SHODAN for Penetration Testers

Michael “theprez98” Schearer

SHODAN for Penetration Testers

- What is SHODAN?
- Basic Operations
- Penetration Testing
- Case Study 1: Cisco Devices
- Case Study 2: Default Passwords
- Case Study 3: Infrastructure Exploitation
- Other Examples
- The Future
- Conclusions

By pen testing, I mean…

- Black/gray/white box testing
- Ethical hacking
- Security auditing
- Vulnerability assessment
- Standards compliance
- Training
- All of the above

SHODAN for Penetration Testers

WHAT IS SHODAN?

What is SHODAN? (1)

- SHODAN (http://www.shodanhq.com/) is a computer search engine designed by web developer John Matherly (http://twitter.com/achillean)
- While SHODAN is a search engine, it is much different than content search engines like Google, Yahoo or Bing

What is SHODAN? (2)

- Typical search engines crawl for data on web pages and then index it for searching
- SHODAN interrogates ports and grabs the resulting banners, then indexes the banners (rather than the web content) for searching

What is SHODAN? (3)

- Rather than to locate specific content on a particular search term, SHODAN is designed to help the user find specific nodes (desktops, servers, routers, switches, etc.) with specific content in their banners
- Optimizing search results requires some basic knowledge of banners

SHODAN for Penetration Testers

BASIC OPERATIONS

SHODAN - Computer Search Engine - Mozilla Firefox (Build 20100202165920)

File Edit View History Bookmarks Tools Help

http://www.shodanhq.com/

Wikipedia (en)

SHODAN - Computer Search Engine

SHODAN

Search

Register | Login

» Popular Searches

cisco-ios last-modified
Finds Cisco-IOS results that do not require any authentication ;-)

default password
Finds results with "default password" in the banner; the named defaults might work!

FTP anon successful
this search does not provide as many results as the other ftp search, but it looks like all the results that come back are successful anonymous logins

IIS 4.0 webservers
Almost all false positives removed by excluding other versions and http error codes

Contact

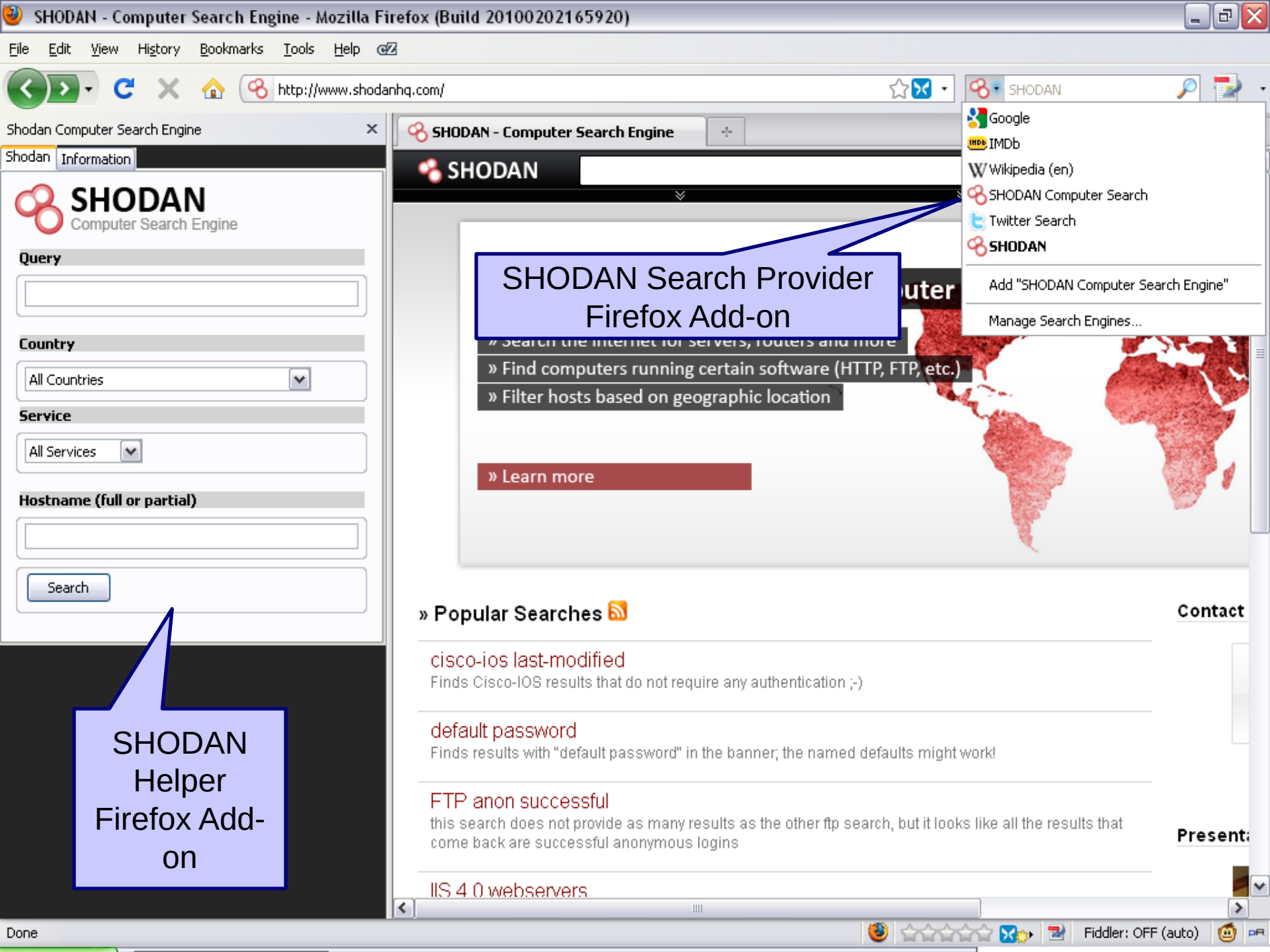
FOLLOW ME ON TWITTER

For direct inquiries:
jmath@surtri.com

Presentations

Done

Fiddler: OFF (auto)

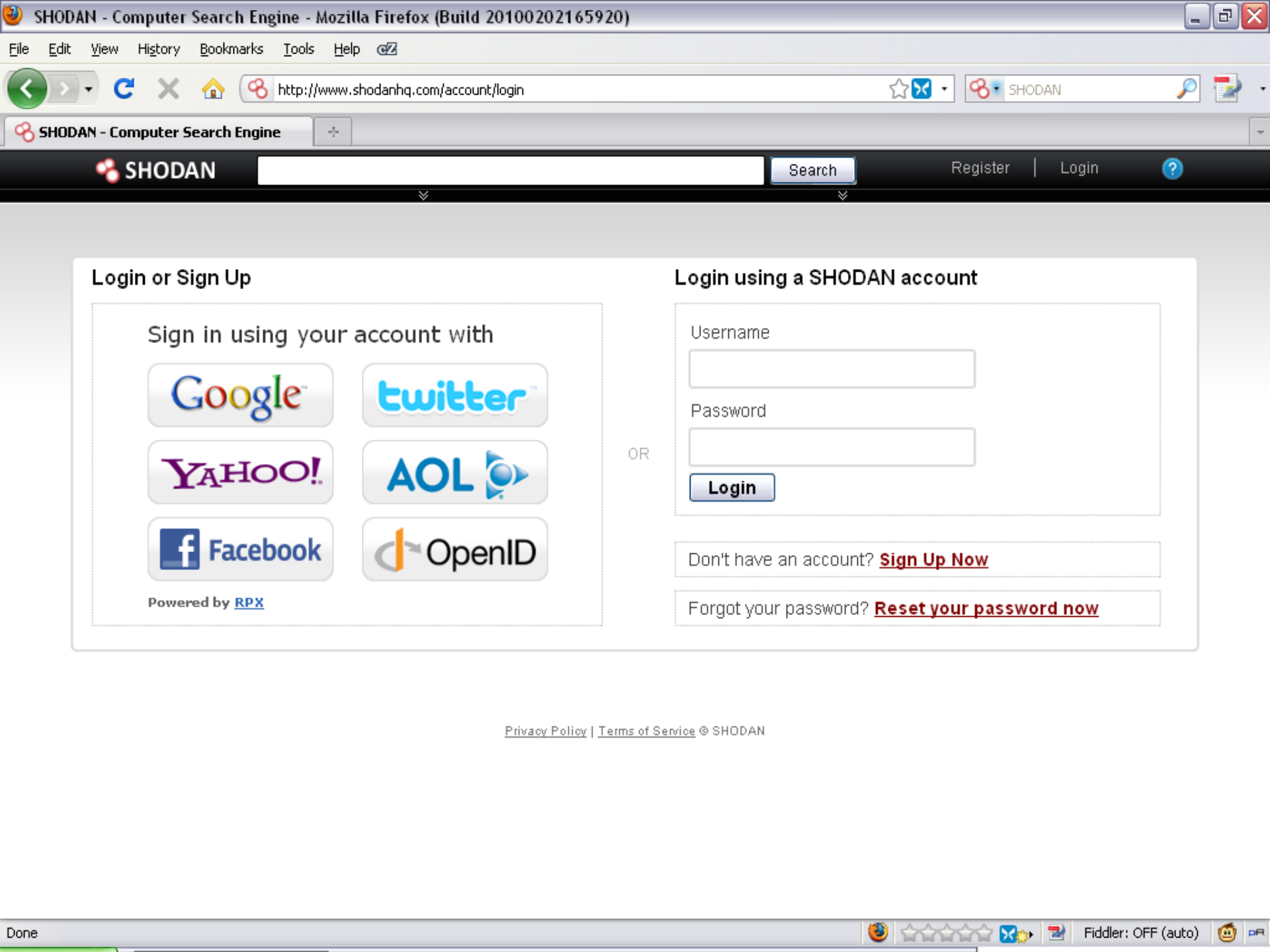

SHODAN - Computer Search Engine - Mozilla Firefox (Build 20100202165920)
File Edit View History Bookmarks Tools Help
http://www.shodanhq.com/
SHODAN
Google
IMDb
Wikipedia (en)
SHODAN Computer Search
Twitter Search
SHODAN
Add "SHODAN Computer Search Engine"
Manage Search Engines...
Shodan Computer Search Engine
Shodan
Information
SHODAN
Computer Search Engine
Query
Country
All Countries
Service
All Services
Hostname (full or partial)
Search
SHODAN - Computer Search Engine
SHODAN
» Find computers running certain software (HTTP, FTP, etc.)
» Filter hosts based on geographic location
» Learn more
» Popular Searches
Contact
cisco-ios last-modified
Finds Cisco-IOS results that do not require any authentication ;-)
default password
Finds results with "default password" in the banner; the named defaults might work!
FTP anon successful
this search does not provide as many results as the other ftp search, but it looks like all the results that come back are successful anonymous logins
IIS 4.0 webservers
SHODAN Search Provider Firefox Add-on
SHODAN Helper Firefox Add-on
Done
Fiddler: OFF (auto)

Basic Operations: Search

- Search terms are entered into a text box (seen below)
- Quotation marks can narrow a search
- Boolean operators + and – can be used to include and exclude query terms (+ is implicit default)

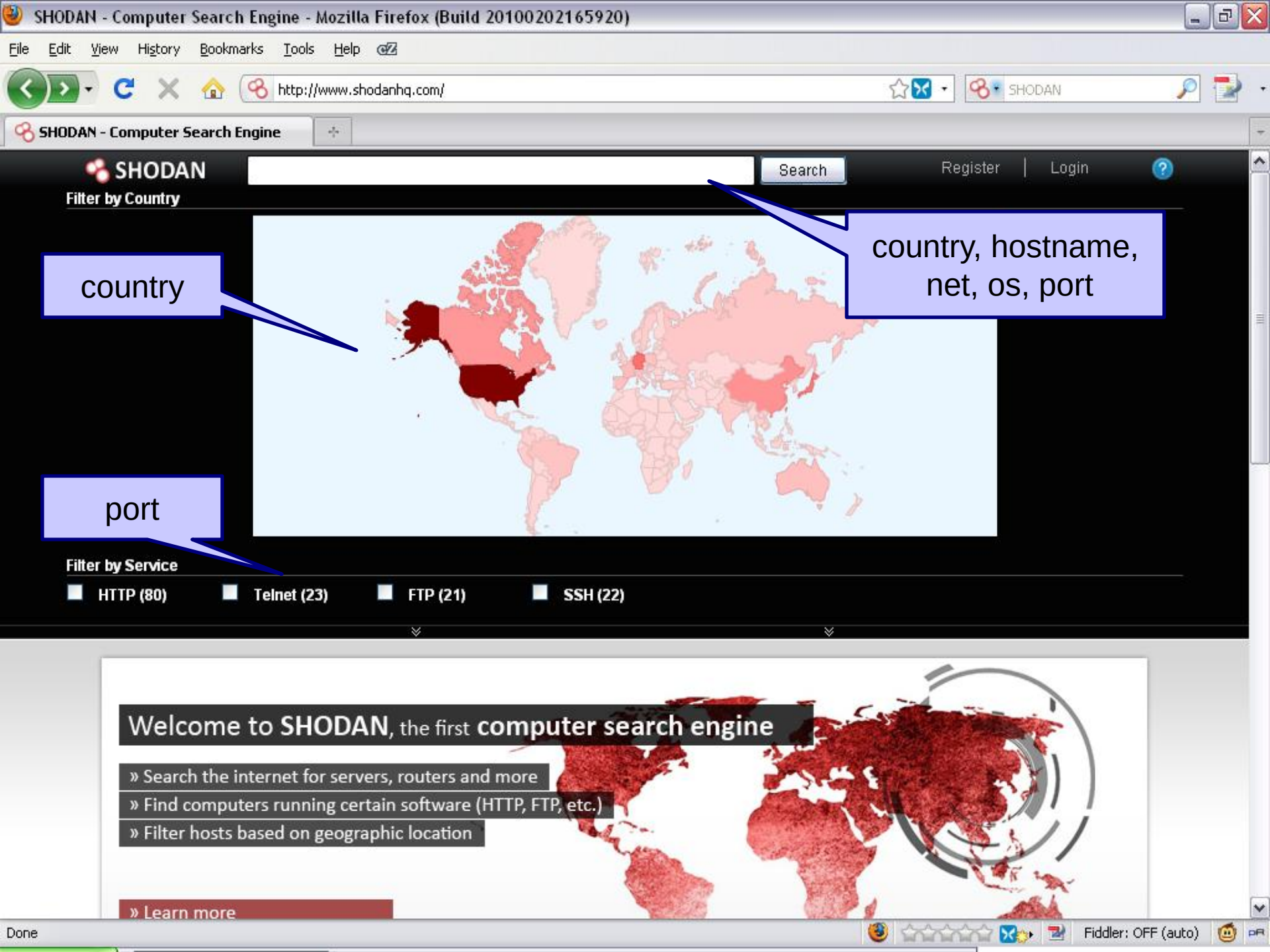
Basic Operations: Login

- Create and login using a SHODAN account; or
- Login using one of several other options (Google, Twitter, Yahoo, AOL, Facebook, OpenID
- Login is *not* required, but *country* and *net* filters are not available unless you login
- Export requires you to be logged in


SHODAN - Computer Search Engine - Mozilla Firefox (Build 20100202165920)
File Edit View History Bookmarks Tools Help
http://www.shodanhq.com/account/login
SHODAN
SHODAN - Computer Search Engine
SHODAN
Search
Register | Login
Login or Sign Up
Sign in using your account with
Google
twitter
YAHOO!
AOL
Facebook
OpenID
Powered by RPX
OR
Login using a SHODAN account
Username
Password
Login
Don't have an account? Sign Up Now
Forgot your password? Reset your password now
Privacy Policy | Terms of Service © SHODAN
Done
Fiddler: OFF (auto)

