

Basic Network Configuration

Table of Contents

| | |
|---|---------------|
| Basic Network Configuration | 25 |
| LAN (local area network) vs WAN (wide area network) | 25 |
| Local Area Network | 25 |
| Wide Area Network..... | 26 |
| Accessing the Wide Area Network (WAN)..... | 27 |
| IP Addresses | 29 |
| Ping a Computer | 30 |
| Possible Pitfall with Routers, Gateways, and Switches | 31 |
| RVON-8 Specific Configuration | 32 |
| Network Terminology | 33 |
| Bridges | 33 |
| Domain Name Server (DNS) | 33 |
| Gateway | 33 |
| Hub | 33 |
| IP Address (Internet Protocol Address) | 33 |
| LAN | 34 |
| Port..... | 34 |
| Routers | 34 |
| Subnet | 34 |
| Switches | 34 |
| WAN | 34 |

Basic Network Configuration

This section covers basic network configuration set up and testing. Also covered are basic concepts and operations, including the difference between LAN and WAN networks and how IP Addressing is used.

In a networked environment, such as a company, typically there are many computers connected together using a **router** or a **switch** (for more information, see router or switch in the definitions section). In larger companies, there may be several different routers distributed in buildings and plant locations. A router allows any LAN-side computer communicate with computers and devices outside the LAN (local area network). Routers send data packets from one place to another place on a network. Routers use network addresses to route packets to the correct destination. For example, in a TCP/IP network, the IP (internet protocol) address of the network interface is used to direct router destinations.

Because routers help computers inside the LAN “talk” with computers outside of the LAN. The security of a company’s LAN may be compromised by gaps of open ports in the router. Security measures may have been instituted to compensate for these vulnerabilities. Consult your network administrator to learn about the security measures taken to protect your network. VPN, or virtual private network, is one such security measure to protect the intelligence of the LAN. A computer outside the LAN must have an address or key known by the VPN to allow access to the LAN. Many companies use a VPN to connect two different LANs, thus allowing the transfer of data between the two networks.

LAN (local area network) vs WAN (wide area network)

Local Area Network

Simply put, a LAN is a computer network that connects a relatively small area (a single building or group of buildings). Most LANs connect workstations and computers to each other. Each computer (also known as a “node”), has its own processing unit and executes its own programs; however, it can also access data and devices anywhere on the LAN. This means that many users can access and share the same information and devices. A good example of a LAN device is a network printer. Most companies cannot afford the budgetary or hardware expense of providing printers for each of its users. Therefore, one printer (i.e., device) is placed on the LAN where every user can access the same printer.

The LAN uses IP addresses to route data to different destinations on the network. An IP Address is a 32-bit numeric address written as four numbers separated by periods (For example, 1.160.10.240).

Note: For more information on IP Addresses, see your local network administrator.

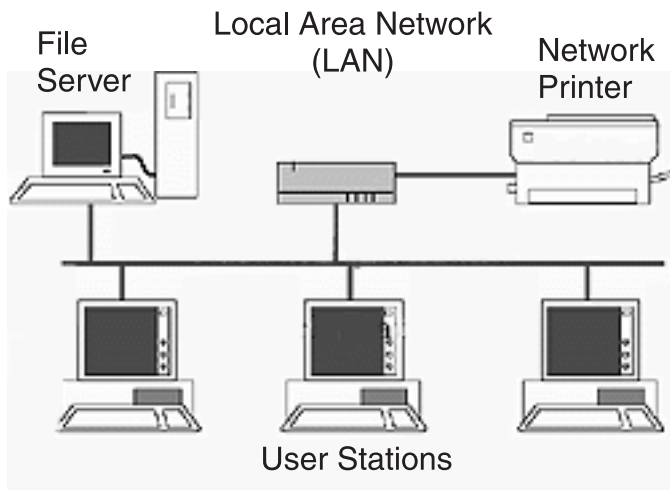


Figure 1. Local Area Network Diagram

Wide Area Network

A wide area network connects two or more LANs and can span a relatively large geographical area. For example, Telex Headquarters in Burnsville, MN is connected to several of its branch offices in Nebraska and Arkansas over the wide area network. The largest WAN in existence is the Internet.

