

Assigning IP Addresses To Routers

John P. Abraham
University of Texas – Pan American
jabraham@utpa.edu

Mary T. Walker
South Texas College
mtwalker@southtexascollege.edu

Abstract

With the proliferation of home based networks, casual computer users are now forced to setup routers that were once in the realm of network engineers. This paper explains the purpose of IP addresses both in the LAN side and the WAN side, sub-netting, network address translation (NAT), DHCP, and DNS, and provides a description of practical approach to set up a commonly used DSL router. Without a modest understanding of these topics it would be very difficult to setup routers, particularly when default settings would not suffice. Many home based networks end up using the DSL modem and a router, either wired or wireless, and in such cases default settings may not work. After introducing necessary background theoretical concepts, this paper will guide the reader through setting up a complicated home network with a DSL modem, a wired router and a wireless router.

Packets originating at a source computer are made into frames while circulating within the local area network (LAN) and sent directly to the destination using the MAC address obtained using the ARP. Those packets intended for a destination outside the LAN are forwarded to the default gateway which is the LAN side IP address of the router. LAN side IP addresses usually are private IP addresses, while the WAN side is a public IP addresses. Consulting the routing table the packets are forwarded to the next hop. Using network address translation (NAT) machines on the LAN side with local IP addresses are mapped on the public IP addresses using port numbers.

Introduction

Virtually every business and home in the U.S. uses some sort of a router. Businesses may have their own IT staff or outsource network related tasks. However, many users are obligated to set up networks in their homes. This requires some basic understanding of theory of networking, more specifically installation of routers. More importantly anyone working routers must have an understanding of the machine addressing schemes, network address translation (NAT), dynamic host configuration protocol (DHCP), and domain name systems (DNS). This paper explains the purpose of IP addresses both in the LAN side and the WAN side, sub-netting, NAT, DHCP, DNS, and provides a practical approach to set up a network with a DSL modem, wired router and a wireless router. Even though this paper deals with DSL routers, installation of

most broadband routers is very similar, and can prove useful since most US homes now use DSL, cable or ISDN broadband networks.

Computer Addressing

Each computer that needs to be networked must have some sort of identification assigned to it. Today most computers communicate with each other through an Ethernet card. In the past an assortment of cards such as Ethernet, Token Ring, and ArcNet had been used. If the reader is still using a card other than Ethernet, please contact the author for specific instructions for that card.

There are two types of addresses: Media Access Control (MAC) and Internet Protocol (IP). A device attached to a network must have at least one network card. Any device having more than one network card is known as a multihomed device. Each Ethernet card comes with a unique 48-bit address programmed in a ROM chip. This address is known as the MAC address or the hardware address, and is used by layer 2 of the Open Systems Interconnection (OSI) model. There are seven layers to this model. The MAC address is used for direct delivery of frames of data within the same physical network. Machines within a LAN discover each other's MAC address using the Address Resolution Protocol (ARP). Discovered addresses are kept in an ARP cache until they become stale.

In order to deliver a packet outside of a local area network, the IP addressing scheme is used. In as much as the MAC addresses are short lived due to replacement of network card or replacement of the entire computer, it is impossible to locate a computer with MAC address alone. The IP address is a 32-bit number that is dynamically obtained at boot time and renewed periodically, or it is statically set by the network administrator.

BITS	8	16	24	31
0	Network address	Host address		
Class A				
10	Network address	Host address		
Class B				
110	Network address	Host address		
Class C				
1110	Multicast address			
Class D				
1111	Reserved for future use			
Class E				

Figure 1 - Classes of IP addresses and number of bits used for network and host portions

For easier human understanding the 32 bits are divided into four octets and written in decimal notation. The Control and distribution of IP addresses are centrally controlled by Internet Assigned Numbers Authority (IANA). This address is used by the third layer of the OSI model and is required to transmit packets of data across the Internet through routers. An IP address is divided into two parts: the network portion and the host portion

as shown in figure 1. Class A uses 8 bits for the network portion and 24 bits for the host portion. The first bit of the network portion is fixed as 0, and can't be changed. Therefore there are only 2^7 (128) class A addresses.

