Wide Area Application Services (WAAS) Express

Deployment Guide

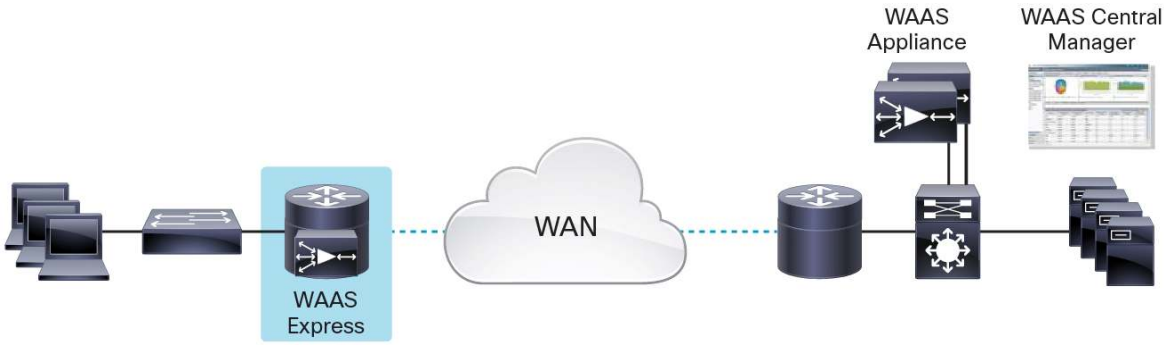
August, 2012

For further information, questions and comments please contact ccbu-pricing@cisco.com

Contents

1. Introduction

Figure 1. Cisco WAAS Express in the Network



Cisco® Wide Area Application Services (WAAS) Express extends the Cisco WAAS product portfolio, with a small-footprint, cost-effective, Cisco IOS® Software solution integrated into the Cisco Integrated Services Router Generation 2 (ISR G2) to offer bandwidth optimization and application acceleration capabilities (See Figure 1 above). Cisco WAAS Express increases remote user productivity, reduces WAN bandwidth costs, and offers investment protection by interoperating with existing Cisco WAAS infrastructure. Cisco WAAS Express is unique in providing network transparency, improving deployment flexibility with on-demand service enablement, and integrating with native, Cisco IOS-based services such as security, NetFlow, and quality of service (QoS).

Cisco WAAS Express optimizes WAN bandwidth using the following technologies:

- **Transport flow optimization (TFO) -** TFO typically represents three activities: TCP optimization, TFO negotiation, and data framing. TCP optimization is performed using binary increase congestion control (BIC) TCP and selective acknowledgements (SACKs).
- **Data redundancy elimination (DRE) -** DRE inspects TCP traffic and identifies patterns within the message. After patterns have been identified, redundant patterns can be safely replaced by small signatures, thus reducing bandwidth consumption significantly. In Cisco WAAS Express, DRE is performed completely in router memory; thus, maximum DRAM is required in every platform.
- **Lempel-Ziv (LZ) compression -** LZ compression is a standards-based compression mechanism that can be used to further decrease the amount of bandwidth consumed by a TCP flow. LZ compression can be used in conjunction with DRE or independently.
- **Optimization for SSL applications -** The SSL Express Accelerator feature integrates transparently with existing data center key management and trust models that both WAN optimization and application acceleration components can use. Encryption key pairs are stored securely in a secure vault on the Cisco WAAS Central Manager and distributed securely to the Cisco WAAS devices in the data center to be stored in a secure vault. This feature allows Cisco WAAS Express to securely apply optimization to connections previously encrypted by SSL/TLS.

- **Enhanced bandwidth optimization for file services and web applications -** The Common Internet File System (CIFS) Accelerator feature provides selected acceleration for file-based CIFS (with Server Message Block Version 1 [SMBv1]) applications and HTTP/S web applications. The CIFS Express Accelerator feature includes write optimizations, read-ahead optimizations, and negative caching. The HTTP/S Express Accelerator feature caches metadata information, which allows Cisco WAAS Express to respond locally to certain HTTP requests. These local responses are based on cached metadata from previously seen server responses and are continuously updated. The accelerator also includes hints to help DRE perform better optimization and offload compression from the web servers.

Cisco WAAS Express is fully interoperable with WAAS on Cisco Services Ready Engine service modules (SM-SRE), WAAS appliances, and can be managed by a common WAAS Central Manager.

This document describes the necessary steps to enable the WAAS Express feature on the branch router and to register the WAAS Express router to be managed by WAAS Central Manager. For simplicity, this document assumes a basic private WAN using Serial link on the WAAS Express router. For specific WAAS appliance deployment configurations (inline, Web Cache Communication Protocol [WCCP]), please consult the WAAS appliance configuration guide in the reference section.

2. Hardware and Software Requirements

- WAAS appliance running WAAS software 5.0.1 or later
- WAAS Central Manager running WAAS software 5.0.1 or later
- WAAS Express
  - Cisco 880 and 890 Series Integrated Services Routers, ISR G2 (1900, 2900, 3900 Series) with maximum DRAM
  - WAAS Express feature license file
  - Cisco IOS version 15.2(3)T or later

For a complete list of compatibility matrixes, please see the WAAS Express data sheet at http://www.cisco.com/en/US/prod/collateral/contnetw/ps5680/ps11211/datasheet_c78-611644.html.

3. WAAS Express Sizing Guidelines

A number of factors are taken into consideration to provide recommended sizing guidelines, such as number of users, number of TCP connections, WAN link capacity, traffic profile, and compression ratio. The recommended sizing assumes each user generates approximately 10 TCP connections. Typical user behaviors assumed that all TCP connections are not active in transferring the same data all the time, thereby producing the data redundancy that is around two to four times. The recommended sizing also assumes that ACL, Firewall, VPN, Network Address Translation (NAT), and QoS are configured (see Table 1).