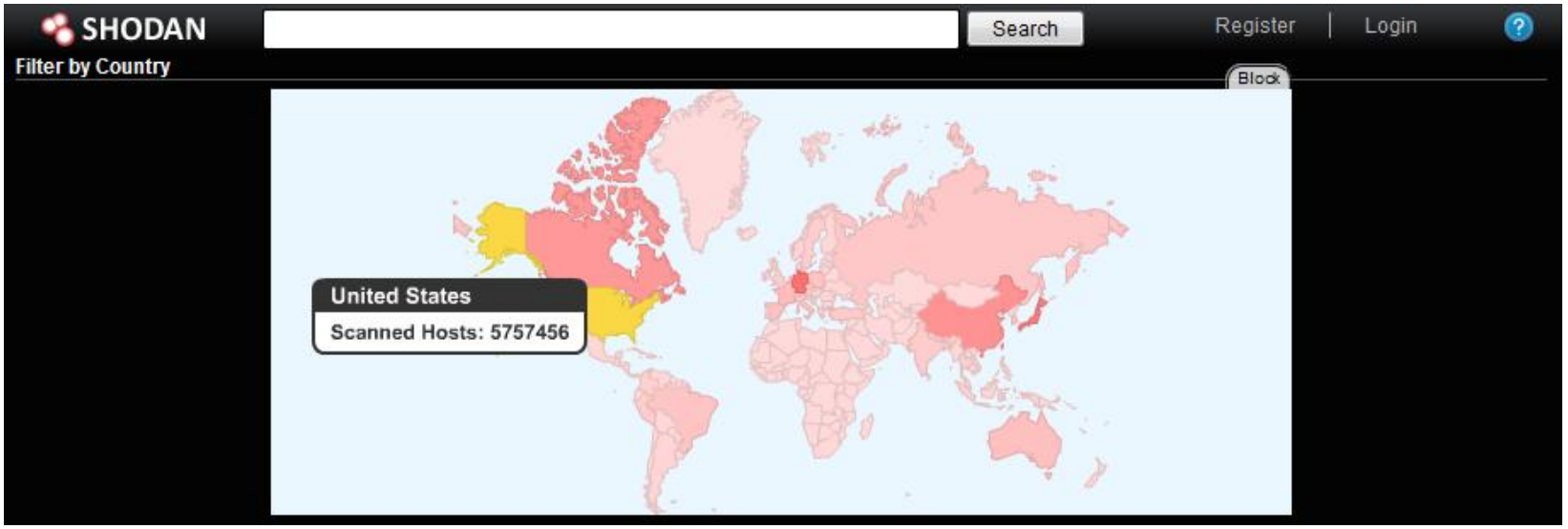
Basic Operations: Filters

- **country:** filters results by two letter country code
- **hostname:** filters results by specified text in the hostname or domain
- **net:** filter results by a specific IP range or subnet
- **os:** search for specific operating systems
- **port:** narrow the search for specific services


SHODAN - Computer Search Engine - Mozilla Firefox (Build 20100202165920)
File Edit View History Bookmarks Tools Help
http://www.shodanhq.com/
SHODAN - Computer Search Engine
SHODAN
Search
Register | Login
Filter by Country
country
country, hostname, net, os, port
port
Filter by Service
HTTP (80)
Telnet (23)
FTP (21)
SSH (22)
Welcome to SHODAN, the first computer search engine
» Search the internet for servers, routers and more
» Find computers running certain software (HTTP, FTP, etc.)
» Filter hosts based on geographic location
» Learn more
Done
Fiddler: OFF (auto)

Basic Operations: Country Filter

- Filtering by country can be accomplished by clicking on the country map (available from the drop down menu)
- Mouse over a country for the number of scanned hosts for a particular country



SHODAN - Computer Search Engine - Mozilla Firefox (Build 20100202165920)

File Edit View History Bookmarks Tools Help

http://www.shodanhq.com/?q=apache+country%3ACH

SHODAN - Computer Search Engine

SHODAN apache country:CH Search Logout

Home Search Directory My Se Analytics/ Exports

Save Export Data

Find all ‘apache’ servers in Switzerland

Results **1** - **10** of about **24404** for **apache country:CH**

217.26.51.29
FreeBSD 4.4
Added on 13.04.2010

```
HTTP/1.0 500 Internal Server Error
Date: Tue, 13 Apr 2010 02:52:11 GMT
Server: Apache/2.2.13 (FreeBSD) mod_hogi/0.7.1 mod_ssl/2.2.13 OpenSSL/0.9.8k DAV/2
Vary: accept-language,accept-charset
Accept-Ranges: bytes
Connection: close
Content-Type: text/html; charset=iso-8859-1
Content-Language: en
```

217.162.49.29
Added on 13.04.2010

217-162-49-29.dclient.hispeed.ch

```
HTTP/1.0 302 Found
Server: Apache/0.6.5
Pragma: no-cache
Date: Sun, 01 Jan 2001 00:00:00 GMT
Expires: Sun, 01 Jan 2001 00:00:00 GMT
Cache-Control: max-age=0, must-revalidate
Connection: close
Location: /relink_web.stm
Content-type: text/html
```

195.141.44.29
Linux recent 2.4
Added on 13.04.2010

```
HTTP/1.0 200 OK
Date: Tue, 13 Apr 2010 00:41:57 GMT
Server: Apache/1.3.27 (Unix) ChiliSoft-ASP/3.6.2 mod_gzip/1.3.26.1a mod_perl/1.27 FrontPage/5.0.2.2510 mod_ssl/2.8.14
OpenSSL/0.9.7b PHP-CGI/0.1b
Last-Modified: Sat, 23 May 2009 02:50:12 GMT
```

Done Fiddler: OFF (auto)

SHODAN - Computer Search Engine - Mozilla Firefox (Build 20100202165920)

File Edit View History Bookmarks Tools Help

http://www.shodanhq.com/?q=apache+2.2.3

SHODAN - Computer Search Engine

SHODAN apache 2.2.3 Search Logout

Home Search Directory My Searches /Exports

Find ‘apache’ servers running version 2.2.3

Save Export Data

Results **1** - **10** of about **1307968** for **apache 2.2.3**

» Top countries matching your search

United States	382,244
Germany	64,188
France	21,339
Canada	19,037

Top four countries matching your query

95.187.51.29
Linux recent 2.4
Added on 13.04.2010

```
HTTP/1.0 200 OK
Date: Tue, 13 Apr 2010 02:56:22 GMT
Server: Apache/2.2.3 (CentOS) DAV/2 PHP/5.3.2 mod_ssl/2.2.3 OpenSSL/0.9.8e-fips-rhel5
X-Powered-By: PHP/5.3.2
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

66.159.51.29
Linux recent 2.4
Added on 13.04.2010

```
HTTP/1.0 200 OK
Date: Tue, 13 Apr 2010 02:59:32 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.2.12
Content-Length: 62
Connection: close
Content-Type: text/html; charset=UTF-8
```

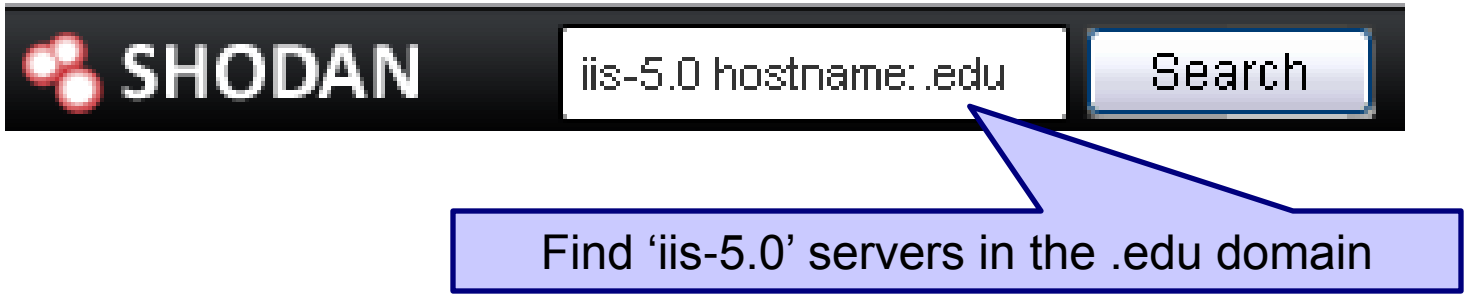
209.145.51.29
Linux recent 2.4
Added on 13.04.2010

```
HTTP/1.0 200 OK
Date: Tue, 13 Apr 2010 03:01:28 GMT
Server: Apache/2.2.3 (CentOS)
```

Done Fiddler: OFF (auto)

Basic Operations: Hostname Filter

Search results can be filtered using any portion of a hostname or domain name



Basic Operations: Net / OS Filters

- The net filter allows you to refine your searches by IP/CIDR notation
- The OS filter allows you to refine searches by operating system

Basic Operations: Port Filter

- SHODAN can filter your search results by port
- Current collection is limited to ports 21 (FTP), 22 (SSH), 23 (Telnet), and 80 (HTTP), while the overwhelming majority of collection is HTTP
- More ports/services coming (send requests to the developer via Twitter)

Basic Operations: Searches

- Popular searches are available on the main page
- Logged in users can save searches and share them with other users

Basic Operations: Export

- SHODAN lets you export up to 1,000 results per credit in XML format
- Credits can be purchased online
- Sample data export file is available

```
<shodan>
     <summary date="2010-03-16 23:23:19.921034" query="apache" total="6287987"/>
     <host country="US"
            hostnames="1stadvantagebailbond.com"
            ip="198.171.76.21"
            port="80"
            updated="16.03.2010">
           HTTP/1.0 200 OK
           Date: Tue, 16 Mar 2010 07:43:07 GMT
           Server: Apache/1.3.41 (Unix) FrontPage/5.0.2.2635 mod_ssl/2.8.31 OpenSSL/0.9.7m
           Last-Modified: Tue, 17 Nov 2009 17:40:25 GMT
           ETag: "19258d5-591-4b02e009"
           Accept-Ranges: bytes
           Content-Length: 1425
           Content-Type: text/html
     </host>
     ...
</shodan>
```

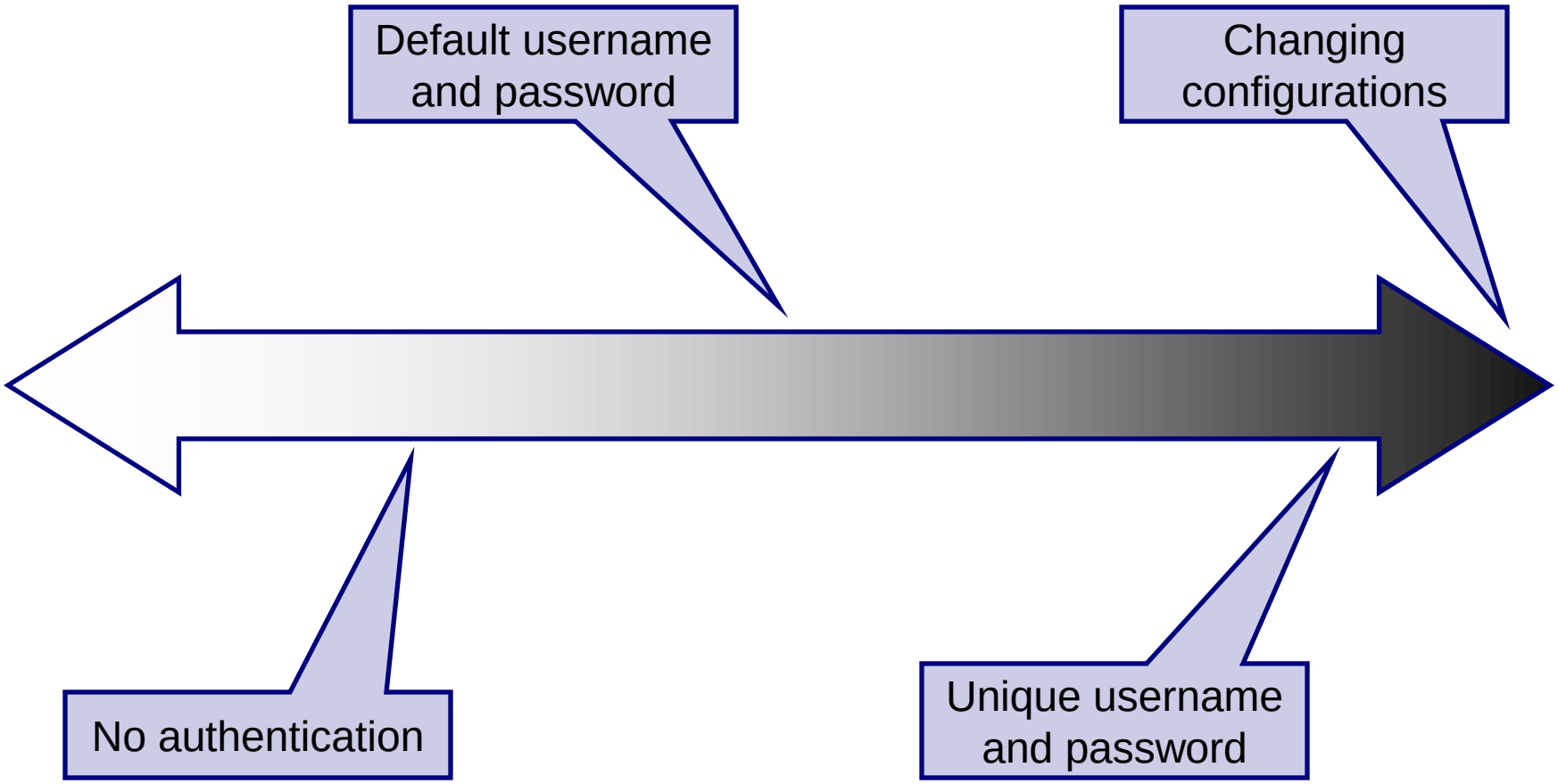
SHODAN for Penetration Testers

PENETRATION TESTING

Pen Testing: Ethics (1)

- Is it acceptable under any circumstances to view the configuration of a device that requires no authentication to view?
- What about viewing the configuration of a device using a default username and password?
- What about viewing the configuration of a device using a unique username and password?
- Changing the configuration of any device?

Pen Testing: Ethics (2)



Pen Testing Applications

- Using SHODAN for penetration testing requires some basic knowledge of banners including HTTP status codes
- Banners advertise service and version
- Banners can be spoofed (unlikely?)

Pen Testing: HTTP Status Codes

Status Code	Description
200 OK	Request succeeded
401 Unauthorized	Request requires authentication
403 Forbidden	Request is denied regardless of authentication

Pen Testing: Assumptions

- “200 OK” banner results will load without any authentication (at least not initially)
- “401 Unauthorized” banners with *Www-authenticate* indicate a username and password pop-up box (authentication is possible but not yet accomplished, as distinguished from “403 Forbidden”)
- Some banners advertise defaults

SHODAN for Penetration Testers

CASE STUDY: CISCO DEVICES

Case Study: Cisco Devices

Here is a typical “401 Unauthorized” banner when using the simple search term “cisco”:

```
HTTP/1.0 401 Unauthorized
Date: Tue, 01 Dec 2009 16:09:46 GMT
Www-authenticate: Basic realm="level_15 or view_access"
Connection: close
Accept-ranges: none
Server: cisco-IOS
```

Take note of the *Www-authenticate* line which indicates the requirement for a username and password

Case Study: Cisco Devices

Now consider an example of a “200 OK” banner which does not include the *Www-authenticate* line:

