Converged Network Analyzer Fundamentals Guide
for the Converged Network Analyzer (CNA), Adaptive Path Controller-Enterprise (APC-E), Adaptive Path Controller-Internet (APC-I), and the CNA Server Products

Version 4.1
Copyright 2008, Avaya Inc.
All Rights Reserved

This document contains information related to CNA software (as defined below) and Documentation ("Product"). "Documentation" means this document and Avaya's information manuals in printed or electronic form containing operating instructions and performance specifications that Avaya or its suppliers generally make available to users of its products, and which Avaya delivers to End User with the Products. "End User" means any customer of Avaya or its authorized resellers, or any end user of the Product. See the Software and Documentation DVD/CD inserts for additional legal and licensing information.

Notice
Changes and corrections to the information in this document may be incorporated in future releases.

Disclaimer
Avaya, its affiliates or subsidiaries ("Avaya") are not responsible for any modifications, additions or deletions to the original published version of the Documentation unless such modifications, additions or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants, directors, officers, and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to the Documentation to the extent made by the End User.

Warranty
Avaya provides a limited warranty on the Product. Refer to your customer sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for the Product, while under warranty, is available through the following web site: http://www.avaya.com/support

License
USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE AT: http://www.avaya.com/support ("GENERAL LICENSE TERMS"). DO NOT USE THE PRODUCT IF YOU DO NOT WISH TO BE BOUND BY THE GENERAL LICENSE TERMS. IN ADDITION TO THE GENERAL LICENSE TERMS, THE FOLLOWING LICENSE TERMS AND RESTRICTIONS WILL APPLY TO THE PRODUCT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. "Hardware" means the standard hardware products, originally sold by Avaya and ultimately utilized by End User.

If your system is running in a TDM environment, the following license restriction applies:

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

If your system is running in an IP environment, the following license restriction applies:

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

For all systems, the following license restriction applies:

Shrinkwrap License (SR). With respect to Software that contains elements provided by third party suppliers, End User may install and use the Software in accordance with the terms and conditions of the "shrinkwrap" or "clickwrap" license accompanying the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User's request (see "Copyright" below for more information).

Copyright
Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Certain Software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on Avaya's web site at http://support.avaya.com/ThirdPartyLicense.

The disclaimers of warranties and limitations of liability set forth in the Third Party Terms do not affect any express warranty or limitation of liability that may be provided to you by Avaya pursuant to the license terms covering the Product contained in a separate written agreement between you and Avaya. To the extent there is a conflict between the General License Terms or your customer sales agreement and any Third Party Terms, the Third Party Terms shall prevail solely for such Third Party Components.

Security and virus disclaimer
End User's decision to acquire products from third parties is End User's sole responsibility, even if Avaya helps End User identify, evaluate or select them. Avaya is not responsible for, and will not be liable for, the quality or performance of such third party products or their suppliers. ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO END USER' SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Avaya does not warrant that this Product is immune from or will prevent unauthorized use of telecommunication services or facilities accessed through or connected to it. Avaya is not responsible for any damages or charges that result from either unauthorized uses or from incorrect installations of the security patches that are made available from time to time.

Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to securityalerts@avaya.com.

Trademarks
All trademarks identified by ® and ™ are registered trademarks or trademarks of Avaya Inc. All other trademarks are the property of their respective owners.
Contents

BGP on the Engine Module .................................................. 31
Assigning USTATs to Providers ........................................ 34

Index ................................................................................. 39
Chapter 1: Introduction

In this chapter

- About CNA
- Intended audience
- Documentation library
- Typographic Conventions
- System requirements
- Supported browsers and operating systems
- Subnet Integration

About CNA

The Avaya Converged Network Analyzer (CNA) product line includes performance reporting and dynamic routing solutions. This product line includes Converged Network Analyzer (CNA), Adaptive Path Controller-Enterprise (APC-E), Adaptive Path Controller-Internet (APC-I), VoIP Monitoring Manager, Chatter, and the CNA Server. The CNA product line can be configured to do any or all of the following:

- improve the Internet experience of your customers, by speeding the return of packets being downloaded from your web servers
- improve the Internet experience of your local network users, by optimizing the routes used to deliver their requests to external web sites
- improve the speed and reliability of your Internet VPN connections
- optimize your cost of service, by distributing traffic load among your service providers according to individual ISPs' billing rates (see polling usage interval in the CNA Command Reference Guide) and traffic thresholds
- selection of service provider (SP) for a given subnet on its analysis of measured traffic, not on statistical assumptions (load balancing) or the predefined rules of the Border Gateway Protocol (BGP).
- selected service provider link is observed to be experiencing significant delays that degrade its ability to deliver packets to a specific subnet, the product line can—if you allow
Introduction

it—update your network routing tables so that your routers will use a different service provider for traffic to that subnet.

● configure the system to favor the lowest-cost or the least utilized service provider.

● use the system in report only mode, in which traffic is measured and analyzed but routes are not actually asserted to your edge routers.

Intended audience

This document is intended for use by IP administrators. You should have a detailed knowledge of how IP subnets work, including an in-depth familiarity with the Border Gateway Protocol (BGP).