Table 1. Recommended Sizing

Platform	TCP Connections	WAN Capacity	DRAM Required
880 ISR	75	1.5 Mbps	768 MB
890 ISR	75	2 Mbps	768 MB
1921 ISR*	50	0.512 Mbps	-
1941 ISR	150	4 Mbps	2.5 GB
2901 ISR	150	6 Mbps	2.5 GB
2911-2921 ISRs	200	6 Mbps	2.5 GB

Platform	TCP Connections	WAN Capacity	DRAM Required
2951 ISR	200	6 Mbps	4 GB
3925-3945 ISRs	400	10 Mbps	4 GB

* Cisco 1921 routers have fixed, non-expandable memory. DRE is disabled on these platforms.

4. Before You Start

Please be aware of the following limitations before you start:

- Ensure that WAAS permanent license is already installed, or 'waas enable' is already applied to the interface and licensing agreement has been accepted
- If SSH version 2 is enabled, downgrade to SSH version 1.99

5. Prepare the Router to Register with WAAS Central Manager

The WAAS Express router needs to be configured with SSH and basic credentials in order for WAAS Central Manager to log in to the router and perform the registration process.

Important: It is necessary that the router clock is up to date and synchronizes to the same time as WAAS Central Manager. NTP is highly recommended.

5.1.1 Configure Network Time Protocol (NTP)

Configure the NTP server and make sure the time is synchronized (see Figure 2). Time zone configuration is optional.

Figure 2. Configuration of NTP and Time Synchronization

```
Router(config)#ntp server 171.68.10.80
Router(config)#clock timezone PST -8
Router(config)#clock summer-time PDT recurring

Router#shownтp status
Clock is synchronized, stratum 3, reference is 171.68.10.80
nominal freq is 250.0014 Hz, actual freq is 249.9758 Hz, precision is 2**21
reference time is D3B07C59.8EBD59E0 (17:05:45.557 PDT Tue Jul 17 2012)
clock offset is 0.1285 msec, root delay is 78.59 msec
root dispersion is 3942.52 msec, peer dispersion is 437.59 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000102142 s/s
system poll interval is 64, last update was 51 sec ago.

Router#show clock
17:06:38.420 PDT Tue Jul 17 2012
```

5.1.2 Enable SSH and Log in

WAAS Central Manager needs to log in to the WAAS Express router through SSH. It is recommended to configure the domain name before creating a Rivest, Shamir, and Adelman (RSA) key (Figure 3). An RSA key size of 2048 bits is recommended.

Figure 3. Generating an RSA Key

```
Router(config)#ip domain-name example.com
Router(config)#crypto key generate rsa modulus 2048

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
(elapsed time was 4 seconds)

Jul 18 00:13:39.425: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Note: SSH version 2 is not supported for the CM registration process. Make sure that you see the following output before you proceed. If version 2.0 is displayed in the output below, disable it using 'no ipssh version 2.'

Verify that the correct version of SSH is enabled in the WAAS Express router (Figure 4).

Figure 4. SSH Version Verification

```
Router#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCaEw/9NT5uH/A3/h63h0kyAlbX+OyZKdTVqie7xFPR
amp40kUfutsK2TxTq/Qr/GAmzLVO94rnXI5++j9B5L8cZoMwysR6V7uPvr6IA3GWMv6bEdPVTepwBkwo
al0Vuiqx0q9eFCqG2UCDX5B/eilxu5zjROl3juacPlKPwpIYVkHSlr/KfUwD3Zmgn1TYntFJ3R3HMAK5
p1c9W5tVv92s7NMtJ/SHtCvW7GzK0ihJRuARykokJkuKK9+uz1sO6DdnNnyQFmGmar+ZEvtXRiZAhBNa
ElPebsXXX/9hqcS3NSdU9h60Wyy4K67W6H2XKZienUcrf+e8j0HGNM3hDObj
```

The next step is to configure authentication. Since this example uses local authentication, the username and password need to be the same as the credentials configured in section 0 (Figure 5).

Figure 5. Credentials

```
Router(config)#username waasx privilege 15 password waasx
Router(config)#line vty 0 4
Router(config-line)#login local
```

Note: If the source interface that you want to use for registration is different from the WAN interface, as a workaround, you will need to specify the interface before you proceed. The example below specifies that the IP address of Loopback1000 will be used for WAAS registration (Figure 6).

Figure 6. Example Configuration

```
Router(config)#ip http client source-interface Loopback1000
```

6. WAAS Express License Installation (Optional)

If a WAAS Express permanent license is not already installed when WAAS Express is enabled for the first time, a licensing agreement is prompted for users to accept before WAAS Express can be enabled. This license starts with a 60-day evaluation and will automatically change into Right-To-Use (RTU) afterward.

For the WAAS Express router bundle, the WAAS Express permanent license is pre-installed from the factory. This step only applies if a WAAS Express license is purchased as an add-on or upgrade.

6.1 Checking for WAAS Express License File

You can use the command **show license detail WAAS_Express** to view the current license. If the router already has a WAAS Express license installed, the output looks similar to what is listed in Figure 7. If your router already has a license installed, you can skip to step 0 - Enable WAAS Express.

Figure 7. WAAS Express License Installed

```
Router#show license detail WAAS_Express
Index: 1        Feature: WAAS_Express                    Version: 1.0
        License Type: Permanent
        License State: Active, Not in Use
        License Count: Non-Counted
        License Priority: Medium
        Store Index: 6
        Store Name: Primary License Storage
```

6.2 How to Obtain a License File

A PAK will be provided after you purchase the WAAS Express license. At the time of placing an order, you can choose the PAK to be mailed to you or electronically mailed. Collect the output of **show license udi** command (see Figure 8). Note the product ID (PID) and serial number (SN).

Figure 8. Output