Wide Area Network (WAN)

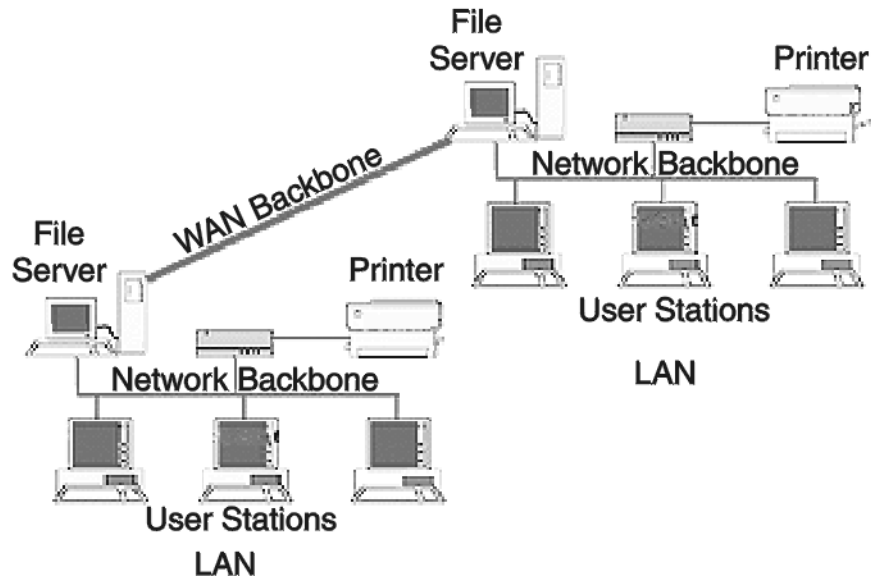


Figure 2. Wide Area Network Diagram.

Accessing the Wide Area Network (WAN)

Figure 3 shows LAN IP addresses using a common IP address, 10.2.100.x (192.168.x.x is another common address). Most devices are shipped with these addresses as its default. It is recommended to use these addresses for LANs.

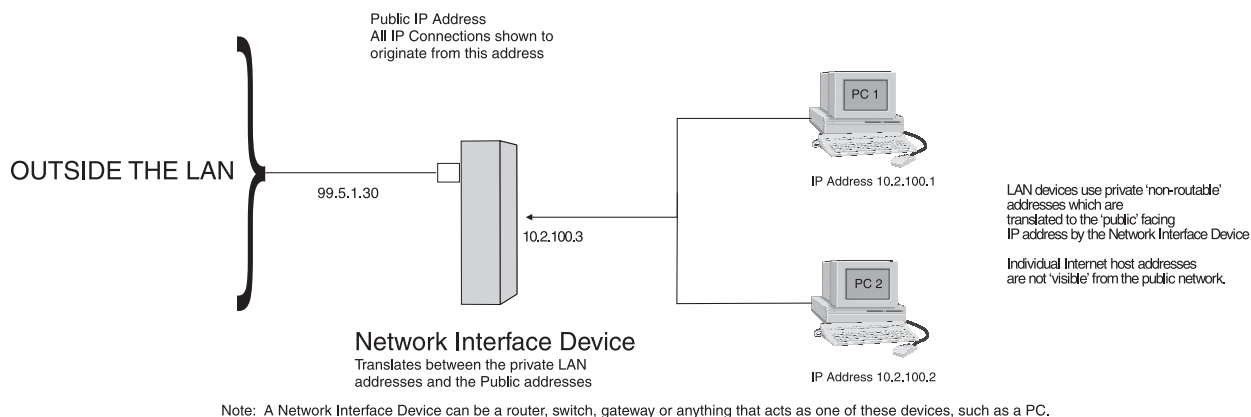


Figure 3. Network Address Translation

Network Address Translation (NAT)

Using the initial IP address, then converting it to a valid WAN IP address is how the network address translation works in theory. Once the IP address is changed, it is up to the network interface device (such as a router, gateway, switch, etc.) to keep track of which computers are talking on which ports. For example, if two local devices (PC1 and PC2 in Figure 3) both wanted to talk via port 1031, then the network interface device would have to change one of the port requests to the next available port, 1032.

Ports

In general, a network port is an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic. When you type an address into the *address bar* of a web browser, your computer goes to find an IP address for the url you are requesting (<http://www.telex.com>). To obtain this address, the computer contacts a DNS server (Domain Name Server). Once the IP address is found, it tries to connect to the http port of the network device (port 80). See Table 1 for a list of the more well-known Port numbers.

