# Chapter 3: DataPower as a Network Device

Add a note hereThe DataPower appliance is fundamentally a network device; it communicates with other nodes on an IP network. Networking really matters; IP networking settings have to be correct before anything else. Working from the bottom of the stack up, IP connectivity is required for HTTP connections, matching actions, processing policies, and any other interaction with the device to be possible.

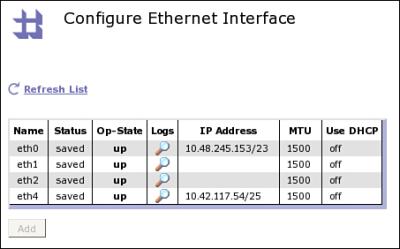
Add a note hereIf you are already well versed in IP networking, or if you simply need to configure the device using settings provided by your network administrator, this chapter covers the basic configuration of the network stack. [Chapter 4](http://www.books24x7.com/assetviewer.aspx?bkid=30903&destid=403#403), [“Advanced DataPower Networking,”](http://www.books24x7.com/assetviewer.aspx?bkid=30903&destid=403#403) contains more theory and a more detailed look at advanced scenarios for those who want to learn more about networking and how the device behaves as part of a network.

**Add a note here****Interface Configuration**

Add a note hereThis section discusses how to configure the device’s network interfaces. We assign IP addresses and netmasks, show how to control low-level TCP/IP settings, configure the routing table with both static and dynamic routes, and so on. If you don’t know what any of these configuration steps mean, don’t worry! Remember, this chapter is focused on configuration. [Chapter 4](http://www.books24x7.com/assetviewer.aspx?bkid=30903&destid=403#403) explains the theory and terminology.

Add a note hereDataPower appliances come with four physical network interfaces, referred to as eth0, eth1, eth2, and eth4. The eth4 interface is also referred to as mgmt0 and is often used as a management interface, although it is almost identical to the other three interfaces. The biggest difference is that if you do not explicitly assign an IP address to the Secure Shell (SSH) service, it first attempts to bind to the management interface, and only if this interface has not been explicitly defined will it bind to 0.0.0.0, which means it will listen on all configured interfaces.

Add a note hereConfiguration of the network interfaces of the device is carried out in the default domain, by clicking on Network→Interface→Ethernet Interface in the Navigation Bar on the left side (see Figure 3-1).

[](javascript:PopImage('IMG_30','http://images.books24x7.com/bookimages/id_30903/03fig01.jpg','453','282'))  
Add a note hereFigure 3-1: Network interfaces.

Add a note hereThis appliance in Figure 3-1 has two network interfaces configured: eth0 and eth4. The summary page shows the IP address and netmask in CIDR format.

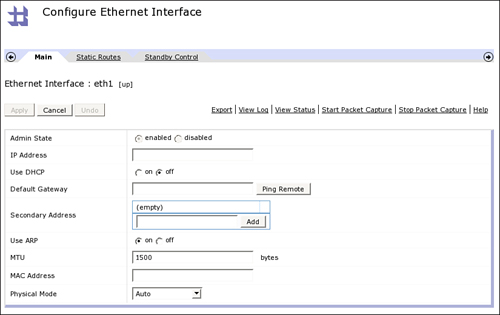
**Tip: Drinking CIDR?**

Add a note hereCIDR, pronounced “Cider,” is a way of expressing variable length subnet masks by simply stating the number of masking bits. It is usually shown by suffixing an IP address with the character / and the number—for instance the 10.48.245.153/23 in Figure 3-1. For more details on subnet masks, see [Chapter 4](http://www.books24x7.com/assetviewer.aspx?bkid=30903&destid=403#403).

Add a note hereVirtual LAN sub-interfaces, utilizing the IEEE 802.1Q tagging protocol, can also be created and configured in a similar manner to Ethernet interfaces, using Network→Interface→VLAN Sub-interface. These sub-interfaces are attached to a physical Ethernet interface, and multiple VLAN sub-interfaces can be created on a single Ethernet interface. More on VLAN sub-interfaces can be found in [Chapter 4](http://www.books24x7.com/assetviewer.aspx?bkid=30903&destid=403#403).

