

## Quick Configuration Guide

# Cisco Media Monitoring Feature - Remote Data Collection with Web Services Management Agent

Last Updated: 2/3/2011

### Introduction

This quick configuration guide provides an overview and reference configuration of features necessary to enable remote data collection and management for the Cisco Media Monitoring feature. This guide is meant to provide a level of familiarity Web Services Management Agent (WSMA) feature and to provide a reference configuration which includes configuration of any desired security mechanisms for authenticating, authorizing and encrypting the transport and validating the commands to be executed by the router.

### Quick Start Summary Steps

Configure WSMA

1. Enable a transport mechanism
2. Configure authentication and authorization methods
3. Create WSMA profiles
4. Enable WSMA agents

### Requirements

The objective of this document is to provide familiarity with the WSMA facility, specifically how it may be used to configure Cisco Media Monitoring feature and to use WSMA for retrieval of data. In order to have hands-on experience with the feature the following is the minimum equipment requirements.

Table 1: Basic Equipment Requirements

Item	Quantity	Notes
IOS router or switch with performance-monitor and Mediatrace software	2	
RTP/TCP traffic generator and sink	1 generator 1 sink	The generator and sink are used to generate and receive traffic for both Mediatrace and performance-monitor to monitor. Examples of RTP generators: Cisco IP phones, Cisco Telepresence, Tandberg Video Conferencing equipment, Video LAN client[4], Cisco Video SLA Assessment Agent (VSAA), packETH [5], IOS IPSLA Video Operation (IPSLA-VO) Examples of RTP sinks: Cisco IP phones, Cisco Telepresence, Tandberg Video Conferencing equipment, Video LAN client, Cisco Video SLA Assessment Agent (VSAA), IPSLA VO
Workstation	1	The workstation will represent a management platform that has capability to interact with a WSMA enable network device. In these exercises a Linux workstation with the Wget CLI application is used to send and retrieve SOAP requests.

For support of the Cisco Mediatrace feature, IOS 15.1(3)T was used for the examples in this configuration guide.

```

Cisco IOS Software, C1861 Software (C1861-ADVENTERPRISEK9-M), Version 15.1(3)T,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Mon 15-Nov-10 20:58 by prod_rel_team

ROM: System Bootstrap, Version 12.4(11r)XW3, RELEASE SOFTWARE (fc1)

1861-AA0213 uptime is 2 days, 23 hours, 36 minutes
System returned to ROM by reload at 11:51:51 EST Fri Jan 7 2011
System restarted at 11:52:53 EST Fri Jan 7 2011
System image file is "flash:c1861-adventerprisek9-mz.151-3.T.bin

```

Figure 2: Router code version utilized.

## Introduction to Web Services

Several features combine together to provide a web services based access into a router or switch to the Command Line, Executive Filesystem, and Notification interfaces. A web service known as WSMA provides the first line of entry to the device. WSMA is a web service and also implements the Simple Object Access Protocol (SOAP), for encapsulating messages to and from the CLI, EXEC, Filesys and Notify interfaces.

## High Level Steps

The high level steps that will be performed as an example configuration of WSMA and the Cisco Mediatrace feature are as follows:

Step	Where
1. Enable a transport mechanism (Router)	Network device
2. Configure authentication and authorization methods for the transport and Exec interfaces	Network device
3. Create WSMA profiles that define parameters for the agent	Network device
4. Enable WSMA agents that provide access to exec, CLI, filesys and response systems Apply WSMA profile to WSMA agents.	Network device

### 1. Enable a transport mechanism (Router)

It is necessary to configure a transport service on the router or switch that allows the Web Service Management Agent (WSMA) to receive messages. The agent interoperates with four possible transports, so select one of the following transports for the agent to utilize:

- HTTP
- Secure HTTP (HTTPS)
- Secure Shell (SSH)
- TLS

For these exercises a Linux workstation with the Wget software package is being utilized to post requests and receive data from the network nodes that are enabled with WSMA. Wget is a non-interactive command line tool and can utilize the HTTP, HTTPS or FTP transports.

