâm của hầu hết các mạng không dây là điểm truy cập không dây, về trường hợp này bạn có thể tham khảo về mô hình 3Com mà chúng tôi lấy ví dụ như trong hình A bên dưới.



Hình A: Điểm truy cập không dây 3Com

Điểm truy cập không dây chính là thiết bị kết nối một mạng không dây với một mạng chạy dây. Chúng thực hiện chức năng như một hub cho các máy khách không dây. Điểm truy cập không dây cũng gồm có cổng Ethernet chuẩn dùng để kết nối đến mạng chạy dây. Cổng này cho phép sự truyền thông hai chiều giữa hai mạng.

Mặc dù việc sử dụng điểm truy cập là phương pháp được sử dụng nhiều nhất trong quá trình thiết lập một mạng không dây, tuy nhiên đó không phải là một yêu cầu bắt buộc. Bạn có thể sử dụng card mạng không dây với hai chế độ hoạt động: sơ sở hạ tầng và ad hoc. Khi hoạt động trong chế độ ad hoc, card mạng có thể truyền thông với nhau một cách trực tiếp mà không cần đến điểm truy cập. Tuy nhiên sử dụng điểm truy cập sẽ làm cho mạng của bạn dễ dàng hơn trong việc quản lý, cho phép truyền thông với mạng không dây và cho phép bạn kiểm soát tốt hơn về vấn đề bảo mật.

Gateway băng thông rộng

Có đến hàng triệu băng tần khác nhau và các mô hình của gateway băng thông rộng cho mạng không dây (cho ví dụ như trong hình B) được cung cấp trên thị trường với rất nhiều tính năng khác nhau. Mặc dù vậy chúng vẫn có một số đặc điểm chung như: kết nối trực tiếp với modem DSL hoặc modem cáp của bạn và chia sẻ kết nối băng thông rộng với các máy khách không dây thông qua một điểm truy cập không dây. Hầu hết các mô hình cũng đều có một hub đính kèm có thể dùng cho các máy khách chạy dây. Một điều thú vị nhất

về các gateway băng thông rộng không dây là hầu hết trong số chúng đều cung cấp các tính năng chỉ available cho một số các tập đoàn lớn với một số năm nhất định. Nhìn chung, các sản phẩm như vậy thường có giá từ 200\$ đến 600\$, phụ thuộc vào các tính năng được cung cấp trong chúng.



Hình B: Một ví dụ về gateway băng thông rộng không dây

Card PCI không dây

Các laptop thường sử dụng card mở rộng PCMCIA, trong khi đó trên các máy trạm thường thiên về sử dụng card PCI hơn. Mặc dù vậy cả hai cách thức thực hiện đều cho phép hỗ trợ card mạng không dây. Hình C bên dưới thể hiện card mạng PCI không dây của Linksys. Hình D là một card PCMCIA. Thành phần màu đen ở cuối card là anten của card. Cả hai card đều hoạt động ở cùng một tốc độ 11 Mbps, tuy nhiên lại dùng cho các kiểu máy khác nhau.



Hình C: Card PCI không dây



Hình D: PCMCIA card

USB NIC không dây

Một kiểu NIC không dây khác đó là USB NIC. Điều thú vị với các USB NIC đó là chúng có thể làm việc với cả các laptop và máy trạm. Các bạn có thể tham khảo ví dụ về USB NIC không dây trong hình E bên dưới.



Hình E: USB NIC không dây

Cầu Ethernet không dây

Cầu Ethernet không dây cung cấp kết nối giữa mạng không dây và mạng chạy dây với nhau. Trong khi điểm truy cập không dây cho phép các máy khách không dây kết nối với các mạng chạy dây (và ngược lại), thì cầu Ethernet không dây lại cho phép các thiết bị chạy dây hoạt động trên một mạng không dây.

Cho ví dụ, một trong những máy in laser có card JetDirect đi kèm có thể cho phép cắm trực tiếp vào mạng. Trong trường hợp này bạn muốn làm việc trên mạng không dây nhưng không có card không dây. Giải pháp có thể thực hiện được ở đây là cắm card mạng của máy in vào cổng RJ-45 trên cầu Ethernet không dây. Ở tình huống này, máy in sẽ duy trì địa chỉ IP của nó với danh nghĩa một cầu nối. Khi các máy khách cần truy cập vào máy in, các bảng định tuyến sẽ hướng chúng đi qua điểm truy cập không dây để đến được cầu không dây, sau đó đến máy in. Trong kịch bản này, bạn đang sử dụng cầu Ethernet không dây để kết nối một thiết bị riêng lẻ vào một mạng không dây, tuy nhiên

cũng có thể kết nối cả một đoạn mạng nào đó vào mạng không dây thông qua cầu này. Mặc dù vậy, nếu bạn có kế hoạch kết nối nhiều thiết bị hãy sử dụng điểm truy cập không dây để tiết kiệm và hiệu quả hơn.



Hình F: Cầu Ethernet không dây

Chạy dây cho không dây

Thông thường, khi bạn tạo một mạng không dây, bạn sẽ phải bắt đầu quá trình bằng cách kết nối điểm truy cập của mình vào mạng chạy dây thông qua một kết nối cáp thông thường (không phải cáp chéo). Khi kết nối chạy dây đến điểm truy cập được thiết lập, bạn phải sử dụng một trong những máy khách trên mạng chạy dây để cấu hình điểm truy cập.

Các vấn đề về giao diện web

Hầu hết các điểm truy cập không dây đều có thể được cấu hình thông qua giao diện web. Các khối đều có máy chủ web đi kèm để quản lý một site cấu hình web. Cũng tương tự như vậy, các khối cũng có máy chủ DHCP đi kèm để có thể phân phối địa chỉ IP đến các máy khách không dây. Nếu mạng của bạn đã có máy chủ DHCP rồi, khi đó bạn nên vô hiệu hóa máy chủ DHCP của điểm truy cập không dây đi nhằm ngăn chặn việc lọc các địa chỉ IP đã được đăng ký bởi máy chủ DHCP khác.

Việc kết nối vào điểm truy cập không dây được thực hiện hoàn toàn đơn giản, bạn chỉ cần mở Internet Explorer, nhập vào địa chỉ IP của điểm truy cập không dây. Ở thao tác này, bạn cần phải xem tài liệu đi kèm với điểm truy cập không dây để xem địa chỉ IP nào được sử dụng, tuy nhiên địa chỉ thường hay được sử dụng nhất vẫn là 192.168.0.1. Ban

đầu có thể sẽ hơi khó khăn cho việc kết nối đến một site cấu hình của điểm truy cập không dây. Tuy nhiên nếu bạn gặp phải vấn đề nào đó, hãy kiểm tra để bảo đảm rằng Internet Explorer không bị cấu hình để sử dụng proxy server. Nếu mạng của bạn phụ thuộc vào proxy server, khi đó hãy bổ sung thêm một địa chỉ IP của điểm truy cập không dây vào bảng địa chỉ nội bộ (LAT) của proxy server, và bạn có thể truy cập vào site cấu hình mà không cần hủy bỏ cài đặt proxy client của máy trạm.

Bạn cũng có thể bắt gặp lỗi kiểu trong subnet. Cho ví dụ, nếu mạng của bạn sử dụng subnet mask là 255.255.0.0 và điểm truy cập không dây của bạn sử dụng subnet mask là 255.255.255.0, khi đó mạng của bạn sẽ không thể truyền thông với điểm truy cập không dây. Trong trường hợp này bạn có thể xếp đặt mọi thứ vào một subnet chung hoặc cập nhật các bảng định tuyến của mình nhằm cung cấp một đường dẫn logic đến điểm truy cập không dây.

Cấu hình

Khi bạn đã tạo một kết nối đến trang cấu hình của điểm truy cập không dây, lúc này hãy bắt đầu quá trình của mình. Bạn phải chọn các thiết lập mà mình muốn sử dụng, sau đó cấu hình các máy khách không dây để sử dụng các thiết lập giống nhau. Quá trình cấu hình thực sự cho một điểm truy cập không dây diễn ra khác nhau phụ thuộc vào các nhà sản xuất thiết bị, tuy nhiên các thông tin cơ bản mà bạn cần phải cung cấp hoàn toàn giống nhau. Trong các phần bên dưới, chúng tôi sẽ giới thiệu cho các bạn về các thiết lập không dây quan trọng này.

Vùng dịch vụ LAN không dây

Vùng dịch vụ LAN không dây hay vẫn được gọi là SSID, chính là nơi xác minh mạng không dây. Thông thường, vùng dịch vụ LAN không dây đều đặt tên bằng văn bản. Cho ví dụ, bạn có thể đặt tên cho vùng dịch vụ LAN không dây của mình là “Mạng không dây của Công Ty A” nào đó. Một tên duy nhất như vậy sẽ bảo đảm rằng bạn không bị sử dụng nhầm lẫn SSID bên cạnh.

Tên khối

Điểm truy cập không dây có phạm vi đủ lớn phục vụ cho hầu hết các văn phòng nhỏ nào. Mặc dù vậy, trong các tòa nhà lớn, một điểm truy cập không dây có thể không đủ để cung cấp tất cả sự bao phủ cần thiết. Trong các tình huống giống như vậy, cần phải sử dụng nhiều điểm truy cập không dây. Theo cách đó các card mạng không dây hoạt động tương tự như điện thoại cell phone. Khi một người dùng roaming một tòa nhà bằng một laptop, wireless NIC sẽ tìm kiếm các điểm truy cập có sẵn hiện đang được cung cấp với tín hiệu lớn nhất và kết nối đến điểm truy cập này cho tới khi tín hiệu đó trở thành yếu và cần thay thế bằng một điểm truy cập khác. Tên của khối chính là phương pháp wireless NIC

sử dụng để phân định điểm truy cập nào mà nó đang truyền thông với.

Kênh

Tuy các điểm truy cập không dây 802.11B làm việc ở phạm vi dải tần 2.4-GHz nhưng vẫn có các kênh khác nhau nằm bên trong dải phổ 2.4-GHz. Nhìn chung thường có 9 kênh có sẵn nhưng một số mô hình cũ hơn chỉ có ba đến sáu kênh. Việc thiết lập một kênh không dây cũng đơn giản như việc điều chỉnh sóng vô tuyến trong xe ô tô để bắt được một trạm phát sóng nào đó.

Vậy tại sao cần có nhiều kênh đến vậy? Một lý do ở đây là nhằm giúp bạn tìm ra một kênh không bị ảnh hưởng bởi các hệ số môi trường. Cho ví dụ, khi thiết lập số kênh là 3, điện thoại không dây sẽ ảnh hưởng đến hiệu suất mạng. Một lý do khác cho các kênh này là sự riêng tư. Hãy hình dung rằng bạn đang hoạt động trên kênh 6 nhưng một văn phòng bên cạnh bạn cũng hoạt động cùng với kênh đó. Thông thường, nó sẽ phát sinh vấn đề ở đây trừ khi bạn chọn sử dụng SSID mặc định. Nếu điều đó xảy ra, hai mạng sẽ xuyên nhiễu lẫn nhau.

Việc sử dụng kênh khác nhau với ở bên cạnh nhau sẽ cho bạn mang lại hiệu suất tốt hơn. Giống như cáp đồng, mỗi một kênh có một số lượng hạn chế băng thông nhất định. Thông thường, bạn phải có đến khoảng 64 máy tính trên một kênh trước khi hiệu suất bão hòa, nhưng nếu một máy khách nào đó đang sử dụng kết nối nặng, thì những suy biến về hiệu suất có thể xuất hiện chỉ với một số máy tính online khác.

WEP

Wireless Encryption Protocol (WEP) là một công nghệ mã hóa để ngăn chặn một kẻ thứ ba có thể xâm nhập vào kênh của bạn để ăn cắp các gói dữ liệu khi đang phát chúng trên không khí, bên cạnh đó việc sử dụng chúng cũng cho phép bạn tăng được khả năng truy cập vào các thông tin nhạy cảm. WEP có một số hệ số khác nhau: 40 bit (hiện nay gần như không sử dụng), 64 bit và 128 bit.

Việc kích hoạt WEP thường là vấn đề chọn giữa mã hóa 64-bit hay 128-bit và sau đó chọn mật khẩu cho WEP. Mật khẩu cho WEP phải là một số hexa 13 ký tự (cho 64 bit) hoặc 26 ký tự cho (128 bit). Ý tưởng ở đây là rằng các số này không phải dùng để truyền tải mà dùng để mã hóa vào cấu hình của điểm truy cập và cấu hình máy khách. Khi một máy khách gửi đi một thông báo đến điểm truy cập, gói dữ liệu sẽ được mã hóa bằng cách sử dụng mật khẩu WEP với tư cách là key. Khi điểm truy cập nhận thông báo, nó có thể giải mã nó vì đã có sẵn key cần thiết.

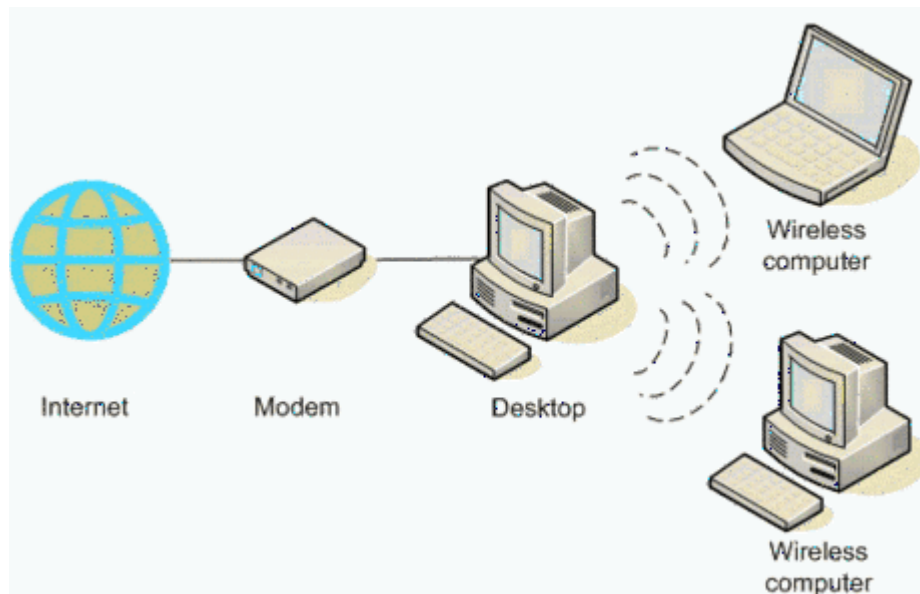
**Các bạn phải đặt IP tĩnh cho tất cả các máy tính trong mạng nha.
Một máy chủ và tối đa 9 máy khách kết nối vào mà thôi.**

Win XP

Thiết lập mạng vô tuyến dạng Ad-hoc

Gửi vào 1/1/2008 - 5:08

Nếu muốn nối mạng không dây cho vài ba chiếc laptop trong nhà thì việc đầu tiên bạn nghĩ đến là gì? Chạy ra ngoài hàng mua 1 wireless router hay 1 WAP à, hay mua gấp 1 bộ modem PLC? Từ từ, còn có một phương án khác tiết kiệm và hiệu quả hơn rất nhiều đấy: Mạng Ad-hoc.