A serious problem with the 32-bit IP addressing scheme is the depletion of IP addresses. There are not enough addresses for all the computers in the world. Various solutions have been used to overcome this deficiency. For instance, subnet masking allows a large block of IP addresses to be broken into smaller networks. The University of Texas Pan American was given a class B block of network addresses. From Table 1 it can be ascertained that 16 bits are used for the network portion and 16 bits are used for the host portion. The first two bits of the network portion are fixed as 10 and cannot be changed. Therefore, there are only 2^{14} (16,384) class B networks in the world. Class B networks can have 2^{16} (65,536) minus 2 or 65,534 hosts. All zeros and all ones have special meanings and cannot be used as host addresses. Default subnet mask for a class B address is 255.255.0.0, meaning that it is assumed all 65,534 computers are on one network. If this class B network is sub netted to have 256 smaller networks, the subnet mask will be 255.255.255.0. If it is sub netted to have 32 subnets, only the most significant 5 bits of the third octet needs to be turned to all ones giving a subnet mask of 255.255.248.0. For further information refer to (Abraham).

Network Address Translation (NAT) is another solution to the problem of depletion of network address. NAT provides for security, as well. IANA (RFC 1597 and 1918) has set aside three blocks of addresses, Class A, B and C, that can be repeatedly used by different organizations. These blocks are 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255, respectively. Routers are programmed not to route packets bearing these network addresses and packets are restricted to the network itself. This allows anyone to set up a TCP/IP local area network. However, many of these organizations using the private IP need to access the Internet. In order to access the Internet, there must be at least one public IP assigned to that network's gateway. A computer with a private IP address can access the Internet using the NAT installed in the router. The router keeps track of the local IP address of the computer and assigns a socket (port number) to handle the traffic. Devices with public IP addresses are intrusion prone. Devices outside the LAN cannot initiate communication with a machine having a private IP address. Thus machines with private IPs are more secure as long as they do not initialize communication with mischievous sites and download scripts, virus, worms, knowingly or unknowingly. Address translation can take place with one public IP address or a pool of IP addresses.

Routing

A router, a layer 3 device, directs traffic of packets destined for a device outside of the local area network. All traffic between directly connected devices takes place using layer 2. Layer 2 handles frames, while layer 3 handles packets. A router is a special purpose computer designed to direct packet traffic having input ports, output ports, routing processor and a switching fabric (Behrouz). Frames from a directly connected device are received by the input ports and where physical and data link layer functions

are performed. From the received frames packets are reconstructed and stored in the buffer. These packets are then directed to the switching fabric which in turn directs them to appropriate output queues. The most popular switching fabrics are the Crossbar and Banyan switches. The routing processor deciphers the destination IP address from the packet and performs a table lookup to determine the output port to which the packet must be directed. The output ports receive the packets, convert them to frames to be forwarded to the appropriate directly connected device, which may be another router or a device on the local area network.

The routing processor can determine whether a packet is destined to a device within the same network or outside of it by ANDing the destination address with the net mask. If it is destined to another network, the router must decide on which output port (interface) that packet must be sent over. To determine the route there are several sets of rules referred to as routing protocols; the two most common ones being Routing Information Protocol (RIP) and Open Shortest Path First (OSPF). Each router keeps a routing table that is statically assigned, dynamically created, or both. Routers share routing information with each other. As it receives a packet, the router determines if it belongs to self or it must be forwarded. There are various forwarding methods, such as Next-hop, Network-Specific, Host-Specific and Default (Behrouz). When a router encounters a network address that is not in its table, it sends that packet over the default path. A time to live (TTL) is assigned to each packet and is decremented as it passes through a router; the packet is discarded as the TTL becomes 0. This prevents a packet from circulating indefinitely.

Assigning IP addresses to routers

A sample network with two routers and resulting two networks are drawn in Figure 2. All discussions that follow will refer to this figure for IP addressing and device layout. The routers used in this example are Netopia 3500 gateway router and Linksys 2.4 G Wireless router.

As mentioned earlier, a router is a multihomed device having more than one Ethernet port. Each port must have an IP address assigned to it. The WAN side IP addresses must have a public IP addresses while the LAN side could be either public or private IP addresses. For illustrative purposes, refer to Figure 2 and assume that two routers are used, one to connect the LAN with attached desktops and printers to the Internet and another one to provide wireless connections to laptops. Screen captures of such a setup are given in Figures 3 and 4. Figure 3 illustrates the configuration of the main gateway router that is connected to the internet. The public IP address given by the broadband Internet Service Provider (ISP) is 71.150.80.159 and this address is assigned to the WAN side. For the LAN side, any of the private IP addresses groups mentioned may be used; 192.168.0.1 is used here.