Documentation library

You can download the following documents at http://support.avaya.com:

Table 1: Documentation library

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Document No.</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNA Installation Guide</td>
<td>14-300539</td>
<td>● Hardware specifications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Installing a CNA server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Installing a CNA Agent Device</td>
</tr>
<tr>
<td>CNA Fundamentals Guide</td>
<td>14-601298</td>
<td>● Product overview</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Configuration fundamentals</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Configuring a new CNA server</td>
</tr>
<tr>
<td>CNA Monitoring Guide</td>
<td>14-601299</td>
<td>Current path monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Collecting endpoint addresses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Server-based measurement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Agent-based measurement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Decision policies and application models</td>
</tr>
<tr>
<td>Adaptive Path Controller-Enterprise Guide</td>
<td>14-601303</td>
<td>● Adaptive path control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● High availability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● WAN cost and load optimization</td>
</tr>
</tbody>
</table>
## Table 1: Documentation library (continued)

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Document No.</th>
<th>Content</th>
</tr>
</thead>
</table>
| Adaptive Path Controller-Internet Guide | 14-602423      | • Configuring your routers  
                                    |                           | • Polling routers         |
|                                       |                | • VPN integration                                                       |
| CNA Operator Guide                    | 14-601304      | • Web interface                                                        |
|                                       |                | • Server-based measurement reports                                     |
|                                       |                | • Agent-based measurement reports                                       |
| CNA Appendices                        | 14-601329      | • Diagnostic tools                                                     |
|                                       |                | • Supported MIBs                                                        |
|                                       |                | • Upgrade procedure                                                     |
|                                       |                | • Migrating configuration files between hardware models                 |
|                                       |                | • API                                                                   |
| CNA Command Reference Guide           | 14-300540      | Describes all CLI commands for the CNA server.                           |
| CNA Release Notes                    |                | • New features                                                          |
|                                       |                | • Supported hardware platforms, browsers, and operating systems         |
|                                       |                | • Resolved issues                                                       |
|                                       |                | • Known issues                                                          |

To set up user accounts for the web site's Support area, call:

- 1 (877) 733-5511 in the United States
- 001 (978) 552-0444 outside of the United States

Or you can send an e-mail message to support@avaya.com.
### Typographic Conventions

Table 2 shows the typographical conventions that are used in this book:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| **Courier type** | The Courier type face is used to denote one of the following:  
  ● Text as displayed on a monitor  
  ● Command syntax examples. |
| **bold** | Bold text denotes command keywords (words that must be entered exactly as shown). |
| **italics** | Italics can mean any of the following:  
  ● filenames  
  ● book titles  
  ● command argument names and values  
  ● new terms not commonly understood |
| **<>** | Words enclosed in angle brackets should be replaced by user-specific data. In the following example, the words *userid* and *password* should be replaced by actual user ID and password values:  
  Login: `<userid>`  
  Password: `<password>` |
| **[]** | Square brackets are used to denote command line arguments that are optional. |
System requirements

The CNA Web client requires Sun’s Java Plug-in 1.5 with update 11. For information about installing the plug-in, see Java Version in Web Interface chapter of the Fundamentals Guide.

Other requirements will vary depending on whether you will be using the CNA system to optimize web or VPN traffic.
Web traffic optimization

If you are using the CNA system to optimize your Web site traffic, your subnet should meet the following requirements:

- Multi-homed connectivity to the Internet (at least two service providers)
- Full BGP feed from at least one of your service providers
- DNS implementation that provides the following:
  - address rotation (ability to round-robin destination addresses in reply to successive requests)
  - high availability, in which the DNS server conducts health checks and won’t return a destination if the target server is not in operation (GSLB—global server load balancer—is strongly recommended, though some form of direct-server return is a viable alternative. For information on getting packets through firewalls, see Active Measurement VIPs in Chapter 4: Server-Based Measurement of the CNA Monitoring Guide. For information on preventing health checks from skewing traffic measurements, see Chapter 6: Decision Policies and Application Models in the CNA Monitoring Guide.
- If Network Address Translation (NAT, as defined in RFC 2663) is in place between the CNA system and your service providers, you must ensure that remote-side responses to CNA measurement-traffic packets arrive at the USTAT’s VIP with original, or natural, addressing intact
- Edge routers must support BGP4 (as defined in RFC 1771 and RFC 1657) and Policy Based Routing (PBR)

VPN optimization

If you are using the CNA system to optimize VPN traffic, your subnet should meet the following minimum requirements:

- Multi-homed connectivity in at least one direction between your headquarters and remote sites (either two Internet service providers, or one ISP and a private line, such as frame relay)
- Edge routers must support BGP4 (as defined in RFC 1771 and RFC 1657) and Policy Based Routing (PBR) or equivalent.
Supported browsers and operating systems

Table 3 shows the browsers and operating systems on which the CNA Web interface has been tested.

Table 3: Supported Browsers, Operating Systems

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Browsers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 2000</td>
<td>Internet Explorer 6.0</td>
</tr>
<tr>
<td>Microsoft Windows XP</td>
<td>Internet Explorer 6.0, 7.0</td>
</tr>
<tr>
<td></td>
<td>Firefox 2.0</td>
</tr>
</tbody>
</table>

Subnet Integration

The CNA system needs three separate channels of communication through your subnet, one for each of the following purposes:

- **management**—subnet protocols (such as http, telnet, ssh, syslog, and snmp)
- **measurement**—test/data stream traffic between remote prefixes and VIPs (virtual IP addresses)
- **control**—IBGP peering between engine services and the edge routers

See Figure 1.
The management connectivity layer needs only as much access to your subnet as you want to give it, based on an assessment of who you want to be able to use the CNA web and command line interfaces. Management access to the device is through the management ethernet port.

The measurement layer must be able to communicate through your edge routers with traffic endpoints, either surfers on the other side of the Internet cloud or your remote VPN sites. USTAT modules and the EFC module must be connected to interfaces on the edge routers. These connections require some form of policy-based routing (PBR). Traffic can be channeled through a GRE tunnel, a VLAN, or a dedicated physical interface, for example. If you use a dedicated physical interface, there can be no routed hops between the CNA port and the edge router. The addresses configured on the CNA system for this purpose (called VIPs, or virtual IP addresses) must not be subject to Network Address Translation (NAT).

The control layer must be able to establish an iBGP peering relationship with your edge routers. TCP connections will be opened between the CNA system to the edge routers. Basic IP is sufficient for this layer. You may also elect to configure active probes using ICMP responses. BGP peering occurs on the engine module.