```
HTTP/1.0 200 OK
Transfer-encoding: chunked
Accept-ranges: none
Expires: Tue, 08 Jun 1993 06:55:45 GMT
Server: cisco-IOS
Last-modified: Tue, 08 Jun 1993 06:55:45 GMT
Connection: close
Cache-control: no-store, no-cache, must-revalidate
Date: Tue, 08 Jun 1993 06:55:45 GMT
Content-type: text/html
```

Case Study: Cisco Devices

A comparison of the two banners finds the second banner to include the *Last-modified* line which does not appear when *Www-authenticate* appears:

```
HTTP/1.0 401 Unauthorized
Date: Tue, 01 Dec 2009 16:09:46 GMT
Www-authenticate: Basic realm="level_15 or view_access"
Connection: close
Accept-ranges: none
Server: cisco-IOS
```

```
HTTP/1.0 200 OK
Transfer-encoding: chunked
Accept-ranges: none
Expires: Tue, 08 Jun 1993 06:55:45 GMT
Server: cisco-IOS
Last-modified: Tue, 08 Jun 1993 06:55:45 GMT
Connection: close
Cache-control: no-store, no-cache, must-revalidate
Date: Tue, 08 Jun 1993 06:55:45 GMT
Content-type: text/html
```

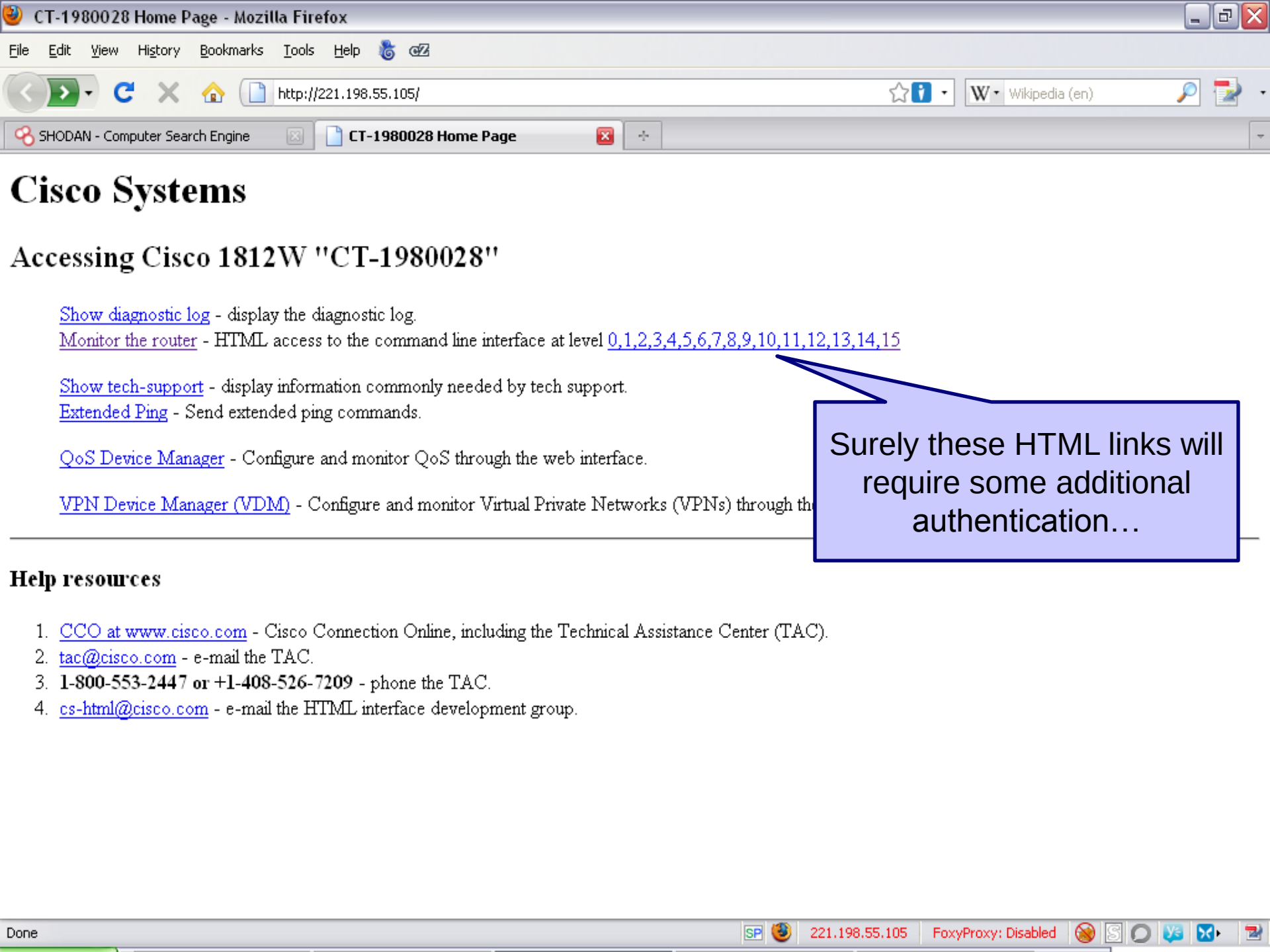
In fact, among “cisco” results these two lines are more than 99% mutually exclusive

Case Study: Cisco Results

Search	Results
cisco	251,742
cisco-ios	226,184
cisco www-authenticate	225,402
cisco last-modified	4,265
cisco last-modified www-authenticate	56

Case Study: Cisco Results

- This suggests that Cisco “200 OK” banners that include the *Last-modified* line do not require any authentication (at least not initially)
- The results on the previous slide suggest there are potentially **4,200+** Cisco devices that do not require authentication


CT-1980028 Home Page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://221.198.55.105/
Wikipedia (en)
SHODAN - Computer Search Engine
CT-1980028 Home Page
Cisco Systems
Accessing Cisco 1812W "CT-1980028"
Show diagnostic log - display the diagnostic log.
Monitor the router - HTML access to the command line interface at level 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
Show tech-support - display information commonly needed by tech support.
Extended Ping - Send extended ping commands.
QoS Device Manager - Configure and monitor QoS through the web interface.
VPN Device Manager (VDM) - Configure and monitor Virtual Private Networks (VPNs) through th
Surely these HTML links will require some additional authentication…
Help resources
1. CCO at www.cisco.com - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. tac@cisco.com - e-mail the TAC.
3. 1-800-553-2447 or +1-408-526-7209 - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.
Done
221.198.55.105
FoxyProxy: Disabled

CT-1980028 /level/15/exec/-/configure/http - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://221.198.55.105/level/15/exec/-/configure/http

SHODAN - Computer Search Engine | CT-1980028 /level/15/exec/-/co...

CT-1980028

Home Exec Configure

Command

Output

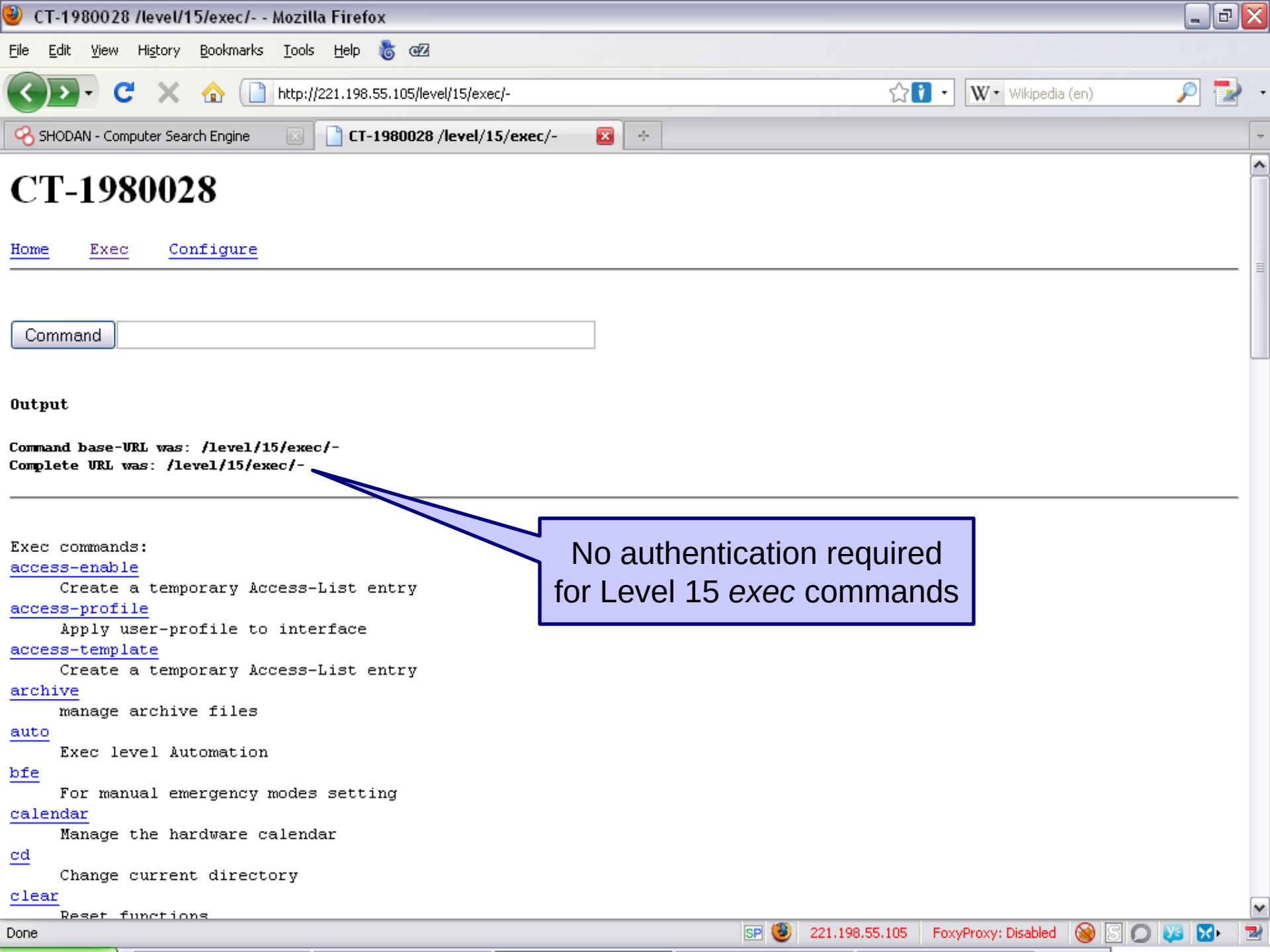
```
Command base-URL was: /level/15/exec/-
Complete URL was: /level/15/exec/-/configure/http
Command was:  configure http
```

Configure commands:

aaa
    Authentication, Authorization and Accounting.
access-list
    Add an access list entry
alias
    Create command alias
appfw
    Configure the Application Firewall policy
appletalk
    Appletalk global configuration commands
archive
    Archive the configuration
arp
    Set a static ARP entry
async-bootp
    Modify system bootp parameters

Nope. No authentication required for Level 15! No authentication required for *configure* commands

Done 221.198.55.105 FoxyProxy: Disabled


CT-1980028 /level/15/exec/- - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://221.198.55.105/level/15/exec/-
Wikipedia (en)
SHODAN - Computer Search Engine
CT-1980028 /level/15/exec/-
CT-1980028
Home Exec Configure
Command
Output
Command base-URL was: /level/15/exec/-
Complete URL was: /level/15/exec/-
Exec commands:
access-enable
Create a temporary Access-List entry
access-profile
Apply user-profile to interface
access-template
Create a temporary Access-List entry
archive
manage archive files
auto
Exec level Automation
bfe
For manual emergency modes setting
calendar
Manage the hardware calendar
cd
Change current directory
clear
Reset functions
No authentication required for Level 15 exec commands
Done
221.198.55.105
FoxyProxy: Disabled

CT-1980028

Home Exec Configure

Command

show running-config

Output

Command base-URL was: /level/15/exec/-
Complete URL was: /level/15/exec/-/show/running-config/CR
Command was: show running-config

```
Building configuration...