## 2. Configure authentication and authorization methods for the transport and Exec interfaces

For the examples, the HTTPS transport will be utilized, and the sessions will be authenticated using AAA with Cisco ACS 5.1. Multiple different authentication mechanisms are possible but AAA is a common method utilized by many customers and provides a more interesting configuration to illustrate. With HTTPS, the data transported by HTTP will be encrypted between the Linux workstation and the network node. It is recommended to utilize a secure transport such as HTTPS or SSH as passwords may be transmitted.

The HTTPS transport is enabled and AAA authentication is applied. Secure HTTP utilizes web certificates to exchange encryption keys between the session endpoints, and a web certificate configuration is a prerequisite for HTTPS on the router. The following commands were entered to enable HTTPS transport and set the authentication method to local, which utilizes locally configured usernames.

```
Router1(config)#
ip http secure-server
ip http authentication local
username HTTPtest password 0 cisco
```

Figure 2: Configuration of the secure HTTPS transport and authentication method

The web certificates may be created locally by the router, or managed by a central server. In this lab example, locally signed web certificates are used, and no explicit commands were entered. When HTTPS is enabled the configuration for local web certificates is automatically generated, and looks as follows.

```
Router1(config)#ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

3845-AA0216(config)#
*Jan 10 14:49:22.573: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Jan 10 14:49:22.629: %PKI-4-NOAUTOSAVE: Configuration was modified. Issue "write
memory" to save new certificate
```

Figure 3: Automatic web certificate creation

To validate whether a certificate is available utilize the crypto pki command set.

```
Router1#sh crypto pki certificate
Router Self-Signed Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: General Purpose
  Issuer:
    cn=IOS-Self-Signed-Certificate-2886318522
  Subject:
    Name: IOS-Self-Signed-Certificate-2886318522
    cn=IOS-Self-Signed-Certificate-2886318522
  Validity Date:
```

```
start date: 14:49:22 EST Jan 10 2011
end   date: 19:00:00 EST Dec 31 2019
Associated Trustpoints: TP-self-signed-2886318522
```

Figure 4: Validation of crypto certificate

To validate the status of the HTTP server the following CLI commands may be used. Note that secure HTTP and HTTP are separate services and when utilizing HTTPS, the HTTP service should normally be disabled. Otherwise secure and non secure HTTP are both enabled and circumvents the value of enabling HTTPS.

```
Router1#sh ip http server status
HTTP server status: Disabled
HTTP server port: 80
HTTP server active supplementary listener ports:
HTTP server authentication method: local
HTTP server digest algorithm: md5
HTTP server access class: 0
HTTP server base path:
HTTP server help root:
Maximum number of concurrent server connections allowed: 5
Server idle time-out: 180 seconds
Server life time-out: 180 seconds
Maximum number of requests allowed on a connection: 1
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-128
-sha
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:
HTTP secure server active session modules: ALL
```

Figure 5: Validation of HTTP server status

Before proceeding with further configuration of WSMA, validate that HTTPS and your chosen authentication method are correctly working. A simple way to do this is browsing with a web client to the router or switch and ensure you can successfully connect to the network device before proceeding. Below is an example of this. Note that since locally significant web certificates are used, the browser has prompted whether the certificate is trusted and then proceeds to request the authentication. Your results may vary depending on the browser utilized, but the idea is to ensure that a successful HTTPS connection can be made.