Each network device can be set up to respond or not respond to the various ports. The function of responding or “hosting a service” is called “serving”.

| | Packet before translation | | | | Packet after translation | | | |
|---------------|---------------------------|-------------|----------------|-------------|--------------------------|-------------|----------------|-------------|
| | Source | | Destination | | Source | | Destination | |
| | IP Address | Port Number | IP Address | Port Number | IP Address | Port Number | IP Address | Port Number |
| To Internet | 10.2.100.2 | 1031 | 192.156.136.22 | 80 | 99.5.1.30 | 1031 | 192.156.136.22 | 80 |
| From Internet | 192.156.136.22 | 80 | 99.5.1.30 | 1031 | 192.156.136.22 | 80 | 10.2.100.2 | 1031 |

Table 1 Packet Translation

If a second work station on the LAN wants to communicate to the same server, and happens to use the same source port number, then the LAN Modem will translate the source port number as well as the source IP address. In Table 2, a second LAN computer wants to access a web page. The NAT device now uses port 1032 for this connection where it used port 1031 in Table 1.

| | Packet before translation | | | | Packet after translation | | | |
|---------------|---------------------------|-------------|----------------|-------------|--------------------------|-------------|----------------|-------------|
| | Source | | Destination | | Source | | Destination | |
| | IP Address | Port Number | IP Address | Port Number | IP Address | Port Number | IP Address | Port Number |
| To Internet | 10.2.100.1 | 1031 | 192.156.136.22 | 80 | 99.5.1.30 | 1032 | 192.156.136.22 | 80 |
| From Internet | 192.156.136.22 | 80 | 99.5.1.30 | 1032 | 192.156.136.22 | 80 | 10.2.100.1 | 1031 |

Table 2. Packet Translation

Amazingly, all the address translation that occurs takes place automatically in order to make web browsing and other functions easier. This is also a way for large web hosting services to speed up the network by having different devices perform different functions.

| Port Number | Description |
|-------------|---------------------------------------|
| 1 | TCP Port Service Multiplexer (TCPMUX) |
| 5 | Remote Job Entry (RJE) |
| 7 | ECHO |
| 18 | Message Send Protocol (MSP) |
| 20 | FTP - Data |
| 21 | FTP - Control |
| 23 | Telnet |
| 25 | Simple Mail Transfer Protocol (SMTP) |
| 29 | MSG ICP |
| 37 | Time |
| 42 | Host Name Server (Nameserv) |
| 43 | Whols |
| 49 | Login Host Protocol (Login) |
| 53 | Domain Name Server (DNS) |
| 69 | Trivial File Transfer Protocol (TFTP) |
| 70 | Gopher Service |
| 79 | Finger |
| 80 | HTTP |
| 103 | X.400 Standard |
| 108 | SNA Gateway Access Server |
| 109 | POP2 |
| 110 | POP3 |
| 115 | Simple File Transfer Protocol |

| Port Number | Description |
|-------------|--|
| 118 | SQL Services |
| 119 | Newsgroup (NNTP) |
| 137 | NetBIOS Name Service |
| 139 | NetBIOS Datagram Service |
| 143 | Interim Mail Access Protocol (IMAP) |
| 150 | NetBIOS Session Service |
| 156 | SQL Server |
| 161 | SNMP |
| 179 | Border Gateway Protocol (BGP) |
| 190 | Gateway Access Control Protocol (GACP) |
| 194 | Internet Relay Chat (IRC) |
| 197 | Directory Location Services (DLS) |
| 389 | Lightweight Directory Access Protocol (LDAP) |
| 396 | Novell Netware over IP |
| 443 | HTTPS |
| 444 | Simple Network Paging Protocol (SNPP) |
| 445 | Microsoft-DS |
| 458 | Apple QuickTime |
| 546 | DHCP Client |
| 547 | DHCP Server |
| 563 | SNEWS |
| 569 | MSN |
| 1080 | Socks |