Add a note hereTo modify the Ethernet settings, users must have appropriate permissions. The access profile must include access to the Ethernet interface under the Network section for the device. [Chapter 12](http://www.books24x7.com/assetviewer.aspx?bkid=30903&destid=2003#2003): [“Device Administration,”](http://www.books24x7.com/assetviewer.aspx?bkid=30903&destid=2003#2003) shows in detail how to grant these permissions.

Add a note hereAssuming that the user has the correct permissions, clicking the name of an interface leads to the configuration screen for that interface. If you click eth1, you will see the screen displayed in Figure 3-2; it controls the configuration for the interface. The example in Figure 3-2 deals with the configuration of the interface eth1. The settings make changes to the behavior at both the data link layer and the network layer.

[](javascript:PopImage('IMG_31','http://images.books24x7.com/bookimages/id_30903/03fig02_alt.jpg','825','520'))  
Add a note hereFigure 3-2: Configuration screen for interface eth1.

Add a note hereEach of the settings can be configured on the main interface tab, which is explained in more detail in Table 3-1.

| Add a note hereTable 3-1: Explanation of Interface Configuration Settings  [[http://www.books24x7.com/images/b24-bluearrow.gif](http://www.books24x7.com/outputobject.asp?bookid=30903&chunkid=606573916&objectid=ch03table01&objecttype=spreadsheet)Open table as spreadsheet](http://www.books24x7.com/outputobject.asp?bookid=30903&chunkid=606573916&objectid=ch03table01&objecttype=spreadsheet) | |
| --- | --- |
| **Add a note hereSetting** | **Add a note hereExplanation** |
| Add a note hereIP Address | Add a note hereThe main IP address assigned to this interface, followed by the subnet mask. The subnet mask can be in CIDR format (Classless Inter-Domain Routing) as a suffix onto the end of the IP address or in dotted quad format, in which case it must be separated from the IP address with a space. |
| Add a note hereUse DHCP | Add a note hereThis setting determines whether the Dynamic Host Configuration Protocol (DHCP) should be used to configure this interface. Because these are server class appliances, it is unlikely that DHCP would be used, but if it is needed (for instance in an environment where DHCP is mandated and static leases are assigned for accounting purposes), it is available. |
| Add a note hereDefault Gateway | Add a note hereThe node that should be the default gateway address for this interface. For the vast majority of configurations, there should only ever be one interface that is configured with a default gateway (also known as default router). Some more complex scenarios, which may necessitate more than one default gateway, are discussed in greater detail in [Chapter 4](http://www.books24x7.com/assetviewer.aspx?bkid=30903&destid=403#403). |
| Add a note hereSecondary Address | Add a note hereThis is a list of “secondary addresses” or IP aliases that are assigned to this interface. The appliance responds on this interface to an Address Resolution Protocol request for any IP address configured here. Important: This is different than having more than one interface! This setting configures more than one address on a single interface. IP aliasing is a powerful concept which is often used to have multiple services listening on the same port (e.g. port 80 or port 443); [Chapter 4](http://www.books24x7.com/assetviewer.aspx?bkid=30903&destid=403#403) contains an example of where they might be used. |
| Add a note hereUse ARP | Add a note hereThis setting specifies whether the appliance should respond to Address Resolution Protocol (ARP) requests for this interface. It is likely that this should be left to the default of On. This is discussed in more detail in [Chapter 4](http://www.books24x7.com/assetviewer.aspx?bkid=30903&destid=403#403). |
| Add a note hereMTU | Add a note hereThe Maximum Transmission Unit (MTU) is the size of the largest packet that the Ethernet interface should process. The default of 1500 is the largest allowed by the Ethernet protocol, but there may be valid reasons for reducing this. Only change this setting if told to by your network administrator. |
| Add a note hereMAC Address | Add a note hereThis setting enables you to override the hardware address of the interface. This is discussed further in [Chapter 4](http://www.books24x7.com/assetviewer.aspx?bkid=30903&destid=403#403); it is unlikely that you will need to change this. |
| Add a note herePhysical Mode | Add a note hereChoose the form of negotiation for the physical link speed of the interface. The default of Auto may be right, but this is the single most commonly changed “advanced” setting on this screen and your network administrator may require it to be explicitly set. |