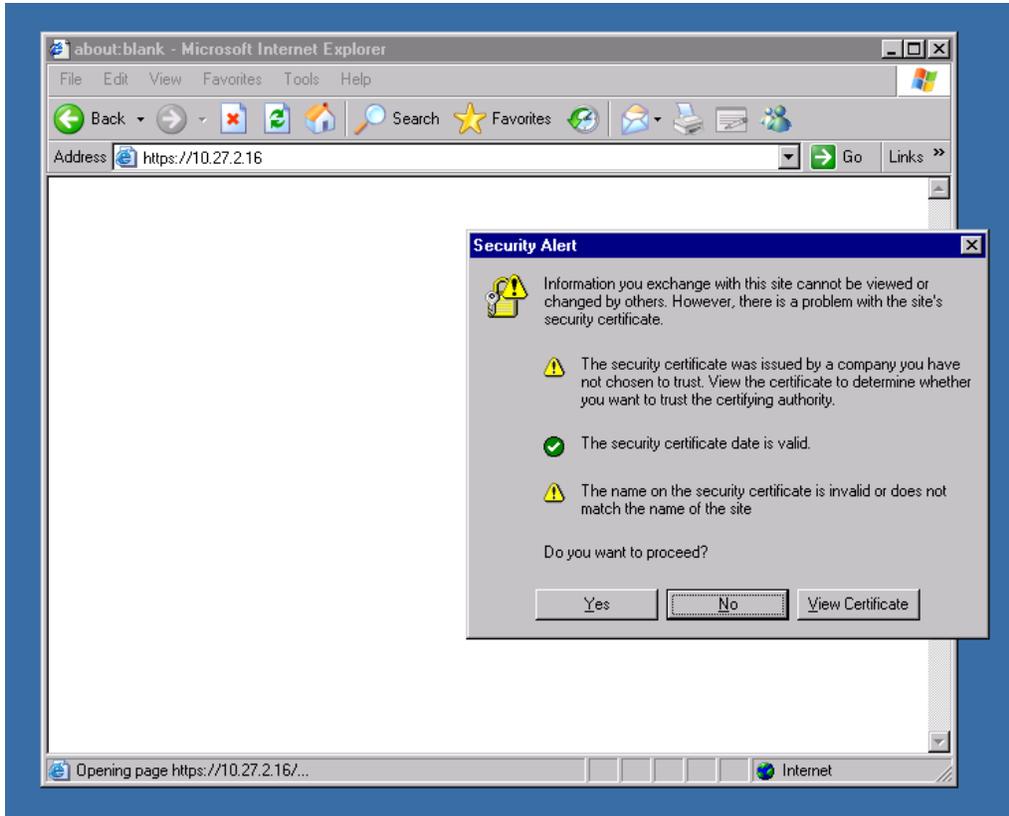


Figure 6: Validate HTTPS connectivity

### 3. Create WSMA profiles that define parameters for the agent

WSMA profiles allow modular grouping of commands that can then be applied to a WSMA agent.

Two types of profile exist, listeners and initiators. For these examples, a listener type profile is required. Listener profiles define instances of web services that service externally originated connections, and initiators are used when the local device will initiate a connection. In the example below, a profile with name "test" is created and configured with the secure HTTP transport. WSMA can provide authorization of commands that are sent within the SOAP message and this is enabled with the command "wsse".

When WSSE is enabled it is necessary to include a WSSE section in the SOAP message as will be seen shortly. There are no specific commands to configure the authorization method. The method specified by the transport section, in this example HTTPS, will also determine the method utilized for WSSE.

```
Router1 (config)#
wsma profile listener test
transport https
wsse
```

Figure 7: Creating a WSMA profile

This profile is now ready to be applied to a Web Service Management Agent.

#### 4. Enable WSMA agents that provide access to exec, CLI, fileys and response systems. Apply WSMA profile to WSMA agents.

Four different types of WSMA's exist.

- EXEC Agent
- Config Agent
- Filesys Agent
- Notify Agent

To allow connection to the Exec interface which allows the use of Media Monitoring show commands, and to perform configuration of Media Monitoring features, the Exec and Config agent are the minimum agents required.

Each agent is enabled with a separate command that specifies the WSMA profile that will be used for the specific agent.

```
Router1 (config)#
wsma agent exec profile test
wsma agent config profile test
wsma agent filesys profile test
wsma agent notify profile test
```

Figure 8: Enable WSMA agents and apply profiles

In this example, all four agents have been enabled and each specifies the same WSMA listener profile.

#### WSMA integration with Mediascope

Mediascope is a standalone GUI based application that illustrates how WSMA may be utilized by a management application to build a network map that incorporates data from Mediatrace along a network path. It utilizes the WSMA capability on the network devices and utilizes both HTTP and SSH transports. Mediascope does not perform WSSE authentication of the requests. The following is a sample of a configuration for use with Mediascope.