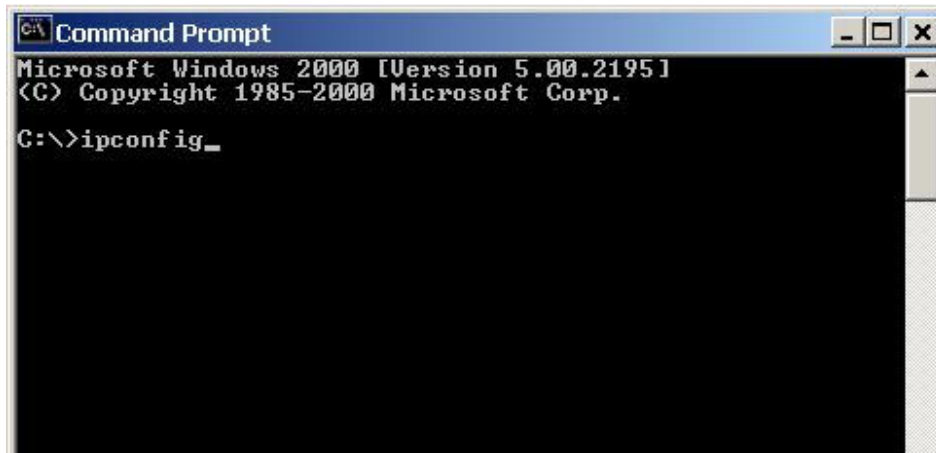
Table 3. Well-Known TCP Port Numbers

IP Addresses

If you do not know your IP Address, you can open a DOS screen in a Windows®-based environment and bring up the ipconfig screen.

To find your IP Address using ipconfig, do the following:

1. From the Start Menu, open a **Command Prompt** screen.

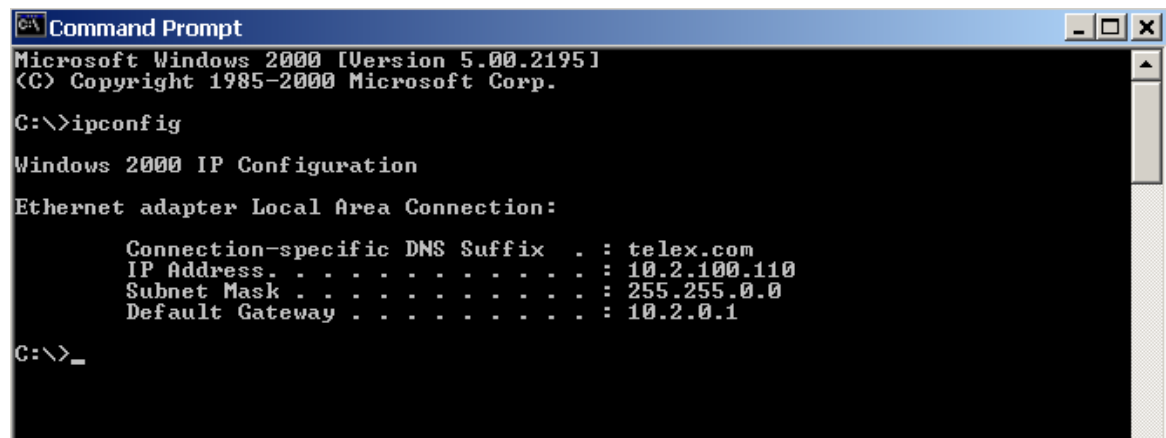


```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig_
```

2. At the prompt, type **ipconfig**, then press **Enter**.

The IP configurations appear for your machine, such as the DNS suffix, IP Address, Subnet Mask, and Default Gateway.



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : telex.com
    IP Address. . . . .               : 10.2.100.110
    Subnet Mask . . . . .             : 255.255.0.0
    Default Gateway . . . . .         : 10.2.0.1