Current configuration : 8995 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname CT-1980028
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
no aaa new-model
!
```

CT-1980028

Home Exec Configure

Command

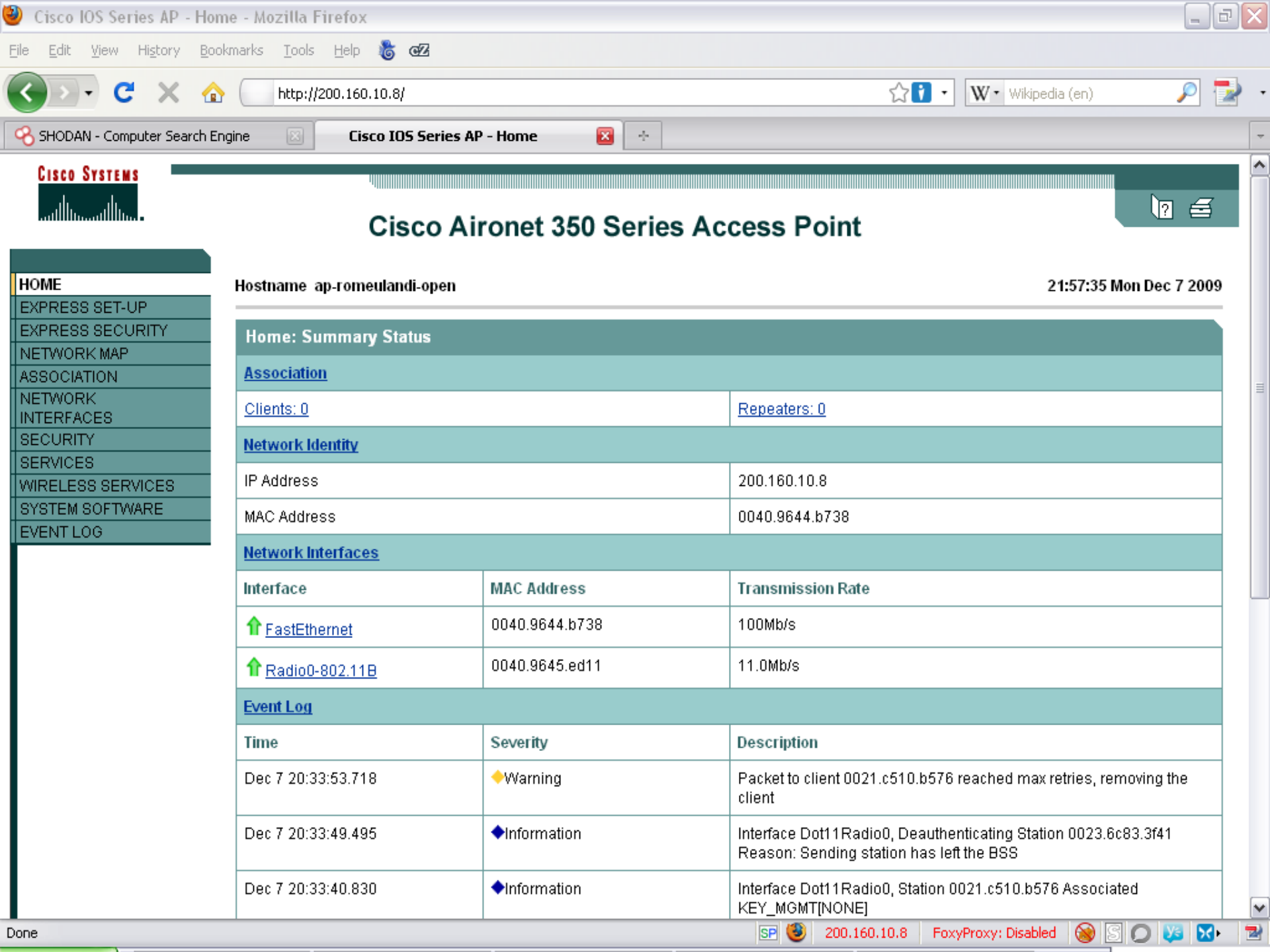
show cdp neighbors

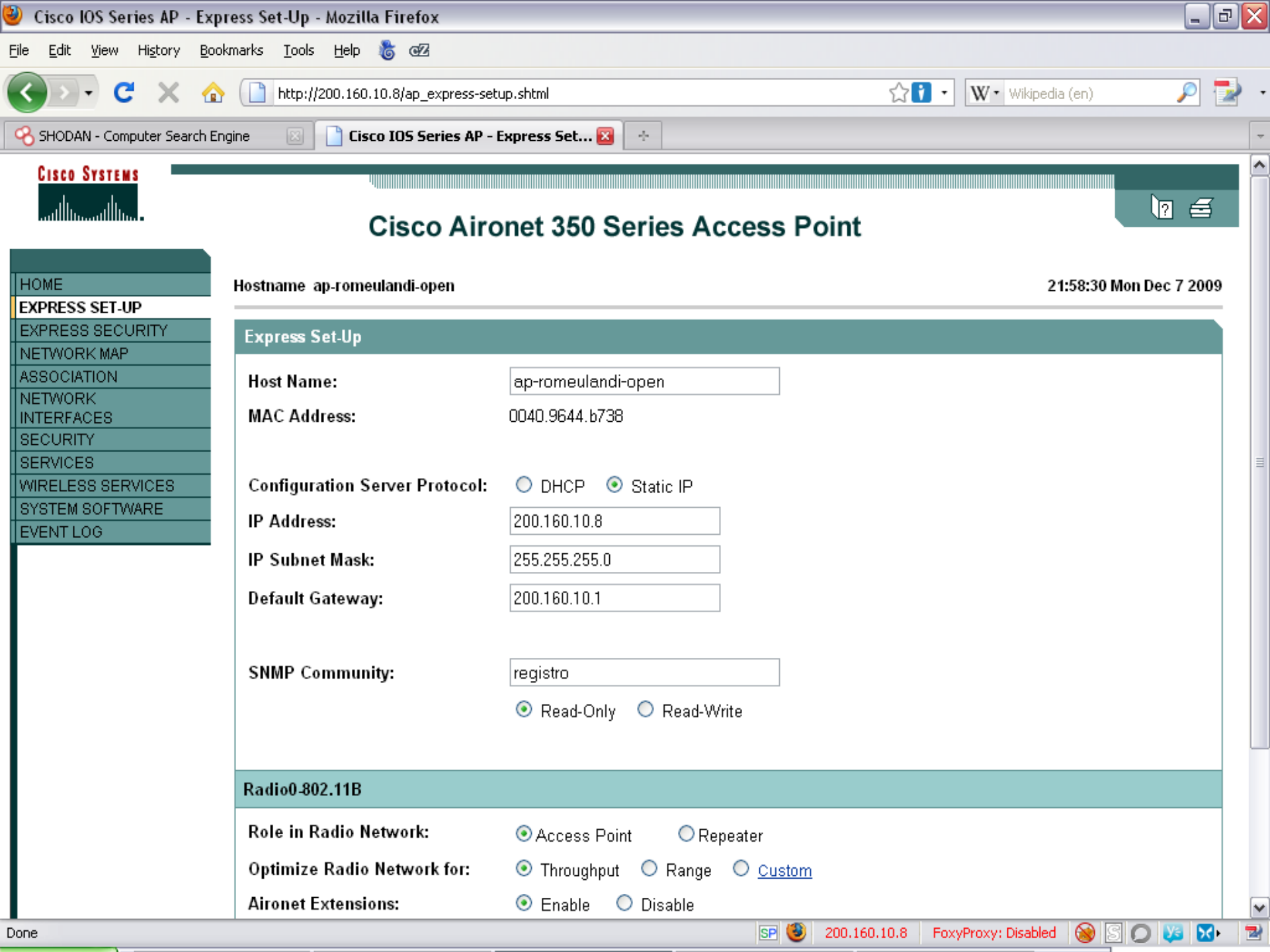
Output

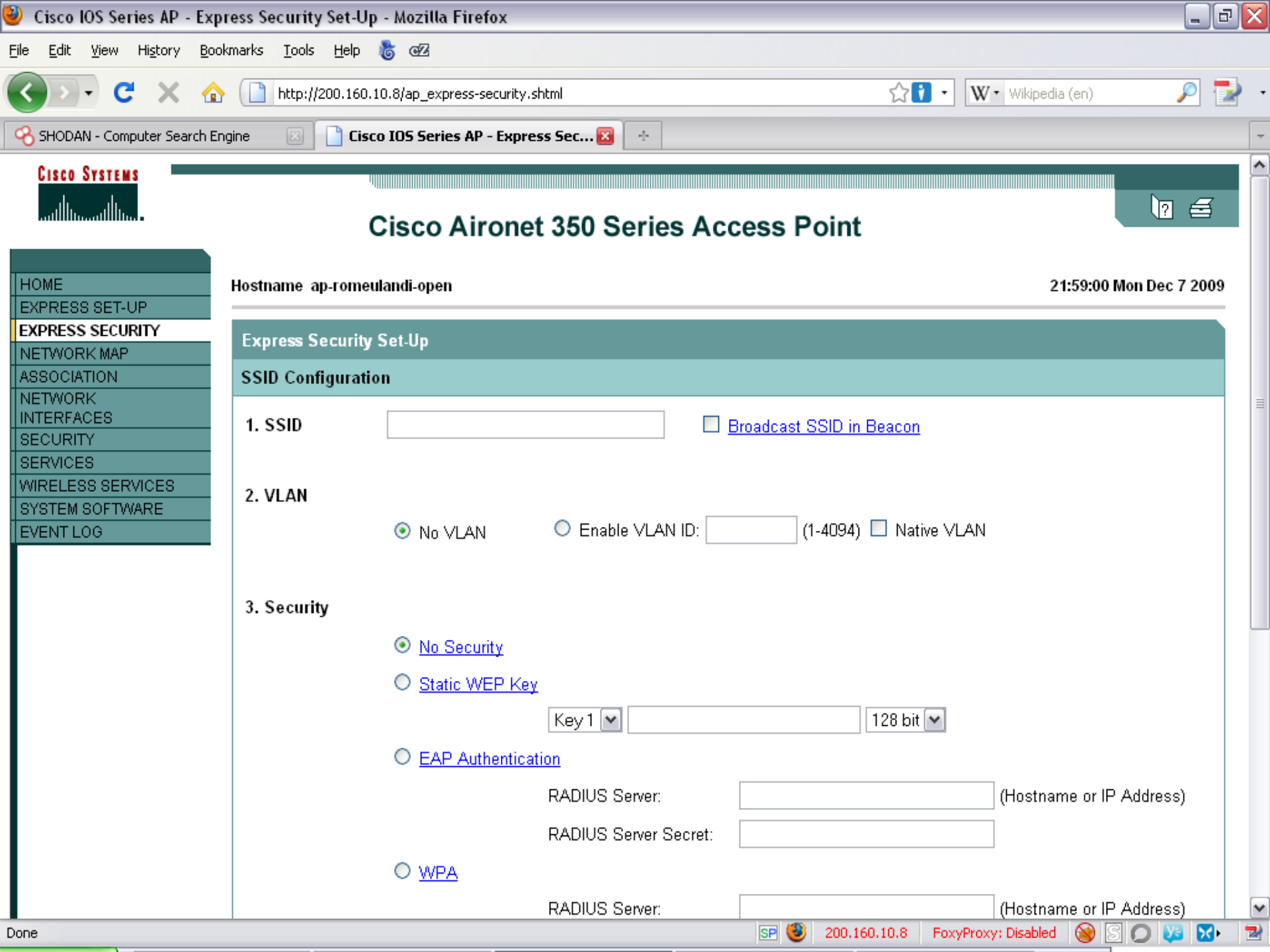
Command base-URL was: /level/15/exec/-
Complete URL was: /level/15/exec/-/show/cdp/neighbors/CR
Command was: show cdp neighbors