Note: When HTTP is used as a transport, the passwords for HTTP and WSSE authentication are sent in clear text across the network.

```
Router1 (config)#
wsma agent exec profile http
wsma agent config profile http
wsma agent filesys profile ssh
wsma agent notify profile ssh
!
wsma profile listener http
no wsse authorization level 15
transport http
!
wsma profile listener ssh
no wsse authorization level 15
transport ssh
!
```

Figure 20: WSMA configuration for Mediascope

#### APPENDIX II Complete router configuration

The unabbreviated configuration below is from the Mediatrace initiator router, after the Mediatrace has been configured.

```

1861-AA0213#sh run
Load for five secs: 1%/0%; one minute: 5%; five minutes: 7%
Time source is NTP, 08:57:23.238 EST Tue Jan 25 2011

Building configuration...

Current configuration : 12188 bytes
!
! Last configuration change at 08:54:15 EST Tue Jan 25 2011 by md
! NVRAM config last updated at 08:54:16 EST Tue Jan 25 2011 by md
!
version 15.1
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname 1861-AA0213
!
boot-start-marker
boot system flash:c1861-adventerprisek9-mz.151-3.T.bin
boot-end-marker
!
!
logging buffered 4096
logging console informational
enable password lab
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+ local
!
!
!
!
aaa session-id common
!
clock timezone EST -5 0
clock summer-time EST recurring
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-1608151484
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-1608151484
  revocation-check none
!
!
crypto pki certificate chain TP-self-signed-1608151484
certificate self-signed 02
  3082022B 30820194 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31363038 31353134 3834301E 170D3131 30313235 31333532
  31325A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 36303831
  35313438 3430819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100AFCD 0E2300B3 BF7E85D5 FBB29726 2FAD0C86 17F0D81A 1482E876 ED5201B3
  BA82CA0F E93FB89D 0ADE347D 3412BD39 C3811286 D48CD908 82BD464B F942E127
  AF08C3C3 55FF233D 1D29C2F9 4CAD6142 623F7EB8 CE66507E 032FFE4D 9DB6A326
  8B4D7BA9 5F357A48 39A1A60B 585F5169 B540E940 928C0896 505740AD B27710F4
  A8370203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
  551D2304 18301680 148AA9F8 36CDDCBD C16FCE5A F8F23DD2 140C6E6C A5301D06
  03551D0E 04160414 8AA9F836 CDDCBDC1 6FCE5AF8 F23DD214 0C6E6CA5 300D0609
  2A864886 F70D0101 04050003 81810010 BDC5DBCD 05119824 C48900F3 845DB265
  B3931C78 3D99BFC9 243C6B78 64D12E15 6F819E7A ACBD42A7 633BF02D 2AD88BC7