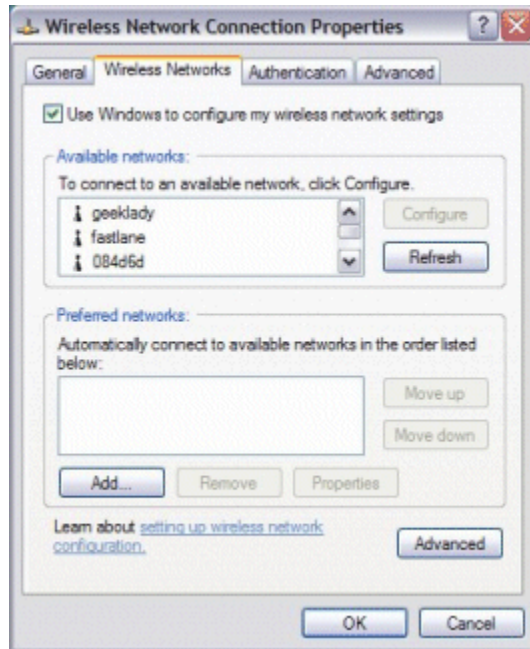
Sở đồ nguyên lý mạng chia sẻ kết nối dạng Ad-hoc

Ý tưởng của mạng Ad-hoc (theo tiếng Anh có nghĩa là "vì mục đích") là xây dựng 1 mạng kết nối (chủ yếu là vô tuyến) giữa các thiết bị đầu cuối mà không cần phải dùng các trạm thu phát gốc (BS). Các thiết bị đầu cuối sẽ tự động bắt liên lạc với nhau để hình thành nên 1 mạng kết nối tạm thời dùng cho mục đích truyền tin giữa các nút mạng. Ad-hoc đầu tiên được phát triển cho mục đích quân sự, nhưng do ưu điểm về giá thành và sự linh động, ngày nay, mọi người đều có thể được sử dụng nó. Nếu bạn đang ở chung phòng với 1 nhóm bạn sử dụng laptop, được trang bị Windows XP và các card giao tiếp vô tuyến theo chuẩn 802.11b với duy nhất 1 đường LAN kết nối ra Internet thì mạng Ad-hoc là một lựa chọn phù hợp nhất.

Tôi đã biết đến mạng Ad-hoc từ khá lâu, nhưng chỉ sau khi dùng mạng này ở nhà 1 người bạn tôi mới thấy thật sự ngạc nhiên về tốc độ và sự đơn giản, tiết kiệm chi phí

của phương pháp này. Tôi mong rằng bài viết này sẽ giúp nhiều người có thêm 1 lựa chọn kết nối không dây trong nhà phù hợp với điều kiện của mình.

Đặt cấu hình cho máy chủ:



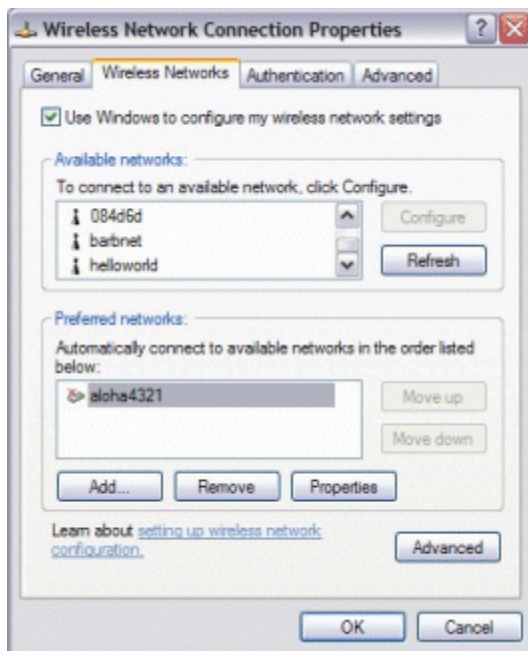
- Đầu tiên bạn hãy bỏ hết những điểm truy cập không dây (WAP) mà máy tính của bạn đang liên kết để đảm bảo nó chỉ làm việc duy nhất với mạng Ad-hoc mà chúng ta đang thiết lập.

- Tiếp theo, kích vào tab "Advanced", chọn "Computer to computer (ad hoc) networks only" và xóa lựa chọn "Automatically connect to non-preferred networks"

- Kích lại vào tab "Wireless Networks". Dưới phần "Preferred Networks", kích "Add". Trong phần hộp thoại "Wireless Network Properties", đặt tên mạng Adhoc của mình vào "Network name (SSID)". Nhớ đánh dấu chọn "computer-to-computer network".

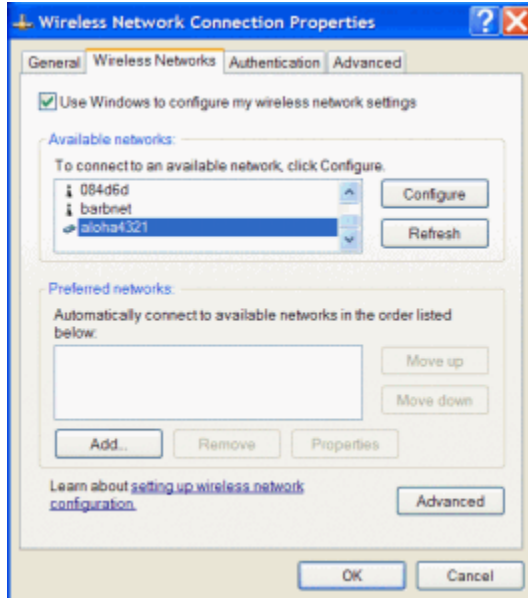


- Thiết lập "Wireless Equivalency Protocol (WEP)" chưa cần phải làm ngay ở bước này vì ta nên lập mạng Ad-hoc chạy trơn tru trước khi mã hóa dữ liệu. Sau này, quyết định có dùng mã hóa dữ liệu hay không phụ thuộc vào môi trường. Trong đa số trường hợp, nên dùng tính năng này.



- Để ý đến dấu x đỏ bên cạnh tên mạng. Khi có 1 máy khác trong vùng phủ sóng và liên kết với máy chủ này, dấu x đỏ sẽ mất đi.

Đặt cấu hình cho máy khách:



- Khi nằm trong phạm vi phủ sóng của máy chủ, trên máy khách sẽ xuất hiện tên của mạng Ad-hoc mà máy chủ vừa tạo ra. Chọn tên này, kích "Configure". Vì chưa thiết lập WEP nên kích tiếp vào "OK".

Chia sẻ kết nối

Sau khi đã thiết lập được 1 kết nối giữa máy chủ và máy khách, ta sẽ thiết lập cấu hình chia sẻ kết nối Internet.

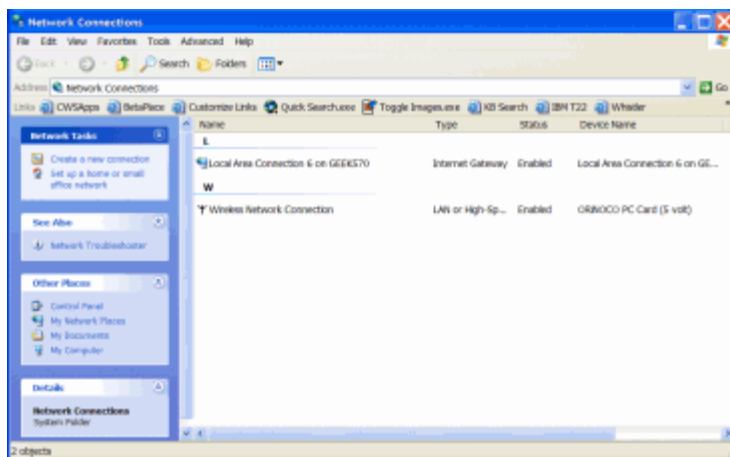
- Mở "Network Connections" trên máy chủ, (chọn Start>Control Panel>Switch to classic view>Network Connections).

- Chọn kết nối internet để chia sẻ, chọn "Allow other network users to connect through this computer's Internet connection" trong tab "Advanced".

- Nếu chưa có firewall, bạn nên thiết lập "Internet Connection Firewall (ICF)" tại bước này.

- Có thể tùy chọn cho những người dùng khác kiểm soát hay thay đổi kết nối này.

Sau khi kết thúc việc thiết lập cấu hình cho ICS, cửa sổ "Network Connection" sẽ xuất hiện trên máy chủ với trạng thái "shared" và "Enable". Trên cửa sổ "Network Connection" của máy khách, kết nối này sẽ hiển thị là "Internet Gateway".



- Máy khách sẽ nhận được 1 địa chỉ ip nội bộ dạng 192.168.0.* từ DHCP của máy chủ và được thông ra Internet.

Đặt cấu hình cho WEP:

Sau khi đã thiết lập thành công mạng Ad-hoc, trở lại "Network Properties" để thiết lập cho WEP.

- Trên máy chủ, mở "Wireless Network Properties", chọn "Data encryption (WEP enabled)".



Như vậy bạn đã hoàn tất quá trình thiết lập và chia sẻ kết nối internet bằng chức năng thiết lập mạng Ad-hoc của Windows XP.

Anh Ngọc (theo microsoft.com)

Win vista

TẠO MỘT MẠNG WIRELESS AD HOC

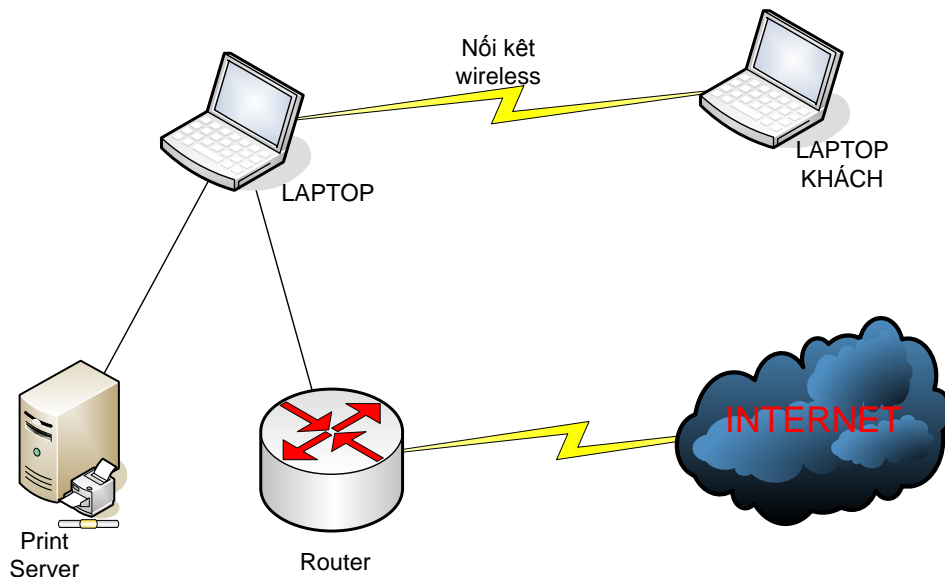
Nếu bạn sử dụng một mạng wireless một cách nhất quán, một mạng wireless infrastructure hầu như sẽ là sự lựa chọn tốt nhất. Tuy nhiên, đôi khi bạn muốn xây dựng một mạng wireless trong chỉ một thời gian ngắn sao cho hai hoặc nhiều máy tính có thể giao tiếp tạm thời hoặc sao cho bạn có thể chia sẻ dễ dàng nối kết Internet của máy tính với một máy tính khác – ví dụ, khi một người bạn ghé thăm với laptop mang theo. Trong trường hợp này, bạn có thể tạo một mạng wireless ad hoc (đặc biệt), như được mô tả trong bài dưới đây, thay vì xây dựng một mạng wireless infrastructure.

Bước 1: Thêm các adapter mạng nếu cần thiết

Bước đầu tiên trong việc xây dựng mạng wireless ad hoc là thêm một adapter mạng wireless vào bất cứ một PC nào bạn muốn sử dụng trong mạng và không có một adapter. Hầu hết các laptop gần đây và hiện tại có một adapter mạng wireless do đó có thể bạn không cần thêm một adapter này.

Bước 2: Hoạch định mạng Wireless

Một khi mỗi PC gia nhập mạng có một adapter mạng wireless, bạn có thể hoạch định mạng. Việc hoạch định hầu như không mất thời gian, đặc biệt nếu mạng gồm chỉ một vài PC như trong mạng mẫu được minh họa trong hình sau:



Hãy ghi nhớ những điểm sau đây:

- **Địa điểm:** Hầu hết các adapter mạng wireless không quản lý các khoảng cách bằng nhau mà các wireless access point phủ sóng, do đó bạn sẽ đạt được hầu như các kết quả nhất quán – và các tốc độ truyền dữ liệu cao hơn – nếu các PC nằm trong khoảng cách của nhau và không có vật cản trên đường. Nghĩa là các tín hiệu wireless truyền tối đa qua các sàn nhà và trần nhà – thường tốt hơn các vách tường nhất là các vết rãnh dây và hốc.

▪ **Phương pháp mã hóa:** Tất cả các PC phải sử dụng cùng một loại mã hóa – ví dụ, WPA hoặc WEP.

Ghi chú

Windows XP giới hạn chỉ sử dụng WEP cho các mạng ad hoc, vì vậy nếu mạng của bạn sẽ gồm một hoặc nhiều PC chạy trên Windows XP, bạn sẽ không thể thực thi sự an ninh chặt chẽ - nhưng WEP sẽ đầy đủ cho việc sử dụng tạm thời. Nếu tất cả PC chạy Windows Vista, bạn có thể sử dụng WPA – nhưng một số người thấy rằng WPA gây ra sự cố với các mạng ad hoc và phải quay trở về WEP.

▪ **Chia sẻ các nguồn tài nguyên.** Bất kỳ một PC vốn là một nguồn tài nguyên chia sẻ với những PC khác cần truy cập các nguồn tài nguyên đó.

Bước 3: Thêm các PC vào mạng

Thiết lập một mạng wireless hầu như là một vấn đề cho tất cả PC tham gia mạng sử dụng cùng một tên mạng (SSID) và cùng một phương pháp mã hóa. Phần này hướng dẫn cách thiết lập mạng trong Windows Vista.