```
        this[0] = "CN-CNC-VPNHUB-1";
        this[1] = "10.97.248.1";
        this[2] = "Cisco 3745";
        this[3] = "Tunnel0";
        this[4] = "Tunnel0";
        this[5] = "R S I ";
        this[6] = "CN-CNC-VPNHUB-2";
        this[7] = "10.65.8.1";
        this[8] = "Cisco 3745";
        this[9] = "Tunnel1";
        this[10] = "Tunnel1";
        this[11] = "R S I ";
```

command completed.


Cisco IOS Series AP - Home - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://200.160.10.8/
Wikipedia (en)
SHODAN - Computer Search Engine
Cisco IOS Series AP - Home
Cisco Systems
Cisco Aironet 350 Series Access Point
HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP
ASSOCIATION
NETWORK INTERFACES
SECURITY
SERVICES
WIRELESS SERVICES
SYSTEM SOFTWARE
EVENT LOG
Hostname ap-romeulandi-open
21:57:35 Mon Dec 7 2009
Home: Summary Status
Association
Clients: 0
Repeaters: 0
Network Identity
IP Address
200.160.10.8
MAC Address
0040.9644.b738
Network Interfaces
Interface
MAC Address
Transmission Rate
FastEthernet
0040.9644.b738
100Mb/s
Radio0-802.11B
0040.9645.ed11
11.0Mb/s
Event Log
Time
Severity
Description
Dec 7 20:33:53.718
Warning
Packet to client 0021.c510.b576 reached max retries, removing the client
Dec 7 20:33:49.495
Information
Interface Dot11Radio0, Deauthenticating Station 0023.6c83.3f41 Reason: Sending station has left the BSS
Dec 7 20:33:40.830
Information
Interface Dot11Radio0, Station 0021.c510.b576 Associated KEY_MGMT[NONE]
Done
200.160.10.8
FoxyProxy: Disabled


Cisco IOS Series AP - Express Set-Up - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://200.160.10.8/ap_express-setup.shtml
Wikipedia (en)
SHODAN - Computer Search Engine
Cisco IOS Series AP - Express Set...
Cisco Systems
Cisco Aironet 350 Series Access Point
HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP
ASSOCIATION
NETWORK INTERFACES
SECURITY
SERVICES
WIRELESS SERVICES
SYSTEM SOFTWARE
EVENT LOG
Hostname ap-romeulandi-open
21:58:30 Mon Dec 7 2009
Express Set-Up
Host Name: ap-romeulandi-open
MAC Address: 0040.9644.b738
Configuration Server Protocol: DHCP Static IP
IP Address: 200.160.10.8
IP Subnet Mask: 255.255.255.0
Default Gateway: 200.160.10.1
SNMP Community: registro
Read-Only Read-Write
Radio0-802.11B
Role in Radio Network: Access Point Repeater
Optimize Radio Network for: Throughput Range Custom
Aironet Extensions: Enable Disable
Done
200.160.10.8
FoxyProxy: Disabled


Cisco IOS Series AP - Express Security Set-Up - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://200.160.10.8/ap_express-security.shtml
Wikipedia (en)
SHODAN - Computer Search Engine
Cisco IOS Series AP - Express Sec...
Cisco Systems
Cisco Aironet 350 Series Access Point
HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP
ASSOCIATION
NETWORK INTERFACES
SECURITY
SERVICES
WIRELESS SERVICES
SYSTEM SOFTWARE
EVENT LOG
Hostname ap-romeulandi-open
21:59:00 Mon Dec 7 2009
Express Security Set-Up
SSID Configuration
1. SSID
Broadcast SSID in Beacon
2. VLAN
No VLAN
Enable VLAN ID:
(1-4094)
Native VLAN
3. Security
No Security
Static WEP Key
Key 1
128 bit
EAP Authentication
RADIUS Server:
(Hostname or IP Address)
RADIUS Server Secret:
WPA
RADIUS Server:
(Hostname or IP Address)
Done
200.160.10.8
FoxyProxy: Disabled

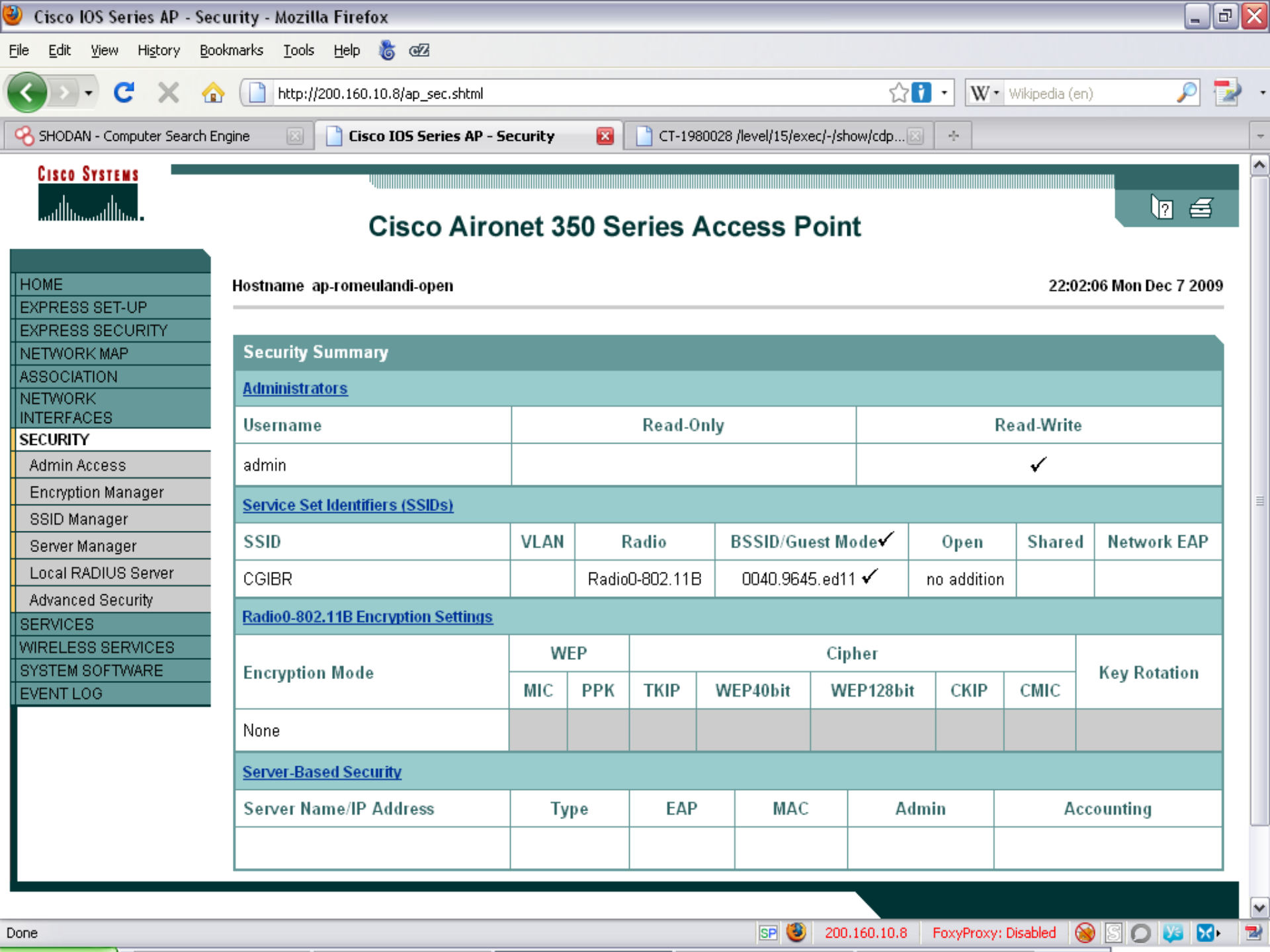
Cisco Systems

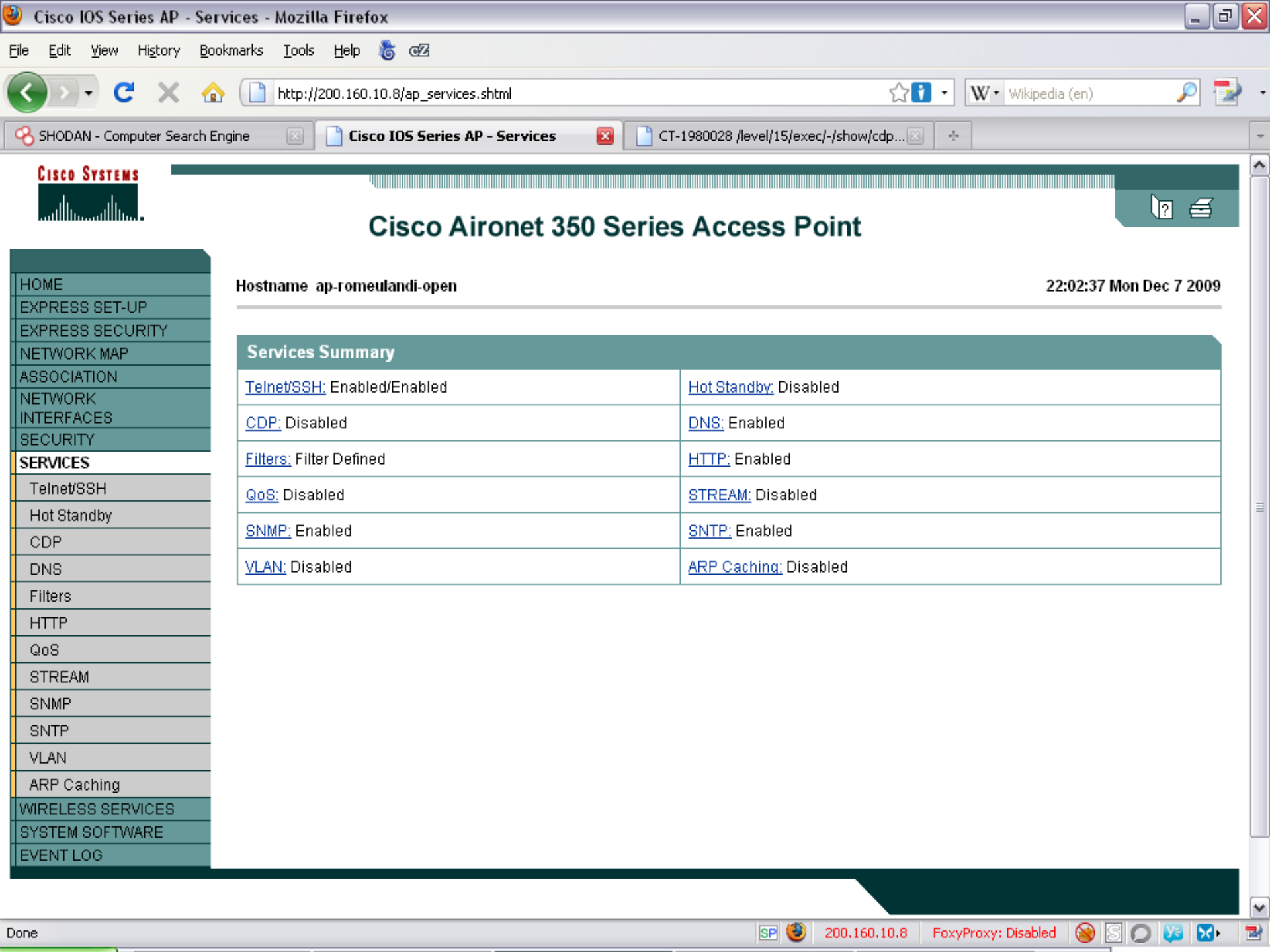
Cisco Aironet 350 Series Access Point

Hostname ap-romeulandi-open **22:01:40 Mon Dec 7 2009**

Network Interfaces: Summary

System Settings		
IP Address (Static)	200.160.10.8	
IP Subnet Mask	255.255.255.0	
Default Gateway	200.160.10.1	
MAC Address	0040.9644.b738	
Interface Status	FastEthernet	Radio0-802.11B
Software Status	Enabled ↑	Enabled ↑
Hardware Status	Up ↑	Up ↑
Interface Resets	0	1
Receive		
Input Rate Timespan	5 minute	5 minute
Input Rate (bits/sec)	2000	1000
Input Rate (packets/sec)	4	2
Time Since Last Input	00:00:00	04:27:34
Total Packets Input	54958045	56487586


Cisco IOS Series AP - Security - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://200.160.10.8/ap_sec.shtml
Wikipedia (en)
SHODAN - Computer Search Engine
Cisco IOS Series AP - Security
CT-1980028 /level/15/exec/-/show/cdp...
Cisco Systems
Cisco Aironet 350 Series Access Point
HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP
ASSOCIATION
NETWORK INTERFACES
SECURITY
Admin Access
Encryption Manager
SSID Manager
Server Manager
Local RADIUS Server
Advanced Security
SERVICES
WIRELESS SERVICES
SYSTEM SOFTWARE
EVENT LOG
Hostname ap-romeulandi-open
22:02:06 Mon Dec 7 2009
Security Summary
Administrators
Username | Read-Only | Read-Write
admin | | ✓
Service Set Identifiers (SSIDs)
SSID | VLAN | Radio | BSSID/Guest Mode | Open | Shared | Network EAP
CGIBR | | Radio0-802.11B | 0040.9645.ed11 ✓ | no addition | |
Radio0-802.11B Encryption Settings
Encryption Mode | WEP | Cipher | Key Rotation
MIC | PPK | TKIP | WEP40bit | WEP128bit | CKIP | CMIC
None
Server-Based Security
Server Name/IP Address | Type | EAP | MAC | Admin | Accounting
Done
200.160.10.8
FoxyProxy: Disabled


Cisco IOS Series AP - Services - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://200.160.10.8/ap_services.shtml
Wikipedia (en)
SHODAN - Computer Search Engine
Cisco IOS Series AP - Services
CT-1980028 /level/15/exec/-/show/cdp...
Cisco Systems
Cisco Aironet 350 Series Access Point
HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP
ASSOCIATION
NETWORK INTERFACES
SECURITY
SERVICES
Telnet/SSH
Hot Standby
CDP
DNS
Filters
HTTP
QoS
STREAM
SNMP
SNTP
VLAN
ARP Caching
WIRELESS SERVICES
SYSTEM SOFTWARE
EVENT LOG
Hostname ap-romeulandi-open
22:02:37 Mon Dec 7 2009
Services Summary
Telnet/SSH: Enabled/Enabled
Hot Standby: Disabled
CDP: Disabled
DNS: Enabled
Filters: Filter Defined
HTTP: Enabled
QoS: Disabled
STREAM: Disabled
SNMP: Enabled
SNTP: Enabled
VLAN: Disabled
ARP Caching: Disabled
Done
200.160.10.8
FoxyProxy: Disabled

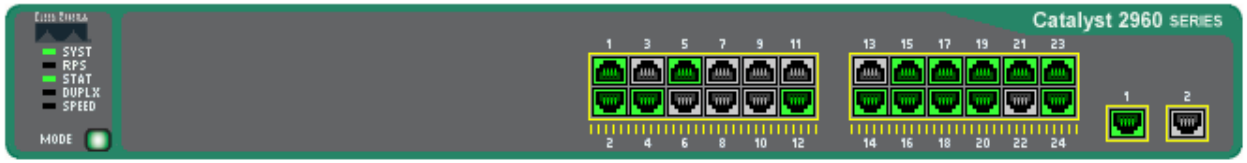
Catalyst 2960 Series Device Manager - STCM-sw1.cb3.bck Language: English

Refresh | Print | Smartports | Software Upgrade | Legend | Help

Uptime: 1 year, 32 weeks, 2 days, 19 hours, 28 minutes

Next refresh in **55** seconds

View : Status



Move the pointer over the ports for more information.

Contents

- Dashboard
- Configure
- Monitor
- Maintenance
- Network Assistant

Dashboard

Switch Information

Host Name:	STCM-sw1.cb3.bck
Product ID:	WS-C2960-24TT-L
IP Address:	217.75.0.230
MAC Address:	00:1E:BD:B8:18:80
Version ID:	V03
Serial Number:	FOC1149W02J
Software:	12.2(35)SE5
Contact:	
Location:	

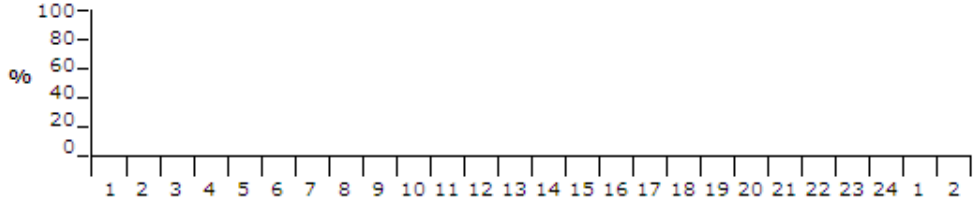
Switch Health

View Trends

Bandwidth Used	Packet Error	Fan	Temp
0%	0%	OK	OK

Port Utilization

View Trends | View Port Statistics



217.75.0.230 : Cisco Device Manager - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://217.75.0.230/xhome.htm

SHODAN - Computer Search Engine | 217.75.0.230 : Cisco Device Mana...

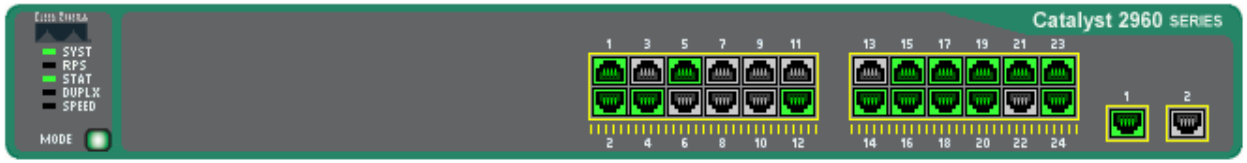
Catalyst 2960 Series Device Manager - STCM-sw1.cb3.bck Language: English

Refresh Print Smartports Software Upgrade Legend Help

Uptime: 1 year, 32 weeks, 2 days, 19 hours, 28 minutes

Next refresh in **27** seconds

View : Status



Move the pointer over the ports for more information.

Contents

- Dashboard
- Configure
  - Smartports
  - Port Settings
  - Express Setup
  - Restart / Reset
- Monitor