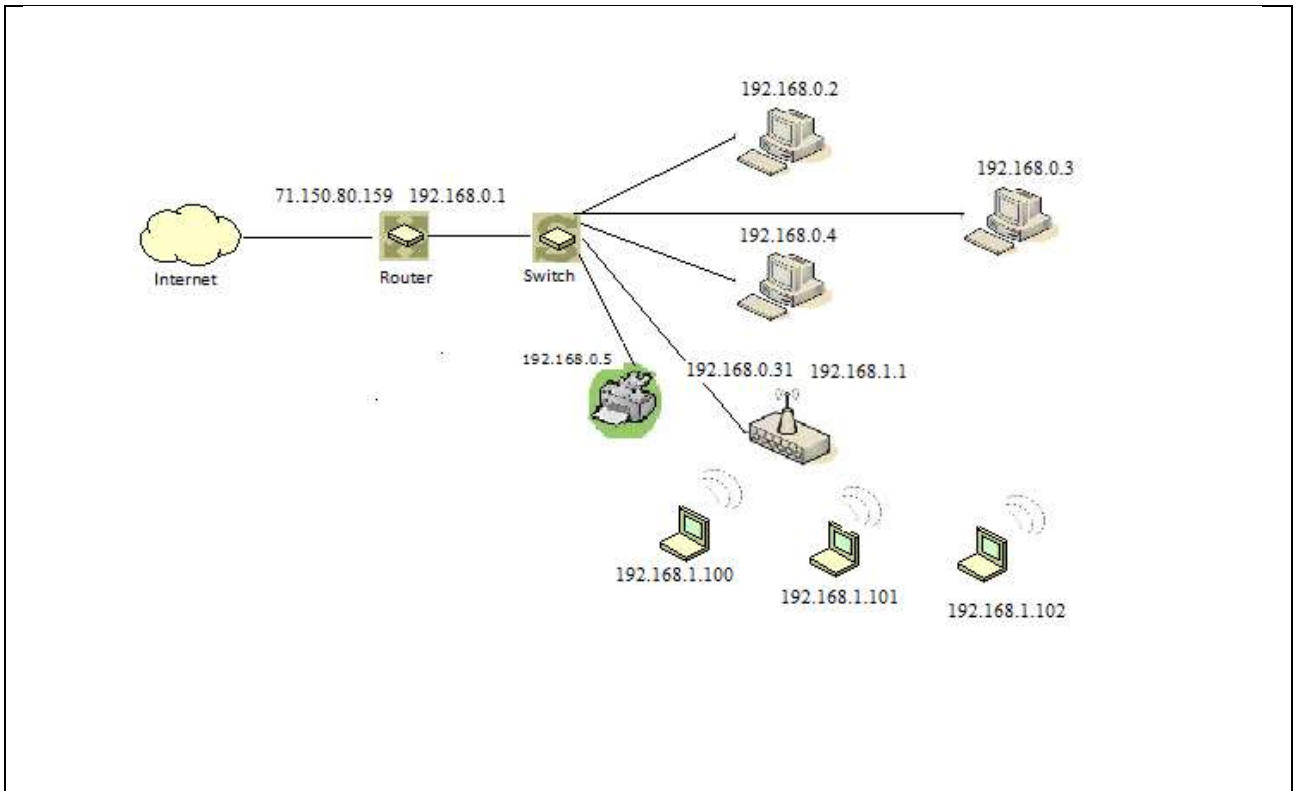


Figure 2 - Sample Network

All wired machines will be connected to this gateway router either through a separate switch or a built-in switch in the router. Most home routers come with a four port switch built-in alleviating the necessity for a separate switch. All devices connected to this router must have IP addresses ranging from 192.168.0.1 to 192.168.0.254. The WAN side of the wireless router will also receive one of these addresses. From figure 2 we see that the four computers and one printer connected to the gateway router have address 192.168.0.1 to 192.168.0.5. From figure 4, we can see that the IP address assigned to the WAN side of the wireless router is 192.168.0.31.

netopia			
Home			
Configure Troubleshoot Security Install			
General Information			
Hardware	Cayman 3546 WAN ADSL LAN 4-port Switch		
Serial Number	1216383		
Software Version	6.3.0R7	BreakWater Firewall	ClearSailing
Product ID	1117		
WAN			
Status	Up		
Local Address	71.150.80.159	Peer Address	71.150.87.254
Connection Type	Always On		
NAT	On		WAN Users
			Unlimited
LAN			
IP Address	192.168.0.1		
Netmask	255.255.255.0		
DHCP Server	On		DHCP Leases
			3 out of 71 leases in use
DNS-1	68.94.157.1		DNS-2
			68.94.156.1
© 2002 Netopia, Inc.			