```
Router#show license udi
Device#   PIDSN              UDI
------------------------------------------------------------------------------
*0        CISCO2911/K9FHH122500AZCISCO2911/K9:FHH122500AZ
```

Visit the Cisco License Activation Portal (http://www.cisco.com/go/license) and enter the PAK, product ID, and serial number information, along with your contact email address. A license file will be generated and emailed to you.

6.3 Install WAAS Express License

Once you have the license file, you need to install the license on the router by first copying the license file to the router. In the example below, the license file, **FHH122500AZ_20100811190225615.lic,** is stored on the router flash. Invoke the **license install** command to install the license. Note the message **1/1 licenses were successfully installed** indicates that the WAAS Express license is now installed. Issue the **show license detail WAAS_Express** command, which displays that the license is currently active but is not in use.

In Figure 9 note that WAAS Express is also supported in the Non-Payload Encryption (NPE) image. The only difference is that SSL Express Accelerator is not available in the NPE image, which does not allow any encryption capability.

Figure 9. WAAS Express Support

```
Router#license install flash0:FHH122500AZ_20100811190225615.lic
Installing licenses from "flash0:FHH122500AZ_20100811190225615.lic"
Installing...Feature:WAAS_Express...Successful:Not Supported
1/1 licenses were successfully installed
0/1 licenses were existing licenses
0/1 licenses were failed to install

Router#show license detail WAAS_Express
Index: 1        Feature: WAAS_Express                     Version: 1.0
        License Type: Permanent
        License State: Active, Not in Use
        License Count: Non-Counted
        License Priority: Medium
        Store Index: 6
        Store Name: Primary License Storage
```

7. Enable WAAS Express

WAAS Express is designed to be enabled with just a single configuration command. The first step is to configure the necessary addresses and routing configuration on the network. WAAS Express must be applied on all designated WAN interfaces. Under interface configuration mode, configure **waas enable** will enable the feature. The example below uses Serial 0/2/0 as a WAN interface (see Figure 10).

As stated in previous section, if there is no license file installed when you enable WAAS for the first time, you will be prompted with EULA to acknowledge. This is a one-time action and you need to answer **yes** to EULA in order to proceed.

Figure 10. Configuring with '**waas enable'** Command

```
Router(config)#intserial0/0/0
Router(config-if)#waas enable
PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO PRODUCT FEATURE OR USING SUCH
PRODUCT FEATURE CONSTITUTES YOUR FULL ACCEPTANCE OF THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires an additional license from Cisco,
together with an additional payment. You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the product, including during the 60 day evaluation period, is
subject to the Cisco end user license agreement
```

```
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day evaluation period, your use of the product feature will be
governed solely by the Cisco end user license agreement (link above),
together with any supplements relating to such product feature. The
above applies even if the evaluation license is not automatically
terminated and you do not receive any notice of the expiration of the
evaluation period. It is your responsibility to determine when the
evaluation period is complete and you are required to make payment to
Cisco for your use of the product feature beyond the evaluation period.

Your acceptance of this agreement for the software features on one
product shall be deemed your acceptance with respect to all such
software on all Cisco products you purchase which includes the same
software. (The foregoing notwithstanding, you must purchase a license
for each software feature you use past the 60 days evaluation period,
so that if you enable a software feature on 1000 devices, you must
purchase 1000 licenses for use past the 60 day evaluation period.)

Activation of the software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? [yes/no]: yes
Router(config-if)#
Jul 18 01:14:27.778: %WAAS-6-WAAS_ENABLED: WAAS is enabled on interface
serial0/0/0
Jul 18 01:14:27.918: %LICENSE-6-EULA_ACCEPTED: EULA for feature WAAS_Express 1.0
has been accepted. UDI=CISCO2951/K9:FTX1541AJS7; StoreIndex=8:Built-In License
Storage
```

Note: If using a sub-interface or logical-interface, i.e. Serial 0/2/0.1, Dialer1, Tunnel1, etc, configure **waas enable** under the sub-interface or logical-interface.

If the memory requirement is met and license is valid, the command will be accepted and a log message is generated to indicate that WAAS Express is enabled. Enter the command on other backup WAN interfaces that require WAAS Express to be enabled.

WAAS Express utilizes Cisco Classification Policy Language (C3PL) similar to those used by features like QoS and zoned-based firewall. The first time the WAAS Express is enabled, the default policy map, class maps, and parameter map will be generated. The default policy map and parameter maps are named **waas_global**. The WAAS Express-related policy map, class map, and parameter map are of type **waas**.

Use the command **show waas status** to show the interfaces that have WAAS Express turned on, along with license type, maximum number of flows supported by the platform, and total active and optimized connections (see Figure 11).

Figure 11. Example of Interface with 'show was status' Command

```
Router#showwaas status

IOS Version: 15.2(3)T
WAAS Express Version: 2.0.0

WAAS Enabled Interface       Policy Map

WAAS Feature License
    License Type:                          Permanent

DRE Status                        : Disabled
LZ Status                         : Disabled
CIFS-Express AO Status            : Disabled
SSL-Express AO Status             : Disabled
HTTP-Express AO Status            : Disabled

