

Configuration

1 System: 192.168.3.26

Collection: **192.168.3.26 (2008-05-14 10:04:43)**

Generated: **Wednesday, May 14, 2008 10:05:03 AM**

For: **Test User test.user@email.com**

By: Ecora Auditor Professional 4.5 - Cisco Module 4.5.8118.18311

Using: Full Report (Configuration Report)

Description: The Configuration report provides detailed documentation of configuration settings for compliance audits, disaster recovery plans, security assessments, migration plans, troubleshooting, and preserving IT knowledge and decisions.

Full Report

Table of Contents

- 1 System Management 3**
 - 1.1 Services 3
 - 1.2 Boot System 3
 - 1.3 Password Management 3
 - 1.4 System Clock 3
 - 1.5 HyperText Transfer Protocol (HTTP) Server 3
 - 1.6 Logging 4
 - 1.7 Simple Network Management Protocol (SNMP) 4
 - 1.8 Connection and System Banners 4
 - 1.9 Network Time Protocol (NTP) 4
- 2 Interfaces 5**
 - 2.1 Ethernet0/0 5
 - 2.2 Serial0/0 5
 - 2.3 Ethernet0/1 5
 - 2.4 Serial0/1 6
 - 2.5 Serial0/1.1 6
 - 2.6 Serial0/1.2 6
- 3 Internet Protocol (IP) 7**
 - 3.1 IP Access Control Lists (ACL) 7
 - 3.2 Name Resolution 7
 - 3.3 Network Address Translation (NAT) 7

4 Internet Protocol Routing 8

 4.1 Static Routes 8

 4.2 Key Chains 8

5 Interactive Access 8

 5.1 Console 0 8

 5.2 Auxiliary 0 9

 5.3 VTY 0-4 9

Collected Not-Collected Legend

| | |
|----------------|--|
| DEFAULT | The value presented in the report was not directly reported by the target, but implied by the current value or lack of a value for the attribute |
| *UA* | Unavailable attribute. The current configuration or version of target platform does not provide a value for this attribute. More detail in logs |
| *FC* | Collection of value failed |
| *NS* | Value not selected for collection |

Organization Example Company

This report of the routing domain for **Example Company** has been prepared at the request of from the data set collected on **May-14-2008_10-04-43**.

This data set is composed of 1 router.

- **Cisco2611 (192.168.3.26)**

Failed connections: ***NULL***

Cisco2611 (192.168.3.26)

Hostname: **Cisco2611**.

Platform Series: **C2600**.

Cisco IOS® Version: **12.0(5)T1**.

Cisco IOS® Image Name: **C2600-IS-M**.

Processor Board ID: **JAD0352079I**.

Running Image File: **flash:aaa0536.bin**.

ROM Version: **11.3(2)XA4**.

Uptime: **21 weeks, 1 day, 23 hours, 14 minutes**.

Configuration Register: **0x2102**.

The running config was last modified on **09:53:55 EST Mon Dec 17 2007**.

1 System Management

Cisco routers provide for the configuration of some basic system management features.

- Services
- Boot System
- Password Management
- System Clock
- HyperText Transfer Protocol Server
- Logging
- Simple Network Management Protocol
- Connection and System Banners
- Network Time Protocol

1.1 Services

Password encryption is **disabled**.

Minor TCP/IP servers are **enabled**.

Minor UDP/IP servers are **DEFAULT: disabled**.

Log messages are time stamped with the **time since the system was rebooted**.

Debug messages are time stamped with the **current date and time**.

1.2 Boot System

Boot system configuration: ***NULL***

1.3 Password Management

The enable password for level **DEFAULT: 15** is **enabled**. The encryption type is **DEFAULT: 7**.

The enable secret for level **DEFAULT: 15** is **enabled**. The encryption type is **5**.

1.4 System Clock

The configured timezone is **EST**.

The difference from UTC is **-5** hours.

Daylight savings time is **DEFAULT: disabled**.

1.5 HyperText Transfer Protocol (HTTP) Server

The HTTP server is **enabled**.

The HTTP server is listening on port **8080**.
 HTTP server access is controlled by ACL **1**.
 Authentication is based on the **local**.

1.6 Logging

The console receives **DEFAULT: debugging** and more severe messages.
 Terminal lines (other than console) receive **DEFAULT: debugging** and more severe messages.
 The logging buffer receives **DEFAULT: debugging** and more severe messages. The size of the logging buffer is **DEFAULT: 4096 bytes**.
 The history table receives **DEFAULT: warnings** and more severe messages. The size of the history table is **500 messages**.
 The syslog servers receive **DEFAULT: informational** and more severe messages in the **DEFAULT: local7** facility.
 Syslog Servers: ***NULL***

1.7 Simple Network Management Protocol (SNMP)

The SNMP Agent is **DEFAULT: disabled**.