```

```
BEE8C057 A1746AF9 6ED6510F 1CF255A2 32E37260 1B525931 4F69FA80 811C1A2D
3BA5E808 2B0A0871 4E418149 84D2D45A 92F1FEF7 CF98CA26 EA4F502F 0330F5D8
190C450E E871EAD5 E5B2D3D9 2EED15
quit
dot11 syslog
!
flow record discovery
match ipv4 dscp
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match interface input
collect ipv4 source mask
collect ipv4 destination mask
collect transport tcp flags
collect interface output
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect application name
!
!
flow record type performance-monitor media-rate
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect routing forwarding-status
collect ipv4 dscp
collect ipv4 ttl
collect interface input
collect interface output
collect counter bytes
collect counter packets
collect counter bytes rate
collect counter packets dropped
collect timestamp interval
collect application media packets rate variation
collect application media event
collect monitor event
!
!
flow exporter ecmd-rtp-1-capture
destination 10.27.0.2
source Vlan10
transport udp 2055
template data timeout 10
option interface-table
option application-table
!
!
flow exporter test1
template data timeout 1
!
!
flow monitor discovery
record discovery
exporter ecmd-rtp-1-capture
cache timeout active 60
!
no ip source-route
ip cef
!
!
!
!
ip dhcp pool site-1000-vlan-1000
```

```
network 10.1.3.0 255.255.255.128
default-router 10.1.3.1
dns-server 10.1.160.6
domain-name medianet.cisco.com
option 150 ip 10.1.1.18
!
ip dhcp pool s1000-cts1k-1
host 10.1.3.5 255.255.255.128
hardware-address 001d.a238.a680
default-router 10.1.3.1
dns-server 10.1.160.6
domain-name medianet.cisco.com
option 150 ip 10.1.1.18
!
ip dhcp pool s1000-7970-cts1k-1
host 10.1.3.4 255.255.255.128
client-identifier 0100.2290.5983.a4
default-router 10.1.3.1
dns-server 10.1.160.6
domain-name medianet.cisco.com
option 150 ip 10.1.1.18
!
ip dhcp pool ipc-zz0140
host 10.1.3.7 255.255.255.128
client-identifier 0100.1de5.ea78.08
default-router 10.1.3.1
dns-server 10.1.160.6
domain-name medianet.cisco.com
option 150 ip 10.1.1.18
!
ip dhcp pool s1000-7961-zz0103-1
host 10.1.3.6 255.255.255.128
client-identifier 0100.235e.18ee.3c
default-router 10.1.3.1
dns-server 10.1.160.6
domain-name medianet.cisco.com
option 150 ip 10.1.1.18
!
ip dhcp pool medianet-tme-aakhter-2
host 10.1.3.8 255.255.255.128
client-identifier 0100.1125.ce94.f3
default-router 10.1.3.1
dns-server 10.1.160.6
domain-name medianet.cisco.com
option 150 ip 10.1.1.18
!
ip dhcp pool s1000-7985-zz0103-1
host 10.1.3.9 255.255.255.128
client-identifier 0100.5060.03aa.87
default-router 10.1.3.1
dns-server 10.1.160.6
domain-name medianet.cisco.com
option 150 ip 10.1.1.18
!
ip dhcp pool s1000-7942-zz0103-1
host 10.1.3.10 255.255.255.128
client-identifier 0100.1d45.2d54.e8
default-router 10.1.3.1
dns-server 10.1.160.6
domain-name medianet.cisco.com
option 150 ip 10.1.1.18
class class-default
!
ip dhcp pool medianet-tme-aakhter-3
host 10.1.3.3 255.255.255.128
client-identifier 0100.016c.c9eb.48
default-router 10.1.3.1
dns-server 10.1.160.6
domain-name medianet.cisco.com
option 150 ip 10.1.1.18
!
```



```
match access-group name web-app
!
!
policy-map type performance-monitor all-apps
class telepresence-CS4
  flow monitor inline
  record default-rtp
  exporter ecmd-rtp-1-capture
  monitor metric rtp
  clock-rate 96 48000
  clock-rate 112 90000
class IPVS-traffic-rtp
  flow monitor inline
  record default-rtp
  exporter ecmd-rtp-1-capture
  monitor metric rtp
  clock-rate 96 30000
class voice-EF
  flow monitor inline
  record default-rtp
  exporter ecmd-rtp-1-capture
class IPVS-traffic-http
  flow monitor inline
  record default-tcp
  exporter ecmd-rtp-1-capture
class video-conf-AF41
  flow monitor inline
  record default-rtp
  exporter ecmd-rtp-1-capture
class SAP-HTTP
  flow monitor inline
  record default-tcp
  exporter ecmd-rtp-1-capture
class IPTV
  flow monitor inline
  record media-rate
  exporter ecmd-rtp-1-capture
!
!
!
!
!
!
!
!
!
!
interface Loopback0
  ip address 10.10.2.13 255.255.255.255
  ip ospf 1 area 0
!
interface FastEthernet0/0
  description 3845-AA0216 Fa0/0/1 via NETEM (BB1105)
  ip address 10.1.3.130 255.255.255.192
  ip nbar protocol-discovery
  ip flow monitor discovery input
  ip pim sparse-dense-mode
  ip ospf 1 area 0
  load-interval 30
  speed 100
  full-duplex