As long as these conditions are met, it doesn’t matter how you physically connect the CNA system into your subnet.

There are three basic configurations possible, each with its own trade-offs to be considered.

**Outside the Firewall**

If the CNA system is entirely outside of your firewall, the management port, which can provide access to the CNA system via such protocols as http, telnet, snmp and ssh, will be exposed. (Individual protocols can be enabled or disabled by user configuration.)
See Figure 2.

Figure 2: CNA system entirely outside the firewall

Security measures available to you include:

- access lists on the CNA system as well as edge router interfaces
- secure shell (ssh) instead of telnet
- Secure Sockets Layer (SSL)
- authentication (local, RADIUS and TACACS+)


Inside the Firewall

If the CNA system is placed inside your firewall, you will need to provide a GRE tunnel, or some other means of passage through the firewall, for measurement traffic. You must also allow the CNA engine module to establish a BGP peering relationship with your edge routers. See Figure 3.
Across the Firewall

If your organization’s security policies permit it, the device can be configured to work with measurement traffic outside the firewall and the management port inside (engine port can be either). See Figure 4.

The management interface can be protected with access lists implemented on both your firewall and on the CNA system to define the type of access you want to allow through the management ethernet interface.
You can implement access lists on measurement interfaces to deny any traffic other than HTTP. And, you can implement an access list on the engine ethernet interface to allow the edge routers to send packets during BGP sessions.

**Figure 5: CNA system partially inside the firewall**

If you have given your web servers some firewall protection, you can place the CNA device on the same subnet and still be outside of your internal subnet.

---

**Configuration Sequence**

The following sequence of steps presents an abbreviated list of things you need to do to get a newly installed CNA system configured and ready to optimize traffic between your web servers and Internet end users. (In order to optimize VPN traffic, you will also need to configure the CNA system and your edge routers as shown in Chapter 4: VPN Integration of the Adaptive Path Controller-Internet Guide.)

The following list is derived from the steps that are explained in detail in Chapter 3: Configuring a New CNA Server Device of this book and Chapter 2: Configuring Your Routers of the Adaptive Path Controller-Internet Guide.

See the sections listed in parentheses for more detailed information about individual steps.
Note:
This manual addresses the integration of a CNA system into a generic subnet environment. This subnet has been intentionally made simple so that the documentation can focus on the steps required to make the CNA system operational. In an actual, real-world deployment, there will be numerous departures from the simplified subnet presented here, requiring different specific configurations. For example, the steps itemized below call for GRE tunnels between the measurement ports and Cisco edge routers. The actual system requirement is for some form of dedicated link, either virtual or physical, not necessarily a GRE tunnel, and the system will work with brands other than Cisco.

To set up a new CNA system and make it operational, do the following:

1. Install the chassis into a rack. (See the companion document *Avaya CNA Server Installation Guide* for details.)

2. Connect a terminal to the console connector on the management module. (See the companion document *Avaya CNA Server Installation Guide* for details.)

3. Physically connect the ethernet ports to the subnet.

4. Boot your CNA system.

5. Using the console port to connect a terminal to the 5000-series Management module or the 3300-model base unit, configure the FastEthernet interfaces.

6. Configure a default static route for the CNA system’s engine.

7. Configure the engine to recognize your service provider access links.

8. Configure BGP peering with the CNA engine.

9. Associate USTAT modules or 3000-series measurement ports with service provider access links and virtual IP addresses (VIPs), and configure GRE (Generic Routing Encapsulation) tunnels.

10. On your edge routers, configure GRE tunnel interfaces.

11. On your edge routers, configure policy-routing route maps for the GRE tunnels.

12. On your edge routers, configure the routing between your edge routers and the CNA system.

13. On your edge routers, configure IBGP peerings with the CNA system.

14. On your edge routers, configure the CNA system as a route reflector client.

15. To obtain subnet traffic measurements through passive user tests, place HTML image tags in your web pages and configure your DNS server to direct requests for the image to your USTAT modules.

16. To obtain subnet traffic measurements from targeted endpoints are scheduled intervals, configure active probes on the CNA system.

17. On the CNA system, enable the decision-maker process.
Traffic Measurement Data

At this stage, if you have completed all of the steps listed in the Configuration Sequence section, the CNA system should now be operational. The CNA engine will fill its internal database with prefixes obtained from your BGP feed.

Before the CNA system can do anything meaningful with these prefixes, however, it needs to gather data about how fast each of your service providers can pass traffic between your subnet and destinations in each of these prefixes.

The CNA system has two mechanisms for measuring the speed of packet delivery from your web server to individual end users: passive traffic tests and active probes.

You can use either of these methods exclusively, or you can use both simultaneously.

User Traffic Tests

User traffic tests (UTTs) are passive measurements of the time it takes to complete a TCP handshake during the delivery of a single-pixel transparent GIF that has been requested by an Internet user who has contacted your web site. This test requires that you place an HTML image tag somewhere on your web page, and that you configure your DNS server to direct requests for the URL contained in the image tag to one of your USTAT modules.

See Chapter 4: Server-Based Measurement in the CNA Monitoring Guide for more information.

Active Measurement Probes

Active probes are traffic tests that are initiated by the CNA system. You identify a specific host in a subnet of interest and the CNA system will contact it, either by initiating and immediately closing a TCP session, or by sending an ICMP echo request, at regular intervals. The time it takes to complete the opening handshake of the TCP session or complete the ICMP ping is recorded in the CNA database. (You can configure the method used: TCP or ICMP.)

See Chapter 4: Server-Based Measurement in the CNA Monitoring Guide for more information.

NetFlow, SPAN Data Streams

Active measurement targets can be automatically generated from data sent to the optional Endpoint Flow Collection module (EFC) by a NetFlow or SPAN (Switched Port Analyzer) data source.

