Cisco WAAS relies on network interception to be integrated into the network as well as to receive packets from flows that should be optimized. Cisco WAAS supports the following out-of-path deployment mechanisms, which are all able to place the WAE logically in-path but physically off-path: WCCPv2, PBR, and ACE.

Cisco WAAS Network Module models 302, 502, 522
The Cisco WAE network module (NME-WAE) product family for the Integrated Services Router (ISR) provides a single device solution for enterprise branch offices. The Cisco WAAS Network Module for the Integrated Services Router models 302 and 502 require a **minimum** IOS version of 12.4(9)T1 and are supported in the ISR models 2811, 2821, 2851, 3825, and 3845. Model 522 is supported only in ISR model 3825 and 3845 and requires a **minimum** IOS version of 12.4(15)T1.

Web Cache Communication Protocol, Version 2 (WCCPv2)

WCCPv2 is the preferred off-path interception mechanism for WAAS. WCCP with WAAS is currently supported on a variety of routing platforms, including the Integrated Services Router (ISR models 1800, 2800, and 3800), 3700 series Access Routers, Cisco 7200 series routers (with NPE-400, NPE-G1, NPE-G2 only),7600 routers, and ASR 1000 series routers. WCCP is also supported on a variety of switching products, including the Catalyst 3560/3750, Catalyst 4500/4948, and Catalyst 6500.

WCCP Platform Support

The following platforms are recommended for use with Cisco WAAS and the WCCP tcp-promiscuous services:

- Cisco Integrated Services Routers (1800, 2800, 3800)
- Cisco 3700, 7200 (NPE-400, NPE-G1, and NPE-G2 only), 7600, and ASR 1000 Series Routers
- Cisco Catalyst 3560 and 3750 Series Switches
- Cisco Catalyst 4500 and 4948 Series Switches
- Cisco Catalyst 6500 Series Switches

The following table lists the key capabilities of each platform:

Platform	OS Version	Forwarding	Return	Assignment	Direction	Redirect List
IOS (Software-based)	< 12.4(20)T	GRE	GRE	Hash	In or Out	Yes
IOS (Software-based)	> 12.4(20)T	GRE or L2	GRE or L2	Hash or Mask	In or Out	Yes

ASR 1000 Series	2.1 XE	GRE or L2	GRE or L2	Mask	In	Yes
Cisco 7600 Series	12.2(18)SXD1	GRE or L2	GRE	Hash or Mask	In or Out	Yes [1]
Catalyst 3560/3750	12.2(37)SE	L2	GRE or L2	Mask	In	Yes [2]
Catalyst 4500/4948	12.2(31)SG	L2	L2	Mask	In	No
Catalyst 6500 (Sup2)	12.1(13)E	GRE or L2	GRE	Hash or Mask	In or Out	Yes [1]
Catalyst 6500 (Sup32/Sup720)	12.2(18)SXD1	GRE or L2	GRE or L2	Hash or Mask	In or Out	Yes [1]

[1] The following options are supported in the redirect list: source & destination IP addresses (host or subnet), individual source and destination port numbers ("eq" operator only), DSCP, TOS and precedence operators ("dscp", "precedence" and "tos" keywords), IP options ("options" keyword), and logging.
[2] Only 'permit' entries are supported.

The following platforms support WCCP, but their implementation is not compatible with WAAS:

- Catalyst 6500, Sup1a
- Cisco PIX/ASA Firewalls
- Catalyst 3550 Series Switch

IOS Recommendations

The following IOS versions are recommended for interoperability with WAAS:

Note
The IOS recommendations in this document are based on available documentation and bug scrubs for the WCCP (and related) components only. Customer impacting defects may exist in other features that would require the customer to run a different IOS version. These recommendations should not be considered a replacement for lab validation and testing. Customers are strongly encouraged to test their specific platform, software, and configuration in a lab environment prior to attempting a production deployment.

Platform / Version	Minimum Recommended Version
12.2	12.2(26) or 12.2(14)T
12.3	12.3(13) or 12.3(14)T5
12.4	12.4(10), 12.4(9)T1, 12.4(11)T3, 12.4(15)T5, 12.4(20)T

ASR 1000	2.1 XE
Catalyst 6500, Sup2	12.2(18)SXF13
Catalyst 6500, Sup32	12.2(18)SXF13
Catalyst 6500, Sup720 (Native)	12.2(18)SXF13
Catalyst 6500, Sup720 (Hybrid)	CatOS 8.5 & 12.2(18)SXF13
Catalyst 4500/4900	12.2(40)SG
Catalyst 3560/3750	12.2(46)SE

Configuration Recommendations

The following best practices should be followed for implementing WCCP on a software-based platform:

- GRE Forwarding (Default)
- Hash Assignment (Default)
- Inbound or Outbound Interception
- "ip wccp redirect exclude in" on WCCP client interface (outbound interception only)
- WAAS Egress Method: IP Forwarding, Negotiated Return, Generic GRE Return

The following best practices should be followed for implementing WCCP on a hardware-based platform:

- L2 Forwarding
- Mask Assignment
- Inbound Interception
- No "ip wccp redirect exclude in"
- WAAS Egress Method: IP Forwarding, Generic GRE (Cat6k PFC-based systems only)

This combination of configuration options will ensure WCCP interception is handled completely in hardware on hardware-based platforms. There is no impact on switch CPU utilization or forwarding performance in these cases.