- Maintenance
- Network Assistant

Port Settings

Port	Description	Enable	Speed	Duplex
Fa0/18	SWS Spam firewall	☑	Auto	Auto
Fa0/19	IomegaNAS	☑	Auto	Auto
Fa0/20	Fix-IT DRAC port	☑	Auto	Auto
Fa0/21	Fix-IT Webfarm	☑	Auto	Auto
Fa0/22	Lynxtec Hosted ser	☑	Auto	Auto
Fa0/23	ESP Server	☑	Auto	Auto
Fa0/24	SWS Spam firewall	☑	Auto	Auto
Gi0/1	Uplink to SW12	☑	Auto	Auto

Submit Cancel

Done FoxyProxy: Disabled

217.75.0.230 : Cisco Device Manager - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://217.75.0.230/xhome.htm

Wikipedia (en)

SHODAN - Computer Search Engine | 217.75.0.230 : Cisco Device Mana...

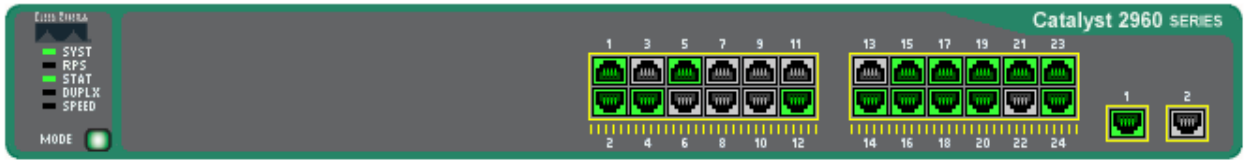
Catalyst 2960 Series Device Manager - STCM-sw1.cb3.bck Language: English

Refresh Print Smartports Software Upgrade Legend Help

Uptime: 1 year, 32 weeks, 2 days, 19 hours, 28 minutes

Next refresh in **5** seconds

View : Status



Move the pointer over the ports for more information.

Contents

- Dashboard
- Configure
  - Smartports
  - Port Settings
  - Express Setup
  - Restart / Reset
- Monitor
- Maintenance
- Network Assistant

Network Settings

Management Interface (VLAN ID):

IP Address: 217 . 75 . 0 . 230 Subnet Mask: 128.0.0.0

Default Gateway: 77 . 107 . 225 . 1

Switch Password: Confirm Switch Password:

Optional Settings

Host Name: STCM-sw1.cb3.bck

Telnet Access: Enable Disable

Telnet Password: Confirm Telnet Password:

Submit Cancel

Done

FoxyProxy: Disabled

217.75.0.230 : Cisco Device Manager - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://217.75.0.230/xhome.htm

SHODAN - Computer Search Engine | 217.75.0.230 : Cisco Device Mana...

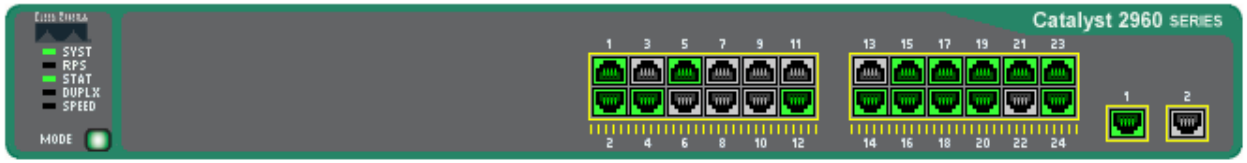
Catalyst 2960 Series Device Manager - STCM-sw1.cb3.bck Language: English

Refresh Print Smartports Software Upgrade Legend Help

Uptime: 1 year, 32 weeks, 2 days, 19 hours, 29 minutes

Next refresh in **37** seconds

View : Status



Move the pointer over the ports for more information.

Contents

- Dashboard
- Configure
  - Smartports
  - Port Settings
  - Express Setup
  - Restart / Reset
- Monitor
  - Trends
  - Port Status
  - Port Statistics
- Maintenance
- Network Assistant

Port Status

Port ▲	Description	Status	VLAN	Speed	Duplex
Fa0/1	APC Managed PDU	●	55	100	full
Fa0/2	Brillo Connection	●	1	100	full
Fa0/3	Sanquay Temp Firew	○	55		
Fa0/4		●	171	100	full
Fa0/5	Kirby - WF	●	104	10	full
Fa0/6		○	1		
Fa0/7		○	1		
Fa0/8		○	1		
Fa0/9		○	1		
Fa0/10		○	1		
Fa0/11	Sqnquay-CMR	○	801		
Fa0/12	AcomGUY Hosted ser	●	55	100	full
Fa0/13		○	1		
Fa0/14	Jacc.IT - PWCC WF	●	40	100	full

Done FoxyProxy: Disabled

Cisco SDM Express: 220.231.101.130

Help | About | Exit

Cisco SDM Express

Tasks

- Overview
- Basic Configuraton
- LAN
- Internet (WAN)
- Firewall
- DHCP
- NAT
- Routing
- Security
- Reset to Factory Default

Tools

- Ping
- Telnet
- Cisco SDM
- Software Update

Overview

LAN

Total Supported LAN: 2
Configured LAN Interface: 2

Internet (WAN)

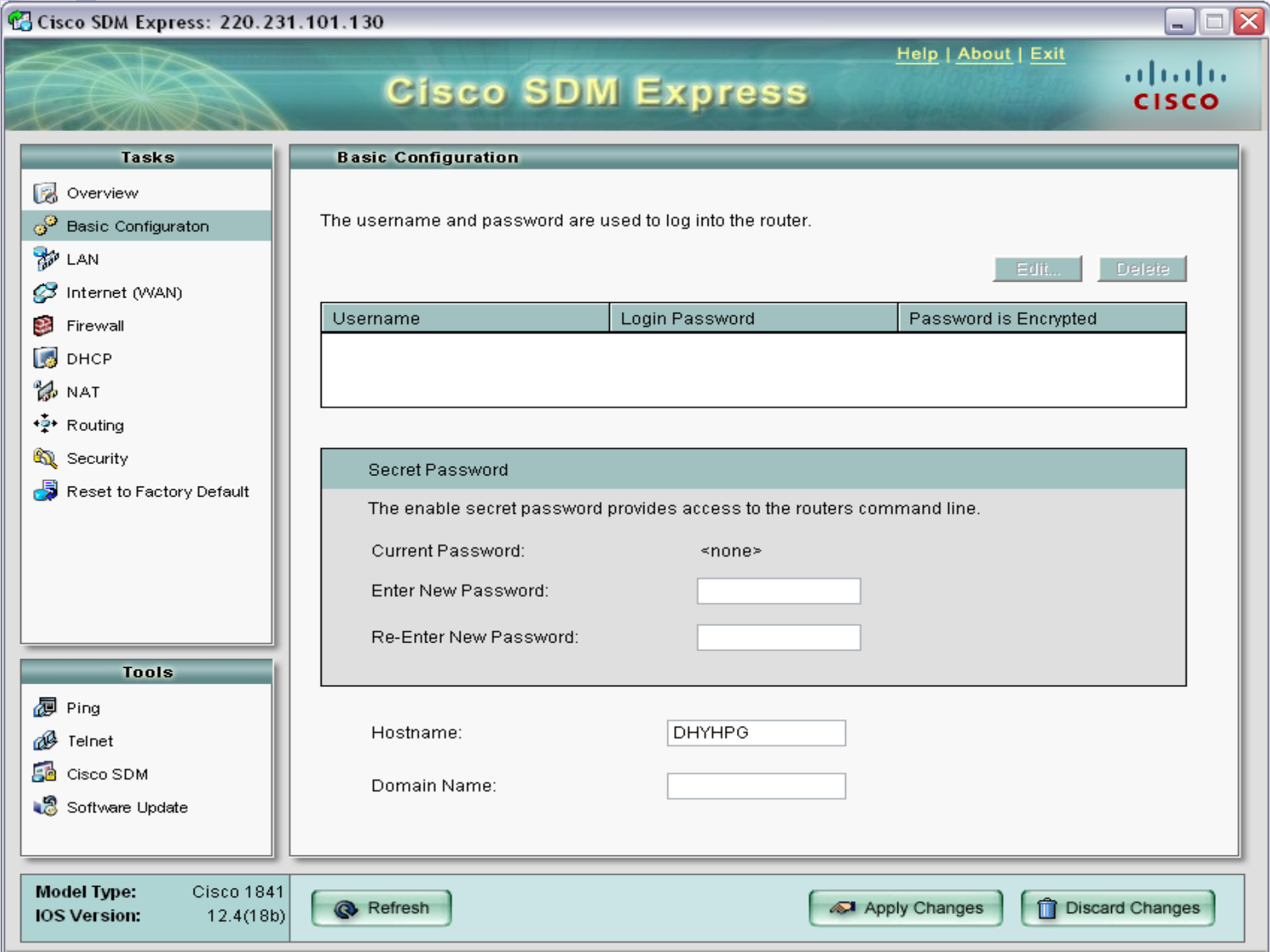
Total Supported WAN: 0
Total WAN Connections: 0

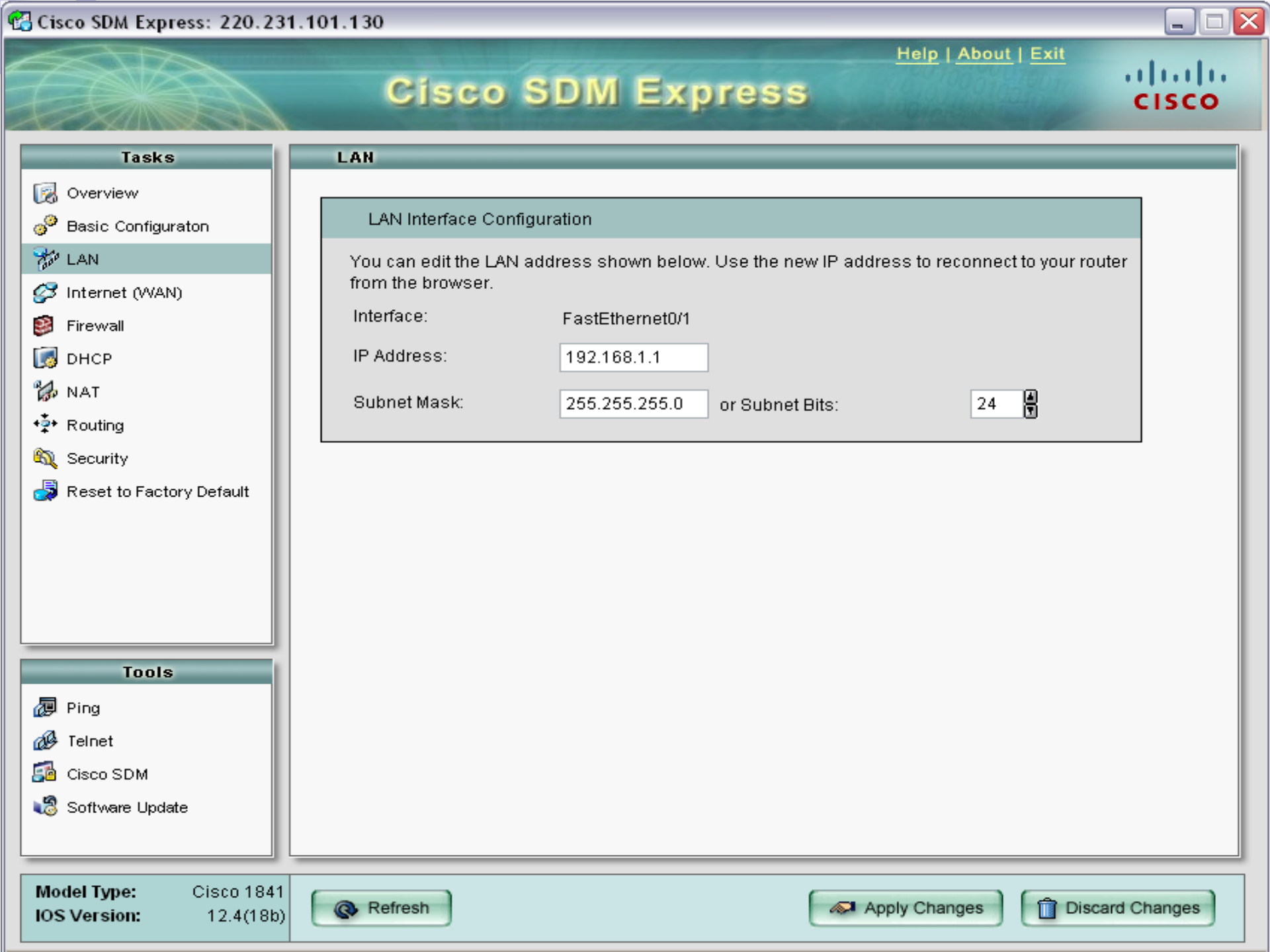
Firewall

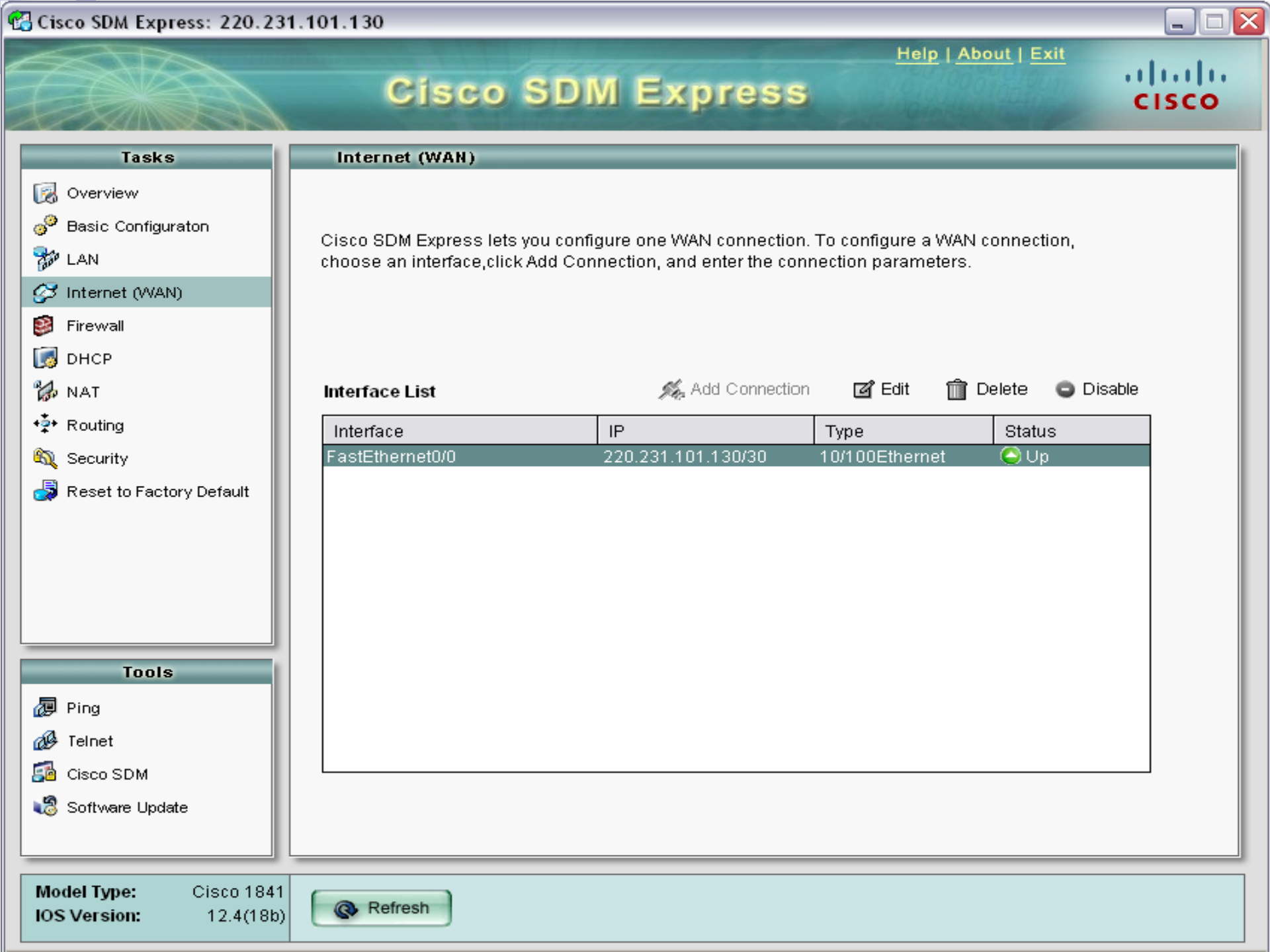
Firewall: Not Supported

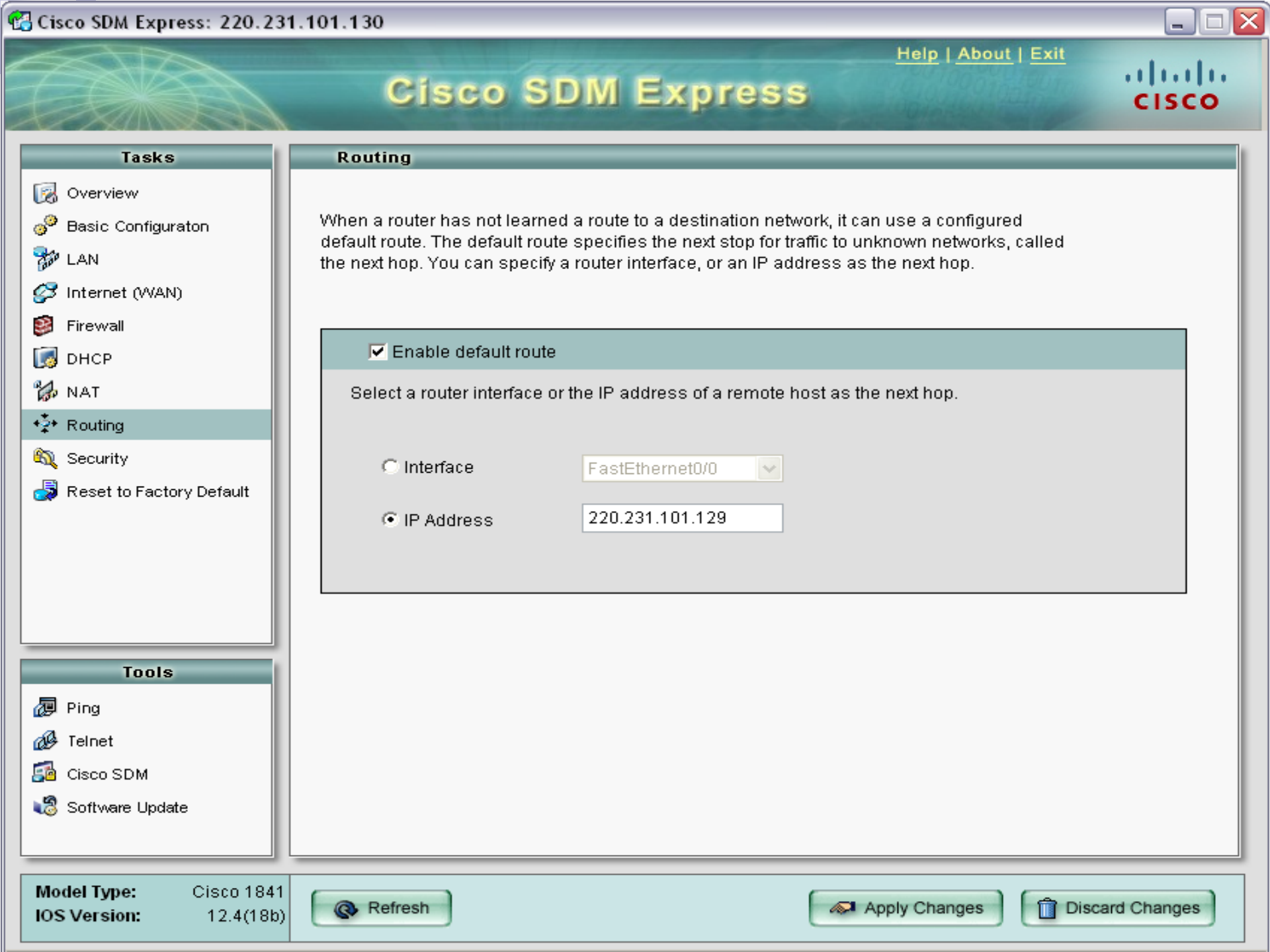
Model Type: Cisco 1841
IOS Version: 12.4(18b)

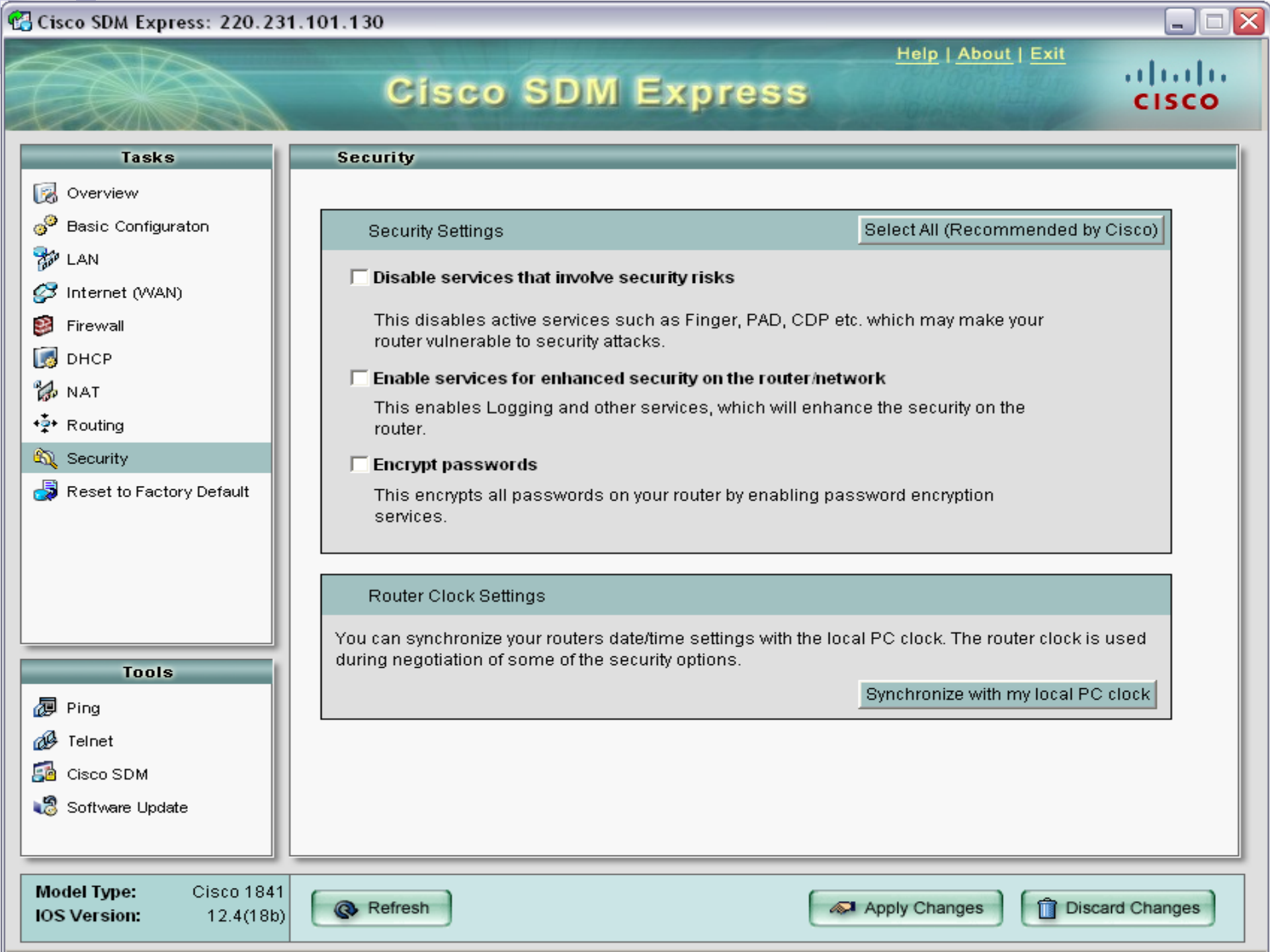
Refresh


Cisco SDM Express: 220.231.101.130
Help | About | Exit
Cisco SDM Express
cisco
Tasks
Overview
Basic Configuraton
LAN
Internet (WAN)
Firewall
DHCP
NAT
Routing
Security
Reset to Factory Default
Tools
Ping
Telnet
Cisco SDM
Software Update
Basic Configuration
The username and password are used to log into the router.
Edit...
Delete
Username
Login Password
Password is Encrypted
Secret Password
The enable secret password provides access to the routers command line.
Current Password:
<none>
Enter New Password:
Re-Enter New Password:
Hostname:
DHYHPG
Domain Name:
Model Type:
Cisco 1841
IOS Version:
12.4(18b)
Refresh
Apply Changes
Discard Changes


Cisco SDM Express: 220.231.101.130
Help | About | Exit
Cisco SDM Express
cisco
Tasks
Overview
Basic Configuraton
LAN
Internet (WAN)
Firewall
DHCP
NAT
Routing
Security
Reset to Factory Default
Tools
Ping
Telnet
Cisco SDM
Software Update
LAN
LAN Interface Configuration
You can edit the LAN address shown below. Use the new IP address to reconnect to your router from the browser.
Interface:
FastEthernet0/1
IP Address:
192.168.1.1
Subnet Mask:
255.255.255.0
or Subnet Bits:
24
Model Type:
Cisco 1841
IOS Version:
12.4(18b)
Refresh
Apply Changes
Discard Changes


Cisco SDM Express: 220.231.101.130
Help | About | Exit
Cisco SDM Express
cisco
Tasks
Overview
Basic Configuraton
LAN
Internet (WAN)
Firewall
DHCP
NAT
Routing
Security
Reset to Factory Default
Tools
Ping
Telnet
Cisco SDM
Software Update
Internet (WAN)
Cisco SDM Express lets you configure one WAN connection. To configure a WAN connection, choose an interface,click Add Connection, and enter the connection parameters.
Interface List
Add Connection
Edit
Delete
Disable
Interface
IP
Type
Status
FastEthernet0/0
220.231.101.130/30
10/100Ethernet
Up
Model Type:
Cisco 1841
IOS Version:
12.4(18b)
Refresh


Cisco SDM Express: 220.231.101.130
Help | About | Exit
Cisco SDM Express
cisco
Tasks
Overview
Basic Configuraton
LAN
Internet (WAN)
Firewall
DHCP
NAT
Routing
Security
Reset to Factory Default
Tools
Ping
Telnet
Cisco SDM
Software Update
Routing
When a router has not learned a route to a destination network, it can use a configured default route. The default route specifies the next stop for traffic to unknown networks, called the next hop. You can specify a router interface, or an IP address as the next hop.
Enable default route
Select a router interface or the IP address of a remote host as the next hop.
Interface
FastEthernet0/0
IP Address
220.231.101.129
Model Type: Cisco 1841
IOS Version: 12.4(18b)
Refresh
Apply Changes
Discard Changes


Cisco SDM Express: 220.231.101.130
Help | About | Exit
Cisco SDM Express
cisco
Tasks
Overview
Basic Configuraton
LAN
Internet (WAN)
Firewall
DHCP
NAT
Routing
Security
Reset to Factory Default
Tools
Ping
Telnet
Cisco SDM
Software Update
Security
Security Settings
Select All (Recommended by Cisco)
Disable services that involve security risks
This disables active services such as Finger, PAD, CDP etc. which may make your router vulnerable to security attacks.
Enable services for enhanced security on the router/network
This enables Logging and other services, which will enhance the security on the router.
Encrypt passwords
This encrypts all passwords on your router by enabling password encryption services.
Router Clock Settings
You can synchronize your routers date/time settings with the local PC clock. The router clock is used during negotiation of some of the security options.
Synchronize with my local PC clock
Model Type: Cisco 1841
IOS Version: 12.4(18b)
Refresh
Apply Changes
Discard Changes

SHODAN for Penetration Testers

CASE STUDY: DEFAULT PASSWORDS

Case Study: Default Passwords (1)

- The ‘default password’ search locates servers that have those words in the banner
- This doesn’t suggest that these results will be using the defaults, but since they’re advertising the defaults they would potentially be the lowest hanging fruit

Case Study: Default Passwords (2)

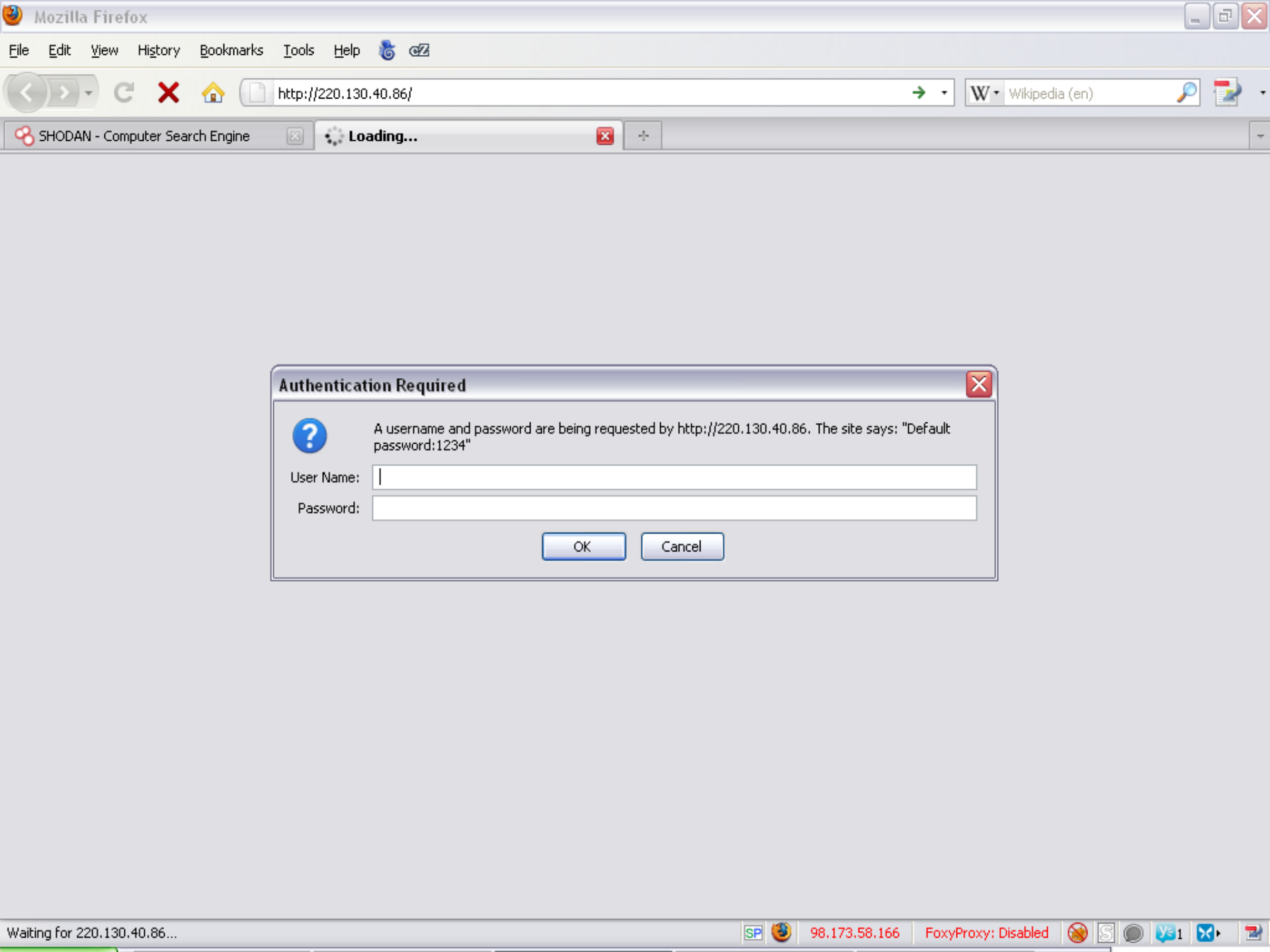
An example of a ‘default password’ result:

```
HTTP/1.0 401
Date: Sat, 21 Dec 1996 12:00:00 GMT
Www-authenticate: Basic realm="Default password:1234"
Server: PrintSir WEBPORT 1.1
```

The server line indicates this is likely to be a print server; also note the “401” and *Www-authenticate* which indicates the likelihood of a username and password pop-up box

Case Study: Default Passwords (3)

- This does not suggest that this device is using the default password, but it does mean that it is a possibility
- While no username is listed, a null username or “admin” is always a good guess
- And did it work?


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://220.130.40.86/
Wikipedia (en)
SHODAN - Computer Search Engine
Loading...
Authentication Required
A username and password are being requested by http://220.130.40.86. The site says: "Default password:1234"
User Name:
Password:
OK
Cancel
Waiting for 220.130.40.86...
98.173.58.166
FoxyProxy: Disabled


Edimax Print Server - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://220.130.40.86/
Wikipedia (en)
SHODAN - Computer Search Engine
Edimax Print Server
EDIMAX
NETWORKING PEOPLE TOGETHER
Device Setup
Setup Wizard
System Tools
¨t²Î¸ê°T
¦L¸ï¾÷ ¸¨°A
TCP / IP ¸¨°A
SMB ¸¨°A
SNMP ¸¨°A
NetWare ¸¨°A
AppleTalk ¸¨°A
¦C¦L¦o³A¾¹¨Æ¨t²Î¨]©w.
¨t²Î¸ê°T
¸Ë¸m¦W¦Ù : PSCC789E
¦C¦L¦ø³A¾¹¦W¦Ù : EPSON680
¾÷«¬¸¹½X : PS1206P
¶}©l®É¶¡ : 2.6.21
µwÅé(MAC)¦a§} : 00:00:B4:CC:78:9E
USB Port Number : No
LPT Port Number : 1
µL½u¯Ï¯°ô¸ô¸¨°A : No
Raw Printing : Enable
IPP Printing : Enable
LPR Printing : Enable
AppleTalk Printing : Enable
NetWare Printing : Enable
SMB : Enable
SNMP : Enable
NetBEUI : Disable
Done
220.130.40.86
FoxyProxy: Disabled

SHODAN for Penetration Testers

CASE STUDY: ~~INFRASTRUCTURE EXPLOITATION~~ How to PWN an ISP

Cisco Systems

Accessing Cisco WS-C3750G-12S

Telnet - to the router.

Show interfaces - display the status of the interfaces.
Show diagnostic log - display the diagnostic log.
Monitor the router - HTML access to the command line interface at level 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
Connectivity test - ping the nameserver.

Show tech-support - display information commonly needed by tech support.
Extended Ping - Send extended ping commands.

Web Console - Manage the Switch through the web interface.

Help resources

1. CCO at www.cisco.com - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. tac@cisco.com - e-mail the TAC.
3. **1-800-553-2447 or +1-408-526-7209** - phone the TAC.
4. cs-html@cisco.com - e-mail the HTML interface development group.

Home Exec Configure

Command

Output