See Chapter 2: Collecting Endpoint Addresses in the CNA Monitoring Guide for more information.
 Asserting Routes

Once the CNA system has accumulated sufficient data, it can begin choosing the best link to a specific subnet. How much data is sufficient is an option that can be set using the CLI.

However, the CNA system will not assert its choices to your edge routers until you enable route-assert mode. Prior to that time, you can monitor the performance of the CNA system and view the reports it generates to gain insight into the performance of your service provider links.

See Route Assertion in Chapter 3: Adaptive Path Control of the Adaptive Path Controller Guide for more information.
Chapter 2: Configuration Fundamentals

Chapter Contents

- Configuration Overview
- Current Path Configuration
- User Accounts
- Password Recovery
- Data Management
- Email
- Privacy Policies
- Character Set

Configuration Overview

Configuration management is done through a Command Line Interface (CLI), implemented as part of the Converged Network Analyzer (CNA).

Beginning with CNA 3.0, you can configure the device using a template. The template is used to create a complete configuration for monitoring the current path. You can initiate the configuration template by using the `generate-config current path` command.

Once you have initiated the template, enter the appropriate values when prompted. The system will recognize specified values that are used multiple times in the template. You will be prompted once for this specific value to ensure that unexpected errors are not entered.

The system will overwrite the startup configuration with the values entered through the template. Before overwriting the startup configuration, the system will save the configuration with a time stamp and a unique name to identify the file. The unique naming convention is as follows: `startup-config-yyyyymmdd-hhmm.cfg` The saved configuration files will be shown when the `ls cfg` command is executed.

When the template is complete, the prompt asks if you want to save this configuration as your start-up configuration. If you answer yes, the newly generated startup-config is saved. If you answer no, you will be asked whether you want to discard the generated configuration or get one more chance to save it.
The generated configuration will take effect after the next reload as new the running-configuration. You have another chance to undo the changes by executing recover startup-config.

You should save the running configuration as a file in the device repository, as a startup configuration. To do so, use the `copy` command:

```
copy running-config startup-config
```

Entering the command `help` (or its equivalent, the question mark character—?) will display a list of all commands available to you at your current location in the CLI.

The `end` and `exit` commands both move you up one level in the configuration mode hierarchy. That is, if you are in engine configuration mode (`config-engine`), the `end` and `exit` commands will move you to configuration mode (`config`). From configuration mode, the two commands will move you to system operations mode. From there, the `exit` command will close the CLI session while the `end` command will have no effect.

Within one of the command configuration modes (`config-engine` or `config-engine-link`, for example), both the `end` and the `exit` commands will place an `end` statement in the configuration to mark the end of a command block.

The `logout` command will immediately close the current CLI session regardless of where you are in the configuration hierarchy.

The CLI responds to several control-key and escape-key combinations which help move the cursor on the command line, and perform simple character-manipulation tasks such as converting between upper and lower case.

To see the complete list of these key combinations, enter `help edit` on the command line.

---

### CNA API

CLI commands can also be entered into the CNA configuration through a client program, using the CNA Application Programming Interface (API). See the CNA Appendices.

---

### Current Path Configuration

Beginning with CNA 3.0, you can configure the Current Path mode using a template. The template is used to create a complete configuration for monitoring the current path. You can initiate the configuration template by using the `generate-config current path` command.

Once you have initiated the template, enter the appropriate values when prompted. The system will recognize specified values that are used multiple times in the template. You will be prompted once for this specific value to ensure that unexpected errors are not entered.
The system will overwrite the existing, or running, configuration with the values entered through the template. Before overwriting the running configuration, the system will save the configuration with a time stamp and a unique name to identify the file. The unique naming convention is as follows: running-config-yyymmdd-hhmm.cfg The saved configuration files will be shown when the `ls cfg` command is executed.

When the template is complete, the prompt asks if you want to save this configuration as your start-up configuration. If you answer yes, the newly generated running-config is copied as the start-up config. If you answer no, you will be able to save the configuration by executing the `save memory` command or the `copy running-config startup-config` command.

---

**User Accounts**

There is no default user account.

When you boot a CNA system for the first time, you will be given a command prompt without having to log in, but your terminal must be physically connected to the console port on the management module.

There is no telnet access until you have created at least one user account with the `username` command and set an `enable` password with the `enable password` command.

---

**Password Recovery**

The CNA system has a password recovery mechanism that allows you to obtain a command prompt without logging in through a user account.

To use this feature, you must be connected to the management module’s console port.

Boot the device.

The system will show several startup messages:

```
LILO Loading ...........
Uncompressing ramdisk...
Mounting ramdisk...
INIT: version 2.78 booting
```

Copyright 2001 Avaya, Inc. All rights reserved.
Unauthorized access not permitted.

When you see the `Unauthorized access not permitted` message, you have a two-minute window to enter the following on the command line (followed by the ENTER key):

```
-P
```
During a normal boot (without `-p`), the CNA system will next undergo an initialization process and a series of system startup messages will be displayed:

--- CNA System Startup ---

Initialize logging mechanism [ OK ]
Find installed CNA modules [ OK ]
  slot 0 - management [ OK ]
  slot 2 - engine [ OK ]
  slot 3 - reporting [ OK ]
  slot 4 - ustat [ OK ]
  slot 5 - ustat [ OK ]
Start internal communication servers
Load initial boot configuration
Initialize internal DNS
Apply default access restrictions
Out-of-the-box state
Start NTP and synchronize modules

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

When the password recovery process is initiated, however, the CNA System Startup messages should then be overwritten by the following:

Press Enter to Continue

If you get a login: prompt instead of Press Enter to Continue, you will have to reboot the device and try again.