Thiết lập PC đầu tiên trên mạng Wireless

Khi bạn thiết lập PC đầu tiên kết nối với mạng, bạn đang tạo ra mạng. Làm theo các bước sau đây:

1. Chọn Start > Connect To. Windows khởi động Connect To A Network Wizard, vốn hiển thị màn hình Select A Network To Connect To. Màn hình này liệt kê các mạng có sẵn, nếu có.
2. Nhấp link Set Up A Connection Or Network ở góc trái phía dưới để hiển thị màn hình Choose A Connection Option.
3. Chọn mục Set Up A Wireless Ad Hoc (Computer-To-Computer).
4. Nhấp nút Next để hiển thị màn hình Set Up A Wireless Ad Hoc Network, vốn trình bày thông tin về các mạng ad hoc.

Ghi chú

Màn hình Set Up A Wireless Ad Hoc Network khấn định các máy tính và thiết bị trong các mạng ad hoc “phải nằm trong phạm vi 30 feet của nhau”. Điều này không hoàn toàn đúng. Trừ khi có các vách tường hoặc sàn nhà dày trên đường, bạn có thể đạt được những khoảng cách lớn hơn nếu cần thiết.

5. Nhấp nút Next để hiển thị màn hình Give Your Network A Name And Choose Security Options, được minh họa ở dưới đây với các xác lập được chọn:
6. Trong hộp text Network Name, gõ tên mà bạn muốn sử dụng cho mạng.
7. Trong danh sách sổ xuống Security Type, chọn loại an ninh mà bạn muốn:
 - **No Authentication (Open).** Xác lập này cho bất kỳ máy tính trong phạm vi phủ sóng kết nối với mạng mà không tự xác thực. Xác lập này không bao giờ là một tùy ý hay.

- **Web.** Xác lập này sử dụng Wired Equivalent Privacy, vốn cung cấp sử dụng tương đối. Sử dụng WEP nếu bạn cần kết nối các PC Windows XP với mạng.
 - **WAP2-Personal.** Xác lập này sử dụng Wi-Fi Protected Access, vốn cung cấp sự bảo mật tốt. sử dụng WEP2-Personal nếu tất cả PC sẽ kết nối với mạng chạy Windows Vista.
8. Trong hộp thoại text Security Key/Passphrase, gõ nhập password cho mạng, bảo đảm bạn tuân thủ theo các quy tắc được liệt kê kế tiếp cho loại an ninh mà bạn đã chọn ở bước 7. Chọn hộp kiểm Display Characters nếu bạn muốn chắc chắn về những gì bạn đang gõ nhập và tự tin không ai theo dõi bạn.
- WEP. Mã hóa phải là 5 ký tự ASCII (bình thường) hoặc 13 ký tự ASCII – ví dụ, wire0 hoặc wirelessnet99. Một mã hóa 5 ký tự cung cấp sự mã hóa 40 bit, và một mã hóa 13 ký tự cung cấp sự mã hóa 104 bit.

Ghi chú

Hoặc, bạn có thể nhập key WEP dưới dạng 10 ký tự thập lục phân (để tạo sự mã hóa 40 bit) hoặc 24 ký tự thập lục phân (để tạo sự mã hóa 104 bit).

- WAP2-Personal. Bạn có thể sử dụng một password gồm 8-63 ký tự ASCII hoặc 64 ký tự thập lục phân.
9. Chọn hộp kiểm tra Save This Network nếu bạn muốn Windows lưu mạng này để sử dụng sau này. Nếu bạn dự định mạng chỉ sử dụng chỉ một lần, để hộp kiểm này hủy chọn.
10. Nhấp nút Next. Windows thiết lập mạng và sau đó hiển thị một màn hình (được minh họa kế tiếp) cho biết mạng đã sẵn sàng để sử dụng.
11. Nếu bạn muốn chia sẻ kết nối Internet của PC này thông qua mạng wireless, hãy nhấp nút Turn On Internet Connection Sharing, đi qua User Account Control cho chương trình Adhoc Wireless Network (trừ khi bạn đã tắt User Control), và tiến hành các bước còn lại trong danh sách này. Nếu bạn không chia sẻ kết nối Internet nhấp nút Close, và bỏ qua các bước còn lại.
12. Wizard hiển thị màn hình Select The Internet Connection You Want To Share.
13. Trong danh sách xổ xuống Available, chọn nối kết Internet, và sau đó nhấp nút Next. Wizard thiết lập việc chia sẻ và sau đó hiển thị màn hình Internet Connection Sharing Is Enable.
14. Nhấp nút Close để đóng Wizard.

Bây giờ mạng wireless ad hoc được thiết lập, và những PC khác có thể kết nối vào nó.

Thêm một PC mới vào một mạng wireless hiện có

Một khi bạn đã thiết lập một PC cung cấp mạng wireless, bạn có thể kết nối thêm các PC với mạng bằng cách sử dụng một kỹ thuật khác. Làm theo các bước sau:

1. Chọn Start > Connect To. Windows khởi động Connect To A Network Wizard, vốn hiển thị màn hình Select A Network To Connect To. Màn hình này liệt kê các mạng có sẵn.

Thủ thuật

Biểu tượng ở đầu bên trái hàng của mỗi mạng cho thấy loại mạng. Biểu tượng cho một mạng ad hoc cho thấy ba máy tính được liên kết lại với nhau. Nếu danh sách mạng bao gồm nhiều loại mạng, chọn Wireless trong danh sách xổ xuống Show để làm cho danh sách hiển thị các mạng wireless.

2. Nhấp mạng mà muốn kết nối, và nhấp nút Connect. Wizard hiển thị màn hình Type The Network Security Key Or Passphrase được minh họa ở đây.
3. Gõ nhập key mạng trong hộp text Security Key Or Passphrase. Nếu không có người nào chôn qua vai bạn, bạn có thể chọn hộp kiểm Display Character để bỏ qua các dấu chấm mà Wizard hiển thị theo mặc định (vì an ninh của bạn).
4. Nhấp nút Connect. Wizard kết nối PC với mạng, sau đó hiển thị màn hình Successfully Connected.
5. Nếu bạn muốn sử dụng dễ dàng mạng này trong tương lai, chọn hộp kiểm Save This Network. Tuy nhiên, đối với mạng ad hoc tạm thời, có lẽ bạn muốn hộp chọn này được hủy chọn.
6. Nhấp nút Close để đóng wizard. Bây giờ PC được kết nối với mạng.

Bước 4: Ngắt kết nối một PC với mạng Wireless

Khi bạn muốn ngắt một PC trở thành một mạng của wireless, ngắt kết nối PC với mạng đó.

Để ngắt kết nối, nhấp phải vào biểu tượng Network Connection trong vùng thông báo, nhấp chuột hoặc bật sang mục Disconnect From trên menu ngữ cảnh, sau đó nhấp tên của mạng trên menu con. Windows sẽ ngắt kết nối với mạng.

Bước 5: Tắt mạng Ad Hoc

Khi bạn đã thấy xong mạng wireless, bạn có thể tắt nó bằng cách ngắt kết nối tất cả các PC trên nó, như được thảo luận ở phần trước.

Như bạn đã thấy trước đó trong bài này, Windows Vista cho bạn quyết định có nên lưu mạng để sử dụng sau này hay không. Miễn là bạn không chọn hộp kiểm Save This Network trong khi thiết lập mạng, Windows Vista tự động loại bỏ chi tiết của mạng khi bạn ngắt kết nối PC với mạng.

Các tính toán căn bản để thiết lập mạng Wireless Lan



Các tính toán cơ bản để thiết lập mạng wireless LAN

Các bước cơ bản để thiết lập một mạng wireless LAN

Bước 1: Đặt kế hoạch (Khảo sát mạng)

Bước này dựa vào nhu cầu của khách hàng chúng tôi sẽ tìm hiểu và đi đến quyết định tư vấn cho khách hàng. Bước này phải trả lời các câu hỏi dưới đây.

Điều gì khiến cho bạn quyết định triển khai mạng không dây?

Nếu triển khai mạng không dây thì bạn sẽ triển khai theo mô hình nào dưới đây:

Mô hình Adhoc (Peer to Peer): mô hình này thích hợp với mạng nhỏ số lượng vài máy tính, không cần điểm truy nhập Access Point, chỉ cần máy tính có card không dây là có thể chia sẻ tài nguyên.

Mô hình Infrastructure: Mô hình này áp dụng cho hệ thống vừa và lớn. Yêu cầu có điểm truy cập Access Point (hoặc Gateway Access Point). Mô hình này vừa có thể là không dây hoàn toàn, vừa có thể là dùng chung với hệ thống mạng có dây.

Tần số sử dụng cho các thiết bị mạng không dây như Access Point, desktop, laptop, PDA là dải tần nào?

Bao nhiêu User có thể sử dụng một Access Point (hoặc Gateway AP)

Tổng số thiết bị dùng mạng không dây như PC, laptop, PDA, Printer Server...dùng mạng không dây là bao nhiêu.

Từ đó tính được số Access Point (Gateway AP)cần dùng

Bước 2: Chọn loại thiết bị mạng không dây

Chọn Card mạng không dây: USB, PCI, PCI CIA...

Chọn Access Point (hoặc Gateway AP): tốc độ theo chuẩn nào, có các tính năng gì, chẳng hạn như DHCP, lọc MAC, bán kính phủ sóng, tính security..., (nếu là Gateway AP thì có tính năng gì, chẳng hạn như DHCP, NAT, VPN...).

Bước 3: Triển khai mạng

Cài đặt và kết nối các Access Point (hoặc Gateway Access Point) vào mạng

Cài đặt card mạng không dây sau đó kết nối vào hệ thống mạng

Bước 4: Triển khai an ninh mạng

Áp dụng các biện pháp an ninh mạng không dây như

Dùng mã hoá WEP Key

Mã hoá Shared Key

Mã hoá WPA - PSK

Mã hoá WPA (Wireless Protected Access) dùng kết hợp Radius Server nhận thực và mã hoá người dùng

Các yếu tố ảnh hưởng đến quá trình truyền sóng

Dưới đây là sơ đồ quá trình truyền sóng từ phía phát đến phía thu, các yếu tố ảnh hưởng đến quá trình truyền sóng

Công suất đầu ra thiết bị phát. Yếu tố này phụ thuộc vào Access point (AP), chuẩn AP, tốc độ truyền dẫn của AP. Các thông số này thường đi kèm với tài liệu thuyết minh về sản phẩm.

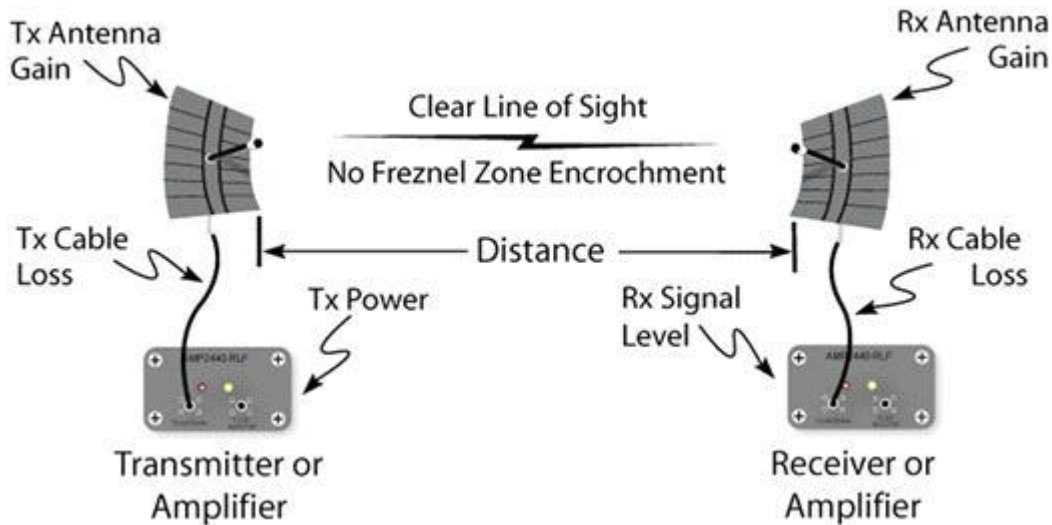
Tổn hao tín hiệu trên cáp phía phát. Tùy từng loại cáp dài hay ngắn, khi sản xuất thường ghi sẵn độ suy hao của loại cáp này.

Khuếch đại tín hiệu trên anten phía phát. Yếu tố này phụ thuộc vào từng loại Anten và khi sản xuất thường ghi sẵn độ khuếch đại

Tổn hao tín hiệu trên đường truyền từ phía phát tới phía thu. Thông số này có công thức để tính toán ($32,4 + 20 \log F$ (Mhz) + $20 \log R$ (km))

Khuếch đại tín hiệu trên Anten thu

Tổn hao tín hiệu trên cáp phía thu
 Độ nhạy của thiết bị phía thu: Độ nhạy của thiết bị phía thu do công nghệ sản xuất sản phẩm, thông số này càng nhỏ thì càng



tốt.

Sơ đồ quá trình truyền sóng từ bên phát đến bên thu

Một số bài toán cụ thể trong mô hình kết nối mạng LAN to LAN ở chế độ bridge

Bài toán 1

Dùng Wap-4000 tốc độ 54Mbps của PLANET, anten Yagi 20dBi, tính toán khoảng cách tối đa khi kết nối 2 mạng Lan giữa 2 toà nhà

Wap-4000 hoạt động ở dải tần 2,4GHz (= 2400MHz) , với tốc độ 54Mbps thì độ nhạy thu là: 68dBi (thông số này tùy vào tốc độ truyền), công suất đầu ra là 13dBi

Công thức tính suy hao khoảng cách = $32,4 + 20\log F(\text{MHz}) + 20\log R(\text{km}) = 32,4 + 20\log 2400 + 20\log R = 100 + 20\log R$

Tổn hao trên cáp phía phát là: -3,5dBi

Khuếch đại trên anten thu là 20dBi (Anten Yagi 20dBi)

Thông số EIRP là thông số tổng cộng để tính toán bài toán có đạt yêu cầu không, thông thường $EIRP > 5$ là tốt. Ở đây ta lấy bằng 5

Tất cả các thông số này được tính toán như bảng dưới đây . Bảng này áp dụng cho tất cả các trường hợp tính toán liên quan đến anten trong mô hình LAN to LAN (Bridge)

Công suất đầu ra phía phát	13
Tổn hao trên cáp phía phát	-3,5
Khuếch đại tín hiệu trên anten phát	20
Suy hao tín hiệu trên đường truyền (suy hao khoảng cách)	$-(100 + 20\log R)$
Khuếch đại trên anten thu	20
Tổn hao trên cáp phía thu	-3,5
Độ nhạy thiết bị thu	- (-68)

EIRP (Effective Isotropic Radiated Power)	5
---	---

Cộng tất cả các thông số trong bảng trên để tính được R

$$EIRP = 5 = 13-7+40+68- (100+20\log R) \Rightarrow R = 2,81\text{km} .$$

Như vậy khi dùng Wap-4000 tốc độ 54Mbps , anten 20dBi thì khoảng cách truyền tối đa được 2,81km.