Maximum Flows                     : 0
Total Active connections          : 0
Total optimized connections       : 0
```

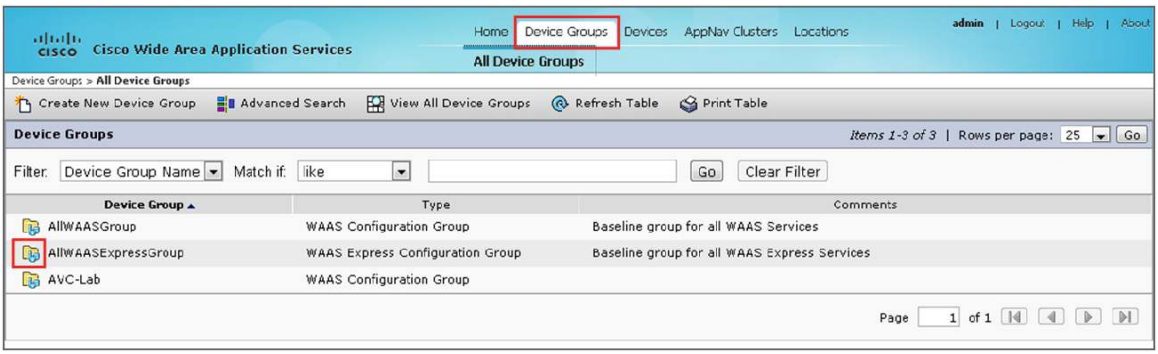
8. Register WAAS Express with WAAS Central Manager

8.1 Configure WAAS Express Credentials on WAAS Central Manager

WAAS Central Manager has a default device group called **AllWAASExpressGroup**. By default, all WAAS Express routers registering with WAAS Central Manager will be assigned to this default group. This default group also has auto-activation policy.

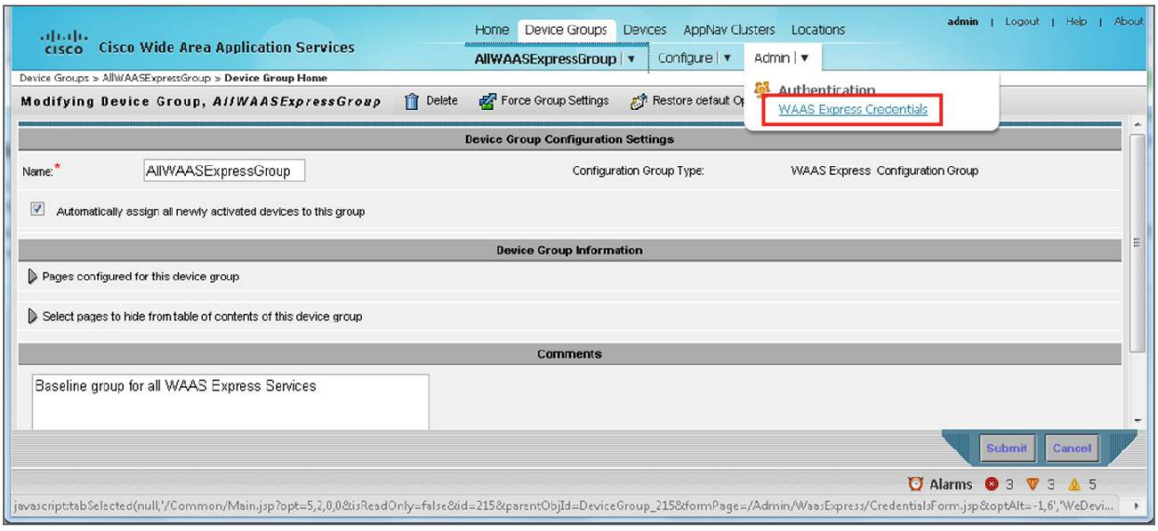
From the main WAAS Central Manager page, click on **Device Groups** and click on the edit icon on the left of device group, **AllWAASExpressGroup (**Figure 12).

Figure 12. AllWAASExpressGroup Interface



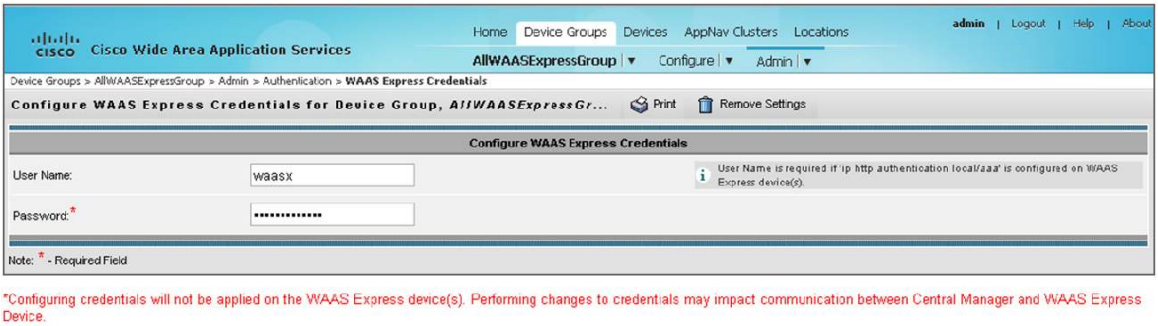
Once you have selected the AllWAASExpressGroup, select **Admin->WAAS Express Credentials** (see figure 13).

Figure 13. Admin->WAAS Express Credentials Interface



Enter the username and password that are the same as what will be configured on WAAS Express router. In the example below, username and password are **waasx** (see Figure 14). Click on **submit** to save the change.

Figure 14. waasx Username and Password Screen

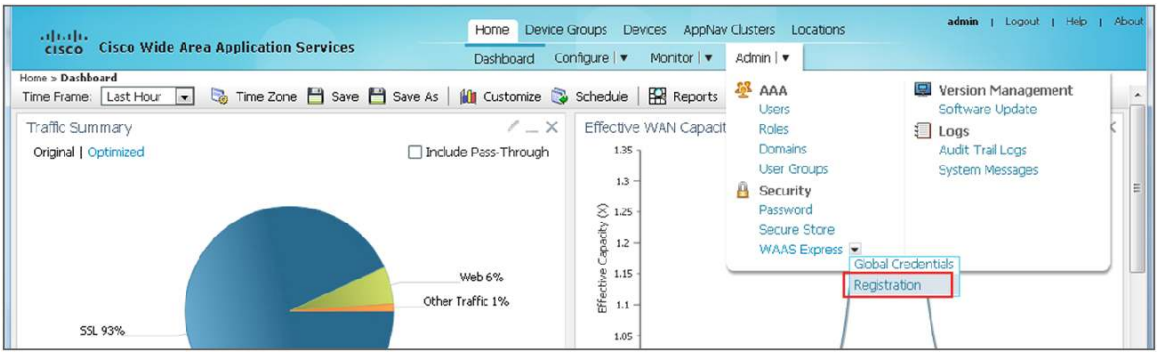


*Configuring credentials will not be applied on the WAAS Express device(s). Performing changes to credentials may impact communication between Central Manager and WAAS Express Device.