C:\>_
```

3. At the prompt, type **Exit** to close the screen.

Note: If you want more detailed parameters for your machine, type **ipconfig/ All**. This screen shows the computers network configuration settings.

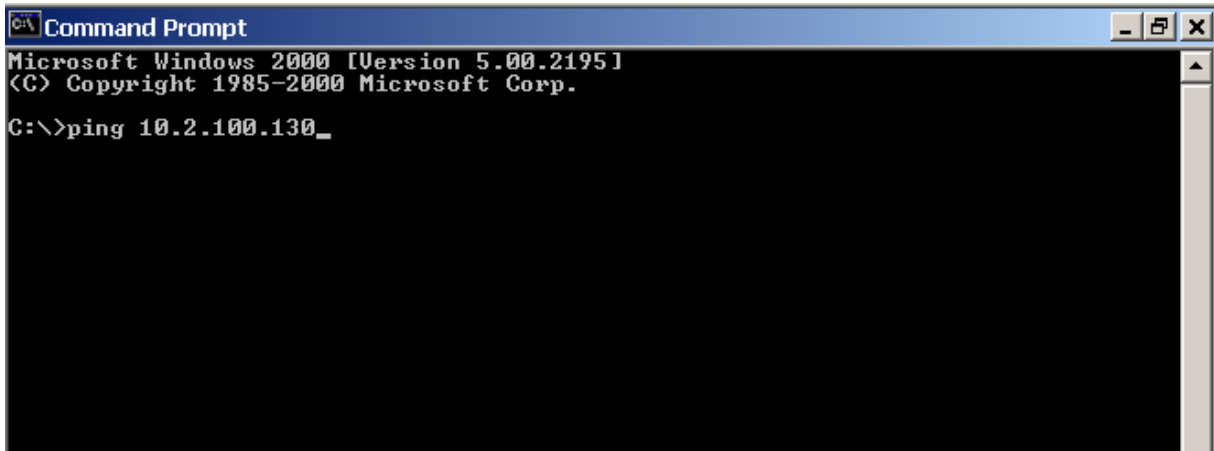
Ping a Computer

Pinging a computer on the network makes sure it is able to be “seen” and receive messages on the network.

Note: You can also ping your RVON-8 card to verify that it is responding over the network by putting the cards IP address in place of the computer IP address.

To ping a computer on the network, do the following,

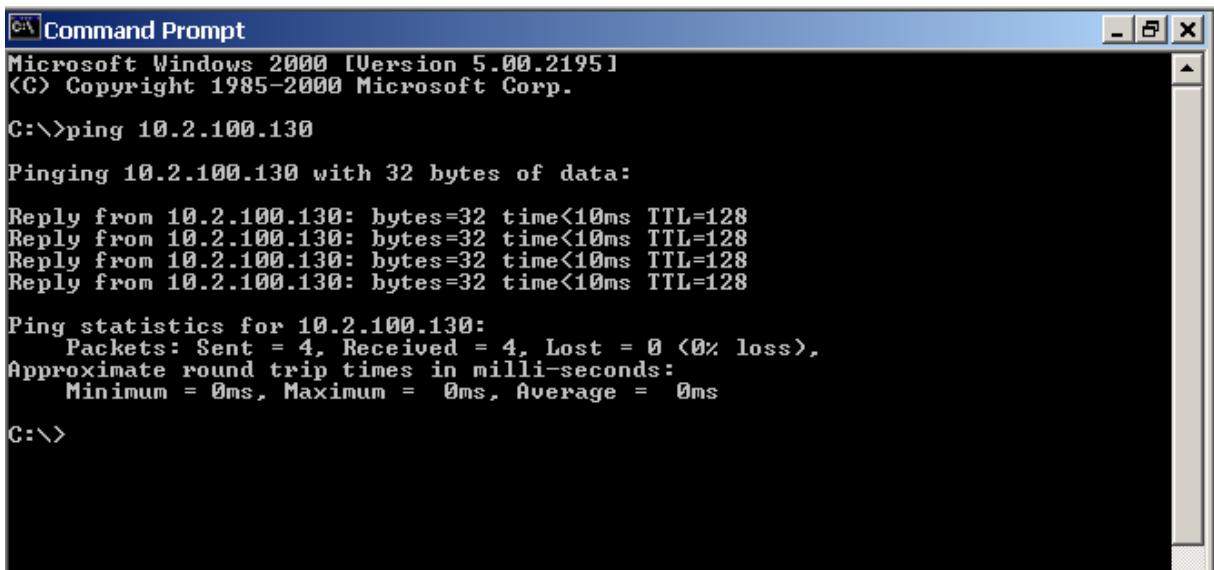
1. From the Start Menu, open a **Command Prompt** screen.



```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ping 10.2.100.130_
```

2. At the prompt, type the **IP Address** of the computer you wish to ping. (for example, 10.2.100.130)
3. Press **Enter**.



```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ping 10.2.100.130

Pinging 10.2.100.130 with 32 bytes of data:

Reply from 10.2.100.130: bytes=32 time<10ms TTL=128
Reply from 10.2.100.130: bytes=32 time<10ms TTL=128
Reply from 10.2.100.130: bytes=32 time<10ms TTL=128
Reply from 10.2.100.130: bytes=32 time<10ms TTL=128

Ping statistics for 10.2.100.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Note: If the computer you are pinging is not responding to the ping, you will receive a time out message in the command prompt screen.