**Tip: Physical Modes**

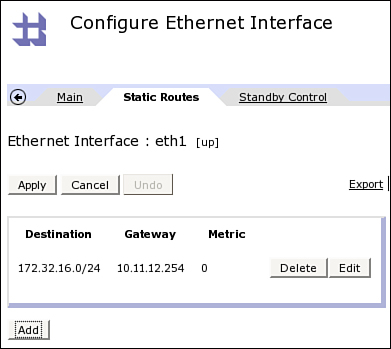
Add a note here[Chapter 4](http://www.books24x7.com/assetviewer.aspx?bkid=30903&destid=403" \l "403" \t "_parent) goes into more detail on the Physical layer, but this setting is worth highlighting here. Most times, auto-negotiation will be fine—but when it isn’t, things can go wrong!

Add a note hereIf you use auto-negotiation, it should be set on both ends. Sometimes, having one side try to auto-negotiate where the other side is set to a fixed speed can end in complete failure to communicate. Also, some specific switches have issues auto-negotiating with newer hardware. If you appear to be getting bad network performance, no link light, packet loss, CRC errors, or the like, this is the setting you should check first!

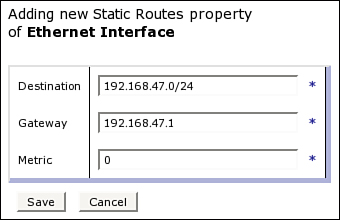
**Static Routes**

Add a note hereNetwork devices maintain an in-memory table of rules that are used to decide how to send traffic to other nodes. These rules are called routes. Many routes are generated dynamically based on the configuration of interfaces, but sometimes there is a need to explicitly add a static entry.

Add a note hereThe second tab on the interface configuration settings page is where you define static routes. This Static Routes tab, as depicted in Figure 3-3, enables you to enter for this interface any static routes that your network administrator may have defined. This is an option not to be taken lightly—an incorrect routing configuration can possibly make the device inaccessible from the network, or even worse can create problems with inconsistent symptoms, which are extremely difficult to debug! [Chapter 4](http://www.books24x7.com/assetviewer.aspx?bkid=30903&destid=403#403) goes into more detail on routing configuration and static routes and where they might be useful—for now only add entries to this tab if your network administrator has asked you to, or if you know what you are doing!

  
Add a note hereFigure 3-3: Static Routes configuration.

Add a note hereIf you do need to add a static route, click the Add button. On the screen that appears, shown in Figure 3-4, type in the destination with subnet mask (either in CIDR format or as dotted quads separated by a space). Also supply the gateway for each static route for this interface.

  
Add a note hereFigure 3-4: Adding new Static Routes.

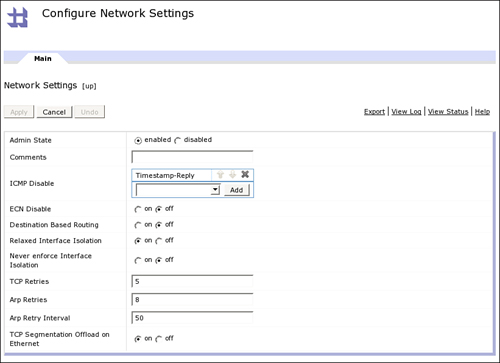
Add a note hereThe metric field is used to differentiate between routes that match for the same destination; if there are two possible routes to a given destination (as will be explained in [Chapter 4](http://www.books24x7.com/assetviewer.aspx?bkid=30903&destid=403#403)), the one with the lowest number is used.