When you press the Enter key, you will be given a command-line prompt:

CNA>

The running configuration will be empty, but you will have access to your previously saved startup configuration, which you can copy to the running configuration. First, enter the enable command (since your running configuration is empty, there is no password), and then the copy command:

CNA> enable
CNA# copy startup-config running-config

Now use the show running-config command.

You can now locate the username commands which you entered previously to create user accounts. If passwords are displayed in clear text, note your log-in password for future reference.
Or, if you had previously configured the CNA system to not display passwords in clear text, you can re-enter the **username** command (enter configuration mode first, with the **configure terminal** command) to change your log-in password:

```
CNA# config t
CNA(config)# username test password test
```

**Note:**

Using the **show startup-config** command to locate a username and password is not enough. You will not be allowed to terminate the CNA session using the **exit** command unless there is a user defined in the running configuration. You must either copy the startup configuration into the running configuration or enter configuration mode (**config**) and create a user with the **username** command before you can exit the CNA session.

---

**Data Management**

The CNA system stores persistent data on a hard drive on the management module. This data includes reports generated hourly from the snapshot image of the live database that is maintained on the engine module; the entire trending database; and trend report template and user-defined query files. You can also create backup copies of the CNA image and startup configuration.

You can manage files on the hard disk from either the CLI or the web interface.

From the CLI, use the **ls** command to see the user-accessible contents of this hard disk, the **backup** command to create backup files and the **restore** command to retrieve data from these backup files and restore them to CNA memory.

In the web interface, use the **Config** menu (or **Config** node in the navigation tree) to open the **Manage Files** and **Backup/Restore** dialogs.

See **Chapter 2: The Web interface** in the **Operator Guide** for more information.

---

**Email**

The CNA system allows you to email a variety of data, including snapshot and trend reports, configurations, and show command output, from either the command line or the management web interface.

You can use the **email** command in the CLI to configure the CNA system to automatically send snapshot reports on a regular schedule.
You can select the **Email** command from the **File** menu in the web interface to send data that is being displayed in the content pane of the web applet.

Before mail can be sent, you need to identify your mail server, either in the CLI or the web interface. The server and port named by the CLI’s `smtp-server` command will be used for all mail, unless you change the server designation in the web interface.

Click the **SMTP Server** button at the bottom of the **E-mail** dialog to change the server name and port. This change is valid for email sent from the applet only; it is not stored on the server and will not affect the automatic mailing of reports. The change will remain in effect as long as the applet continues to run. When you launch a new applet, it will again default to the settings named by the `smtp-server` command.

Data mailed from the applet will be sent to the mail server through the client workstation’s subnet interface.

Reports mailed automatically by the CNA system will be sent through the management module’s `eth0` interface. Image formats (jpeg and png) can be specified with **email format image**.

If you encounter difficulties, verify that both the CNA system’s management module and the workstation in which you run the applet have subnet access to the mail server.

---

**Privacy Policies**

If your organization conforms to the P3P protocol defined by the World Wide Web Consortium ([http://www.w3.org](http://www.w3.org)), you can use the **ip http server header append (deprecated)** command to add a P3P header to the HTTP headers generated by the USTAT web servers.

---

**Character Set**

User-generated text (such things as descriptive text, host names, prefix aliases, group names, and link names, for example) can consist of letters of the alphabet, numerals, hyphens and underscore characters. The first character must be a letter of the alphabet.

You cannot enter more than 256 characters into the CLI for any one command, including keywords.

With a few exceptions, you cannot use any of the following characters in user-defined text:

```
` ; # $ { } ' " < > \
```

The exceptions:

- the single quote character is allowed in a TACACS+ key
• any of these characters can be used in a **match** expression in the **show logging** command

• forward slashes (/), are allowed in filenames, URLs, domain names, and e-mail addresses

• single (’) or double (“) quotes can be used as individual characters in descriptive text and passwords (but not user names, host names, or aliases)

• **all printable characters** can be used in a password, subject to the following:
  
  - If a password contains a space, backslash (\), or exclamation mark (!), then you must quote the entire password (either single (’) or double (“) quotes can be used). Note that a quoted password can not use the same quote symbol as part of the password. E.g., “test 99” could not use double (“) quote as part of the actual password.

  - Examples of legal passwords:
    
    test123
    @#$%^&*()test123_+|~`=-[:;/:,.?><
    “test 1 23”
    ‘test1 23’
    “test ‘1’ 2/3”

If space characters are used in descriptive text blocks, the entire block of text must be enclosed in quote marks. If the text uses a double-quote character, enclose the entire block in single quotes. If the text includes a single-quote character, enclose the entire block in double quotes.

The exclamation mark (!) identifies comment text in configurations. When the CNA system encounters an exclamation mark in text not enclosed in quotes, it will ignore all characters from that point on through the end of the line when parsing the configuration.

To use the exclamation mark as a character in user-defined text, such as a descriptive block, or a password or user ID, enclose the block of text in quotes.

User-defined text is case sensitive; CLI keywords are not.

You can enter **show subnet**, **show SUBNET** or **SHOW subnet**; all will be accepted as valid commands.

However, the CNA system will preserve upper and lower cases for user-generated text. The performance group name **PathControl** is not the same as **pathcontrol**.
Chapter 3: Configuring a New CNA Server Device

Configuring Virtual Module Interfaces

Each software module in the product (with the exception of the reporting module) needs to be associated with an Ethernet interface and a physical connection to your subnet. The reporting module does not require a subnet connection; reports are obtained through the management interface.

Management, engine, USTAT, and EFC modules must use the Ethernet ports assigned to them according to the instructions in the companion document *Avaya CNA Server Installation Guide* and the corresponding labels on the back of the IBM xSeries x306, the IBM xSeries x306M, the IBM xSeries x336, the Dell PowerEdge 850, or the Hewlett Packard DL 320 device.

Once the system has booted and you have connected all of the necessary ports to your subnet, connect a terminal or workstation to the serial console port on the CNA device.

