# Release Notes for Cisco ASR 1000 Series, Cisco IOS XE Release 17.18.x

**First Published:** 2025-11-26

**Last Modified:** 2026-10-13

## About Cisco ASR 1000 Series Aggregation Services Routers

The Cisco ASR 1000 Series Routers carry a modular yet integrated design, so network operators can increase their network capacity and services without a hardware upgrade. The routers are engineered for reliability and performance, with industry-leading advancements in silicon and security to help your business succeed in a digital world that's always on. The Cisco ASR 1000 Series is supported by the Cisco IOS XE Software, a modular operating system with modular packaging, feature velocity, and powerful resiliency. The series is well suited for enterprises experiencing explosive network traffic and network service providers needing to deliver high-performance services.

**Note** For more information on the features and specifications of Cisco ASR 1000 Series Routers, refer to the Cisco ASR 1000 Series Routers datasheet.

For information on the End-of-Life and End-of-Sale Announcements for Cisco ASR 1000 Series routers, refer to the ASR 1000 Series End-of-Life and End-of-Sale Notices.

**Note** Cisco IOS XE 17.18.1a is the first release for Cisco ASR 1000 Series Aggregation Services Routers in the Cisco IOS XE 17.18.x release series.

### Product Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround or other user action. For more information, see https://www.cisco.com/c/en/us/support/web/field-notice-overview.html.

We recommend that you review the field notices to determine whether your software or hardware platforms are affected. You can access the field notices from https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html#%7Etab-product-categories.

### New and Changed Hardware Features

There are no new hardware features for this release.

## New and Changed Software Features in Cisco IOS XE 17.18.5

There are no new software features in this release.

## New and Changed Software Features in Cisco IOS XE 17.18.4

There are no new software features in this release.

## New and Changed Software Features in Cisco IOS XE 17.18.3a

There are no new software features in this release.

## New and Changed Software Features in Cisco IOS XE 17.18.2

| Product Impact | Feature | Description |
|---|---|---|
| Ease of Setup | IPv6 Rule and Rule Set Support in Security Policies | From Cisco IOS XE 17.18.2, you can configure IPv6 data prefix lists, rule with rule sets, and object groups in security policy using Cisco SD-WAN Manager. For more information, see Security Policy |
| Upgrade | IPv6 GRE-TP tunnel as protected link support for SRv6 TI-LFA with IS-IS | From Cisco IOS XE 17.18.2, this feature extends IPv6 GRE-TP tunnel as protected link support for SRv6 TILFA with ISIS. |
| Upgrade | IPv4 GRE-TP tunnel as protected link support for SR-MPLS TI-LFA with OSPFv2 | From Cisco IOS XE 17.18.2 this feature extends IPv4 GRE-TP tunnel as protected link support for SR-MPLS TILFA with OSPFv2. |
| Upgrade | IPv4 GRE-TP tunnel as protected link support for SR-MPLS TI-LFA with IS-IS | From Cisco IOS XE 17.18.2 this feature extends IPv4 GRE-TP tunnel as protected link support for SR-MPLS TILFA with ISIS. |
| **CUBE Features** | | |

| Product Impact | Feature | Description |
|---|---|---|
| Upgrade | Directional attribute compliance for SIPREC responses | From Cisco IOS XE 17.18.2 onwards, for a recorder response with INACTIVE SDP attributes, CUBE stops media packets transmission towards that recorder. |
| Security | Security warnings for usage of legacy TLS and associated weaker ciphers – CUBE and SRST | From Cisco IOS XE 17.18.2 onwards, CUBE and SRST display warning messages during handshake for configurations with legacy TLS (v1.0, v 1.1) and associated weaker ciphers. |
| **Resilient Infrastructure** | | |

| Product Impact | Feature | Description |
|---|---|---|
| Security | Infrastructure Resiliency | |