Chú ý : xem thêm Sơ đồ quá trình truyền sóng từ phía phát đến phía thu để hiểu rõ hơn về các thông số trong bảng đã tính ở trên đồng thời phải xem thêm thông số kỹ thuật của sản phẩm để biết các thông số về công suất phát, độ nhạy thu, tổn hao tín hiệu trên cáp...

Bài toán 2

Yêu cầu về tốc độ và khoảng cách. Giả sử yêu cầu tốc độ mạng không dây phải đạt được là 36 Mb/s, khoảng cách truyền là 10, thiết bị nào của PLANET đáp ứng được yêu cầu này?

Giả sử chọn thiết bị là Wap 4000, anten định hướng Yagi có độ khuếch đại 20 dBi. Dựa vào bài toán 1 ta sẽ tính tất cả các thông số sau đó cộng lại ta được tổng là EIRP, EIRP này phải ≥ 5 nếu không thỏa mãn ta sẽ phải chọn thiết bị khác.

$$\text{Công thức tính suy hao khoảng cách} = 32,4 + 20\log F(\text{Mhz}) + 20\log R(\text{km}) = 32,4 + 20\log 2400 + 20\log 10 = 120\text{dBi}$$

Xem thông số của Access Point Wap-4000 nếu truyền ở tốc độ 36Mbps thì công suất phát là 15dBi, độ nhạy thu là: -76dBi

Công suất đầu ra phía phát	15
Tổn hao trên cáp phía phát	-3,5
Khuếch đại tín hiệu trên anten phát	20
Suy hao tín hiệu trên đường truyền (suy hao khoảng cách)	-(120)
Khuếch đại trên anten thu	20
Tổn hao trên cáp phía thu	-3,5
Độ nhạy thiết bị thu	- (-76)
EIRP (Effective Isotropic Radiated Power)	?

Cộng tất cả các thông số trong bảng ta được $EIRP = 4$ không thỏa mãn. Như vậy ta có thể tăng độ khuếch đại Anten hoặc là thay đổi Access Point có độ nhạy thu và công suất phát cao hơn. Ở trường hợp này ta có thể thay anten

Giải pháp thiết kế mạng LAN sử dụng thiết bị VDSL

Phần 1

1. Hiện trạng

Giả sử một cơ quan có 2 toà nhà cách nhau không quá 1.5 km. Tại mỗi toà nhà hiện đã có các mạng LAN nội bộ.

yêu cầu đặt ra là: kết nối mạng giữa 2 toà nhà này với chi phí thấp và tốc độ truyền đạt 10Mbps.

Trường hợp đặt ra trong tương lai là cơ quan này có thể mở rộng các chi nhánh và yêu cầu kết nối mạng của toàn cơ quan với chi phí thấp và tốc độ chấp nhận 10Mbps.

2. Giải pháp kết nối

Thông thường, theo nguyên lý thiết kế hệ thống mạng thì việc kết nối giữa hai điểm cách xa nhau (1.5 km) như trên chúng ta phải dùng cáp quang để đảm bảo đường truyền. Tuy nhiên, việc sử dụng cáp quang cũng khá tốn kém mà như yêu cầu đặt ra thì tốc độ truyền dẫn không cần cao lắm chỉ đủ để truyền dẫn các thông tin thông thường. Do đó, giải pháp sử dụng đường điện thoại để kết nối là một giải pháp khá hoàn hảo trong trường hợp này

2.1. Giải pháp kết nối VDSL giữa 2 điểm

- Sử dụng dây điện thoại thông thường (loại đi ngoài trời) để kết nối giữa 2 toà nhà
- Tại toà nhà trung tâm (văn phòng công ty chẳng hạn) ta đặt 1 thiết bị VDSL master và tại chi nhánh ta đặt một thiết bị VDSL Slaver. Dây điện thoại sẽ được kết nối vào 2 thiết bị này thông qua hộp đấu dây điện thoại và thiết bị chống sét lan truyền trên đường dây (có thể sử dụng thiết bị chống sét của APC) vào cổng có ký hiệu VDSL
- Máy tính trong mỗi toà nhà sẽ được kết nối vào thiết bị VDSL (thông thường mỗi thiết bị VDSL có 04 cổng RJ45 cho phép kết nối được 4 máy tính) hoặc có thể kết nối Hub/Switch có sẵn tại mỗi toà nhà vào thiết bị.
- Sau khi đấu nối như trên mạng LAN nội bộ của các toà nhà sẽ được kết nối với nhau với tốc độ khoảng 10 Mbps mà không phải cài thêm bất cứ phần mềm hay driver nào. Tốc độ mạng LAN hiện tại sẽ không phụ thuộc vào kết nối VDSL, nếu mạng LAN cũ của các toà nhà có tốc độ 10Mbps hay 10/100Mbps thì tốc độ này vẫn được giữ nguyên trong mạng LAN mới này.

Giải pháp thiết kế mạng LAN sử dụng thiết bị VDSL

Phần 1

1. Hiện trạng

Giả sử một cơ quan có 2 toà nhà cách nhau không quá 1.5 km. Tại mỗi toà nhà hiện đã có các mạng LAN nội bộ.

yêu cầu đặt ra là: kết nối mạng giữa 2 toà nhà này với chi phí thấp và tốc độ truyền đạt 10Mbps.

Trường hợp đặt ra trong tương lai là cơ quan này có thể mở rộng các chi nhánh và yêu cầu kết nối mạng của toàn cơ quan với chi phí thấp và tốc độ chấp nhận 10Mbps.

2. Giải pháp kết nối

Thông thường, theo nguyên lý thiết kế hệ thống mạng thì việc kết nối giữa hai điểm cách xa nhau (1.5 km) như trên chúng ta phải dùng cáp quang để đảm bảo đường truyền. Tuy nhiên, việc sử dụng cáp quang cũng khá tốn kém mà như yêu cầu đặt ra thì tốc độ truyền dẫn không cần cao lắm chỉ đủ để truyền dẫn các thông tin thông thường. Do đó, giải pháp sử dụng đường điện thoại để kết nối là một giải pháp khá hoàn hảo trong trường hợp này

2.1. Giải pháp kết nối VDSL giữa 2 điểm

- Sử dụng dây điện thoại thông thường (loại đi ngoài trời) để kết nối giữa 2 toà nhà
- Tại toà nhà trung tâm (văn phòng công ty chẳng hạn) ta đặt 1 thiết bị VDSL master và tại chi nhánh ta đặt một thiết bị VDSL Slaver. Dây điện thoại sẽ được kết nối vào 2 thiết bị này thông qua hộp đấu dây điện thoại và thiết bị chống sét lan truyền trên đường dây (có thể sử dụng thiết bị chống sét của APC) vào cổng có ký hiệu VDSL
- Máy tính trong mỗi toà nhà sẽ được kết nối vào thiết bị VDSL (thông thường mỗi thiết bị VDSL có 04 cổng RJ45 cho phép kết nối được 4 máy tính) hoặc có thể kết nối

Hub/Switch có sẵn tại mỗi toà nhà vào thiết bị.

- Sau khi đấu nối như trên mạng LAN nội bộ của các toà nhà sẽ được kết nối với nhau với tốc độ khoảng 10 Mbps mà không phải cài thêm bất cứ phần mềm hay driver nào. Tốc độ mạng LAN hiện tại sẽ không phụ thuộc vào kết nối VDSL, nếu mạng LAN cũ của các toà nhà có tốc độ 10Mbps hay 10/100Mbps thì tốc độ này vẫn được giữ nguyên trong mạng LAN mới này.

Giải pháp thiết kế VDSL (phần tiếp theo)

2.2. Giải pháp thiết kế VDSL cho nhiều điểm

Trong trường hợp kết nối mạng cho 1 công ty với 4 toà nhà A,B,C,D chẳng hạn thì ta cần phải chọn một toà nhà làm trung tâm và phương án kết nối sẽ như sau:

- *Phương án 1:* Tại điểm trung tâm sẽ sử dụng một thiết bị Multiport Master VDSL (đa cổng VDSL với 12 cổng master) và nối với 3 điểm còn lại theo cách thức như đã nói ở phần 1. Tại các điểm không phải là trung tâm bắt buộc phải sử dụng thiết bị Slaver VDSL

- *Phương án 2:* Tại điểm trung tâm sẽ sử dụng 3 thiết bị Master VDSL đơn cổng kết nối với 3 thiết bị Slaver VDSL tại 3 điểm còn lại. Các thiết bị Master VDSL tại trung tâm bắt buộc phải được nối tầng với nhau để đảm bảo thông mạng.

Trường hợp cụ thể về khoảng cách khi kết nối:

Giả sử, sau khi chọn điểm B là trung tâm mạng mà khoảng cách kết nối từ điểm C tới điểm B lớn hơn 1.5 km (tức là lớn hơn khoảng cách cho phép của thiết bị) trong khi khoảng cách từ C tới D và từ D đến B nhỏ hơn 1.5 km thì ta có thể thực hiện kết nối từ C tới B thông qua D. Trước hết thiết lập kết nối VDSL giữa C - D và D - B đảm bảo được mạng thông giữa CD và DB sau đó đấu nối tầng thiết bị VDSL tại điểm D, khi đó mạng giữa 3 điểm B,C,D sẽ thông nhau.

PHẦN II

Mô hình kết nối mạng VDSL thứ 2

Trong phần trước chúng ta đã tìm hiểu cách kết nối mạng LAN sử dụng công nghệ VDSL và đường PSTN có sẵn. Vấn đề đặt ra ở trường hợp thứ 2 này là nếu tại các điểm có sẵn mạng điện thoại nội bộ hay muốn nối 1 điện thoại nội bộ từ chi nhánh tới trung tâm thì ta phải làm như thế nào. Phương án kết nối có thể được thuyết minh một cách đơn giản như sau:

- Mua một cặp thiết bị VDSL (01 M & 01 S), 02 thiết bị chống sét lan truyền qua đường điện thoại, 02 hộp đấu dây điện thoại

- Thực hiện các bước đấu nối như sau:

+ Tháo đầu dây gắn vào điện thoại để gắn vào cổng VDSL của thiết bị VDSL Slaver

+ Gắn điện thoại vào cổng Phone của của thiết bị VDSL Slaver

+ Tháo đầu dây gắn vào tổng đài để gắn sang cổng VDSL trên thiết bị Master VDSL

+ Đầu ra của tổng đài được gắn tới cổng Phone của thiết bị VDSL Master

- Đấu nối máy tính vào thiết bị VDSL hoặc đấu nối tầng với Hub/sw có sẵn

- Sau khi đấu nối như trên hai mạng LAN (một tại trung tâm và một tại điểm của 01 máy điện

thoại lẻ trong hệ thống tổng đài nội bộ) sẽ kết nối được với nhau tốc độ khoảng 10MBps mà không cần phải cài đặt thêm phần mềm hay driver nào cả (tốc độ trong mỗi mạng LAN không bị phụ thuộc vào kết nối VDSL, nếu mạng LAN cũ có tốc độ 10MBps hay 10/100MBps thì tốc độ này vẫn được giữ nguyên trong nội bộ mạng LAN này), hệ thống này không ảnh hưởng đến việc gọi điện thoại của tất cả các máy điện thoại trong toàn bộ hệ thống mạng điện thoại tổng đài nội bộ cũng như kết nối ra bên ngoài do mạng điện thoại thông thường sử dụng phổ tần số 0~4KHz còn VDSL sử dụng dải phổ tần số từ 25KHz đến 30MHz.

Giải pháp VDSL cho kết nối nhiều điểm:

-Trong trường hợp kết nối nhiều điểm, thì điểm đặt tổng đài điện thoại là điểm trung tâm. Lúc

này có 02 phương án kết nối:

o Tại điểm trung tâm này sẽ sử dụng 01 thiết bị Multiport Master VDSL (đa cổng Master

VDSL gồm 12 cổng master VDSL) và nối với các điểm còn lại cũng theo cách thức như trên, tại các điểm không phải là trung tâm bắt buộc phải sử dụng thiết bị Slave VDSL. Thiết bị Master VDSL đa cổng có 04 cổng mạng 10/100Mbps nên có thể kết nối trực tiếp 04 máy tính vào thiết bị này hoặc nối tầng thiết bị với HUB hoặc Switch tại trung tâm để mở rộng mạng, tại các điểm dùng thiết bị Slave VDSL cũng có thể kết nối trực tiếp máy tính vào cổng mạng 10/100Mbps của thiết bị hoặc đấu nối tầng với HUB

hoặc Switch để mở rộng mạng.

o Tại điểm trung tâm sẽ sử dụng các thiết bị Master VDSL đơn cổng nối với các thiết bị Slave VDSL ở các điểm còn lại. Các thiết bị Master VDSL tại trung tâm bắt buộc phải nối tầng với nhau để kết nối toàn bộ mạng.

-Việc đấu nối cáp tương tự như đã trình bày ở phần trên cho từng cặp, việc lựa chọn phương án sử dụng Multiport Master VDSL hay nhiều Master VDSL đơn cổng tại trung tâm là tùy theo kinh phí và các yêu cầu mở rộng của hệ thống.

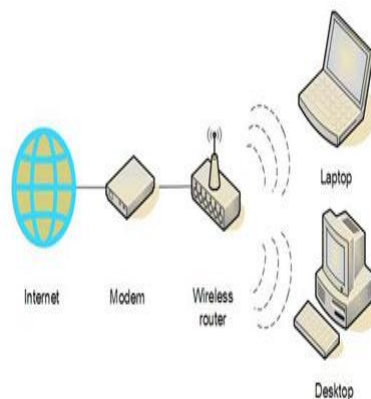
- Việc đấu nối cho nhiều điểm cũng hoàn toàn không ảnh hưởng đến các tính năng của hệ thống tổng đài nội bộ.

- Trong trường hợp hệ thống tổng đài nội bộ đã có hệ thống chống sét thì nên khảo sát cụ thể để đưa ra phương án chống sét cho cả hai hệ thống, trong trường hợp chưa có cần xây dựng như trong hình vẽ minh họa dưới đây.