See the *Avaya CNA Server Installation Guide* for information about creating a local user account and enable password on an device that has never been configured.

Log in and enter the enable password.

Configuration Mode

When you have privileged-level access, enter the `configure terminal` command.

**Note:**

The device will also accept `config t`—whenever you enter enough of a keyword to eliminate ambiguity, Avaya CNA will accept it as though you had spelled out the entire word. Alternately, you can enter a partial word—again, just enough to eliminate ambiguity—and use the TAB key to automatically finish entering the complete word on the command line. If you enter `conf` and then press the TAB key, the system will complete the word `configuration` followed by a space character. You can then enter a question mark (?) to obtain a help prompt advising you about acceptable next entries.

The system should now be in configuration (`config`) mode.
Ethernet Interfaces on Modules

Begin by configuring interfaces for the management, engine, and USTAT modules.

To create an interface on the xSeries system, enter the `interface` command while in `config` mode.

Enter `fastethernet` as the `type` argument.

The `num` and `port` arguments correspond with the labeled Ethernet ports on the rear panel of the xSeries device. The `num` argument is always 0 and the `port` argument is the number on the Ethernet (ETH) port labels next to the actual Ethernet ports. The management module, for example, is implemented on port ETH0, identified as 0/0 to Avaya CNA; the engine module uses port ETH1, or 0/1; and the USTAT module is implemented on port ETH2, or 0/2. The port assignments are the same for all supported IBM xSeries platforms. Configuration of the endpoint flow collection (EFC) module is covered in Chapter 2: Collecting Endpoint Addresses of the Monitoring Guide.

For the management interface, enter the command to configure Ethernet 0 as follows:

```
interface fastethernet 0/0
```

This will place the xSeries device into interface configuration mode (the command-line prompt will display `config-if`).

The `type` argument is not case sensitive. The interface type is displayed by Avaya CNA as `FastEthernet`, but you can enter it all in lower case, or with upper case `F` and `E`.

To assign an address to the interface, enter the `ip address` command with a valid IP address and mask from your subnet address space:

```
ip address 176.16.6.4 255.255.255.224
```

Each interface needs a separate IP address. These addresses can come from private address space.

You can add descriptive text as a reminder of what the interface is for, with the `description` command:

```
description "Management Module"
```

End the configuration of this interface with the `end` command:

```
end
```

Repeat the interface command for the engine module:

```
interface fastethernet 0/1
description "Engine Module"
ip address 172.16.6.4 255.255.255.224
end
```
Repeat the command again to create an interface to be used by your USTAT modules, using the 0/2 port:

```
interface fastethernet 0/2
description "USTAT Modules"
ip address 172.16.6.6 255.255.255.224
end
```

When you have finished, your running configuration should contain a block similar to the following (use the `show running-config` command to see the contents of the running configuration):

```
hostname Avaya_ANS

interface FastEthernet 0/0
description "Management Module"
ip address 172.16.6.4 255.255.255.224
end
interface FastEthernet 0/1
description "Engine Module"
ip address 172.16.6.14 255.255.255.224
end
interface FastEthernet 0/2
description "USTAT Modules"
ip address 172.16.6.6 255.255.255.224
end
```

By default, duplex and speed mode for all interfaces is auto. You can change modes with the `duplex` and `speed` commands.

Host name is “Avaya_CNA” by default; you can change this with the `hostname` command.

At this point, since the management module now has an interface and an IP address, you can disconnect the terminal or laptop from the serial port and log in to the management address via telnet.

Later, you can enable ssh and disable telnet, if you prefer to use a more secure remote access protocol, and you can use a web browser once you have enabled the management module’s HTTP server.

For now, however, either remain connected to the serial port or use telnet.

**Default Gateway**

You need to set a default route for the xSeries system so that it knows how to communicate with your subnet. Choose an address on a router that is accessible to your management hosts and, while in `config` mode, enter the `ip route` command:

```
ip route 0.0.0.0 0.0.0.0 172.16.6.3
```
Configuring a New CNA Server Device

This configures a static route for the management module. To avoid routing conflicts (see Static Routes in Appendix E: Migrating Configurations Between Models of the CNA Appendices), you should also enter engine configuration mode and define a static route for the engine module, as well.

From config mode, enter engine configuration mode:

```
module engine
```

Now create another static route, to match up with the up address your subnet administrator has chosen for the engine module (use the ip next-hop for a gateway router that is local to the engine’s subnet):

```
ip route 0.0.0.0 0.0.0.0 172.16.6.4
```

Service Provider Access Links

Each service provider that is to be managed or monitored by Avaya CNA needs a link object defined in the xSeries configuration.

Naming Service Provider Links

To associate a service provider with a link name, first create the link using the link command. While still in engine configuration mode, enter the following:

```
link provider_1
```

The command’s name argument can be anything you want. In the example here, it is provider_1. This name will be used in the output of various CLI commands and web page reports.

Executing the link command places the CLI in config-engine-link mode. Subsequent commands will be applied to this link.