| Product Impact | Feature | Description |
|---|---|---|
| | | Starting with the Cisco IOS XE 17.18.2 release and in future releases, Cisco software will display warning messages when configuring features or protocols that do not provide sufficient security such as those transmitting sensitive data without encryption or using outdated encryption mechanisms. Warnings will also appear when security best practices are not followed, along with suggestions for secure alternatives.<br><br>This list is subject to change, but the following is a list of features and protocols that are planned to generate warnings in releases beyond the version Cisco IOS XE 17.18.1. Release notes for each release will describe exact changes for that release:<br><br>**1. Plain-text and weak credential storage**: Type 0 (plain text), 5 (MD5), or 7 (Vigenère cipher) in configuration files.<br><br>*Recommendation*: Use Type 6 (AES) for reversible credentials, and Type 8 (PBKDF2-SHA-256) |

| Product Impact | Feature | Description |
|---|---|---|
| | | or Type 9 (Scrypt) for non-reversible credentials.<br>2. **SSHv1**<br>*Recommendation*: Use SSHv2.<br>3. **SNMPv1 and SNMPv2, or SNMPv3 without authentication and encryption**<br>*Recommendation*: Use SNMPv3 with authentication and encryption (authPriv).<br>4. **MD5 (authentication) and 3DES (encryption) in SNMPv3**<br>*Recommendation*: Use SHA1 or, preferably, SHA2 for authentication, and AES for encryption.<br>5. **IP source routing based on IP header options**<br>*Recommendation*: Do not use this legacy feature.<br>6. **TLS 1.0 and TLS 1.1**<br>*Recommendation*: Use TLS 1.2 or later. |

| Product Impact | Feature | Description |
|---|---|---|
| | | 7. **TLS ciphers using SHA1 for digital signatures**<br>*Recommendation*: Use ciphers with SHA256 or stronger digital signatures.<br>8. **HTTP**<br>*Recommendation*: Use HTTPS.<br>9. **Telnet**<br>*Recommendation*: Use SSH for remote access.<br>10. **FTP and TFTP**<br>*Recommendation*: Use SFTP or HTTPS for file transfers.<br>11. **On-Demand Routing (ODR)**<br>*Recommendation*: Use a standard routing protocol in place of CDP-based routing information exchange.<br>12. **BootP server**<br>*Recommendation*: Use DHCP or secure boot features such as Secure ZTP. |

| Product Impact | Feature | Description |
|---|---|---|
| | | 13. **TCP and UDP small servers (echo, chargen, discard, daytime)**<br>*Recommendation*: Do not use these services on network devices.<br>14. **IP finger**<br>*Recommendation*: Do not use this protocol on network devices.<br>15. **NTP control messages**<br>*Recommendation*: Do not use this feature.<br>16. **TACACS+ using pre-shared keys and MD5**<br>*Recommendation*: Use TACACS+ over TLS 1.3, introduced in release Cisco IOS XE 17.18.1 |

# New and Changed Software Features in Cisco IOS XE 17.18.1a

| Product Impact | Feature | Description |
|---|---|---|
| Ease of Use | Hosted Edge Services for SD-Routing Devices | From Cisco IOS XE 17.18.1a release, Cisco Catalyst SD-WAN Manager supports deployment of IOx applications such as Cyber Vision, Thousand Eyes, UTD, and so on. The support to monitor these applications is introduced through Hosted Edge Services monitoring dashboard which offers a simplified user experience for overseeing IOx container applications across multiple devices. The Hosted Edge Services monitoring dashboard is introduced on Cisco Catalyst SD-WAN Manager version 20.18.x. |
| Ease of Use | Certificate Management on SD-Routing Devices | This feature introduces a new certificate authorization setting, Enterprise Certificate Settings, which unifies certificate configurations for SD-Routing devices. Cisco SD-WAN Manager automates certificate management by leveraging protocols like EST (Enrolment over Secure Transport) and SCEP (Simple Certificate Enrolment Protocol). The feature automates the enrolment, and renewal of certificates. |