Figure 3 – Configuration of the router connected to the Internet

Now we turn our attention the Wireless Router as shown in figure 4. As explained the WAN side of this router is given 192.168.0.31 as it is directly wired to the gateway router. For the LAN side any IP address range from 192.168.1.X to 192.168.254.X may be chosen. In this particular example, IP address 192.168.1.1 is assigned to the LAN side of the wireless router. All wireless devices connected to this router will receive IP address in the range from 192.168.1.2 to 192.168.1.254.

The screenshot displays the configuration interface for a wireless router, divided into two main sections: Internet Setup and Network Setup.

Internet Setup

- Internet Connection Type: Automatic Configuration - DHCP
- Optional Settings (required by some ISPs):
 - Router Name: WRT54G
 - Host Name: (empty)
 - Domain Name: (empty)
 - MTU: Auto
 - Size: 1500

Network Setup

- Router IP:
 - Local IP Address: 192 . 168 . 1 . 1
 - Subnet Mask: 255 . 255 . 255 . 0
- Network Address Server Settings (DHCP):
 - DHCP Server: Enable Disable
 - Starting IP Address: 192.168.1.100
 - Maximum Number of DHCP Users: 50
 - Client Lease Time: 0 minutes (0 means one day)
 - Static DNS 1: 0 . 0 . 0 . 0
 - Static DNS 2: 0 . 0 . 0 . 0
 - Static DNS 3: 0 . 0 . 0 . 0
 - WINS: 0 . 0 . 0 . 0

Figure 4 – Wireless router configuration

The DHCP is enabled on both routers. As a new device is turned on (if it does not have a static address already assigned) it would request for an IP address from the DHCP servers connected to it. A DHCP server has a database that among other details keeps track of available IP address, assigned IP addresses with their corresponding MAC address, and remaining lease time for each assigned IP address. From Figure 3, we can see that the DHCP server is enabled and a pool of IP addresses starting from 192.168.1.100 to 192.168.1.149 (inclusive) is available. Each wireless device connected to it will receive one of these addresses. Figure 2 illustrates that the three laptops connected wirelessly received 192.168.1.100, 192.168.1.101 and 192.168.1.102. A DHCP server can assign specified IP addresses to devices requiring static IPs.

Routing Table

Since the printer has an IP address of 192.168.0.5, it is connected to a different network than the wireless notebooks. If notebooks need to access files contained in one of the computers connected to the 192.168.0.0 network, or access the printer, the router needs to be setup to allow that. From Figure 4, we see that all packets containing network address of 192.168.1.0 is either delivered directly to the destination machine using the MAC address or delivered to the wireless router 192.168.1.1. All packets destined to network 192.168.0.0 are delivered to the WAN side of the wireless router (192.168.0.31), which in turn, is directly connected to all those devices. It may use MAC address delivery to the destination devices. All other addresses (Internet traffic) will be forwarded to 192.168.0.1 which is the gateway router.

Destination LAN IP	Subnet Mask	Gateway	Interface
0.0.0.0	0.0.0.0	192.168.0.1	WAN (Internet)
192.168.0.0	255.255.255.0	192.168.0.31	WAN (Internet)
192.168.1.0	255.255.255.0	192.168.1.1	LAN & Wireless

Table 4 - Routing Table Entry List

Conclusion

Installing routers can be intimidating particularly when dealing with assigning IP addresses to attached devices. This paper examined both MAC addressing and IP addressing and the purpose of these addressing schemes. Certain blocks of IP addresses are set aside for private addressing. Private IP addresses are used within an organization's network usually in conjunction with address translation. It was explained how a router can make use of both public IP addresses and private IP addresses to ensure security while allowing access the Internet. Using specific examples assigning IP address to the WAN side and the LAN side of routers was covered. Furthermore, this paper described how to install additional routers within an organization, and how to create routing tables to access file servers and print servers.

References

Abraham, John P., "A Practical Approach to Assigning Subnet Masks," Proceedings of the ETCE/OMAE 2000 Joint Conference, New Orleans, LA 2000.

Behrouz A. Forouzan, TCP/IP Protocol Suite, 3rd Ed., McGraw Hill, 2006. p 151.

Request for Comments (RFC), http://www.ietf.org/iesg/1rfc_index.txt.