Link AS Numbers, IP Addresses

Execute the provider-as command to associate the provider_1 link with the Autonomous System (AS) number of your service provider and the IP address your provider gave you for BGP peering (the address your edge router is peering with):

```
provider-as 10 172.30.100.33
```
Execute the **end** (or **exit**) command to back out of `config-engine-link` mode, and repeat the sequence for each link that will be managed—name the link, give it the AS number and IP address of your service provider, and back out of `config-engine-link` mode:

```
link provider_2
   provider-as 20 172.29.100.33
end
link provider_3
   provider-as 30 172.28.100.1
end
...  
```

When you have finished, your configuration should contain a block of text similar to this:

```
module engine
   link provider_1
      provider-as 10 172.30.100.33
   end
   link provider_2
      provider-as 20 172.29.100.33
   end
   link provider_3
      provider-as 30 172.28.100.1
   end

BGP on the Engine Module

While still in `config-engine` mode, enter the **bgp** command, with your subnet’s AS number as the **as-num** argument:

```
bgp 65002
```

In addition to adding `bgp 65002` to your running configuration, entering the **bgp** command also places the CLI in `config-engine-bgp` mode.

Enter the **neighbor link** command once for each of your links. The command takes **address** and **name** arguments, in the following form:

```
eighbor <address> link <name>
```

The **address** argument should be an IP address of an interface on the edge router that connects your subnet to the service provider identified by the **name** argument.

For this example, assume you have two edge routers. One of them connects your subnet to the service providers you have called `provider_1` and `provider_2` in the xSeries configuration, and the other edge router connects your subnet to the service provider you have configured as `provider_3`.

The interface you use to connect to the first router has the address 172.16.6.1 and your access interface on the second router is 172.16.6.2.
Your BGP neighbor commands should look like the following:

```sql
neighbor 172.16.6.1 link provider_1
neighbor 172.16.6.1 link provider_2
neighbor 172.16.6.2 link provider_3
```

Next, in order to achieve IBGP peering, you need to associate the router IP addresses with AS numbers, using the `neighbor remote-as` command:

```sql
neighbor 172.16.6.1 remote-as 65002
neighbor 172.16.6.2 remote-as 65002
```

**Note:**

All configured links must be associated to a neighbor. The CNA system does not support routerless links.

The AS number in each of the neighbor statements should be your own BGP AS number—the same number you used with the `bgp` command—so that the xSeries device will establish an IBGP peering relationship with the routers.

Your configuration so far is illustrated in Figure 6.
In the diagram, the engine, management and USTAT ports are all connected to the same subnet. This is not a requirement, as long as the engine module is connected to the edge routers for BGP peering, the USTATs are connected to the edge routers for traffic measurements, and the management module is reachable by anybody who needs access to it.

Your xSeries configuration should contain a block of text similar to this:

```
module engine
    bgp 65002
    neighbor 172.16.6.1 link provider_1
    neighbor 172.16.6.1 remote-as 65002
    neighbor 172.16.6.1 link provider_2
    neighbor 172.16.6.2 link provider_3
    neighbor 172.16.6.2 remote-as 65002
end
end
```
Assigning USTATs to Providers

If you haven’t already done so, back out of engine configuration mode by executing the `end` (or `exit`) command until you are in `config` mode.

Now execute the `module` command, specifying `ustat` for the `type` argument and whatever name you want to use for the first USTAT as the `name` argument. You will need to configure one USTAT module for each service provider link. Link name and USTAT name can be the same.

Enter the following:

```
module ustat provider_1
```

This will place the CLI in `config-ustat` mode for the USTAT module to be associated with the `provider_1` link. You need to do two things while in this mode:

- associate the USTAT module to a specific service provider access link
- assign a virtual IP (VIP) address to the USTAT module
- and, if needed, a default gateway for the module

When you are finished, you will need to back out of and then re-enter `config-ustat` mode with a different USTAT name. Note: if you wish to create a GRE (Generic Route Encapsulation) tunnel you will need to use the `interface tunnel` command.

Binding Links

Beginning with your first USTAT module, execute the `link` command to bind a specified link (created earlier, in `config-engine` mode) with the USTAT module currently being configured:

```
link provider_1
```

VIP address

Enter the `vip` command to assign a virtual IP address to the USTAT module:

```
vip 172.25.5.1
```

The VIP is the address that will receive traffic-measurement packets, either during a user traffic test (UTT) handshake or for an active probe. This address must be reachable from the Internet, so it should come from public address space (though examples throughout this document will use only private-space addresses for all interfaces, on both routers and xSeries devices).

If you need dedicated active measurement VIPs for your USTATs (see Chapter 4: Server-Based Measurement and Chapter 5: Configuring Agent-Based Measurement in the CNA Monitoring Guide), you can configure that address here, as well.
The standard VIP can be used for both active probes and passive tests, however, so the active measurement VIP will not be configured as part of this example.

The xSeries system will implicitly append /32 to the address (the CIDR-notation equivalent of a subnet mask of 255.255.255.255). The mask won't show up in all output, but the `show interface` command for the USTAT module will include the following:

```
Link encap:Local Loopback
inet addr:172.25.5.2 Mask:255.255.255.255
```

**USTAT GRE Tunnels**

Enter the `interface tunnel` command to configure the USTAT end of the GRE tunnel:

Define the tunnel:

```
interface tunnel 1
  ip address 172.25.5.130 255.255.255.252
  tunnel destination 10.6.0.1
end
```

Now assign it to a USTAT:

```
module ustat provider_1
  link provider_1
  ip route 10.6.0.1 255.255.255.255 172.16.6.1
  ip route 0.0.0.0 0.0.0.0 tunnel1
end
```

Designate the `tunnel id` argument as 1 for the first tunnel, 2 for the second, and 3 for the third. Each tunnel on a system must have a unique ID.

The tunnel destination address is an IP address on the edge router to which the USTAT is connected. This address can be any valid interface configured on the router. However, for this example, we have followed the common practice of using the router’s loopback address.

Since the loopback address is not in the same logical subnet as the USTAT module’s interface address, we need to explicitly identify a static route to the loopback address.

Use the `ip route` command on the USTAT module to create this static route. In this example, we will create host-specific static routes (by using a mask of 255.255.255.255) to the loopback addresses on the edge routers.