Bạn có thể thiết kế cho mình mạng không dây đơn giản, để chia sẻ truy cập Internet, tập tin, máy in... Bạn có thể lướt Net trong khi bạn đang trong sân, hay ngoài vườn... Để thiết lập một mạng máy tính không dây khá đơn giản, bạn chỉ cần thực hiện qua 4 bước sau:

1. Lựa chọn thiết bị:
2. Kết nối các router không dây
3. Thiết lập cấu hình router không dây
4. kết nối các máy tính

Đối với người sử dụng Windows XP, bản Windows XP SP2 cho phép thiết lập mạng dễ dàng hơn, không những thế bản SP2 còn giúp bạn chống lại hacker, sâu, và những kẻ xâm nhập mạng không dây.



Mô hình mạng không dây cho gia đình

Bước 1: Lựa chọn thiết bị không dây

Trước hết, bạn cần phải có các thiết bị phát sóng không dây. Nếu bạn đang tìm kiếm các sản phẩm trong các cửa hàng, hoặc trên Internet, bạn cần chú ý tới các thiết bị hỗ trợ 3 công nghệ không dây phổ biến hiện nay: 802.11a, 802.11b, 802.11g. Tuy nhiên, chuẩn 802.11g được khuyến khích sử dụng bởi nó cho phép đem lại hiệu năng cao nhất và tương thích với hầu hết các sản phẩm khác.

Các thiết bị cần mua gồm:

- Kết nối Internet băng thông rộng
- Router không dây
- Các máy tính đã tích hợp các thiết bị kết nối không dây, hoặc bạn phải mua thêm các card mạng không dây.

Router không dây

Router chuyển đổi các tín hiệu đến từ kết nối Internet thành các kết nối không dây broadcast, tương tự như trạm phát sóng của thiết bị điện thoại không dây. Bạn cũng chú ý là phải mua router không dây, chứ không phải là các điểm truy cập không dây (*wireless access point*).

Các card mạng không dây

Card mạng không dây kết nối máy tính của bạn tới các router không dây. Nếu bạn có laptop mới, rất có thể máy tính của bạn đã có sẵn card mạng không dây tích hợp. Trong trường hợp khác, bạn cần phải mua card mạng không dây. Nếu bạn cần mua card mạng không dây cho máy để bàn, bạn nên mua loại USB. Nếu bạn đang sử dụng máy tính xách tay, bạn hãy mua loại PC card.

Chú ý: Để tạo kết nối dễ dàng, bạn cần chọn card mạng không dây cùng với hãng sản xuất router không dây. Ví dụ: Bạn sẽ thấy router của Linksys có giá tốt, bạn sẽ chọn luôn card mạng của Linksys. Để mua sắm được dễ dàng hơn bạn nên mua cả bộ từ D-Link, Netgear, Linksys, Microsoft,..Nếu bạn sử dụng máy tính để bàn thì bạn phải chắc chắn là mình đã có sẵn cổng USB. Nếu không có cổng USB thì bạn phải mua thêm card cắm thêm cổng USB.

Bước 2. Kết nối tới router không dây

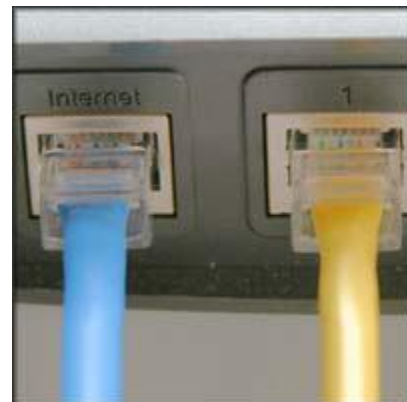
Bạn nên tạm ngắt kết nối vào Internet. Trước hết, cần phải xác định bạn đang sử dụng modem cáp hoặc DSL modem, rồi rút phích cắm điện ra (hoặc tắt nguồn điện).

Sau đó, bạn kết nối router không dây của bạn vào modem. Modem của bạn phải chắc chắn sẽ làm việc tốt (vẫn truy cập được vào Internet). Sau đó, khi mọi thứ đã hoàn thành, máy tính của bạn sẽ kết nối không dây tới router, và router sẽ kết nối Internet qua modem.

Sau đây là bước kết nối router tới modem:

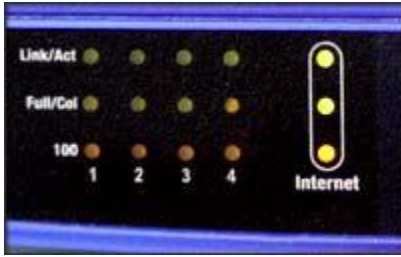
Chú ý: Các hướng dẫn bên dưới được sử dụng cho router Linksys. Nếu bạn sử dụng loại modem khác thì bạn hãy đọc kĩ tài liệu hướng dẫn đi kèm với thiết bị của bạn.

- **Nếu bạn đang có máy tính kết nối trực tiếp vào modem:** bạn cần phải bỏ đầu cắm cáp mạng đằng sau máy tính của bạn, và cắm nó vào cổng có nhãn là Internet, WAN, hoặc WLAN ở đằng sau router không dây của bạn.
- **Nếu bạn không có máy tính đang kết nối vào internet:** Hãy cắm một đầu cắm cáp mạng vào trong modem, và đầu cắm mạng còn lại thì kết nối vào cổng Internet, WAN, hoặc WLAN ở trong router không dây.
- **Nếu bạn có máy tính đang được kết nối tới router:** Bạn hãy gỡ bỏ đầu kết nối mạng ở cổng Internet, WAN, hoặc WLAN trong router cũ, và cắm đầu cắm này vào cổng Internet, WAN, hoặc WLAN của router mới. Và sau đó, đưa



Các cổng của Router không dây

tất cả các đầu cắm cáp mạng từ các cổng của router cũ sang cổng kết nối của router mới. Bạn sẽ không cần router cũ nữa bởi router mới sẽ thay thế công việc.



Đèn tín hiệu cổng Internet

Tiếp đó, sau khi đã kết nối vật lý xong, bạn hãy bật modem cáp hoặc DSL modem của bạn. Đợi vài phút để thiết bị có thời gian kết nối Internet, và sau đó bạn hãy mở router không dây lên. Một vài phút sau đèn ở phần Internet, WAN, or WLAN ở trong router không dây sẽ sáng, điều đó chứng tỏ bạn đã kết nối thành công.

Bước 3: Cấu hình router không dây

Hãy sử dụng một cáp mạng đi kèm với router không dây của bạn, bạn cần tạm kết nối máy tính của mình tới một trong những cổng còn trống của router không dây (bất cứ cổng nào mà không có nhãn Internet, WAN, hoặc WLAN). Bạn hãy bật máy của mình, PC của bạn sẽ tự động kết nối vào router.

Bạn hãy mở IE, và gõ địa chỉ IP để cấu hình router. Có thể bạn sẽ phải gõ mật khẩu. Tên mật khẩu và địa chỉ sẽ rất khác nhau, phụ thuộc vào router mà bạn mua, bạn cần xem hướng dẫn trong tài liệu đi kèm. Bảng dưới đây là một cấu hình các địa chỉ, tên mật khẩu thường được sử dụng mặc định của hãng sản xuất.

Router	Address	Username	Password
3Com	http://192.168.1.1	admin	admin
D-Link	http://192.168.0.1	admin	
Linksys	http://192.168.1.1	admin	admin
Microsoft Broadband	http://192.168.2.1	admin	admin
Netgear	http://192.168.0.1	admin	password

IE sẽ hiển thị trang cấu hình router của bạn. Hầu hết các cấu hình mặc định đều tốt, tuy nhiên bạn cần chú ý:

- **Tên mạng không dây của bạn, thường gọi là SSID:** Cái tên này xác định mạng của bạn. Do đó, bạn cần phải đặt tên khác và không giống như cái tên mà hàng xóm của bạn đang sử dụng.
- **Mã hóa không dây WEP, và bảo vệ truy cập không dây (WPA):** sẽ giúp mạng không dây của bạn bảo mật hơn. Hầu hết các router, bạn cần cung cấp vì kí tự để router của bạn tự sinh các khóa. Bạn hãy gõ các kí tự này duy nhất đừng lặp lại (bạn cũng không cần phải nhớ các kí tự này). Sau đó bạn hãy ghi lại các khóa mà router tự sinh.
- **Mật khẩu quản trị, chia khóa cấu hình mạng không dây:** Cũng giống như các mật khẩu khác, mật khẩu cho router không thể là một từ nào đó trong từ điển, nó cần phải là sự kết hợp các kí tự, số, biểu tượng, nhưng cũng rất quan trọng là bạn phải nhớ chúng, bởi bạn sẽ phải gõ mật khẩu khi đăng nhập để cấu hình lại router.

Các bước cấu hình có thể rất khác giữa các router, nhưng bao giờ trong mỗi lần thiết lập cấu hình cũng là có các mục như: **Save Settings**, **Apply**, và **OK** để lưu lại các thay đổi của bạn. Bây giờ, bạn có thể tắt kết nối mạng từ máy bạn đang dùng để cấu hình.

Bước 4: Kết nối các máy tính

Nếu máy tính của bạn không tích hợp card mạng không dây, bạn hãy cắm thiết bị kết nối mạng không dây vào cổng USB, và hãy đưa anten lên vị trí cao nhất (đặt lên đỉnh của case của máy tính để bàn), hoặc bạn cắm card PC không dây vào khe cắm (máy tính xách tay). Windows XP sẽ tự động nhận các nhận card mạng mới, và có thể sẽ yêu cầu bạn cài đặt phần mềm. Bạn hãy đưa đĩa cài đặt trình điều khiển (driver) cho card mạng khi có yêu cầu. Màn hình hướng dẫn cài đặt sẽ giúp bạn cài đặt trình điều khiển trong vòng vài phút.

Chú ý: Các bước dưới đây cũng sử dụng Windows XP SP2. Nếu bạn sử dụng Windows XP mà chưa có SP2 thì bạn hãy cài đặt bản SP 2 tại <http://www.microsoft.com/windowsxp/sp2/default.mspx>. Windows XP sẽ hiển thị một hộp thoại thông báo đã nhận được mạng không dây.

Để kết nối vào mạng không dây bạn cần làm theo các bước:

- Nhấn chuột phải vào biểu tượng mạng không dây ở góc dưới bên phải màn hình, và nhấn chuột vào **View Available Wireless Networks**. Nếu bạn gặp rắc rối, hãy tham khảo tài liệu đi kèm card mạng. Đừng ngại liên hệ với nhà cung cấp về kỹ thuật nếu bạn gặp khó khăn.
- Cửa sổ kết nối mạng không dây sẽ xuất hiện và bạn sẽ thấy mạng không dây sẽ xuất hiện với tên mà bạn chọn. Nếu bạn không thấy mạng, hãy nhấn **Refresh network list** vào ở trên cùng bên trái. Bạn hãy nhấn vào mạng của bạn, và nhấn vào nút **Connect**.
- Windows XP sẽ đưa ra lời nhắc bạn nhập khóa. Bạn hãy gõ khóa đã được mã hóa mà bạn đã viết lúc trước trong cả hai trường **Network key** và **Confirm network key**, sau đó nhấn **Connect**.



Chú ý: cửa sổ **Wireless Network Connection** vẫn tiếp tục hiện ra **Acquiring Network Address**, có thể là bạn đã gõ nhầm khóa mã hóa.

Windows XP sẽ hiển thị quá trình kết nối vào mạng. Sau khi bạn đã kết vào mạng, bạn có thể đóng cửa sổ Wireless Network Connection.



Kết nối vào mạng không dây thành công

Thiết Lập Mạng Wifi Chia Sẻ Lan Và Internet Không Cần Access Point

Tình huống là hai máy tính muốn chia sẻ file và internet với nhau còn trường hợp chỉ chia sẻ file không thì sẽ nói ở phần sau.

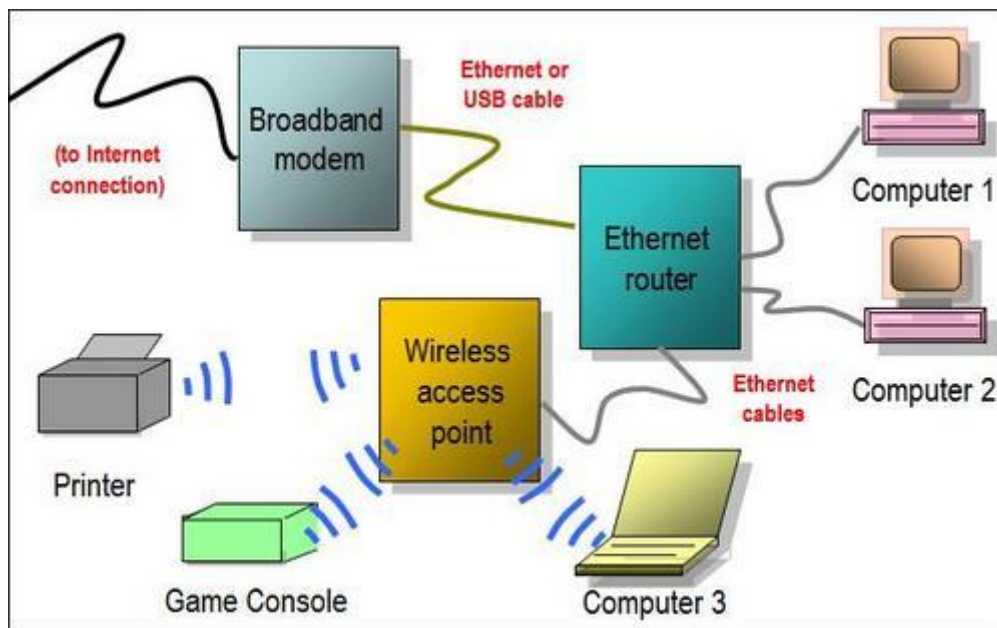
Trước hết cũng nên giới thiệu qua về công nghệ đang rất phổ biến này chứ nhỉ:

WiFi hay Wireless Fidelity được ám chỉ như là công nghệ Lan không dây được phát triển dựa trên chuẩn IEEE 802.11a/b/g. (Bluetooth thì hơi khác à nha, nó sử dụng tần số radio thấp hơn WiFi và dựa trên chuẩn IEEE 802.15.1).