```
Command base-URL was: /level/15/exec/-
Complete URL was:/level/15/exec/-/show/ip/route/CR
Command was: show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is                 to network 0.0.0.0

                      is variably subnetted, 10 subnets, 3 masks
D EX                       [170/28416] via                   2w5d, Vlan401
                           [170/28416] via                 2w5d, Vlan400
D                          [90/3072] via                  2w5d, Vlan401
                           [90/3072] via                 2w5d, Vlan400
D EX                       [170/4226816] via                   3w5d, Vlan401
                           [170/4226816] via                 3w5d, Vlan400
D EX                       [170/3115776] via                   3w5d, Vlan401
                           [170/3115776] via                 3w5d, Vlan400
D EX
           [170/2178816] via                    02:01:41, Vlan401
           [170/2178816] via                  02:01:41, Vlan400
D EX                       [170/3072] via                  2w5d, Vlan401
                           [170/3072] via                  2w5d, Vlan401
```

Home Exec Configure

Command

Output

```
Command base-URL was: /level/15/exec/-
Complete URL was:/level/15/exec/-/show/running-config/CR
Command was: show running-config
```

```
Building configuration...

Current configuration : 10374 bytes
!
! Last configuration change at 06:40:37 EST Tue Apr 6 2010 by
! NVRAM config last updated at 06:40:48 EST Tue Apr 6 2010 by
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname
!
boot-start-marker
boot-end-marker
!
!
username          privilege 15 secret 5
username         privilege 2 secret 5
aaa new-model
!
!
```

Command

Output

```
Command base-URL was: /level/15/exec/-
Complete URL was:/level/15/exec/-/show/cdp/neighbors/CR
Command was: show cdp neighbors
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

                 Gig 1/0/11        173          R S I     CISCO7606 Gig 1/6

                 Gig 1/0/12        143          R S I     WS-C3750G Gig 1/0/12
                 Gig 1/0/2         155           S I      WS-C3750- Gig 1/0/1
                 Gig 1/0/10        167           S I      WS-C3560E Gig 0/25

                 Gig 1/0/9         131          R S I     WS-C3750- Gig 1/0/1
```

command completed.

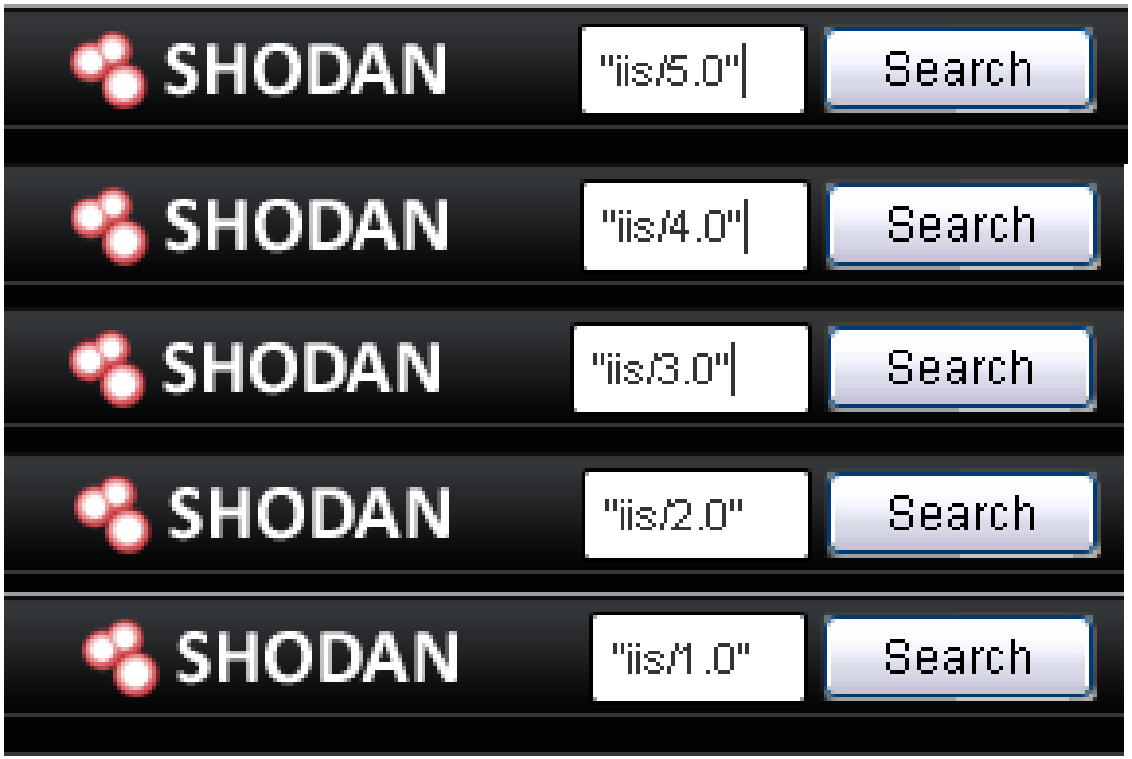
Case Study: *How to PWN an ISP*

- Two Cisco 3750 infrastructure switches with direct access to Cisco 7606 Router
- VLAN IDs for internal ISP network, hotels, condos, apartments, convention center, public backbone…
- SNMP server IP address and community strings

SHODAN for Penetration Testers

OTHER EXAMPLES

Some general observations…



Results **1** - **10** of about **362695** for **"iis/5.0"**

Results **1** - **10** of about **9977** for **"iis/4.0"**

Results **1** - **10** of about **381** for **"iis/3.0"**

Results **1** - **10** of about **42** for **"iis/2.0"**

Results **1** - **10** of about **159** for **"iis/1.0"**

Wireless Network Camera with Pan/Tilt - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://220.248.51.206/

SHODAN - Computer Search Engine | Wireless Network Camera with P...

Logitec

Logitec Wireless Network Camera

Block

設定項目

-- 1つを選択 --

水平移動間隔 0

上下移動間隔 0

Pan Stop Patrol

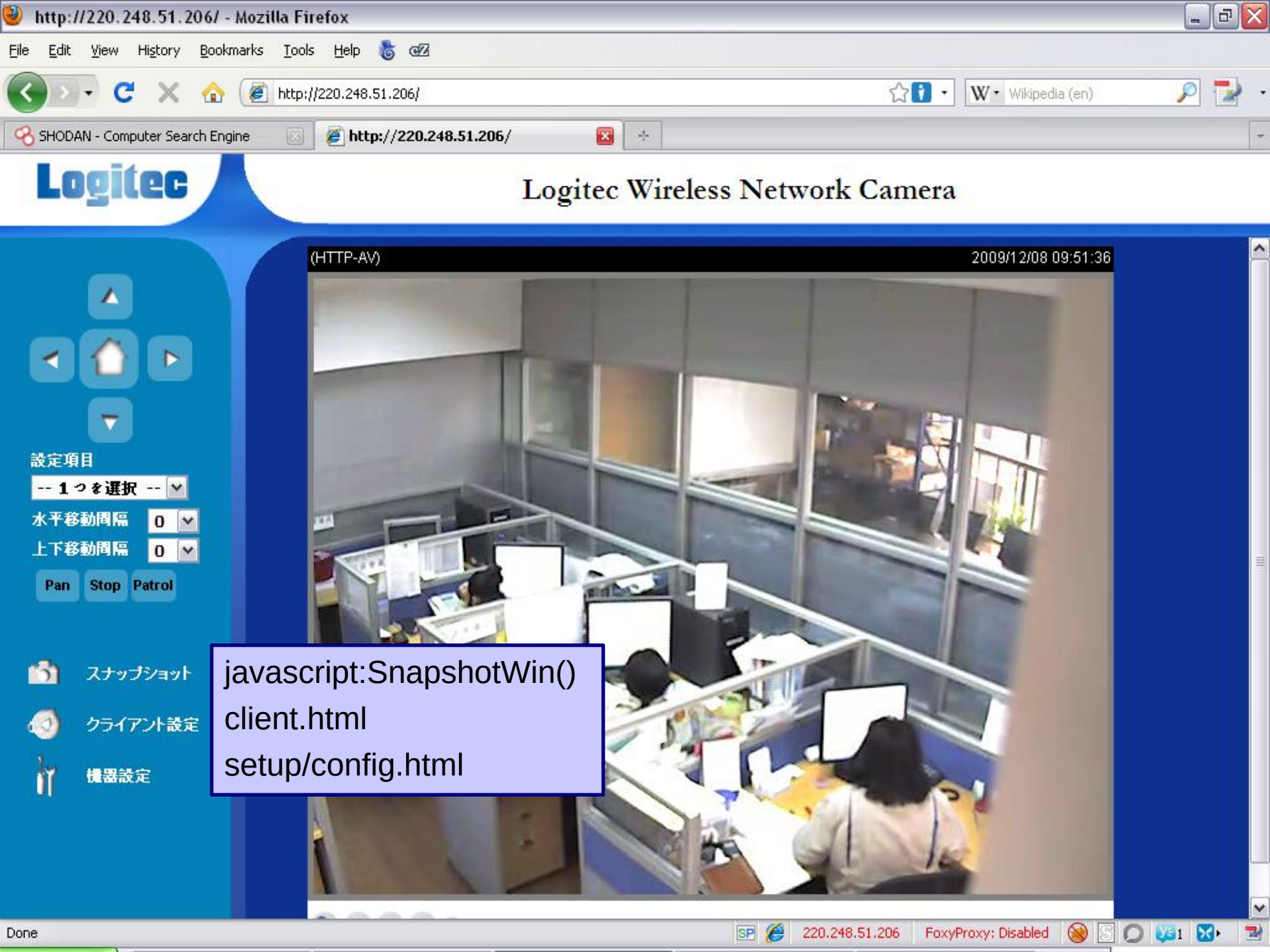
スナップショット

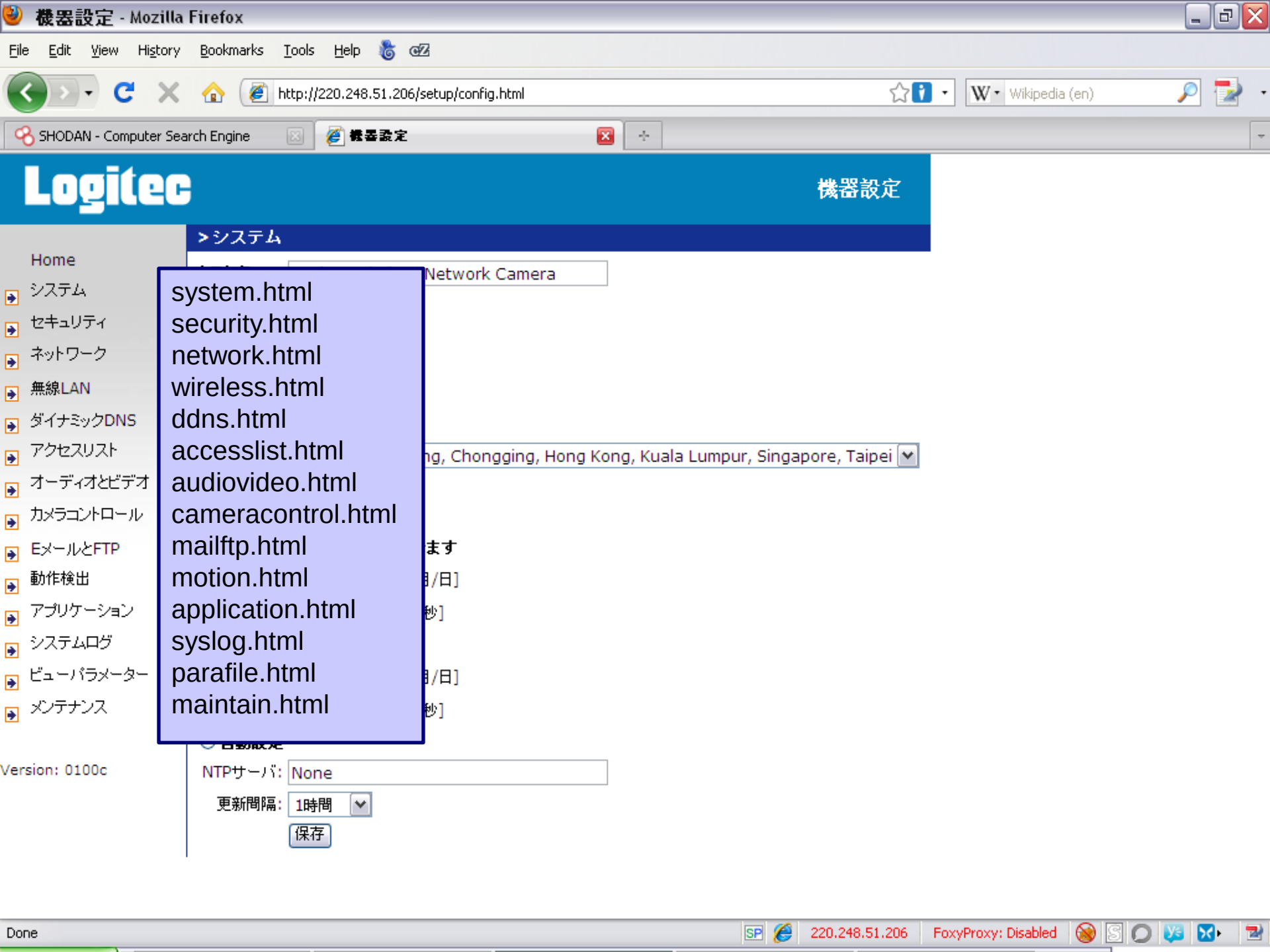
クライアント設定

javascript:SnapshotWin()
client.html

Done

220.248.51.206 FoxyProxy: Disabled


http://220.248.51.206/ - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://220.248.51.206/
Wikipedia (en)
SHODAN - Computer Search Engine
http://220.248.51.206/
Logitec
Logitec Wireless Network Camera
(HTTP-AV)
2009/12/08 09:51:36
設定項目
-- 1つを選択 --
水平移動間隔
0
上下移動間隔
0
Pan
Stop
Patrol
スナップショット
クライアント設定
機器設定
javascript:SnapshotWin()
client.html
setup/config.html
Done
220.248.51.206
FoxyProxy: Disabled


機器設定 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://220.248.51.206/setup/config.html
Wikipedia (en)
SHODAN - Computer Search Engine
機器設定
Logitec
機器設定
> システム
Home
システム
セキュリティ
ネットワーク
無線LAN
ダイナミックDNS
アクセスリスト
オーディオとビデオ
カメラコントロール
EメールとFTP
動作検出
アプリケーション
システムログ
ビューパラメーター
メンテナンス
Version: 0100c
Network Camera
ng, Chongging, Hong Kong, Kuala Lumpur, Singapore, Taipei
NTPサーバ: None
更新間隔: 1時間
保存
system.html
security.html
network.html
wireless.html
ddns.html
accesslist.html
audiovideo.html
cameracontrol.html
mailftp.html
motion.html
application.html
syslog.html
parafile.html
maintain.html
Done
220.248.51.206
FoxyProxy: Disabled

SHODAN for Penetration Testers

THE FUTURE

The Future

- API in the works for program integration
- Summary report for export option
- Software fingerprints
- Collection of HTTPS

SHODAN for Penetration Testers

CONCLUSIONS

Conclusions

- SHODAN aggregates a significant amount of information that isn't already widely available in an easy to understand format
- Allows for passive vulnerability analysis

Bottom line: SHODAN is a potential game-changer for pen testers that will help shape the path for future vulnerability assessments

Authors and add-ons

- John Matherly (http://twitter.com/achillean)
- Gianni Amato (SHODAN Helper)
- sagar38 (SHODAN Search Provider)

SHODAN for Penetration Testers

QUESTIONS

SHODAN for Penetration Testers

Michael “theprez98” Schearer