1.8 Connection and System Banners

Table 1. Connection and System Banners

| Type | Banner Message |
|-------|------------------------------|
| exec | Unauthorized Use Prohibited. |
| login | Unauthorized Use Prohibited. |
| motd | Unauthorized Use Prohibited. |

1.9 Network Time Protocol (NTP)

Table 2. NTP Servers

| Server IP Address | NTP Version | Authentication Key ID | Source IP | Preferred |
|-------------------|-------------|-----------------------|------------------------------------|-----------------------|
| 192.168.0.60 | 2 | 55 | DEFAULT: outgoing interface | DEFAULT: false |

2 Interfaces

The section describes the physical and logical interfaces configured on this router.

2.1 Ethernet0/0

The administrative status is **DEFAULT: enabled**.

The description for this interface is **DEFAULT: not defined**.

Keepalive packets are sent every **DEFAULT: 10 seconds**.

The IP addresses configured are:

- Type **primary** IP Address **192.168.3.26** Mask **255.255.255.0** (subnet **192.168.3.0**, broadcast **192.168.3.255**)

Inbound IP traffic is **DEFAULT: not restricted**.

Outbound IP traffic is **DEFAULT: not restricted**.

Hardware address is **00b0.646e.8dc0**.

2.2 Serial0/0

The administrative status is **disabled**.

The description for this interface is **Point-to-Point with 2500**.

Keepalive packets are sent every **DEFAULT: 10 seconds**.

Primary and secondary IP addresses: ***NULL***

Inbound IP traffic is **DEFAULT: not restricted**.

Outbound IP traffic is **DEFAULT: not restricted**.

The interface is cabled as **DEFAULT: DTE**.

The encapsulation method for this interface is **ppp**.

PPP authentication is **enabled**. The configured methods are: **chap**

2.3 Ethernet0/1

The administrative status is **disabled**.

The description for this interface is **Interface Not Used**.

Keepalive packets are sent every **DEFAULT: 10 seconds**.

The IP addresses configured are:

1. Type **primary** IP Address **20.20.20.20** Mask **255.0.0.0** (subnet **20.0.0.0**, broadcast **20.255.255.255**)

- Type **secondary** IP Address **10.11.10.10** Mask **255.255.255.0** (subnet **10.11.10.0**, broadcast **10.11.10.255**)

Inbound IP traffic is controlled by Access Control List **KnownOffenders**.

Outbound IP traffic is **DEFAULT: not restricted**.

Hardware address is **00b0.646e.8dc1**.

2.4 Serial0/1

The administrative status is **disabled**.

The description for this interface is **Sales Network**.

Keepalive packets are **not sent**.

Primary and secondary IP addresses: ***NULL***

Inbound IP traffic is **DEFAULT: not restricted**.

Outbound IP traffic is **DEFAULT: not restricted**.

The interface is cabled as **DEFAULT: DTE**.

The encapsulation method for this interface is **frame-relay**.

DLCIs are **not configured**.

2.5 Serial0/1.1

The administrative status is **DEFAULT: enabled**.

The description for this interface is **Sales Network Subinterface**.

Keepalive packets are sent every **DEFAULT: 10 seconds**.

The IP addresses configured are:

- Type **primary** IP Address **22.0.0.1** Mask **255.0.0.0** (subnet **22.0.0.0**, broadcast **22.255.255.255**)

Inbound IP traffic is **DEFAULT: not restricted**.

Outbound IP traffic is **DEFAULT: not restricted**.

The interface is cabled as **DEFAULT: DTE**.

2.6 Serial0/1.2

The administrative status is **DEFAULT: enabled**.

The description for this interface is **DEFAULT: not defined**.

Keepalive packets are sent every **DEFAULT: 10 seconds**.

Primary and secondary IP addresses: ***NULL***

Inbound IP traffic is **DEFAULT: not restricted**.
 Outbound IP traffic is **DEFAULT: not restricted**.
 The interface is cabled as **DEFAULT: DTE**.

3 Internet Protocol (IP)

Internet Protocol (IP) provides a number of services and protocols for the control and management of communication between nodes on the Internet.

3.1 IP Access Control Lists (ACL)

The IP Access Control Lists configured are:

- **standard ACL KnownOffenders.**
 - A. Action: **deny** Source: **192.12.3.4** Logging: **enabled**
 - B. Action: **permit** Source: **any** Logging: **enabled**
 KnownOffenders is used in:
 - Ethernet0/1 (inbound)

3.2 Name Resolution

DNS host-to-address resolution is **DEFAULT: enabled**.