8.2 Register the WAAS Express Router with WAAS Central Manager

From the WAAS Central Manager home screen, select **Admin->WAAS Express-> Registration** (Figure 15).

Figure 15. Admin->WAAS Express-> Registration Screen

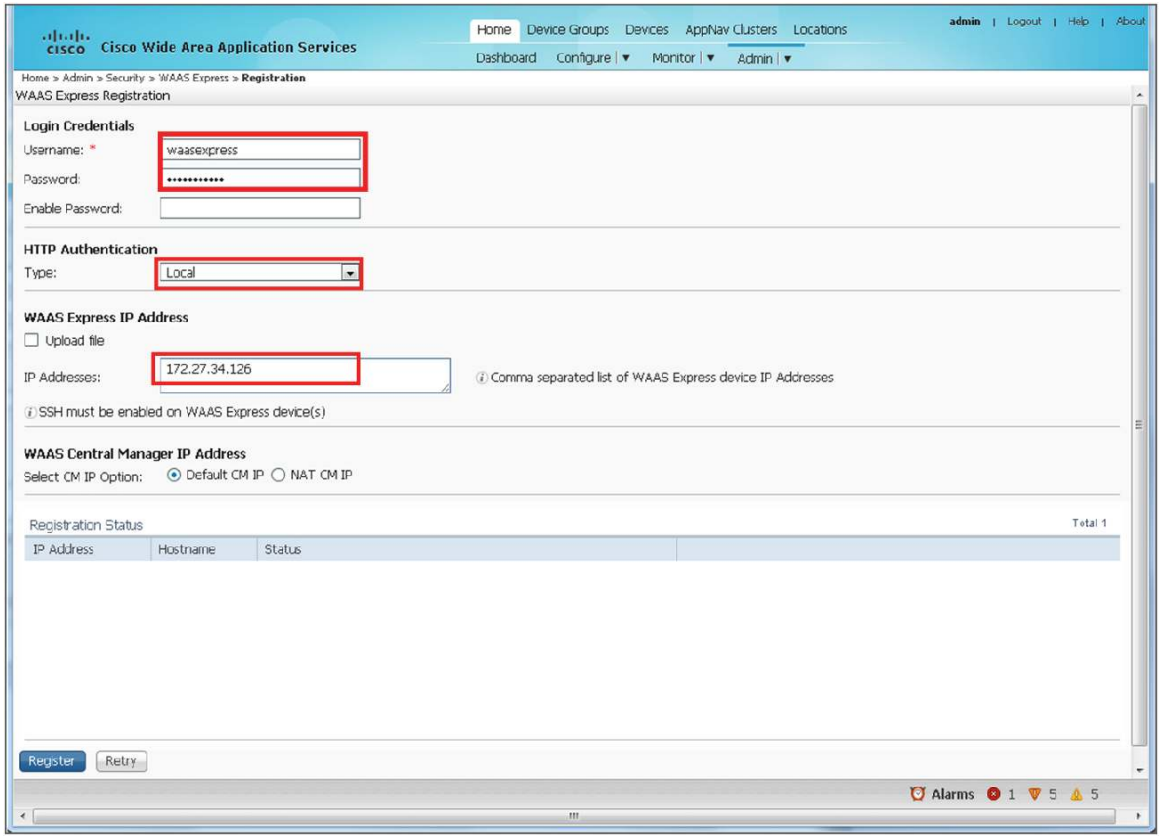


Enter the following information. In this example, local authentication is used.

- Authentication credentials: Must match the login and password allowed for SSH into the router
- Enable Password: Required only if the above authentication credentials do not have privilege 15
- Authentication Type: Local or AAA. If AAA is required, see section 8.4.2 for more information
- IP Addresses: List of addresses to be used for registration separated by comma (,)

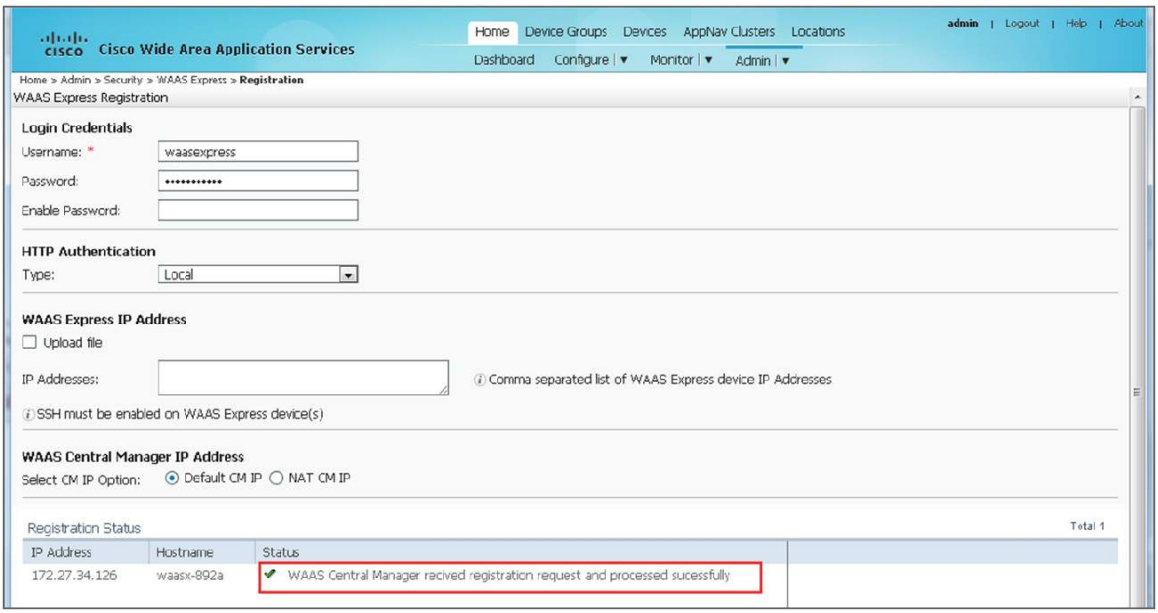
Click Register to start registration. At this point, WAAS Central Manager logs into the router, enters the necessary configuration, and starts the registration process (Figure 16).

Figure 16. Registration Interface



The registration process should complete within about 30 seconds. See the status highlighted in red in Figure 17.

Figure 17. Status Update in Red



In Figure 18, the log message on the WAAS Express router indicates that the registration is successful. Now, the WAAS Express router should show in the device list of the WAAS Central Manager.

Figure 18. Log Message