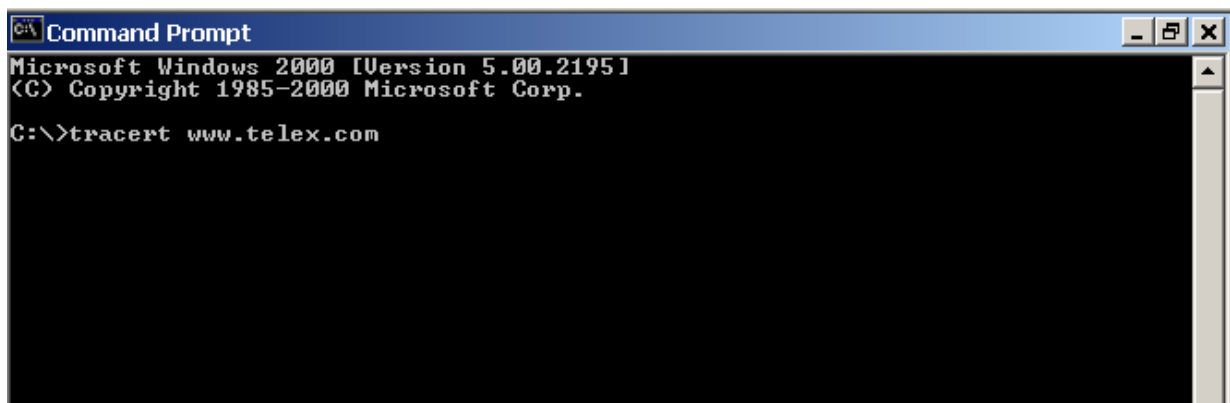
Possible Pitfall with Routers, Gateways, and Switches

Anytime computers communicate through routers, gateways, and switches, they may be allowed or denied the connection. Network interface devices can be configured to block specific outgoing requests, as well as incoming requests, based on the IP address and/or port. This is one of the security mechanisms of a router. This also happens when broadcast messages are sent and received.

To view the path an IP address takes to retrieve information, you can execute a *tracert* from the Command Prompt screen.

To run *tracert*, do the following:

1. From the Start Menu, open a **Command Prompt** screen.
2. At the prompt, type **tracert** and type the url or IP address you want to trace.

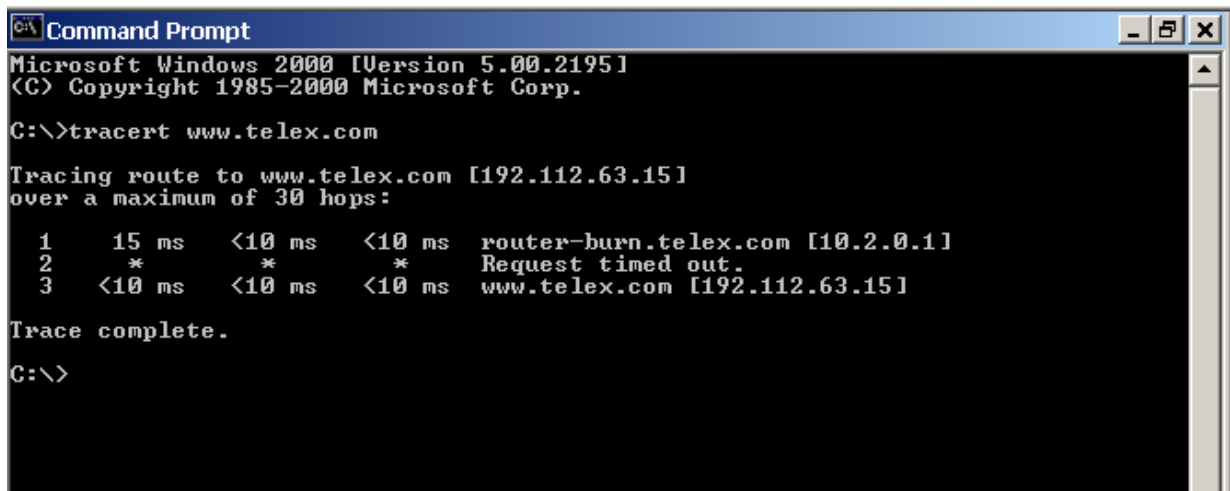


```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>tracert www.telex.com
```