The default IP domain name is **ecora.com**.

Domain Name Servers: ***NULL***

The IP domain list configured is:

- ecora.com

Table 3. Hostname-to-Address Mappings

| Hostname | IP Address | Telnet Port |
|----------|-----------------------------|--------------------|
| matrix | 192.168.0.179, 172.16.0.179 | DEFAULT: 23 |

3.3 Network Address Translation (NAT)

IP Network Address Translation is **enabled**.

The global NAT parameters are:

- The maximum number of entries in the NAT translation table is **DEFAULT: unlimited**.
- The Dynamic Translation Timeout for simple entries is **DEFAULT: 60 seconds**.
- The DNS Timeout is **DEFAULT: 60 seconds**.
- The ICMP Timeout is **DEFAULT: 60 seconds**.
- The TCP Timeout is **DEFAULT: 24 hours**.
- The FIN RST Timeout is **DEFAULT: 60 seconds**.

- The UDP Timeout is **DEFAULT: 300 seconds**.
- The SYN Timeout is **DEFAULT: 60 seconds**.

Pool of IP addresses for Network Address Translation: ***NULL***

Inside Destination translations: ***NULL***

Inside Source translations: ***NULL***

Outside source translations: ***NULL***

insideInterfaces: ***NULL***

outsideInterfaces: ***NULL***

4 Internet Protocol Routing

Internet Protocol (IP) routing is **disabled**.

Classless routing is **enabled**.

Routing Protocols: ***NULL***

4.1 Static Routes

A static route is manually defined by the administrator when the router cannot dynamically build a route to a destination.: ***NULL***

4.2 Key Chains

The Key Chains configured are:

- Key Chain **rip_chain**
 - Key **0**, string **cisco**
 - Accept lifetime valid from **DEFAULT: January 1, 1993**, expires **DEFAULT: never**
 - Send lifetime valid from **DEFAULT: January 1, 1993**, expires **DEFAULT: never**

5 Interactive Access

Interactive access mechanisms use the IOS TTY abstraction. In Cisco IOS terminology, a line refers to an asynchronous serial connection to connect a console, modem, or other auxiliary device to the router. Routers typically have two such lines, a console port and an auxiliary port.

Some models do not provide the auxiliary port. Telnet, LAT, or MOP access to the router is via virtual terminal lines (VTY).

5.1 Console 0

Password checking at login is **DEFAULT: disabled**.

Inbound access to this line is **DEFAULT: not restricted**.

Outbound access to this line is **DEFAULT: not restricted**.
 Allowed inbound transport protocols: **none**.
 Allowed outbound transport protocols: **DEFAULT: telnet**.
 EXEC timeout is **DEFAULT: disabled**.
 Session timeout is **DEFAULT: 10 minutes**.

Table 4. Physical Parameters

| Data Bits | Parity | Stop Bits | Flow Control | Rx Speed | Tx Speed |
|------------|---------------|--------------|---------------|-------------------|-------------------|
| DEFAULT: 8 | DEFAULT: none | DEFAULT: two | DEFAULT: none | DEFAULT: 9600 bps | DEFAULT: 9600 bps |

5.2 Auxiliary 0

Password checking at login is **DEFAULT: disabled**.
 Inbound access to this line is **DEFAULT: not restricted**.
 Outbound access to this line is **DEFAULT: not restricted**.
 Allowed inbound transport protocols: **DEFAULT: none**.
 Allowed outbound transport protocols: **DEFAULT: telnet**.
 EXEC timeout is **DEFAULT: disabled**.
 Session timeout is **DEFAULT: 10 minutes**.

Table 5. Physical Parameters

| Data Bits | Parity | Stop Bits | Flow Control | Rx Speed | Tx Speed |
|------------|---------------|--------------|---------------|-------------------|-------------------|
| DEFAULT: 8 | DEFAULT: none | DEFAULT: two | DEFAULT: none | DEFAULT: 9600 bps | DEFAULT: 9600 bps |

5.3 VTY 0-4

Password checking at login is **enabled**. The encryption type is **DEFAULT: not defined**.
 Authentication is based on **DEFAULT: line password**.
 Inbound access to this line is **DEFAULT: not restricted**.
 Outbound access to this line is **DEFAULT: not restricted**.
 Allowed inbound transport protocols: **DEFAULT: none**.
 Allowed outbound transport protocols: **DEFAULT: telnet**.
 EXEC timeout is **0 minutes 0 seconds**.
 Session timeout is **DEFAULT: 10 minutes**.