```
Jul 18 01:28:28.194: %WAAS-6-WAAS_CM_REGISTER_SUCCESS: IOS-WAAS registered with
Central Manager successfully
```

The WAAS Express device will first stay in the pending state waiting for configuration sync with WAAS Central Manager (see Figure 19).

Figure 19. Pending State of WAAS Express Device

After about five minutes, the status of the WAAS Express router should change to online (see Figure 20).

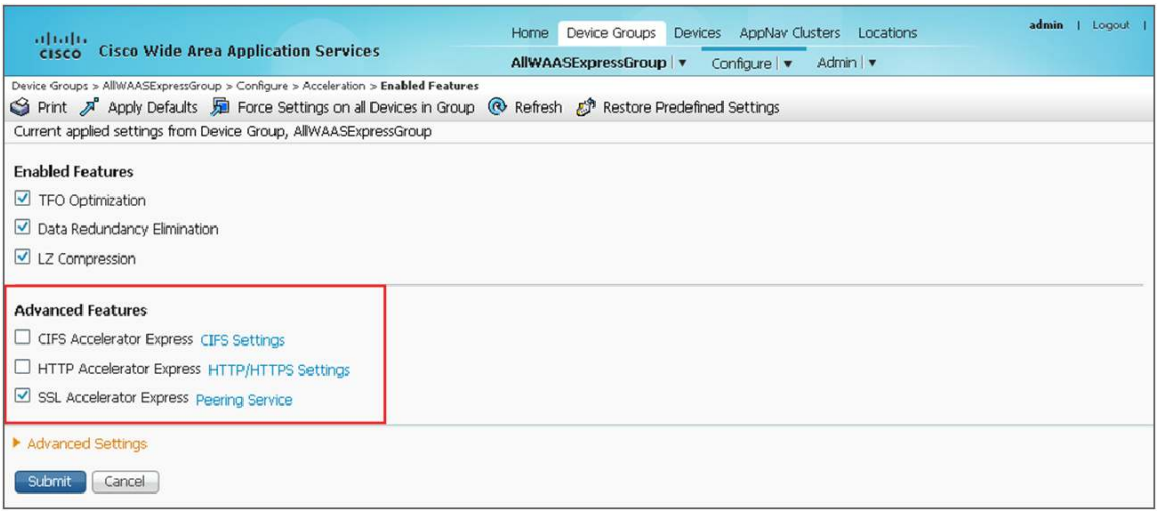
Figure 20. Status Change to Online

8.3 Enable WAAS Express Optimization and Other Advanced Features

8.3.1 Enable Optimization and Other Advanced Features

From within Device Group or Device, go to **Configure->Acceleration->Enabled Features**. In Cisco IOS release 15.2(3)T1, CIFS Express, HTTP Express, and SSL Express Accelerators are introduced (see Figure 21). By default, only SSL Express Accelerator is enabled. Enable other Express Accelerators if needed for your deployment.

Figure 21. SSL Accelerator Express Enablement



Note: To enable SSL Express A/O, additional steps are required at the core WAAS devices. Please refer to http://www.cisco.com/en/US/prod/collateral/contnetw/ps5680/ps6870/deployment_guide_c07-541981.html for instructions on how to enable the SSL optimizer at the core WAAS devices.

8.3.2 Enable WAAS Express on the WAN Interfaces

From within the Device Group or Device, go to Configure->Network->Network Interfaces, and select the interfaces on which WAAS Express needs to be enabled (see Figure 22).

Figure 22. Configuring Network Interfaces

8.4 Other Deployment Considerations

8.4.1 Restrict Access to HTTPS Server

An HTTPS server with authentication is required on the WAAS Express router to communicate with WAAS Central Manager. This means anyone who knows the credentials used by WAAS Central Manager can connect to the router through HTTPS and take control of the router since user credentials used by WAAS Central Manager are configured with privilege level 15. It is recommended that the HTTPS access is restricted. This can be done by using access-class configuration, shown in Figure 23.

Figure 23. Access-Class Configuration

