Chapter 2

Planning Your Router Configuration

This chapter describes the background and concepts necessary for planning your router configuration. It contains a section on determining network parameters and a configuration worksheet. If you review this chapter and complete the worksheet ahead of time, your router configuration will be more straightforward.

2.1 Determining Network Parameters

This section describes the primary decisions you must make to configure your Wireless Router. Each of the following subsections corresponds to a portion of the worksheet in Section 2.2. As you review each subsection, complete that portion of the worksheet.

2.1.1 Global Parameters

Global parameters apply to the router rather than to the interfaces on the router. You must specify the following parameters for each router on your network:

- Hostname
- Internet Protocol (IP) address
- Simple Network Management Protocol (SNMP) variables (community, system contact, and system location)

Hostname

The hostname is the name of your Wireless Router. The default hostname is TAL.The name you specify is used in system prompts, and should be the same as the Domain Name System (DNS) hostname for your router; the hostname should also be unique within a domain. You can use uppercase and lowercase letters and numbers; do not use spaces.

If you are naming more than one router in your network, devise a consistent naming scheme so that identification is easy.

IP Address

Each Wireless Router has its own IP address. This address acts as the default address for the router and as the address for the wireless interface. IP addresses are 32-bit addresses specified in four-part dotted decimal format. Each number is an 8-bit value between 0 and 255. IP addresses are assigned by a central addressing authority. To receive your IP address, contact your Internet service provider or TAL.

For more information about IP addresses, refer to “Subnetting Overview” in Section 2.1.3.

SNMP Variables

The TALnet software includes Simple Network Management Protocol (SNMP) support. SNMP is an application-layer network management protocol that allows network managers to send queries to or set variables on network devices such as routers. SNMP consists of three elements:

- SNMP manager—A network management client program that requests or sets information. SNMP managers run on Network Management Stations (NMSs).
- SNMP agent—A software module on a managed network device, such as a router. The agent contains information the manager can monitor or change, and sends traps to the manager that alerts the manager when network conditions change.
- Management Information Base (MIB)—A repository on the managed network device that contains performance and administrative information about that device. The MIB defines variables maintained by the agent that the manager can request or set. (The term MIB also refers to the document that describes the information that can be read or set on a managed device.)

If you plan to use SNMP, you must define a community and the access that community has to the agent. Specify a community name, which can be a single word using uppercase and lowercase letters and numbers. Then identify the level of access (read-only or read-write).

In addition, you should define two global, or system, MIB variables: *system.sysContact.0* and *system.sysLocation.0*. The system contact variable identifies the person responsible for the router. The system location variable identifies the physical location of the router. Both of these are important when you troubleshoot problems on a router or network. These variables can use uppercase or lowercase letters, numbers, and spaces.

2.1.2 Radio Parameters

The router subsystem communicates with the wireless subsystem through a synchronous serial interface called the wireless interface. You configure this interface using the TALtalk configuration commands. Before you configure your network, you should determine the following information about the radio:

- Symbolic interface name—This name can include uppercase and lowercase letters, hyphens, and numbers, and should indicate the type of interface and the unit number; for example, *radio0*.
- Link-layer address—Each wireless interface has a unique predefined link-layer address that is assigned by TAL or your service provider. The address is an 8-digit hexadecimal address preceded by the characters *0x*. For example, *0x41544D31* and *0x00000001* are valid link-layer addresses. The link-layer address appears in the Address Resolution Protocol (ARP) table.

- Transmission frequency and channel number—The link analyses and performance tests you performed during the hardware installation process help determine the frequency on which you are going to transmit data. By selecting a frequency that only radios on your network are using, you can increase your likelihood of avoiding interference. Table 2-1 lists available frequencies and their channels. Use the same channel for all radios within your wireless network that communicate with each other. For more information about selecting a channel and transmission frequency, refer to Chapter 2 of the *SubSpace 2001 Installation Guide*.

Caution Channels on L-band radios overlap; do not select channels that are adjacent to each other.