3. Press **Enter**.

The details of the tracer route are displayed.



```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>tracert www.telex.com

Tracing route to www.telex.com [192.112.63.15]
over a maximum of 30 hops:
  1    15 ms    <10 ms    <10 ms    router-burn.telex.com [10.2.0.1]
  2     *       *         *         Request timed out.
  3    <10 ms   <10 ms    <10 ms    www.telex.com [192.112.63.15]

Trace complete.

C:\>
```

Note: You will see the message “request timed out” if the IP address/port in or out is denied to the outgoing or incoming message.

4. When you are finished, type **exit** to close the Command Prompt screen.

RVON-8 Specific Configuration

RVON-8 cards use ports for communication of audio and control packets. Because routers can be configured to block certain incoming and outgoing requests, you will need to open the following ports in your network to allow WAN connections to and from a Network Interface Device. See Table 4 for the ports that need to be opened for the RVON-8 card to operate properly.

| Port | Port Description |
|------|----------------------------------|
| 2076 | UDP Call Control Signalling |
| 2077 | UDP Audio Packets |
| 2079 | UDP Telex Proprietary Signalling |
| 2080 | TCP Telex Keypanel Protocol |
| 2081 | UDP Pass Through Serial |
| 2082 | TCP Firmware Download |
| 2100 | Remote Administration |
| 2102 | Authentication Server |

Table 4. Ports necessary for RVON-8 Card Functionality.

Figure 4 is an example of a router configuration screen. Not all routers are configured the same way and may not look exactly like this figure.

LINKSYS Filters **Forwarding** Dynamic Routing Static Routing DMZ Host MAC Addr. Clone Setup

PORT RANGE FORWARDING

Port forwarding can be used to set up public services on your network. When users from the Internet make certain requests on your router, they will be redirected to the specified IP.

| Customized Applications | Ext.Port | Protocol TCP | Protocol UDP | IP Address | Enable |
|-------------------------|--------------|--------------------------|-------------------------------------|------------|-------------------------------------|
| RVON VOIP | 2077 To 2077 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 10.2.210.0 | <input checked="" type="checkbox"/> |
| | 0 To 0 | <input type="checkbox"/> | <input type="checkbox"/> | 10.2.210.0 | <input type="checkbox"/> |
| | 0 To 0 | <input type="checkbox"/> | <input type="checkbox"/> | 10.2.210.0 | <input type="checkbox"/> |
| | 0 To 0 | <input type="checkbox"/> | <input type="checkbox"/> | 10.2.210.0 | <input type="checkbox"/> |
| | 0 To 0 | <input type="checkbox"/> | <input type="checkbox"/> | 10.2.210.0 | <input type="checkbox"/> |
| | 0 To 0 | <input type="checkbox"/> | <input type="checkbox"/> | 10.2.210.0 | <input type="checkbox"/> |
| | 0 To 0 | <input type="checkbox"/> | <input type="checkbox"/> | 10.2.210.0 | <input type="checkbox"/> |
| | 0 To 0 | <input type="checkbox"/> | <input type="checkbox"/> | 10.2.210.0 | <input type="checkbox"/> |
| | 0 To 0 | <input type="checkbox"/> | <input type="checkbox"/> | 10.2.210.0 | <input type="checkbox"/> |
| | 0 To 0 | <input type="checkbox"/> | <input type="checkbox"/> | 10.2.210.0 | <input type="checkbox"/> |
| | 0 To 0 | <input type="checkbox"/> | <input type="checkbox"/> | 10.2.210.0 | <input type="checkbox"/> |
| | 0 To 0 | <input type="checkbox"/> | <input type="checkbox"/> | 10.2.210.0 | <input type="checkbox"/> |
| | 0 To 0 | <input type="checkbox"/> | <input type="checkbox"/> | 10.2.210.0 | <input type="checkbox"/> |

UPnP Forwarding Port Triggering

Apply Cancel

Figure 4. An example of a router configuration screen.

Note: Linksys™ only support up to 253 nodes on a router. This is why it is called a Router/Switch, because there are WAN functions like a router as well as having a 4-port LAN switch. It also does not support simultaneous forward and DHCP.