```
Router(config)#access-list 99 remark -- WAAS Central Manager IP --
Router(config)#access-list 99 permit <WAAS_Central_Manager_IP>
Router(config)#ip http access-class 99
```

8.4.2 Use AAA Server for HTTPS Server Authentication and Authorization

For managing large numbers of WAAS Express routers, it is recommended that the AAA server be used for authentication and authorization, and a separate login be created for WAAS Express routers. The username and password used by WAAS Central Manager to log in to the router can be defined in the AAA server. The user needs to have privilege 15.

In order to perform registration from WAAS Central Manager, and if AAA is required, AAA authentication and authorization must use the **default** method list shown in Figure 24.

Figure 24. Default Method List

```
Router(config)#aaa new-model
Router(config)#aaa group server radius my_acs
Router(config-sg-radius)#server-private <server_address>auth-port 1645 acct-port
1646 key <aaa_key>
Router(config-sg-radius)#ip radius source-interface Loopback1000
Router(config-sg-radius)#exit
Router(config)#aaa authentication login http-login group my_acs
Router(config)#aaa authorization exec http-author group my_acs
Router(config)#! Below areNOT required if the method list highlighted in red
above
Router(config)#! is set to default
Router(config)#ip http authentication aaa login-authentication http-login
Router(config)#ip http authentication aaa exec-authorization http-author
```

8.4.3 Use Role-Based Command Line Interface (CLI) Access to Restrict WAAS CM User Access to Only WAAS-Related Commands

As mention earlier, the user credential used by WAAS Central Manager requires privilege 15. In order to restrict this user to be able to do only WAAS-related operations, role-based CLI access can be used. A CLI view for WAAS can be created. For more information on role-based CLI access, please see the References section. The example in Figure 25 uses view name **waasx**. First, you have to enter the parser view 'root' mode.

Figure 25. Parser View 'Root' Mode

```
Router1#enable view
Password: <your_enable_password_or_secret>


Router#
Nov 5 03:58:56.524: %PARSER-6-VIEW_SWITCH: user unknown successfully set to view
'root'.
```

Then, you can configure the parser view **waasx**, which has the list of commands used by WAAS Central Manager (see Figure 26).

Figure 26. Parser View 'waasx'

```
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#parser view waasx
Router(config-view)#secret waasx
Router(config-view)#commands exec include all show running-config brief
Router(config-view)#commands exec include all show waas
Router(config-view)#commands exec include all show ip
Router(config-view)#commands exec include all show policy-map type waas
Router(config-view)#commands exec include all show class-map type waas
Router(config-view)#commands exec include configure terminal
Router(config-view)#commands exec include all waas
```

```
Router(config-view)#commands exec include all clear waas
Router(config-view)#commands exec include show clock
Router(config-view)#commands exec include show interfaces
Router(config-view)#commands exec include show flash
Router(config-view)#commands exec include show tech-support
Router(config-view)#commands exec include write memory
Router(config-view)#commands configure include all policy-map type waas
Router(config-view)#commands configure include all class-map type waas
Router(config-view)#commands configure include all waas
Router(config-view)#commands configure include all parameter-map type waas
Router(config-view)#commands configure include hostname
Router(config-view)#commands configure include all no policy-map type waas
Router(config-view)#commands configure include all no class-map type waas
Router(config-view)#commands configure include all no parameter-map type waas
Router(config-view)#commands configure include all no waas
Router(config-view)#commands configure include interface
<interface_to_allow_waas_config>
Router(config-view)#command interface include all waas
Router(config-view)#command interface include all no waas
Router(config-view)#commands interface include all ip address
Router(config-view)#commands interface include all speed
Router(config-view)#commands interface include all duplex
Router(config-view)#end
```

If local authentication is used, then the username used by WAAS Central Manager to log in can be associated with the above view (see Figure 27).

Figure 27. Username waasx Privilege 15 View