**Other Network Settings**

Add a note hereThis section describes a number of other network settings that can be configured but that are not specific to a given interface. These include general network settings and DNS settings.

**Add a note here****General Network Settings**

Add a note hereIn addition to the interface-specific configuration settings shown earlier, there are also a number of general network configuration settings that are accessed by clicking Network→Interface→Network Settings in the Navigation Bar on the left side of the console. These settings are shown in Figure 3-5.

[](javascript:PopImage('IMG_34','http://images.books24x7.com/bookimages/id_30903/03fig05_alt.jpg','821','596'))  
Add a note hereFigure 3-5: General network settings affecting all interfaces.

Add a note hereThe settings in this configuration panel are global settings; that is, they affect the behavior of all the interfaces on the device. These settings are more advanced, and it is unlikely that you will need to change any of them. The safest route is to leave them as defaults unless you know exactly what you are doing. Nonetheless, if your network administrator asks whether you are capable of changing the number of TCP retries, you can consult Table 3-2, where each of these settings are explained, and say yes!

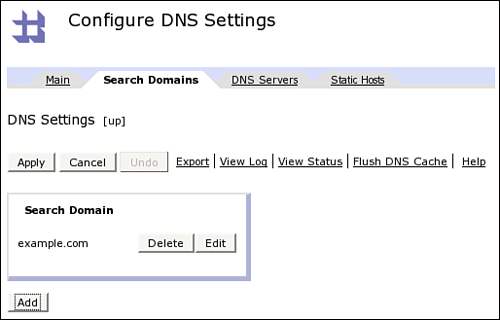
| Add a note hereTable 3-2: Explanation of General Network Settings  [[http://www.books24x7.com/images/b24-bluearrow.gif](http://www.books24x7.com/outputobject.asp?bookid=30903&chunkid=890018785&objectid=ch03table02&objecttype=spreadsheet)Open table as spreadsheet](http://www.books24x7.com/outputobject.asp?bookid=30903&chunkid=890018785&objectid=ch03table02&objecttype=spreadsheet) | |
| --- | --- |
| **Add a note hereSetting** | **Add a note hereExplanation** |
| Add a note hereICMP Disable | Add a note hereThis configuration option allows you to stop the device from responding to ICMP (Internet Control Message Protocol) requests of various kinds. For instance, you may want the device to ignore ICMP Echo Requests or “pings,” which can be configured here. |
| Add a note hereECN Disable | Add a note hereChoose to disable Explicit Congestion Notification TCP sessions. These are used by default, and changing this only affects new TCP sessions because ECN is negotiated at TCP connection establishment during the initial SYN phase. Sometimes network switches and routers have trouble with ECN, although this usually applies to older network hardware; if there are unexplained network problems, try turning on this option, although it should be disabled again if it doesn’t fix the problem. It is unlikely that you will need to change the default setting here. |
| Add a note hereDestination Based Routing | Add a note hereBy default, DataPower appliances send responses to incoming requests via the interface to which a given service is bound, or via the interface on which the incoming request was received if the service is bound to multiple addresses. By setting Destination Based Routing to On, we can enable different behavior where outbound packets for responses are sent using the best possible path to a client irrespective of which interface the request was received on. This is a legacy setting which in most cases should not be enabled. |
| Add a note hereRelaxed Interface Isolation | Add a note hereGenerally speaking, packets will only be accepted on an interface if they are addressed to an IP address on that specific interface. Putting this setting to On will relax this isolation, such that the packet will be accepted if the destination IP address is on the same subnet as one of the addresses on the interface. This option is intended for use with the Destination Based Routing option in the previous entry and in most cases should not be enabled. |
| Add a note hereNever Enforce Interface Isolation | Add a note hereThis setting relaxes the interface isolation described in the previous entry even more, such that any packet with the destination MAC address will be accepted irrespective of the IP address set as the target of the packet. Note that the IP stack will still not handle the packet unless the address is configured somewhere on the device. This option could be used to, for instance, have a “hidden” IP address that does not respond to ARP requests but will be accepted if the address is spoofed onto a packet with the correct MAC destination address. In most instances, you will not need to change the default setting here. |
| Add a note hereTCP Retries | Add a note hereConfigure the number of times the device will try to open a new TCP connection with a SYN packet before giving up. The default of 5 is usually fine for most deployments; modifying this setting changes the time required to detect failures at the network layer. |
| Add a note hereARP Retries | Add a note hereConfigure the number of times the device will try to find the MAC address for a specific IP address using the Address Resolution Protocol (ARP). The default of 8 is usually enough to allow normal network devices to respond and should only be modified where necessary; modifying this setting changes the time required to detect failures at the network layer. |
| Add a note hereARP Retry Interval | Add a note hereThe amount of time, in milliseconds, to wait before trying an ARP request again; the 50 millisecond default along with the default 8 attempts gives a 400 millisecond default total time to respond, which should be enough for most networks; modifying this setting changes the time required to detect failures at the network layer. |
| Add a note hereTCP Segmentation Offload on Ethernet | Add a note hereTCP segmentation offloading is a method of improving the performance of large TCP data transfers by allowing the hardware to split the data up into packets as opposed to allowing the application to do so itself. This setting is enabled by default and should only be disabled in response to specific problems. For instance, in some use cases, TCP segmentation offloading might cause interface resets and other network inconsistencies, and in those cases this setting should be disabled. |