  service-policy type performance-monitor input all-apps
  service-policy type performance-monitor output all-apps
!
interface Integrated-Service-Engine0/0
  no ip address
  shutdown
!
interface FastEthernet0/1/0
  description MANSW-AA0299::Fas 0/16
  switchport access vlan 10
!
```

```
interface FastEthernet0/1/1
  description DATSW-AA0498::Gig 1/28
  switchport access vlan 1000
  shutdown
  spanning-tree portfast
  !
interface FastEthernet0/1/2
  !
interface FastEthernet0/1/3
  description to TC 1/9
  switchport access vlan 1000
  spanning-tree portfast
  !
interface FastEthernet0/1/4
  !
interface FastEthernet0/1/5
  !
interface FastEthernet0/1/6
  !
interface FastEthernet0/1/7
  description to DATSW-AA0298 Gig 1/3
  switchport access vlan 1000
  spanning-tree portfast
  !
interface FastEthernet0/1/8
  !
interface Vlan1
  no ip address
  !
interface Vlan10
  ip address 10.27.2.13 255.255.0.0
  ip flow monitor discovery input
  ntp broadcast client
  !
interface Vlan100
  no ip address
  !
interface Vlan1000
  description Site-1000
  ip address 10.1.3.1 255.255.255.128
  ip nbar protocol-discovery
  ip flow monitor discovery input
  ip pim sparse-dense-mode
  ip igmp version 3
  ip ospf 1 area 0
  !
interface Vlan2000
  no ip address
  !
router ospf 1
  !
  ip forward-protocol nd
  no ip http server
  ip http authentication aaa
  ip http secure-server
  !
  ip flow-cache timeout active 1
  ip flow-export version 9
  ip flow-export destination 10.27.0.1 2055
  ip flow-top-talkers
    top 200
    sort-by bytes
  !
  ip pim ssm default
  ip route 0.0.0.0 0.0.0.0 10.1.3.129
  !
  ip access-list extended fromIPVScamera
    permit ip host 10.1.1.16 any
    permit ip any host 10.1.1.16
  ip access-list extended iptv
    permit udp host 10.1.180.5 232.0.0.0 0.255.255.255
```

```
ip access-list extended tcp
  permit tcp any any
ip access-list extended udp
  permit udp any any
ip access-list extended web-app
  permit tcp any host 10.1.1.10 eq www
  permit tcp host 10.1.1.10 eq www any
!
logging esm config
logging 10.27.0.1
logging 64.102.202.62
access-list 1 permit any
!
!
!
!
snmp-server community public RO
snmp-server community private RW
snmp-server ifindex persist
snmp-server enable traps flowmon
!
tacacs-server host 10.27.150.201 key none
!
!
control-plane
!
!
voice-port 0/0/0
!
voice-port 0/0/1
!
voice-port 0/0/2
!
voice-port 0/0/3
!
voice-port 0/1/0
!
voice-port 0/1/1
!
voice-port 0/1/2
!
voice-port 0/1/3
!
voice-port 0/4/0
  auto-cut-through
  signal immediate
  input gain auto-control
  description Music On Hold Port
mediatrace initiator source-ip 10.1.3.130
mediatrace profile system intfl
mediatrace path-specifier ps1 destination ip 10.1.3.129 port 16386
  source ip 10.1.3.130 port 16386
mediatrace session-params spl
  response-timeout 10
  frequency 30 inactivity-timeout 300
  history data-sets-kept 10
  route-change reaction-time 10
mediatrace 2
  path-specifier ps1
  session-params spl
  profile system intfl
mediatrace schedule 2 start-time now
!
!
mgcp fax t38 ecm
!
mgcp profile default
!
!
!
```

```
privilege configure level 15 mediatrace
banner exec ^C^[]0;1861-AA0213^C
!
line con 0
  exec-timeout 0 0
  password lab
  no modem enable
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
  exec-timeout 0 0
  password lab
  logging synchronous
  exec prompt timestamp
  transport preferred none
  transport input ssh
  transport output all
line vty 5 10
  exec-timeout 0 0
  password lab
  logging synchronous
  exec prompt timestamp
  transport preferred none
  transport input all
!
exception data-corruption buffer truncate
wsma agent exec profile test
wsma agent config profile test
wsma agent filesys profile test
wsma agent notify profile test
!
wsma profile listener test
  transport https
end
```

Figure 22: Complete router configuration of mediatrace initiator

## REFERENCES

- [1] [Configuring Web Service Management Agent](#)
- [2] [Cisco IOS Network Management Command Reference](#)
- [3] [W3C SOAP Reference](#)

## FOR MORE INFORMATION

For more information about Medianet and Enterprise Medianet please visit:

<http://www.cisco.com/web/solutions/medianet/index.html>

[http://www.cisco.com/web/solutions/medianet/ent\\_medianet.html](http://www.cisco.com/web/solutions/medianet/ent_medianet.html)

or contact your local account representative.