Mạng Lan không dây là lựa chọn của bạn nếu:

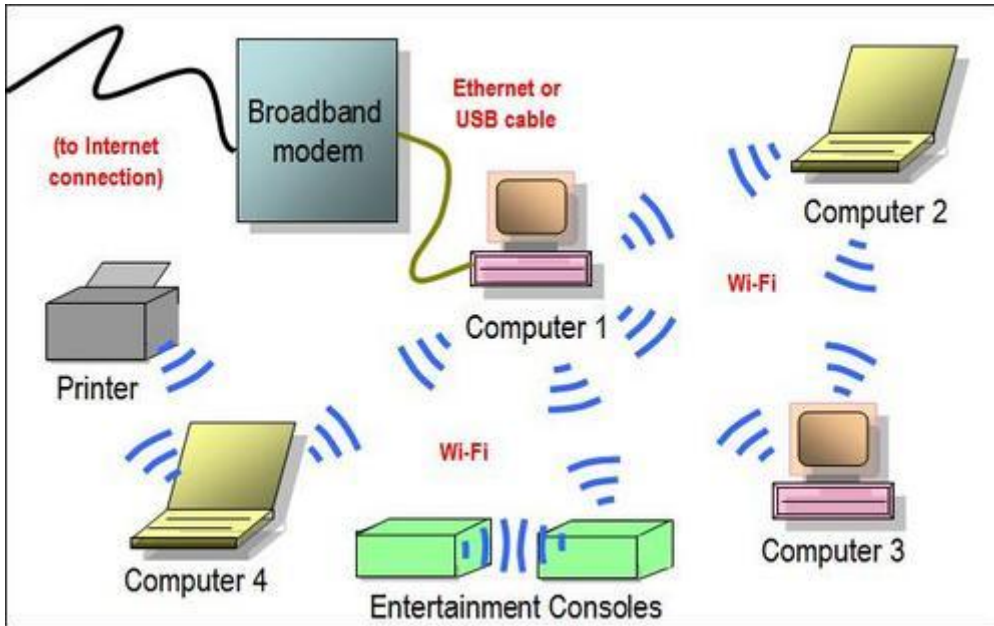
- Bạn muốn di chuyển đến bất cứ đâu trong nhà bạn với chiếc laptop thân yêu mà vẫn kết nối được lan và net (vd; như tui ôm máy PPC vào WC để chat nè)
- Bạn không muốn thêm bất cứ dây dợ lằng nhằng đi lòng vòng trong nhà bạn (đặc biệt là khi nhà bạn có nhiều máy).

Để tạo một mạng không dây ở nhà, phổ biến nhất là dùng một WiFi access point. Một access point đóng vai trò như là một cái Hub hoặc switch như trong một mạng Lan có dây – điểm kết nối trung tâm - kết nối các thiết bị máy tính (pocket pc, laptop, desktop) với nhau hoặc kết nối mạng không dây với mạng có dây hay kết nối với Internet.



Đây là hình minh họa mạng WIFI với access point. Hiện giờ phổ biến loại router kiêm access point với 4 cổng LAN (như Linksys W.. tầm 70\$ thì phải)

Mặt khác, một mạng không dây trong đó máy tính liên kết trực tiếp với nhau không thông qua Access point được gọi là Ad-hoc network.



Mạng WiFi không cần Access point

Và giờ mới là vấn đề chính của chúng ta đó là tạo một mạng Lan Ad hoc để chia sẻ file và kết nối Internet giữa các máy tính trong nhà :

Trước tiên bạn phải chuẩn bị trước;

- Kiểm tra xem chuẩn của card WIFI: card chuẩn a chỉ chơi với chuẩn a, còn card chuẩn b thì chơi được cả b lẫn g (lưu ý card chuẩn b chỉ hỗ trợ đến 11Mbps còn chuẩn g là 54 Mbps)

- Gắn card vào mỗi máy và cài driver (trường hợp nếu bạn chưa làm)

- Xác định mức độ bảo mật cho mạng : ko mã hóa, WEP hoặc WPA. (Lưu ý bạn chỉ có thể dung WPA nếu cả 2 card hỗ trợ nó)

- Đặt máy của bạn trong phạm vi sóng. Thông thường là 50 mét trong nhà. Đọc thêm tài liệu đi kèm card của bạn để biết chi tiết.

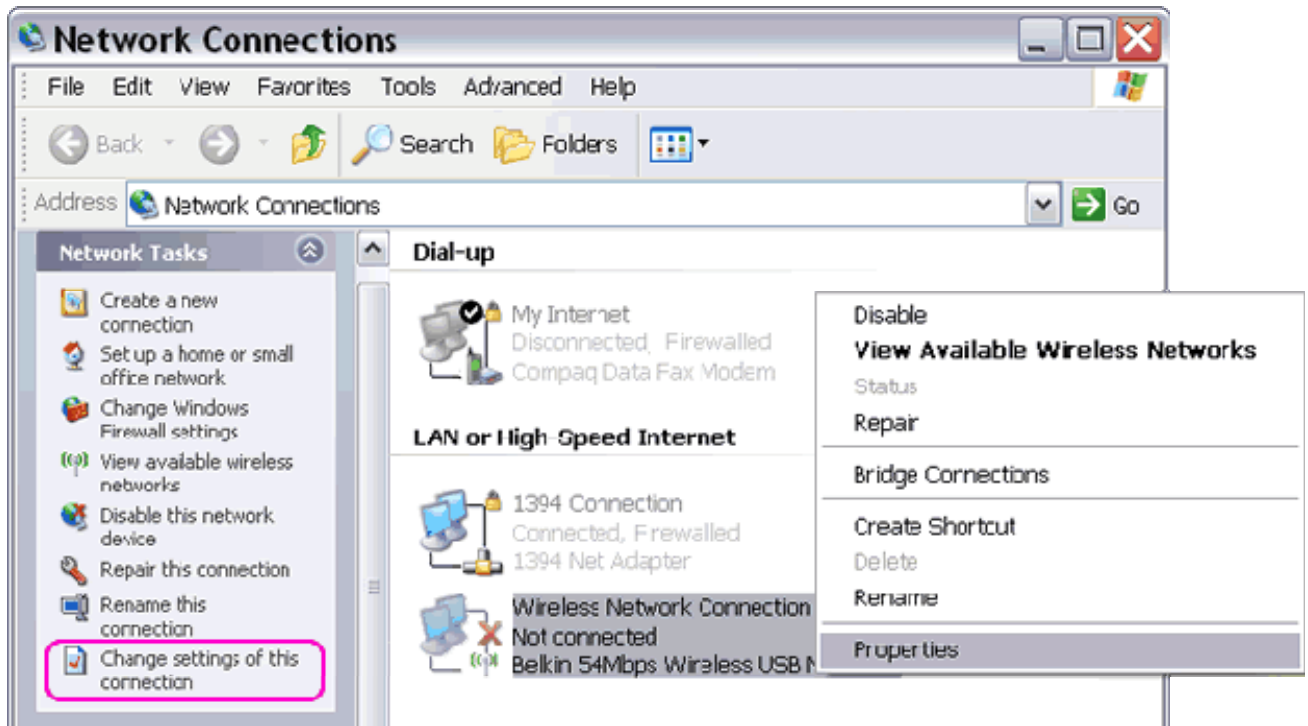
- Để sóng được truyền tốt nhất, bạn nên tránh đặt máy gần những vật chắn kim loại hoặc những nguồn gây nhiễu như lò vi sóng, những thiết bị Bluetooth đang hoạt động, điện thoại mẹ bông con...

- Bạn phải chắc chắn rằng cả hai card WIFI phải hỗ trợ chế độ ad hoc và Windows XP Wireless Zero Configuration (WZC) service. Nếu WZC không được hỗ trợ thì bạn phải dung chương trình đi cùng với card của bạn để tạo mạng ad-hoc.

- Để cho phép chia sẻ file bạn phải đặt tên duy nhất cho mỗi máy và đặt chung cùng work group. Để làm điều này bạn click chuột phải vào My computer icon, chọn Properties rồi đi đến System Properties. Trên Computer name tab, click Change. Sau đó restart máy nha.

I. Cài đặt mạng Adhoc trên máy tính thứ nhất:

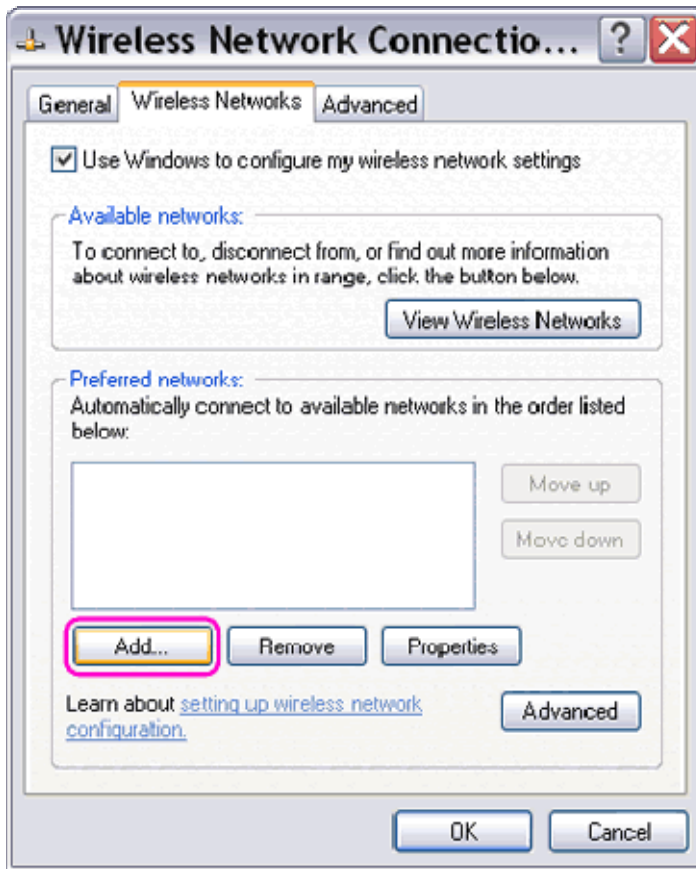
1. Đi đến Control Panel và mở Network Connection folder. Nếu bạn đã nhét card wifi và cài driver cho nó, bạn phải tìm biểu tượng Wireless Network Connection dưới Lan or High-Speed Internet Connection



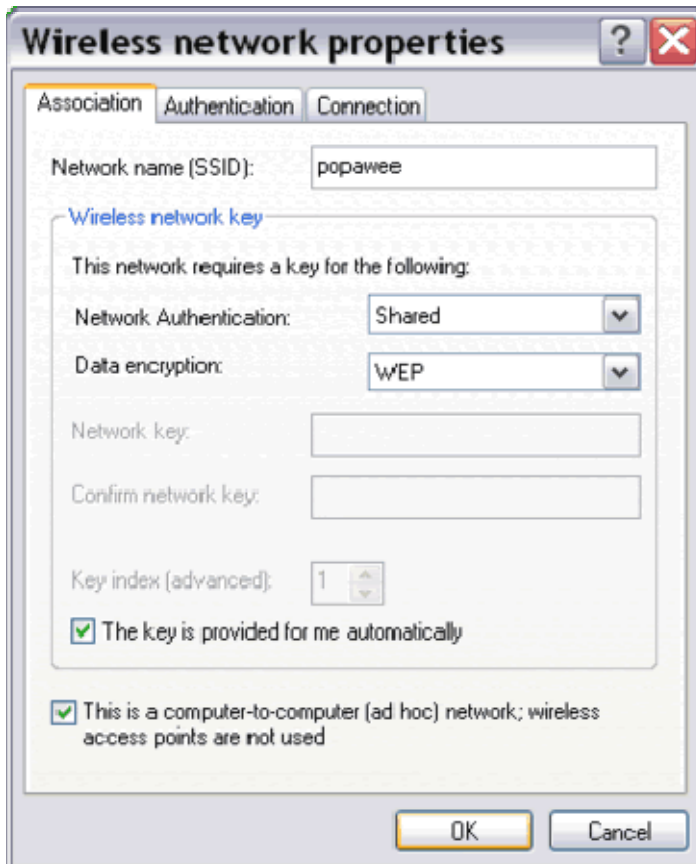
2. Click phải chuột vào Wireless Network Connection và chọn Properties để mở ra cửa sổ Wireless Network Connection Properties.

3. Ở tab Wireless Networks của cửa sổ Wireless Network Connection Properties, chọn Add dưới Preferred networks.

Lưu ý tab Wireless Network chỉ xuất hiện nếu card bạn hỗ trợ Windows XP Wireless Zero Configuration (WZC) service

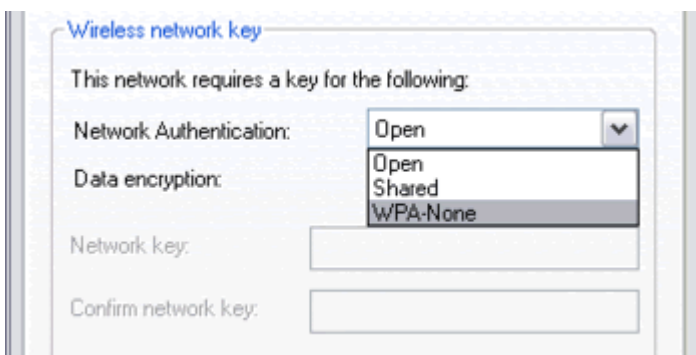


4. Trên tab Association gõ bất kì tên mạng ad-hoc trong Network name (SSID)



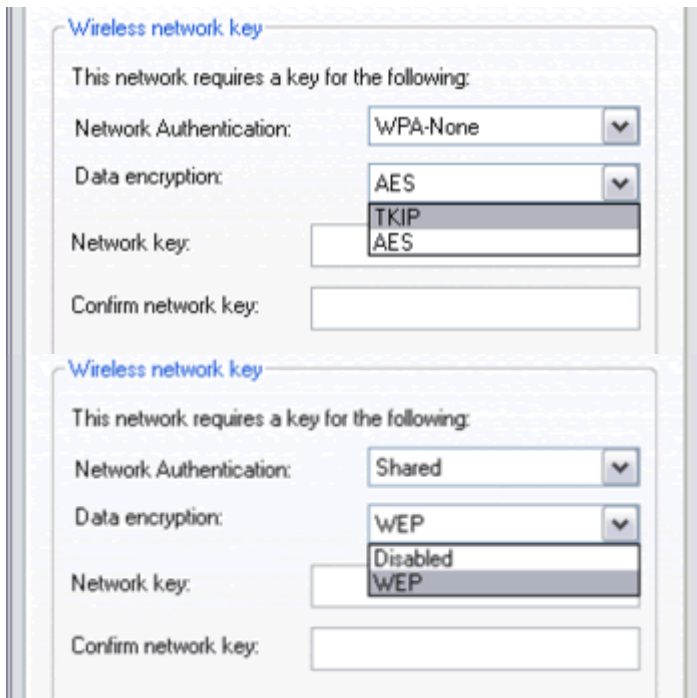
5. Chọn "This is a computer-to-computer (ad hoc) network" và xóa "The key is provided for me automatically" nếu bạn muốn đặt network key một cách thủ công.