**Add a note here****DNS Settings**

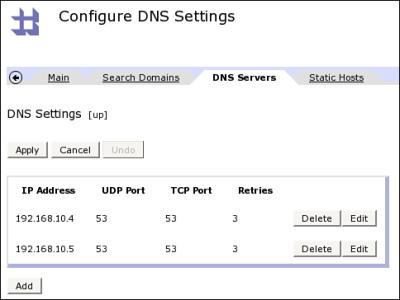
Add a note hereThe Domain Name Service is a way of resolving hostnames to IP addresses, or vice versa. It is possible to configure the DataPower appliance to utilize one or more DNS servers. This may or may not be needed for your environment. Making the appliance dependent on any external service is always adding an element of risk; if there is no *requirement* for an external DNS server, simply do not configure one. If you choose to configure a DNS server, select Network →DNS Settings from the Navigation Bar on the left side. Doing so brings up the screen shown in Figure 3-6.

[](javascript:PopImage('IMG_35','http://images.books24x7.com/bookimages/id_30903/03fig06_alt.jpg','822','292'))  
Add a note hereFigure 3-6: DNS configuration.

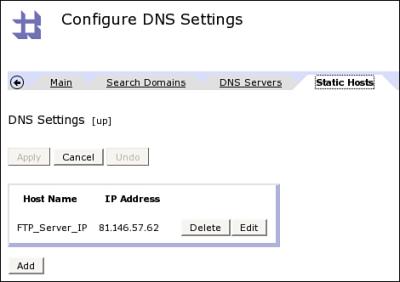
Add a note hereDNS configuration consists of domain stems, which are automatically added to the search if you search by a hostname, along with DNS server configuration and static hosts information. The search domains, shown in Figure 3-7, are the DNS name stems to add if looking up a hostname without a domain name. In the example, if you are on this particular device to perform a DNS look up for say the hostname “www,” this domain name would be appended to make the lookup search for “[www.example.com.](http://www.example.com)”

[](javascript:PopImage('IMG_36','http://images.books24x7.com/bookimages/id_30903/03fig07_alt.jpg','514','329'))  
Add a note hereFigure 3-7: Search domain configuration.