Table 2-1 Transmission Frequency Channels

Channel	L-Band	S-Band
1	904.601	2407.067
2	907.201	2412.265
3	909.801	2417.465
4	912.401	2422.663
5	915.000	2427.863
6	917.599	2433.060
7	920.199	2438.259
8	922.798	2443.457
9	925.397	2448.659
10	—	2453.857
11	—	2459.056
12	—	2464.254
13	—	2469.454
14	—	2474.653
15	—	2479.851

- Transmission power level—The link analyses and performance tests you performed during the hardware installation process help determine the strength of the radio transmission. By adjusting your power, you can control the distance the radio signal travels. Select the lowest possible setting that provides reliable data transmission. See Table 2-2 for available power settings.

Table 2-2 Power Settings

L-Band		S-Band	
mW	**dBm**	**mW**	**dBm**
1	0	1	0
3	4.8	3	4.8
7	8.5	7	8.5
10	10	10	10
17	12.3	17	12.3
23	13.6	23	13.6
32	15	32	15
45	16.5	45	16.5
66	18.2	66	18.2
77	18.9	77	18.9
88	19.4	88	19.4
100	20	100	20
111	20.5	111	20.5
144	21.6	144	21.6
166	22.2	166	22.2
188	22.7	188	22.7
202	23.1	202	23.1
222	23.5	222	23.5
250	24	250	24
277	24.4	271	24.3
303	24.8	293	24.7
333	25.2	314	25
377	25.8	336	25.3
411	26.1	357	25.6
444	26.5	378	25.8
500	27	400	26
555	27.4	442	26.5
599	27.8	483	26.8
655	28.2	525	27.2
699	28.4	566	27.5
755	28.8	608	27.8
800	29	650	28.1

- Pseudorandom noise (PN) code—PN codes, also called spreading codes, allow you to encode network data for transmission. Using PN codes helps to increase channel capacity by allowing you to use a frequency another network in the area might also be using. The value can be an integer between 1 and 8; all radios in your network that communicate with each other must use the same code.

2.1.3 Ethernet Interface Parameters

The Ethernet interface connects the router subsystem to an Ethernet-based local area network (LAN). To configure this interface, you must assign the following parameters:

- Symbolic interface name—This name can include uppercase and lowercase letters, hyphens, and numbers, and should indicate the type of interface and the unit number; for example, *ether0*.
- IP address—The Ethernet IP address must differ from the system IP address that is used for the wireless interface. If you create subnetworks, the Ethernet IP address must be an unused address within the same subnet as any system connected to that interface.
- Subnet mask—Subnetting allows you to partition a single physical IP network into logical subnetworks. In this way, you can hide the details of an internal network organization to external routers. A single router provides the connection to the Internet. Some TALnet commands require that you specify the subnet mask (number of bits); others require that you specify the actual IP address. You should record both.

The following subsections explain IP addressing and subnetting in greater detail.

IP Address Overview

IP addresses consist of a network ID field and a host ID field. In general, the network portion of your IP address is assigned through your Internet Service Provider but originates with the central repository of Internet addresses, InterNIC Information Services. If the host is going to be on the Internet, using a registered IP address is a requirement. The host portion of the IP address is determined by your network administrator.

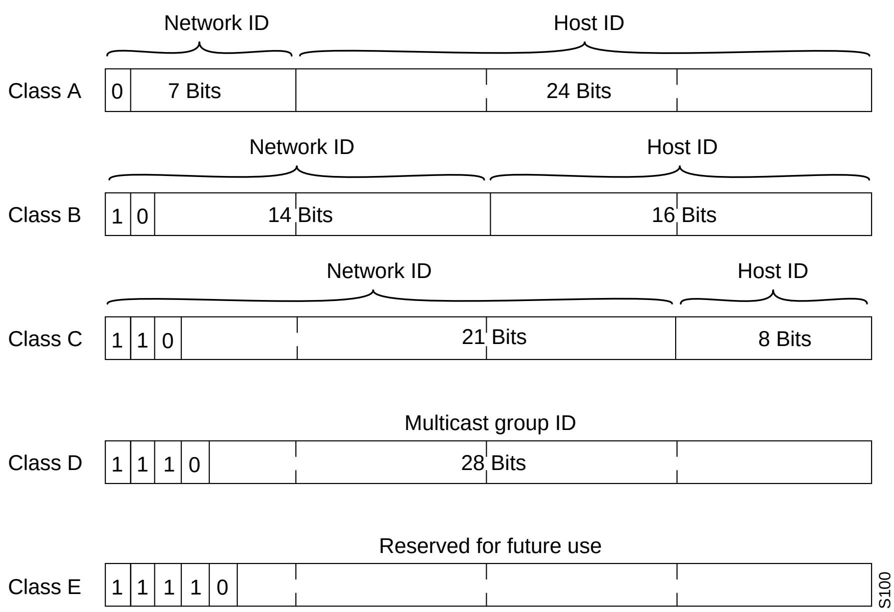
Depending on the class of your network, the number of bits in the network and host fields differs. IP addresses are divided into the following classes:

- Class A addresses allocate the highest (left-most) 8 bits to the network field and set the highest-order bit to 0 (zero). The remaining 24 bits form the host field, allowing more than 16,700,000 hosts per network. Class A addresses range from 0.0.0.0 to 127.255.255.255. Some of the addresses within this range are reserved.
- Class B addresses allocate the highest 16 bits to the network field and set the two highest-order bits to 1, 0. The remaining 16 bits form the host field, allowing more than 65,500 hosts per network. Class B addresses range from 128.0.0.0 to 191.255.255.255. Some of the addresses within this range are reserved.
- Class C addresses allocate the highest 24 bits to the network field and set the three highest-order bits to 1, 1, 0. The remaining 8 bits form the host field, allowing 254 hosts per network. Class C addresses range from 192.0.0.0 to 223.255.255.255. Some of the addresses within this range are reserved.

- Class D addresses are reserved for multicast groups. The highest four bits are set to 1,1,1, 0. Class D addresses range from 224.0.0.0 to 239.255.255.255.
- Class E addresses are reserved for future use. The highest four bits are all set to 1. Class E addresses range from 240.0.0.0 to 255.255.255.255.

Figure 2-1 illustrates these formats.

Figure 2-1 IP Address Formats



No matter which class of network you use, a host portion of all zeros indicates the network address. A host portion of all 1s (represented as 255) indicates the broadcast address. Therefore, the Class C address 192.168.180.0 is a network address, and the Class C address 192.168.180.255 is the broadcast address for that network.

In general, you will be assigned one or more Class C addresses. Therefore, most of the remainder of this discussion considers only Class C addresses.

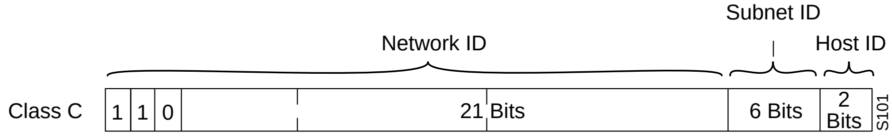
Note Refer to RFC 1166, “Internet Numbers,” for an official description of IP addresses.

Subnetting Overview

You create a subnetwork by dividing the host ID portion of an IP address into a subnet ID and a host ID. When you subdivide the host ID, the host ID must contain at least two bits (two bits allows four addresses, of which two are reserved for network identification and broadcasts). For example, in a Class B network, the host portion of the address uses 16 bits. You can use up to 14 of these bits as the subnet ID. In a Class C network, the host portion of the network uses

8 bits. You can use up to 6 of these bits as the subnet ID. (See Figure 2-2.) In practice, the bits that comprise the subnet ID are the highest bits in the host ID. All interfaces in a subnetwork must have a unique host ID, but the same subnet ID and network ID.

Figure 2-2 Class C Subnet Address Format



A subnet mask tells you how many bits to use in the subnet ID, and includes the number of bits in the network ID plus the number of bits in the subnet ID. For example, in a Class C network, if you use 4 host ID bits for the subnet, the subnet mask is 28. The dotted decimal format of this mask is 255.255.255.240.

Whereas a central addressing authority assigns network IP addresses, you can determine your own subnet address scheme. The following section describes how to do this.