| Product Impact | Feature | Description |
|---|---|---|
| Upgrade | MVPN Ingress Replication (IR) over SRv6 | This feature enables the transport of IPv4 MVPN traffic across an SRv6 network. It simplifies multicast deployment by using the existing SRv6 unicast infrastructure as the underlay. With this feature, the ingress PE router receives multicast traffic and creates a separate unicast SRv6-encapsulated copy for each egress PE router in the multicast group. |
| Upgrade | SRv6 Path MTU Discovery | This feature introduces a mechanism to determine the maximum transmission unit (MTU) for packets traversing an SRv6 underlay network. It ensures efficient packet forwarding by preventing fragmentation and packet drops, thereby allowing network devices to dynamically adjust packet sizes to avoid exceeding link MTU limits. The system relays ICMP Packet Too Big (PTB) messages from the SRv6 underlay to the IPv6/IPv4 overlay network, supporting both Transit-node and Headend-node PTB relay methods. |

| Product Impact | Feature | Description |
|---|---|---|
| Upgrade | SRv6 Flex-Algo with TI-LFA and uLoop Avoidance | From Cisco IOS XE 17.18.1a, Flexible Algorithm enhances SRv6 by including functions like Topology Independent Loop-Free Alternate (TI-LFA) and microloop (uLoop) avoidance. This feature improves network resilience and efficiency. |
| Ease of setup | Cisco Secure Routers Swim and Onboarding Tool | Cisco IOS XE 17.18.1a introduces the Cisco Secure Routers Swim and Onboarding tool that helps customers upgrade and onboard autonomous hardware devices to cloud-hosted or on-premises Catalyst Cisco SD-WAN Manager. |

| Product Impact | Feature | Description |
|---|---|---|
| Ease of setup | Managing NGFW Policies from Security Cloud Control | Security Cloud Control is a cloud-based multi-device manager that facilitates management of security policies to achieve consistent policy implementation. Security Cloud Control helps optimize your security policies by identifying inconsistencies with them and by giving you tools to fix the inconsistencies. From Cisco IOS XE 17.18.1a release, you can integrate Cisco SD-WAN Manager with Security Cloud Control, which allows you to import existing NGFW policies, security objects, and security profiles into Security Cloud Control. With this integration, you can share objects and policies as well as make configuration templates to promote policy consistency across devices. |
| **CUBE Features** | | |
| Ease of Use | Enhanced support for serviceability in SIP recording | From Cisco IOS XE 17.18.1a onwards, serviceability is enhanced to display consolidated information on forked and associated anchor call legs. |

| Product Impact | Feature | Description |
|---|---|---|
| Upgrade | Third-Party GUID capture for correlation between call transfers and SIP-based recording | From Cisco IOS XE 17.18.1a onwards, the Third-Party GUID capture for correlation between calls and SIP-based recording is extended to support transmission of globally unique identifiers (GUIDs) to the recording server during call transfers. |
| Upgrade | IOS UC apps reports smart licensing flex subscription entitlement tag | From Cisco IOS XE 17.18.1a onwards, CUBE and SRST smart licensing reports flex subscription entitlement tag on all the supported platforms. |

# Resolved and Open Bugs for Cisco IOS XE 17.18.x

## Resolved Bugs for Cisco IOS XE 17.18.5

All open bugs for this release are available in the Cisco Bug Search Tool.

| Identifier | Headline |
|---|---|
| CSCwu97838 | RADSEC TLS peer validation fails when unrelated trustpoints share a common PKI Root CA |
| CSCwv55092 | cEdge upgrade rollback due to recursive SNMP BGP trap deprecated-model migration |
| CSCwq96185 | SD-WAN: High Memory Usage and Unexpected Reload Due to a vDaemon Memory Leak |
| CSCwu97716 | Unexpected Device Reload Triggered by DHCP Service Failure During Lease Conflict Scenarios |
| CSCwu83262 | L2TPv3 xconnect session fails to establish when the traffic traverses through IPsec tunnel interface. |
| CSCwu27070 | Unexpected Reload in CPP Server (cpp_sp_svr) Code |
| CSCwu12631 | Posture redirection not working on Sdwan router switch module |
| CSCwt81568 | Route-replicate command is present in configuration but is not taking effect after reload. |
| CSCww06413 | PKCS12 re-import silently fails to install a CA certificate |

