

### Sharing High Speed Internet Access

Broadband or high-speed internet access is widely available from either cable or phone companies. It is relatively inexpensive and can readily be distributed to all users on a network. Although high-speed Internet access can help users work more efficiently its always "on" nature coupled with a fixed Internet Protocol (IP) address opens up your network to hackers. Cable/DSL (Digital Subscriber Line) Routers enable a high speed internet connection to be shared by all network users. They also provide an effective firewall which reduces the likelihood of a hacker breaking into your network .

Cable/DSL Routers are installed between the Cable or DSL Modem and a computer, hub or switch (see diagram in the left margin). The modem, which delivers high speed Internet access, connects via an RJ-45 cable to a port on the back of the router. Additional RJ-45 ports on the router allow 4 or more computers to interconnect utilizing the built in 10/100 Mbps switch and share the Internet connection. Alternately the router can be installed between the modem and a switch or hub allowing a greater number of users to share access. High speed Internet providers typically provide a single IP address to each subscriber. Cable/DSL Routers employ Network Address Translation (NAT) to enable multiple computers to share a single external Internet IP address. Additionally they utilize Dynamic Host Configuration Protocol (DHCP) to assign unique IP addresses to internal computers to enable them to access the Internet.

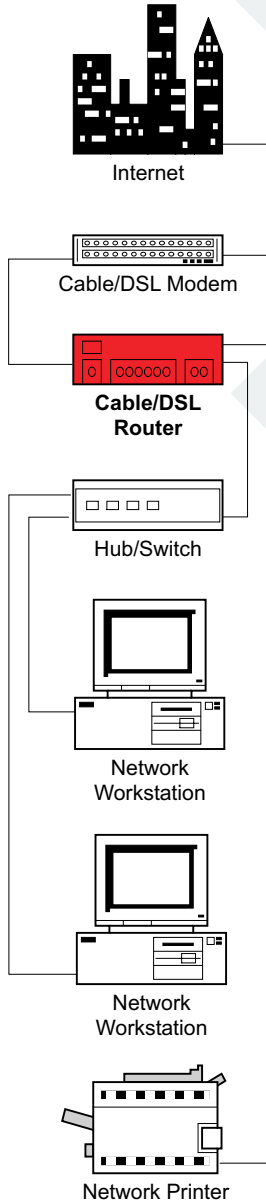
### Network Firewall Protection

Cable/DSL Routers also provide a firewall. Firewalls protect internal networks from hackers by utilizing some nifty tricks. In order for a hacker to gain access your network has to be visible on the Internet. Hackers look for IP addresses which respond to a "ping", basically a "Hello, are you there?". If they receive a response they know the address is in use and try to hack it to gain access. Firewalls intercept "pings" and don't respond making it appear that the IP address is unused. The firewall also monitors outgoing traffic and only allows incoming information to pass through if it is in response to an outgoing request. This simple rule greatly reduces the vulnerability of your network by blocking uninvited access to the network. Firewalls can be configured to open or close access ports enabling a high degree of control over the type of access allowed to your network – for example, certain ports can be left open to enable a mail server to send and receive email while closing ports that allow a web server to operate.

### Virtual Private Network Capability

The Linksys router featured in the illustration includes Virtual Private Network (VPN) connection capability which facilitates very secure interconnection of computers or networks over any distance utilizing the Internet as the carrier thereby eliminating long-distance connection phone charges. The built-in VPN capability utilizes both authentication and encryption to ensure secure transmission of data. Some routers add functionality by including a printer port for connecting a network printer.

The latest generation of Cable/DSL Routers employ wireless technologies for network connection and shared Internet access without physical cabling. This is an ideal solution for small networks located in hard to wire locations, sites which desire the ability to place a computer anywhere, or, for working in the shade of a large tree sipping iced tea on those "too nice to be working" summer days...



Linksys Etherfast Cable/DSL  
VPN Router with 4 Port  
10/100 Switch

Suite 101, 5663 Cornwallis Street  
Halifax, NS, B3K 1B6, Canada  
Email: consulting@on-line.net  
Web Site: www.on-line.net  
Toll Free: 1.866.6 ON-LINE  
1.866.666.5463  
Phone: 902.422.1171  
Fax: 902.492.4608