Determining Your Address Scheme

To determine the addressing scheme for each Class C subnetwork, go through the following decision process. After you analyze these decisions, refer to Table 2-3 and Table 2-4 for practical addressing schemes.

1. Choose the Class C address you are going to divide into logical subnetworks.
2. Determine the number of subnetworks you want to create.
3. Determine the number of hosts you need on each subnetwork.
4. Choose the subnet mask based on the number of subnetworks and hosts per subnetwork.
5. Assign host addresses based on the subnet mask you have selected.

Table 2-3 lists the most common Class C subnet addressing schemes and compares the number of usable hosts and subnetworks available with each.

Table 2-3 Class C Subnetting

Subnet Mask (Decimal)	Subnet Mask (Bits)	Usable Subnets	Usable Host Addresses per Subnet	Usable Host Addresses per Network
255.255.255.192	26[1]	2	62	124
255.255.255.224	27	6	30	180
255.255.255.240	28	14	14	196
255.255.255.248	29	30	6	180
255.255.255.252	30[1]	62	2	124

1. If you select a subnet mask of 26 or 30, you lose over 50% of the usable addresses in a Class C network. Because of this loss of flexibility, you generally do not use these subnet masks.

According to Table 2-3, you can apply the following network topologies depending on the subnet mask you choose:

- If you select a subnet mask of 27 bits (decimal address of .224), you can divide the Class C address into a maximum of 6 subnetworks with 30 hosts in each subnetwork.
- If you select a subnet mask of 28 bits (decimal address of .240), you can divide the physical Class C network into a maximum of 14 subnetworks with 14 hosts in each subnetwork.
- If you select a subnet mask of 29 bits (decimal address of .248), you can divide the physical Class C network into a maximum of 30 subnetworks with 6 hosts in each subnetwork.

Table 2-4 lists usable host addresses, based on the subnet mask you selected. Notice that the number of ranges is the same as the maximum number of subnetworks, and the number of addresses within each range is the number of usable hosts.

Table 2-4 Usable Host Addresses

Subnet Mask 27 (.224)[1]						
.33–.62	.65– 94	.97–.126	.129–.158	.161–.190	.193–.222	
Subnet Mask 28 (.240)						
.17–.30	.33–.46	.49–.62	.65–.78	.81–.94	.97–.110	.113–.126
.129–.142	.145–.158	.161–.174	.177–.190	.193–.206	.209–.222	.225–.238
Subnet Mask 29 (.248)						
.9–.14	.17–.22	.25–.30	.33–.38	.41–.46	.49–.54	.57–.62
.65–.70	.73–.78	.81–.86	.89–.94	.97–.102	.105–.110	.113–.118
.121–.126	.129–.134	.137–.142	.145–.150	.153–.158	.161–.166	.169–.174
.177–.182	.185–.190	.193–.198	.201–.206	.209–.214	.217–.222	.225–.230
.233–.238	.241–.246					

1. Host addresses with all zeros such as .32, .64, and .96 are subnet identifiers. Host addresses with all ones such as .63, .95, and .127 are subnet broadcast addresses. This table does not list subnet identifiers or subnet broadcasts.