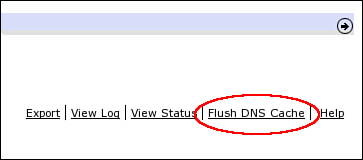
Add a note hereThe next tab, depicted in Figure 3-8, defines the actual DNS servers to be used. They are used in the order included on the screen. The configuration consists of the IP address of the server to use, the port for UDP and TCP connection, and the number of times to retry a failed lookup before giving up.

[](javascript:PopImage('IMG_37','http://images.books24x7.com/bookimages/id_30903/03fig08.jpg','484','364'))  
Add a note hereFigure 3-8: DNS server configuration.

Add a note hereThe last tab is for defining static hosts. These are the equivalent of entries in a hosts file on a distributed operating system—hostnames that are resolved locally on the device to a fixed IP address. The example in Figure 3-9 shows a single hostname, FTP\_Server\_IP, which when resolved on the device will always return the IP address 81.146.57.62.

[](javascript:PopImage('IMG_38','http://images.books24x7.com/bookimages/id_30903/03fig09.jpg','470','332'))  
Add a note hereFigure 3-9: Static hosts settings.

Add a note hereThere is one more important option on the DNS settings page, located on the right side of each tab: the Flush DNS Cache option, as shown in Figure 3-10. Like the vast majority of DNS clients, the DataPower appliance will cache DNS responses locally, and if it needs to look up the same hostname again, it will retrieve it from cache rather than contacting the DNS server again. You can see this cache information by clicking on Status→DNS Cached Hosts on the Navigation Bar. Sometimes, however, you need to be able to make certain that the next lookup goes to the DNS server—for example, if the entry on the server has been updated. This can be done by clicking Flush DNS Cache.

  
Add a note hereFigure 3-10: Click to flush the DNS cache

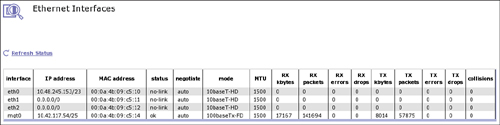
**Network Status Information**

Add a note hereDataPower SOA appliances can provide a lot of information about the status of the network configuration. This information can be invaluable in debugging network issues. This section lists the key tools available to examine the internal workings of the IP stack. If the concepts in this section are not familiar to you, please see [Chapter 4](http://www.books24x7.com/assetviewer.aspx?bkid=30903&destid=403#403).

**Add a note here****Interface Status**

Add a note hereIf you click on Status→Ethernet Interfaces, you can see information about the way that the interfaces have been configured.

Add a note hereAs Figure 3-11 shows, it is possible at a glance to see which interfaces are physically connected, what negotiation mode and speed they have used, IP addresses configured, hardware addresses, received and sent bytes and packets, and so on. One of the chief uses for the interface status page is to debug network errors. Collisions of packets on the network or even packets being dropped can have a serious effect on the function of the device. This behavior may be related to, for instance, a failure to correctly negotiate network speed, as described earlier.

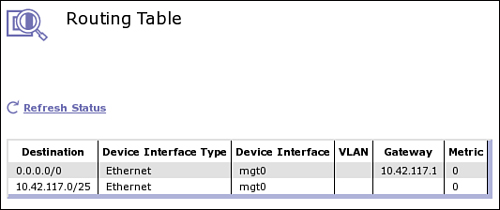
[](javascript:PopImage('IMG_40','http://images.books24x7.com/bookimages/id_30903/03fig11_alt.jpg','1070','267'))  
Add a note hereFigure 3-11: A lot of information is available about the state of network interfaces.

**Tip: DHCP**

Add a note hereWhile it is unlikely you will use DHCP on this enterprise server class appliance, if you do then the Interface Status page is the only way in the GUI to determine the IP address that has been negotiated via DHCP on an interface.

**Add a note here****Routing Table**

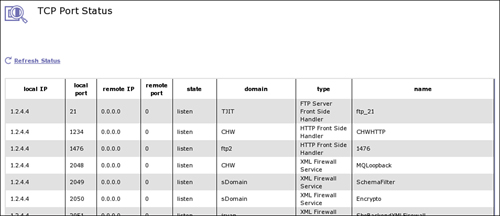
Add a note hereNetwork devices such as the DataPower appliance maintain an in-memory routing table; a list of rules that define how packets should be sent based on the destination addresses. The device’s routing table can be displayed by clicking Status→Routing Table, as shown in Figure 3-12.