```
Use the ip route command a second time on each USTAT to create a default route through the tunnel to the Internet, using the catch-all address 0.0.0.0 0.0.0.0 and the tunnel interface name tunnel1.
```

Back out of `config-ustat` mode using the `end` (or `exit`) command, and repeat the three-part process—association of the link, assignment of the VIP and creation of the GRE tunnel—for each USTAT module in your system.
Associating USTATs With Interfaces

Next, we need to associate the three USTAT modules with the USTAT interface we configured earlier.

Enter the interface command to change to configuration mode for the USTAT interface. Then enter the module command once for each of the three modules that will operate from this interface:

```
interface fastethernet 0/2
module ustat provider_1
module ustat provider_2
module ustat provider_3
end
```

The interface configuration block which you configured earlier should now look like this:

```
interface FastEthernet 0/2
description “USTAT Modules”
ip address 172.16.6.6 255.255.255.224
module ustat provider_1
module ustat provider_2
module ustat provider_3
end
```

The xSeries device now has a basic configuration which will allow it to peer with your edge routers and begin evaluating traffic (though it does not yet have a source of measurement data). Figure 7 depicts your xSeries’s configuration at this stage:
The next step is to configure your edge routers to peer with the xSeries device. See Chapter 2: Configuring Your Routers in the Adaptive Path Controller-Internet Guide.
# Index

## Symbols

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>25</td>
</tr>
</tbody>
</table>

## A

<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>active probe</td>
<td>17</td>
</tr>
<tr>
<td>address rotation</td>
<td>10</td>
</tr>
<tr>
<td>AS number</td>
<td>30, 31</td>
</tr>
</tbody>
</table>

## B

<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup</td>
<td>23</td>
</tr>
<tr>
<td>bgp</td>
<td>10, 31</td>
</tr>
<tr>
<td>bgp peering</td>
<td>30</td>
</tr>
<tr>
<td>BGP4</td>
<td>10</td>
</tr>
</tbody>
</table>

## C

<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>character set</td>
<td>24</td>
</tr>
<tr>
<td>CLI</td>
<td>19</td>
</tr>
<tr>
<td>commands</td>
<td></td>
</tr>
<tr>
<td>bgp</td>
<td>31</td>
</tr>
<tr>
<td>configure terminal.</td>
<td>27</td>
</tr>
<tr>
<td>hostname</td>
<td>29</td>
</tr>
<tr>
<td>interface</td>
<td>28</td>
</tr>
<tr>
<td>ip address</td>
<td>28</td>
</tr>
<tr>
<td>ip http server header append</td>
<td>24</td>
</tr>
<tr>
<td>ip route</td>
<td>29, 35</td>
</tr>
<tr>
<td>link</td>
<td>30, 34</td>
</tr>
<tr>
<td>module</td>
<td>34</td>
</tr>
<tr>
<td>neighbor link</td>
<td>31</td>
</tr>
<tr>
<td>neighbor remote-as</td>
<td>32</td>
</tr>
<tr>
<td>provider-as</td>
<td>30</td>
</tr>
<tr>
<td>show interface</td>
<td>35</td>
</tr>
<tr>
<td>show running-config</td>
<td>29</td>
</tr>
<tr>
<td>tunnel</td>
<td>35</td>
</tr>
<tr>
<td>vip</td>
<td>34</td>
</tr>
<tr>
<td>comments</td>
<td>25</td>
</tr>
<tr>
<td>config t</td>
<td>27</td>
</tr>
<tr>
<td>configure terminal</td>
<td>27</td>
</tr>
</tbody>
</table>

## D

<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>default gateway</td>
<td>29</td>
</tr>
<tr>
<td>direct-server return</td>
<td>10</td>
</tr>
<tr>
<td>DNS</td>
<td>10</td>
</tr>
</tbody>
</table>

## E

<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>exclamation mark</td>
<td>25</td>
</tr>
</tbody>
</table>

## F

<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet</td>
<td>27</td>
</tr>
<tr>
<td>full BGP feed</td>
<td>10</td>
</tr>
</tbody>
</table>

## G

<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRE</td>
<td>16, 34, 35</td>
</tr>
<tr>
<td>GSLB</td>
<td>10</td>
</tr>
</tbody>
</table>

## H

<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>hard disk</td>
<td>23</td>
</tr>
<tr>
<td>high availability</td>
<td>10</td>
</tr>
<tr>
<td>hostname</td>
<td>29</td>
</tr>
</tbody>
</table>

## I

<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBGP</td>
<td>32</td>
</tr>
<tr>
<td>ICMP</td>
<td>17</td>
</tr>
<tr>
<td>interface</td>
<td>28, 35</td>
</tr>
<tr>
<td>ip address</td>
<td>28</td>
</tr>
<tr>
<td>ip http server header append</td>
<td>24</td>
</tr>
<tr>
<td>ip route</td>
<td>29, 35</td>
</tr>
</tbody>
</table>

## J

<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java</td>
<td>9</td>
</tr>
</tbody>
</table>

## L

<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>link</td>
<td>30, 34</td>
</tr>
</tbody>
</table>

## M

<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>module command</td>
<td>34</td>
</tr>
<tr>
<td>multi-homed</td>
<td>10</td>
</tr>
</tbody>
</table>
# Index

## N
- NAT ........................................ 10
- neighbor link ............................. 31
- neighbor remote-as ....................... 32
- network address translator ............... 10

## P
- P3P ........................................ 24
- password recovery ........................ 21
- PBR ......................................... 10
- Platform for Privacy Preferences ........... 24
- plug-in .................................... 9
- policy based routing ....................... 10
- privacy .................................. 24
- provider-as ................................ 30

## R
- restore .................................... 23
- round-robin ................................ 10
- route-assert-mode ......................... 18
- RSOS ....................................... 19

## S
- show interface ................................ 35
- show running-config ....................... 29
- startup configuration ........................ 20
- subsystem .................................. 28

## T
- tcp ......................................... 17
- tunnel ...................................... 35

## U
- user account ................................ 21
- UTT ......................................... 17

## V
- VIP ......................................... 11, 34
- vip command ................................ 34