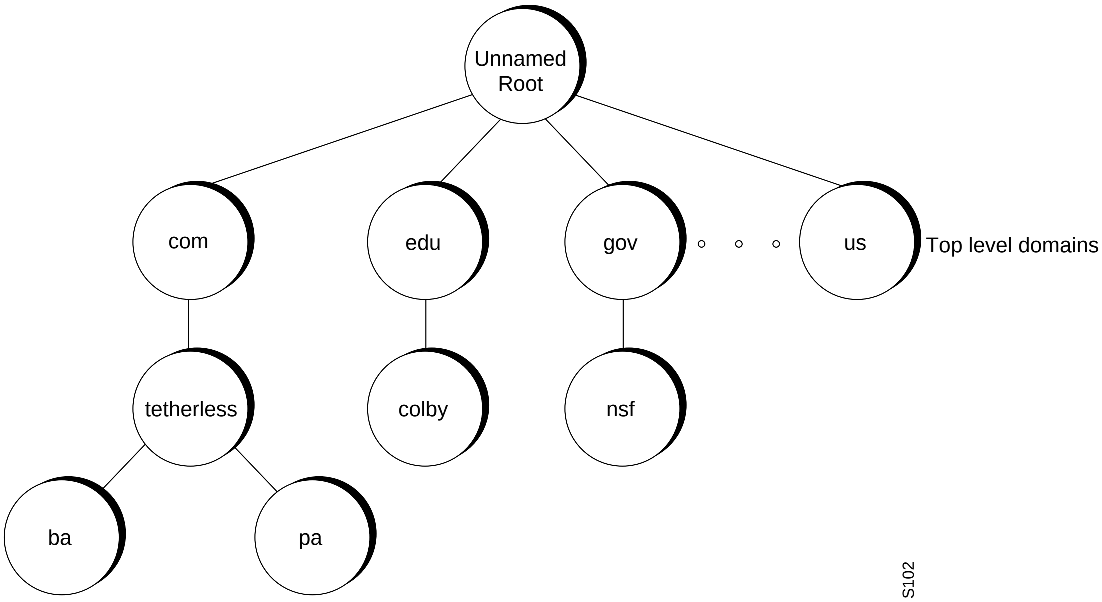
2.1.4 Domain Name System (DNS)

The TALnet software allows your system to map logical, easily recognizable names to IP addresses using the Domain Name System (DNS) so that you can use these easily recognizable names in applications such as the File Transfer Protocol (FTP), ping, and Telnet.

DNS is a distributed database system that associates 32-bit IP addresses with easily recognizable hostnames. Higher-layer applications such as Telnet use hostnames to identify network devices (hosts). The router and other network devices must be able to associate hostnames with IP addresses to communicate with other IP devices.

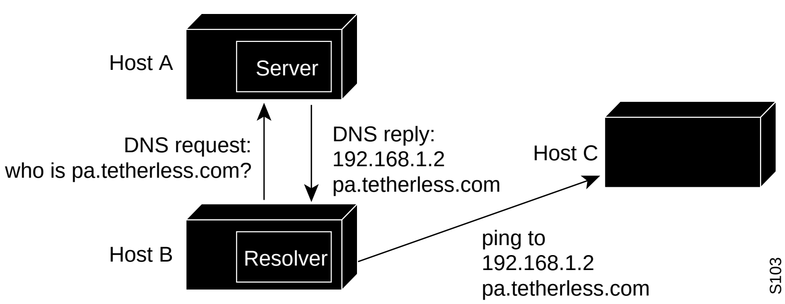
The hostname includes a suffix, called a domain name, that allows a device to be identified by its location in the Internet. The domain name follows a hierarchical naming scheme that uses dots (.) as the delimiting characters. For example, Tetherless Access Ltd. is a commercial organization that the Internet identifies by a *com* domain name, so its domain name is *tetherless.com*. Figure 2-3 illustrates the hierarchy of domain names.

Figure 2-3 Domain Name Hierarchy



To keep track of domain names, IP has defined the concept of a name server. The DNS name server speeds the process of converting names to addresses by holding a cache, or database, of names mapped to IP addresses. The TALnet software includes a DNS resolver that sends DNS requests to the DNS server. In Figure 2-4, Host B wants to ping the router with the domain name *pa.tetherless.com*. Host A has been defined as the name server for the network. Therefore, Host B sends a DNS request to Host A, asking for the IP address of *pa.tetherless.com*. Host A responds with the IP address for Host C. Host B then pings Host C.

Figure 2-4 DNS Name Resolution



To take advantage of DNS, you must identify the domain name of the router you are configuring and the IP address of the name server you want to handle DNS requests. You can define multiple name servers to balance DNS requests.

2.1.5 Routing Information

The primary purpose of routing is to determine the best path on which to send information. Routing tables contain information about different routes in a network; each entry in a routing table provides a variety of information, such as the ultimate destination, the next hop on the way to that destination, and a metric that indicates the number of hops to that destination. When a router receives an incoming packet, it checks the destination address of that packet and attempts to determine the next hop for the packet based on the information in the routing table.