Network Terminology

Bridges

A **bridge** is a device that connects two LANs, or two segments of the same LAN that use the same protocol. Sometimes called “transparent bridges, they work at the OSI model Layer 2. Simply put, they are not concerned with protocols. Their main job is to pass data to a destination address that is predetermined in the data packet.

With a bridge, all your computers are on the same network subnet (*see Subnet*). This means your computers can communicate with each other and have their own Internet connection. If you assign your own IP Addresses be sure to use the same first 3 “octets” of the IP Address (for example, 192.168.0.X).

Domain Name Server (DNS)

A **DNS Server** is an Internet service that translates domain names (for example, in the URL *http://www.telex.com*, the domain name is *telex.com*) into IP Addresses. The Internet is based on IP Addresses which are numeric and since domain names are alphabetic, they are easier to remember. Everytime a domain name is used it must go through the DNS server to be translated into an IP Address.

Gateway

A **gateway** is a node on a network that serves as an entrance to another network. The gateway routes traffic from a computer to an outside network that is serving the web pages. For example, the gateway for a home computer is the ISP provider that connects the user to the Internet.

In a corporate environment, the gateway often acts as a proxy server and a firewall. Gateways are similar to routers and switches in that they forward data to the destination and provide the path for which the data will travel to the destination.

Hub

A **hub** is a common connection point for devices in a network. A hub has multiple ports. When a data packet arrives at a hub, it is copied and distributed to all of its ports so that all nodes on the LAN can see the packets.

There are three types of hubs:

passive hub - this hub serves as a conduit for the data, enabling it to go from one device to another.

intelligent hub (also known as manageable hubs) - this hub includes additional features that enable administrators to monitor traffic through the hub.

switching hub - this hub reads the destination address of each packet and then forwards the data packet to the appropriate port.

IP Address (Internet Protocol Address)

An **IP Address** is an identifier or numerical name for a computer or device on a network. Data between computers are routed over the network using these addresses to identify the computer the message is being sent to and the computer the message is being sent from.

The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. For example, an IP Address looks like 10.100.1.1.

IMPORTANT: When working within an isolated network (meaning there is no Internet access), IP addresses can be assigned at random just as long as they are unique to each computer and device. When the isolated network is connect to the Internet, registered Internet address must be obtained. This is to prevent duplication of addresses.

The four number in an IP add re used in different ways to identify a particular network and host on that network. There are three classes of Internet addresses.

Class A - supports 16 million hosts on each of 127 networks.

Class B - supports 65,000 hosts on each of 16,000 networks.

Class C - supports 254 hosts on each of 2 m million networks.

LAN

A **LAN** is a computer network that connects a relatively small area (a single building or group of buildings). Most LANs connect workstations and computers to each other. Each computer (also known as a “node”), has its own processing unit and executes its own programs; however, it can also access data and devices anywhere on the LAN. This means that many users can access and share the same information and devices. A good example of a LAN device is a network printer. Most companies cannot afford the budgetary or hardware expense of providing printers for each of its users. Therefore, one printer (i.e., device) is placed on the LAN where every user can access the same printer.

The LAN uses IP addresses to route data to different destinations on the network. An IP Address is a 32-bit numeric address written as four numbers separated by periods (For example, 1.160.10.240).

Port

A **port**, when referring to TCP and UDP networks, is an endpoint in a logical connection. The port number identifies the type of port it is. For example, port 80 is used for HTTP traffic.

Routers

A **router** is a device that forward data packets over networks. Most commonly, a router is connected to at least two networks (normally LANs or WANs). Routers are located at gateways, the place where two networks are connected. Routers do little data filtering, they mainly deliver the data.

Subnet

A **subnet** is a portion of a network that shares a common address component. On a TCP/IP network, a subnet is described as all computers or devices whose IP Address have the same prefix.

Subnetting a network is useful because it provides security for the network as well as increases performance of the network. IP networks are divided using subnet masks.

Switches

A **switch** is a device that filters and forwards data packets between networks. Switches operate at the data layer, and sometimes at the network layer.

WAN

A **wide area network** connects two or more LANs and can span a relatively large geographical area. For example, Telex Headquarters in Burnsville, MN is connected to several of its branch offices in Nebraska and Arkansas over the wide area network. The largest WAN in existence is the Internet.