6. Trong mục Network Authentication chọn Open hoặc Share hoặc WPA-None. Trong mạng có access point ta có thêm lựa chọn WPA-PSK và WPA. Trong win XP SP1 bạn chỉ có thể tìm thấy Open hoặc Shared, trừ khi là bạn đã cài thêm bản update cho WPA



7. Trong Data encryption chọn chế độ bảo mật thích hợp với bạn.

Nếu bạn chọn Open hoặc Shared trong Network Authentication bạn sẽ tìm thấy Disabled and WEP in Data encryption. Chọn WEP nếu bạn muốn dữ liệu được mã hóa khi truyền thích hợp với mạng nhỏ và gia đình. Nếu chọn WPA-None in Network Authentication, bạn sẽ thấy TKIP and AES trong Data encryption. Cả hai cái này đều là mức độ mã hóa mạnh nhất

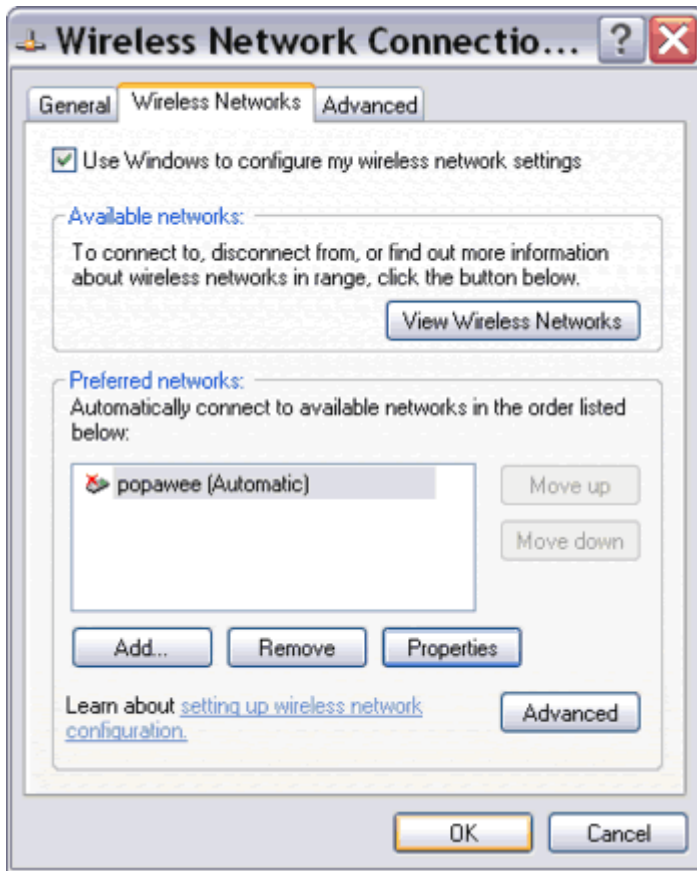


8. Trong Network key gõ chìa khóa bảo mật vô dùng ASCII hoặc kí tự hexadecimal..
Kí tự ASCII có thể chứa chữ cái, số hoặc biểu tượng trong khi hexa chỉ chứa số từ 0-9 và chữ từ A đến F.
Lưu ý: nếu bạn chọn chế độ bảo mật WEP, chìa khóa sẽ phải là 5 kí tự ASCII hoặc 10 kí tự hexa cho mức bảo mật 64 bit và 13 ASCII hoặc 26 hexa cho mức bảo mật 128 bit.
Vd: 12345 (5 kí tự ASCII) hoặc ABC123EF45 (10 kí tự hexa) cho mức mã hóa 64 bit.

9. Trong Confirm network key gõ lại chìa khóa

10. Click OK trong cửa sổ Wireless network properties để lưu lại thay đổi.

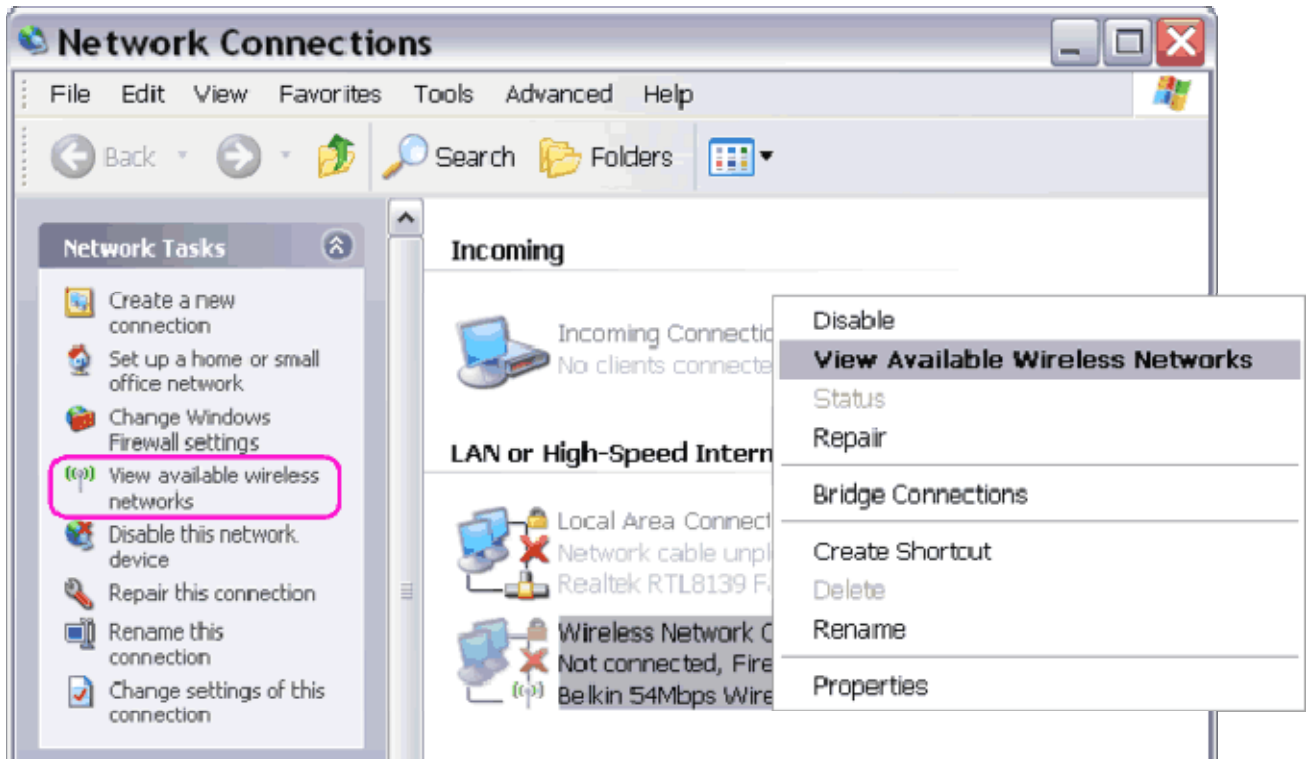
11. Click OK trong cửa sổ Wireless Network Connection properties để lưu lại những thay đổi.



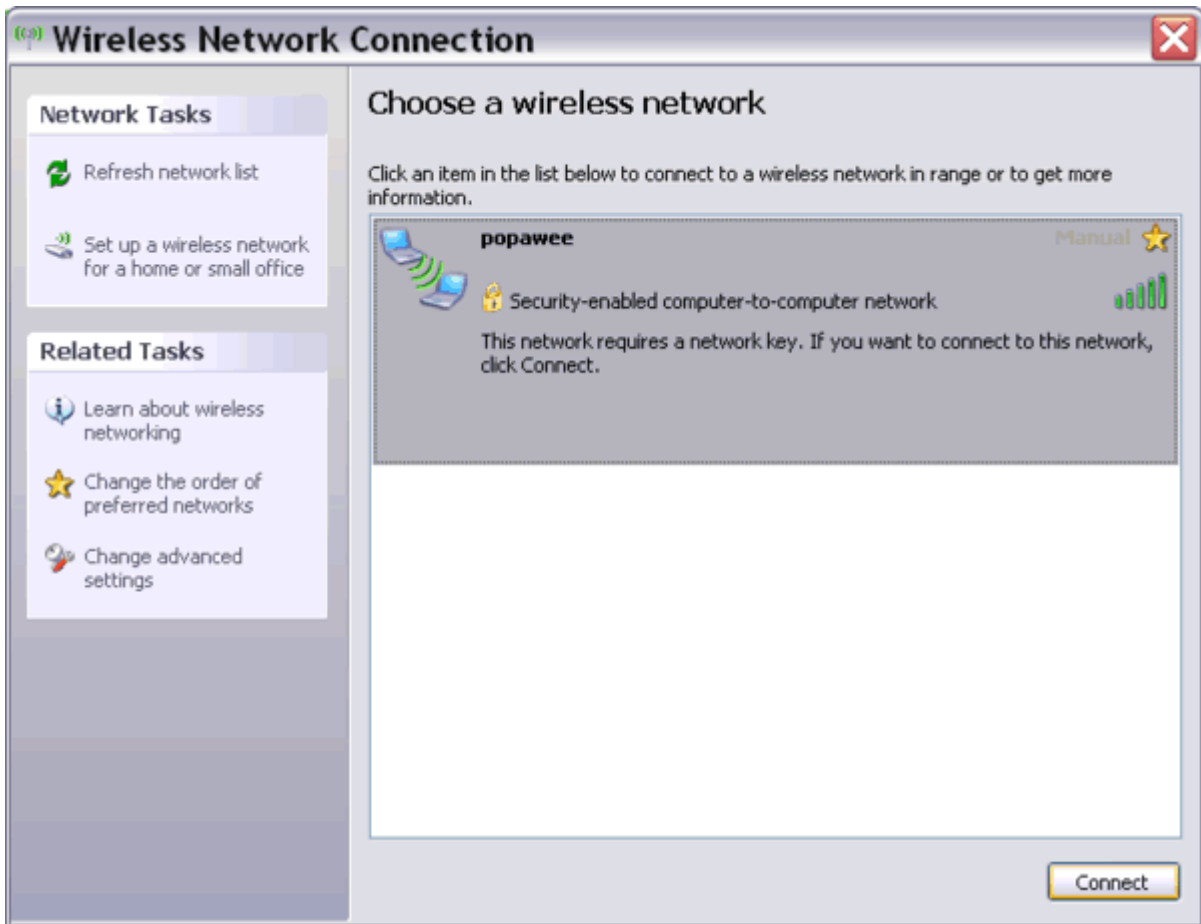
II. Cài đặt mạng Ad-hoc trên máy thứ 2:

1. Mở Network Connections folder.

2. Tìm Wireless Network Connection icon and chọn "View Available Wireless Networks".



3. Cửa sổ Wireless Network Connection sẽ chỉ ra danh sách các mạng không dây được tìm thấy trong phạm vi phủ sóng

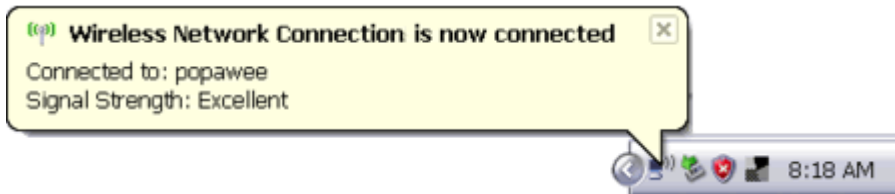


4. Chọn tên mạng vừa tạo và ấn CONECT.

5. Gõ “CHÌA KHÓA” như trên máy 1 khi một thông báo hiện ra và chọn Connect. Nếu bạn không chọn "The key is provided for me automatically" trong phần setup ở máy 1 thì hãy để trống phần network key và ấn Connect.



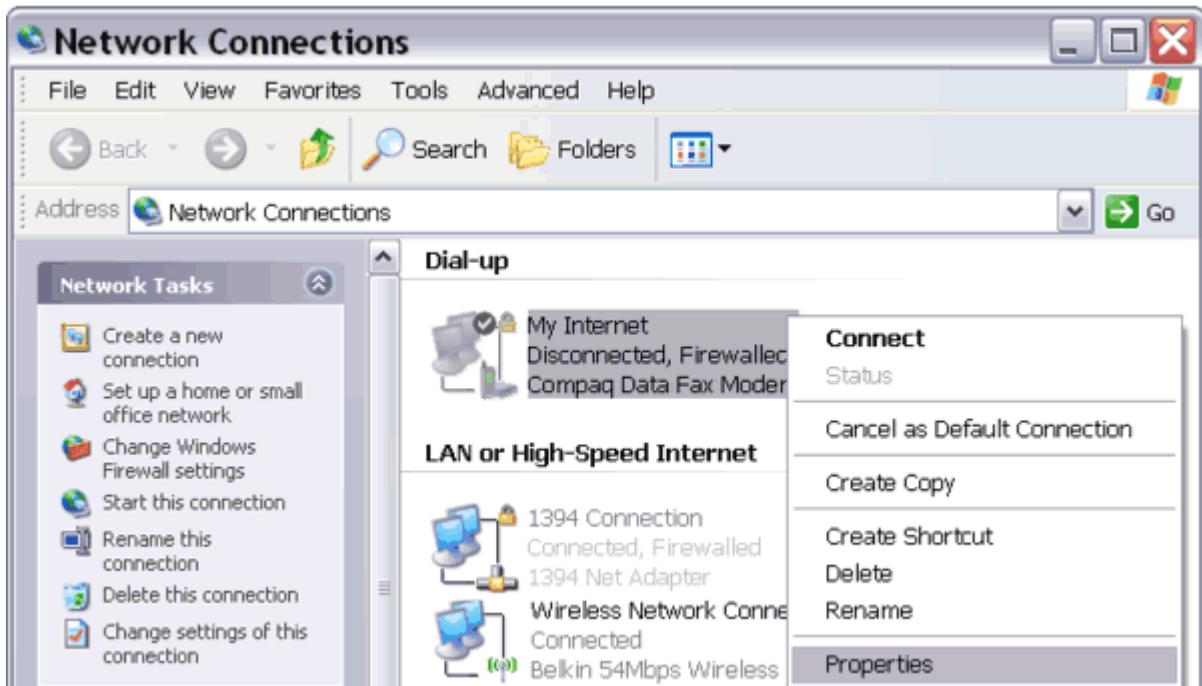
Bây giờ mạng WI-FI adhoc giữa hai máy đã được kết nối:



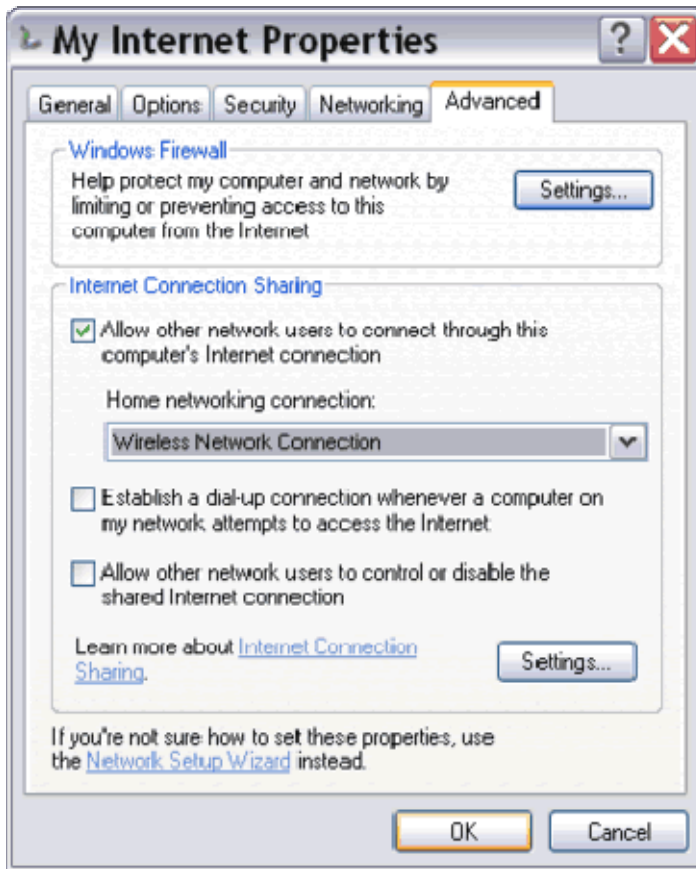
CHIA SẺ KẾT NỐI INTERNET:

Trên máy kết nối trực tiếp với Internet

1. Mở thư mục Network Connections .
2. Tìm kết nối Internet bạn muốn chia sẻ. Click chuột phải lên kết nối đó và chọn Properties.