Static and Dynamic Routing

You must decide whether to use static or dynamic routing algorithms to perform routing functions:

- If you use static routing, you must create routing tables before you begin routing. These routing tables do not change unless you change them. Because static routing does not send periodic routing updates to other routers, it conserves bandwidth. Use static routing only if network traffic is predictable and network design is simple; for example, if you have a network with only one connection to other networks.
- If you use dynamic routing, each router in your network dynamically maintains a routing table. The Routing Information Protocol (RIP) is an interior gateway protocol that enables dynamic routing. The TALnet software supports RIP versions 1 and 2.

Note If you use subnets that do not fall on 8-bit boundaries, you cannot use RIP-1. You can use RIP-2 because RIP-2 includes the information about the subnet masks with each advertised route.

Routing Information Protocol (RIP)

RIP uses User Datagram Protocol (UDP) datagrams to exchange routing information. Each router sends routing information updates every 30 seconds. If a router does not receive an update from another router for 180 seconds or more, it marks the routes served by the nonupdating router as being unusable. If there is no update after 240 seconds, the router removes all routing table entries for the nonupdating router.

The measure, or metric, that RIP uses to rate the value of different routes is the hop count. The *hop count* is the number of different media links on which a datagram must travel to reach a destination. A directly connected network has a metric of 1; an unreachable network has a metric of 16. Therefore, using RIP, your internetwork cannot have paths to remote destinations that are longer than 15 hops.

Figure 2-5 Sample Internetwork Using RIP

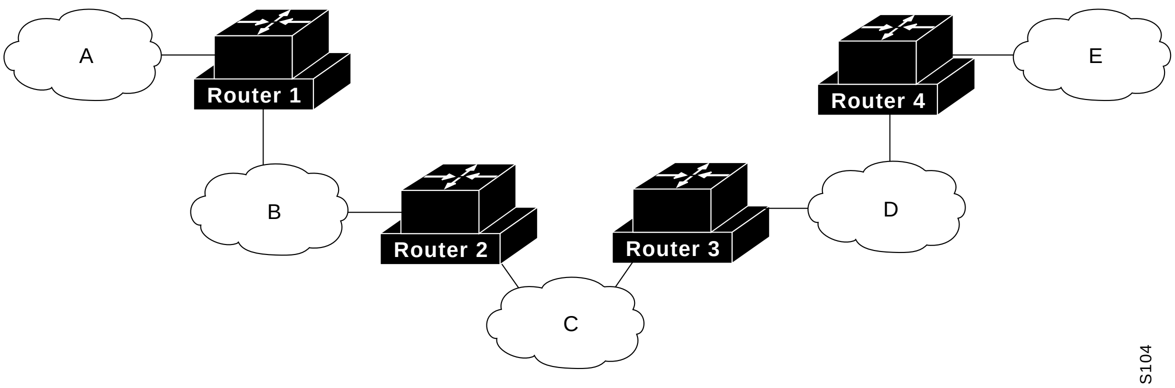


Table 2-5 illustrates the routing table for a datagram travelling from a host on Network C to hosts on other networks within the internetwork. For example, to send a datagram from a host on Network C to Network E, the datagram travels across three hops:

- The first hop is across the Network C media to Router 3 (the next-hop router).
- The second hop is from Router 3 across Network D to Router 4.
- The third hop is from Router 4 to the destination on Network E.

Table 2-5 RIP Routing Table for Datagrams Sent from a Host on Network C

Destination Network	Next-Hop Router	Number of Hops
A	2	3
B	2	2
C	None (deliver directly)	1
D	3	2
E	3	3

Note RIP is documented in RFC 1058. RIP-2 is documented in RFC 1723.

Additional Routing Parameters

After you determine whether you are going to use static or dynamic routing, you need to determine the following:

- Default route—Whether you are using static or dynamic routing, you should designate the IP address of a default router. If no other entry in the routing table is valid, packets are sent to this default router, ensuring that all datagrams are handled in some way.