[](javascript:PopImage('IMG_41','http://images.books24x7.com/bookimages/id_30903/03fig12_alt.jpg','533','224'))  
Add a note hereFigure 3-12: The routing table can be displayed.

Add a note hereThe information in the routing table includes any specific routes that relate to a given interface, any default routes that have been configured, and any static routes that have been added. More information on routing can be found in [Chapter 4](http://www.books24x7.com/assetviewer.aspx?bkid=30903&destid=403#403).

**Add a note here****TCP Port Status**

Add a note herePossibly the most-often used network status screen is the TCP Port Status. This is the equivalent of a netstat -an on a distributed platform. It lists the TCP sockets on a given device, what state they are in, what the source and destination addresses and ports are, and so on. If you look for just the sockets that are in “listen” state, you can see all the services that are active on a device, which domain they are in, and what port/interface they are bound to. Figure 3-13 demonstrates this extremely useful functionality.

[](javascript:PopImage('IMG_42','http://images.books24x7.com/bookimages/id_30903/03fig13_alt.jpg','954','413'))  
Add a note hereFigure 3-13: TCP port status.

Add a note hereThe most important use of this screen is to check which services are listening on which ports. There can only be a single service (such as an XML Firewall or a Front Side Handler) listening on a given IP address and port combination; if due to a misconfiguration or miscommunication, two services have been configured to listen on the same IP address and port, only the first one that tries to bind will be able to start. Using the TCP port status screen, if a service is down we can easily check to see whether another service is using its IP address and port combination, to see whether that is the reason the service didn’t start.

**Add a note here****ARP Table**

Add a note hereThe Address Resolution Protocol (ARP) resolves IP addresses to physical Ethernet addresses. As with most nodes on an IP network, the device maintains an ARP cache, and you can list the current cache of nodes for which ARP has completed in the ARP table, like arp -a on distributed platforms. The ARP table can be displayed using the show netarp command in the CLI, as in Listing 3-1.

Add a note hereListing 3-1: Address Resolution Table

Add a note herexi50# show netarp

IP address MAC address Interface Interface Type VLAN

---------- ----------- --------- -------------- ----

192.168.10.4 00:15:2c:b2:ac:00 eth0 Ethernet

192.168.10.114 00:1e:37:90:3c:af eth0 Ethernet

xi50#

Add a note hereThe device’s ARP cache contains the hardware addresses of all the nodes with which the appliance communicates. This particular device contains only two hosts in its ARP cache, because there are only two other nodes currently communicating with it.

## Network Configuration Checklist

Add a note hereHow should the network interfaces be configured? The following set of starter questions can be asked of your network administrator to provide the basic information required:

* Add a note hereHow many of the four network interfaces on my device should I configure? Note that it is common for production servers to have more than one.
* Add a note hereFor each interface, what is the IP address and netmask that I should use? Ideally, ask for the netmask in CIDR format—or read the [next chapter](http://www.books24x7.com/assetviewer.aspx?bkid=30903&destid=403#403) to find out what that means and how to calculate it!
* Add a note hereWhat should the default gateway be, and which interface should it use? It is most likely that only one default gateway should be configured.
* Add a note hereDo I need to configure any static routes, and if so what are they?

Add a note hereThese four simple questions coupled with the rest of the configuration information in this chapter will give you all the information you need to successfully configure networking on the device.

## Summary

Add a note hereThis chapter explained the basic use of the administrative console for configuring the main networking features of the DataPower device. [Chapter 4](http://www.books24x7.com/assetviewer.aspx?bkid=30903&destid=403#403) goes into more detail about networking and describes some of the advanced networking configuration that the appliance is capable of.