3. Trong tab Advanced , chọn "Allow other network users to connect through this computer's Internet connection" và chọn "Wireless Network Connection" từ hộp thả xuống.



4. Sau đó bấm vào Setting.

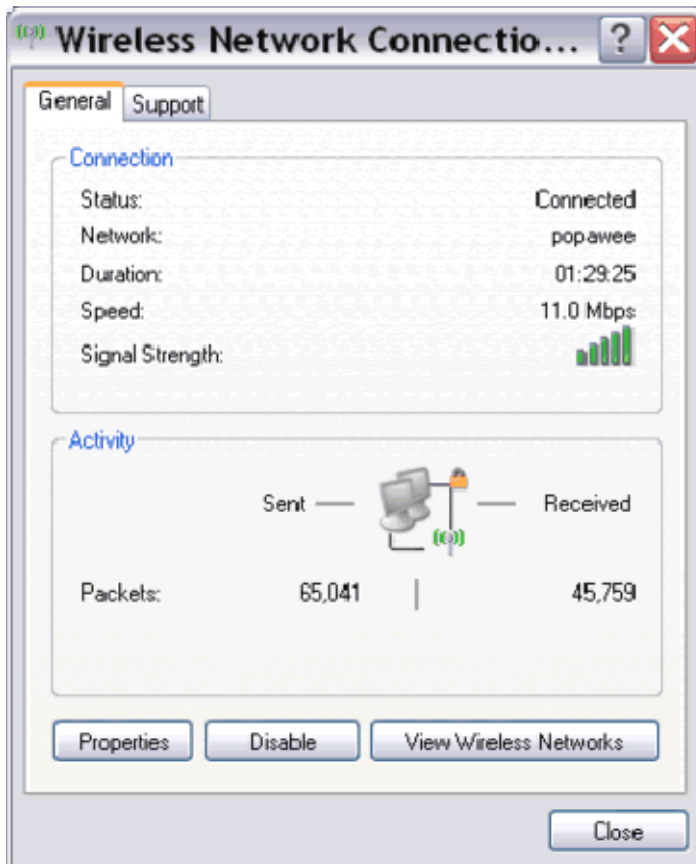
5. Tích chọn các dịch vụ cần thiết, như DHCP, DNS....

6. Bấm OK, sau đó máy sẽ thông báo là đổi địa chỉ IP của Wireless thành 192.168.0.1 cứ để mặc định.

7. Trong phần IP của card wifi máy kia để động

8. Chọn repair ở wireless connection để hai máy nhận lại nhau.

Bây giờ bạn đã kết thúc quá trình tạo mạng WIFI adhoc và thiết lập chia sẻ Internet cho 2 máy. Để truy cập tài nguyên máy khác bạn phải thiết lập network sharing cho từng tài nguyên.



Trường hợp chỉ chia sẻ file giữa 2 máy không thôi thì bạn đặt IP tĩnh cho cả hai WIFI connection ở cả hai máy, không được đặt IP trùng nhau nha

Vd :

Máy 1: IP : 192.168.0.1

Subnet Mask : 255.255.255.0

Máy 2:IP: 192.168.0.2

Subnet Mask : 255.255.255.0

Rồi bật tắt lại Wifi cho 2 máy nhận lại nhau.

Thiết lập một mạng không dây trong Windows XP

Đây là một hướng thiết lập mạng không dây (hay được gọi là Wifi) trong windows XP. Hãy cùng theo dõi bài dưới đây để được hướng dẫn cụ thể nhé!



Thiết lập router mới.

Bước 1:

Lưu ý rằng nếu mua một bộ router, tất cả các router đều tương thích với Windows XP. Đây là bộ adapter không dây có tính tương thích khác nhau đối với Windows XP. Nếu router của bạn không phải là mới, hãy bật và để chế độ "**Detecting your wireless adapter**".

Bước 2:

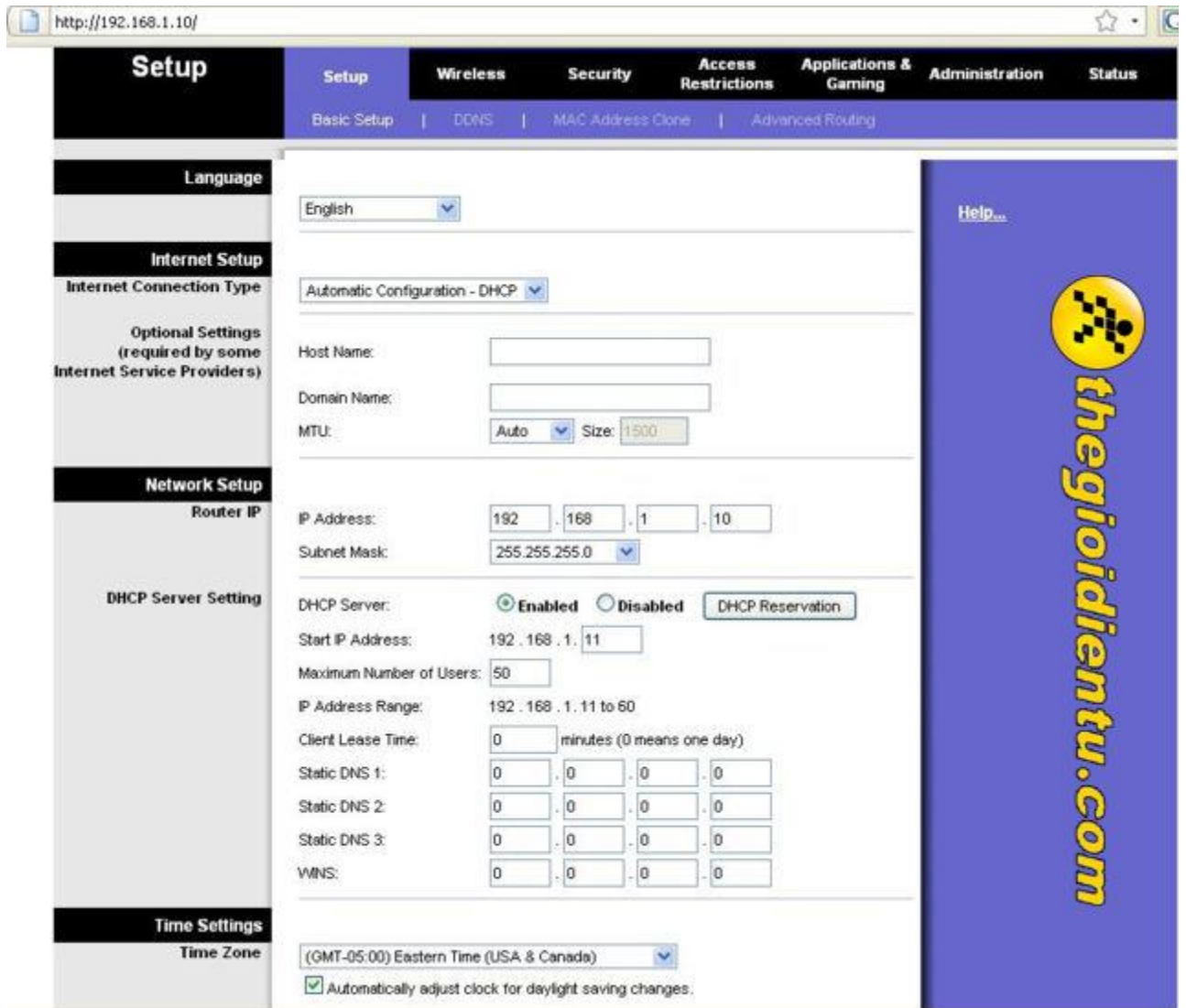
Cắm ổ router của bạn vào ổ cắm internet của bạn nếu bạn muốn chia sẻ internet.

Bước 3:

Cắm ổ router vào máy tính với cáp Ethernet.

Bước 4:

Gõ vào trình duyệt của bạn địa chỉ "**192 .168.0.1**" hoặc bất cứ địa chỉ của máy chủ web router.



Bước 5: Nhập tên người dùng và mật khẩu (thường là "admin" và "admin")

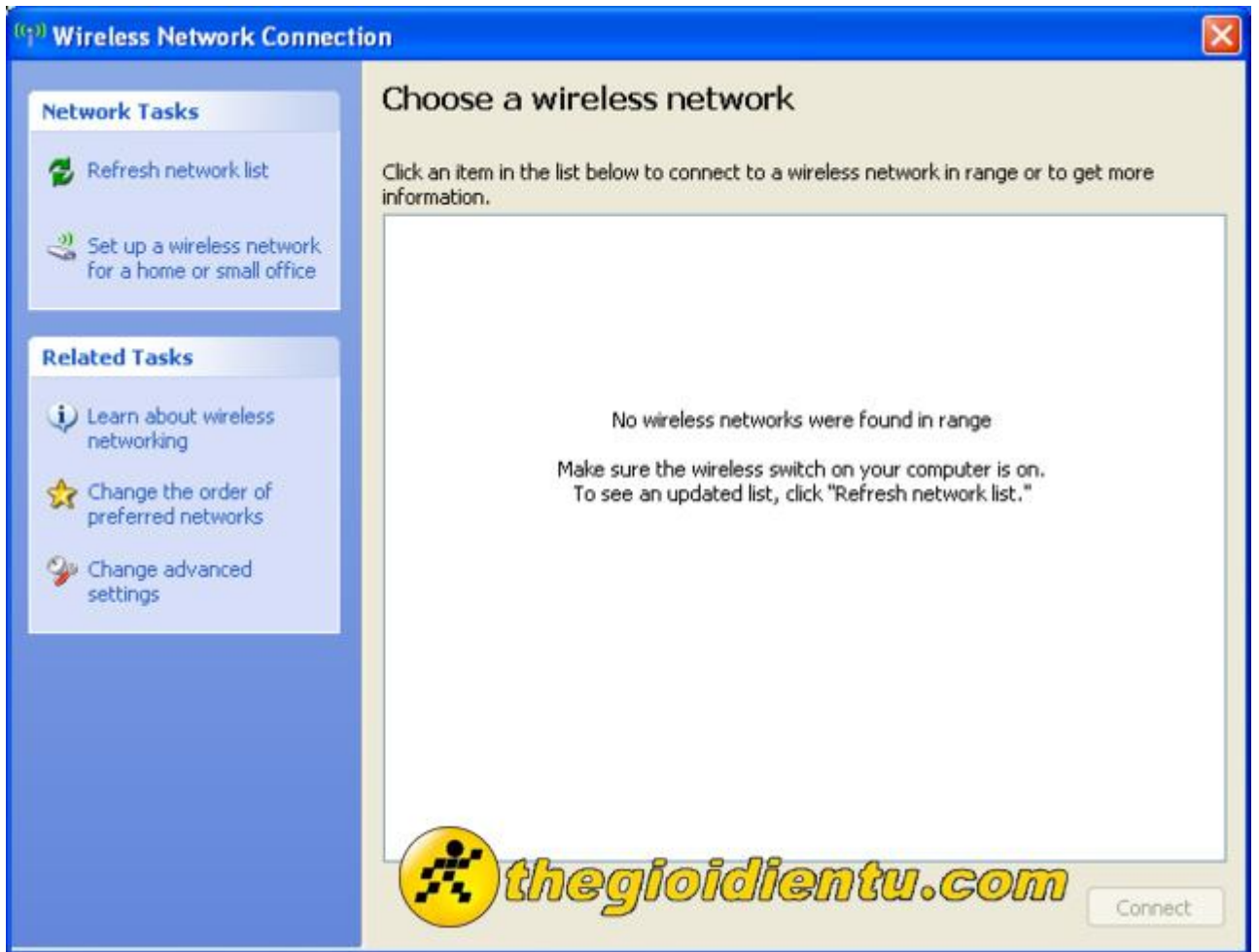
Bước 6: Kích hoạt mạng không dây và để chế độ (WEP hoặc WPA) và gõ vào mật khẩu mạng.

Kiểm tra adapter không dây của bạn

- Adapter không dây của bạn được phát hiện tự động bởi Windows XP.
- Kiểm tra Device Manager.

Kết nối vào mạng

Bước 1: Nếu kết nối của bạn xuất hiện trong **Wireless Connection Manage**, hãy kết nối với nó.




Bước 2:Chạy Wireless Network Setup Wizard.




Bước 3: Cung cấp một cái tên SSID nếu bạn muốn



Bước 4: Chọn cách thức mã hóa (WEP hoặc WPA) và nhập vào.

Wireless Network Setup Wizard 

Enter a WEP key for your wireless network. 

The WEP (or Wired Equivalent Privacy) key must meet one of the following guidelines:

- Exactly 5 or 13 characters
- Exactly 10 or 26 characters using 0-9 and A-F


A longer WEP key is more secure than a short one.

Network key: (0 characters)

Confirm network key: (0 characters)

Hide characters as I type

On the last page of this wizard, you can print this key and your other network settings for safekeeping.

 **thegioidientu.com**

Bước 5: Điều chỉnh một vài tùy chọn:



Bước 6: Kết nối.



 [thiết lập wifi, Windows XP](#)