- RIP neighbor address—If you use dynamic routing, you must specify at least one network or host to which routing updates will be sent. A routing process listens to updates from other routers on these networks and broadcasts its own routing information on those same networks.

2.1.6 User Authorization

You can provide users with different levels of access to the Wireless Router by setting up a table of users. In particular, you can define the level of changes the user is authorized to make, the interface on which the user can make PPP connections, and the root directory used for FTP transfers. You can define the following levels of authorization:

- FTP—To allow a user to read, write, and overwrite files from an FTP connection, use an authorization flag of 0x07. You must also specify the root directory.
- Operator—To allow an operator to interactively modify the configuration without changing the configuration file and rebooting the router, use an authorization flag of 0x10. If a user with operator privileges modifies the configuration interactively, changes are not saved when the router reboots.
- PPP—To allow the user to connect to the Wireless Router using the Point-to-Point Protocol (PPP), use an authorization flag of 0x20. You must also specify the interface on which the user can make PPP connections.
- System administrator—To provide FTP and operator privileges, and also allow the user to log in through the service console, use an authorization flag of 0x47. You must also specify the root directory. If you define one user with administrator privileges, all users will be prompted for a username and password when they attempt to access the Wireless Router through the service console. If you do not define any system administrator users, any user can access the Wireless Router through the service console.

2.2 Configuration Worksheet

Complete the worksheet in Table 2-6 for each router in your network. Table 2-7 provides a sample completed worksheet for your reference. This sample worksheet contains the values that are used in the sample configuration file in Chapter 3.

Table 2-6 Blank Configuration Worksheet

Global Parameters			
Router hostname: ________			
Router IP address: ________			
SNMP community: ________		Community access: ________	
System contact: ________		System location: ________	
Radio Parameters			
Radio model: (Circle one)	L-band	S-band	
Symbolic interface name: ________		Link-layer address: ________	
Channel number: (S-band: 1-15; L-band: 1-9) ________		Power: ________	PN code: (1–8) ________
Ethernet Interface Parameters			
Symbolic interface name: ________		IP address: ________	
Mask address: (decimal) ________		Subnet mask: (bits) ________	
DNS Information			
Domain name: ________			
Name server IP address: ________			
Routing Information			
Dynamic routing: (Circle one)	Yes	No	
Default router address: ________		RIP neighbor address 1: ________	
		RIP neighbor address 2: ________	
Users			
• User 1:	Username: ________	Password: ________	
Privileges: (Circle all that apply)	FTP (0x07)	Operator (0x10) PPP (0x20)	Administrator (0x47)
• User 2:	Username: ________	Password: ________	
Privileges: (Circle all that apply)	FTP (0x07)	Operator (0x10) PPP (0x20)	Administrator (0x47)

Table 2-7 Sample Completed Configuration Worksheet

Global Parameters			
Router hostname:	*TAL*		
Router IP address:	*192.168.0.1*		
SNMP community:	*public*	Community access:	*read-only*
System contact:	*John Doe*	System location:	*TAL*
Radio Parameters			
Radio model: (Circle one)	L-band	S-band	
Symbolic interface name:	*radio0*	Link-layer address:	*0x7D10FFFF*
Channel number: (S-band: 1-15; L-band: 1-9)	*5*	Power: *1 mW*	PN code: (1–8) *5*
Ethernet Interface Parameters			
Symbolic interface name:	*ether0*	IP address:	*192.168.0.1*
Mask address: (decimal)	*255.255.255.0*	Subnet mask: (bits)	*24*
DNS Information			
Domain name:	*yourdomain.com*		
Name server IP address:	*198.41.0.4*		
Routing Information			
Dynamic routing: (Circle one)	Yes	No	
Default route address:	*192.168.0.2*	RIP neighbor address 1:	
		RIP neighbor address 2:	
Users			
• User 1:	Username: *operator*	Password: *faux*	
Privileges: (Circle all that apply)	FTP (0x07)	Operator (0x10)	PPP (0x20) Administrator (0x47)
• User 2:	Username: *admin*	Password: *super*	
Privileges: (Circle all that apply)	FTP (0x07)	Operator (0x10)	PPP (0x20) Administrator (0x47)