```
Router(config)#username waasx privilege 15 view waasxpassword waasx
```

If you use the AAA profile, the user can be associated with a view using the following.

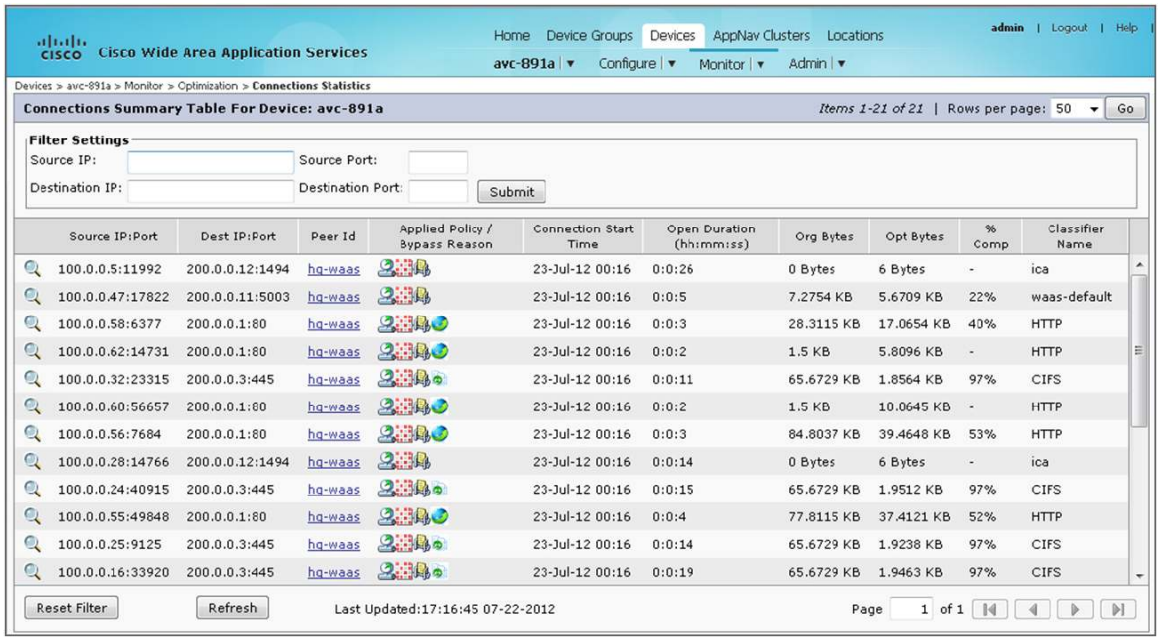
RADIUS Cisco av-pair: shell:cli-view=<view_name>

TACACScustom shell attribute: cli-view=<view_name>

9. Validating the Connection Optimization

From WAAS CM, select the WAAS Express device to monitor, and go to **Monitor->Connection Statistics**. This lists all the optimized connections and their status (see Figure 28).

Figure 28. Optimized Connections and Status



Viewing the list of connections from WAAS Express Cisco IOS CLI is also supported (Figure 29). Please note the meaning of the Accel field below:

T: TFO, L: LZ, D: DRE, H: HTTP Express AO, S: SSL Express AO, and C: CIFS Express AO

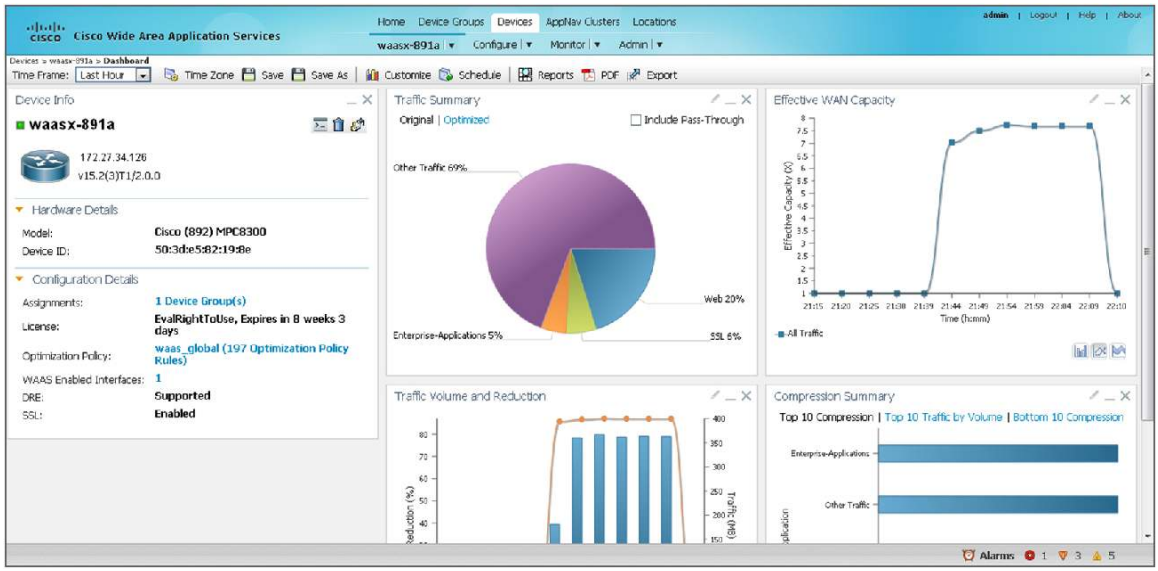
Figure 29. List of Connections

```
Router#showwaas connection
ConnID     Source IP:PortDestIP:PortPeerIDAccel

1524       100.0.0.7      :37830  200.0.0.3      :445    44d3.ca91.d0e1TCDL
1518       100.0.0.3      :16522  200.0.0.12     :1494   44d3.ca91.d0e1TDL
1523       100.0.0.6      :25928  200.0.0.7      :443    44d3.ca91.d0e1TSHDL
1522       100.0.0.5      :2067   200.0.0.4      :143    44d3.ca91.d0e1TDL
1520       100.0.0.4      :41509  200.0.0.1      :80     44d3.ca91.d0e1THDL
1521       100.0.0.5      :2066   200.0.0.2      :25     44d3.ca91.d0e1TDL
1517       100.0.0.2      :63031  200.0.0.11     :5003   44d3.ca91.d0e1TDL
1519       100.0.0.1      :7349   200.0.0.9      :33636  44d3.ca91.d0e1TDL
```

WAAS Central Manager can also display several optimization statistics by periodically polling the WAAS Express router. This can be seen by viewing the device portal page on the WAAS Central Manager (Figure 30).

Figure 30. Optimization Statistics



10. WAAS Express Interoperation With Other Cisco IOS Features

WAAS Express has been tested and validated to work with the following services which are integrated into Cisco IOS Software.

- VPN technologies include site-to-site VPN with crypto map and static Virtual Tunnel Interface (VTI), Dynamic Multipoint VPN (DMVPN), EasyVPN, and Group Encrypted Transport VPN (GETVPN)
- Access control list (ACL)
- QoS
- NAT
- Zone-Based Firewall
- Cisco IOS Intrusion Prevention System (IPS), starting with Release 15.2(3)T
- Performance Agent (PA), for monitoring application response time. For more information on how PA can be used with WAAS Express, please see http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps11709/ps11671/guide_c07-664643.html
- Multiple WAN links support for equal cost-load balancing; only per-flow load balancing is supported

11. References

- WAAS Express product page: http://www.cisco.com/en/US/products/ps11211/index.html
- Cisco Software License Activation Portal: http://www.cisco.com/go/license
- Persistent self-signed certificates: http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtpsscer.html
- Role-based CLI access: http://www.cisco.com/en/US/docs/ios/ios_xe/sec_user_services/configuration/guide/sec_role_base_cli_xe.html
- Manually importing certificates: http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrsapem.html
- Simple Certificate Enrollment Protocol (SCEP): http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a00801405ac.shtml
- Online Certificate Status Protocol (OCSP): http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_ocsp.html
- WAAS 5.0 Configuration Guide - How to enable SSL acceleration: http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v501/configuration/guide/policy.html#wp1191888

12. For More Information

For more information on Cisco WAAS Express visit http://www.cisco.com/en/US/prod/collateral/contnetw/ps5680/ps6870/qa_c67-611645_ps11211_Products_Q_and_A_Item.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C07-713403-00 08/12