| Identifier | Headline |
|---|---|
| CSCwt42293 | Device: Cellular interface flap causing crypto enrollment failure |
| CSCwr02102 | Router intermittently loses ip address dynamically assigned to tunnel interface |
| CSCwt98537 | QoS unsupported configuration makes route processor crash |
| CSCwq08386 | Device platform Tier 3 throughput clarification |
| CSCwt75037 | Device in controller mode crashes with Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69) |
| CSCwr69095 | DNS requests for vBond fail |
| CSCwu00043 | LSC certificate failure "CRYPTO_PKI: Failed to add ca req pool entry 538" in scale environment |
| CSCwu61766 | SDWAN edge router OMPD crash on malformed SD-WAN identity IP-to-user update from vSmart pxGrid integration |
| CSCwu00657 | Device: SFP PID Mismatch (30-1599-01) : should display SFP-10G-T-X instead of SP7052-C/RTXL185-500-C88 |
| CSCws92932 | Unexpected reload due to Segmentation Fault on TPS IPC Process |
| CSCwu27937 | system-report handling has a conflict - unrelated processes may dump core after a cpp/ucode fault. |
| CSCwt66413 | ncsshd process fails to terminate after "no netconf" and netconf refuses connection |
| CSCwt56693 | L2TP: Seeing "protocol l2tpv2 L2TP_CLASS_011" config getting lost with clear ppp all cli |
| CSCws80808 | Loopback interface in Mgmt-intf VRF becomes unreachable via Management interface |
| CSCwt13176 | Memory leak detected in TLS testcase |
| CSCwt84502 | Critical Process cpp_ha_top_level_server crash (rc=69) Crash after adding zone based firewall setup configuration on the router |
| CSCwv37592 | Unable to configure no exec under async line or async range IOS-XE SDWAN |
| CSCwu21682 | Segmentation Fault at Process = SASCheckInit (or other process) |
| CSCwu93056 | Device may reload after remove an endpoint. |
| CSCwt51797 | RIPv2 will stop sending multicast routing updates after interface flap |
| CSCwu47545 | Ucode Code Crash while Printing Log for FW Drop for Packet with Invalid Header |
| CSCwr74339 | vman crashed @ __GI___clock_nanosleep in router reload and power cycle test |
| CSCwr47230 | Upgrade failed "Install operation not allowed because verification of image ..... is in progress." |

| Identifier | Headline |
|---|---|
| CSCwt69544 | QFP Ucode device crash |
| CSCwu97638 | Unexpected reload due to ACL pointer corruption with SNMPv3 |
| CSCwt51754 | Router reloaded after adding voice related configuration |
| CSCwt25903 | Not able to disable "log" feature in NGFW Policies vManage for "Drop" rules. |
| CSCwu45273 | LISP ITR sources locally-originated control-plane packets from the numerically lowest configured RLOC IP instead of the outbound interface address |
| CSCwu11498 | show interface counter become abnormal |
| CSCwv39390 | Router generates FMANRP_ESS-3-ERREVENT logs with tracebacks |
| CSCwu50735 | MACSEC fails to connect at boot up on device |
| CSCws95879 | ICMP TTL Expired packet sent via incorrect VRF |
| CSCwu76495 | SDWAN: Crash while updating Adaptive QOS Session Policy due to minimal traffic size |
| CSCwt34226 | SSH Connectivity Issue with On-Demand Next Hop in Segment Routing Traffic Engineering (SR-TE) |
| CSCwt29648 | BadIpChecksum drop when Segment-routing MPLS is configured over IPSEC/GRE over VDSL interface on device |
| CSCwu01733 | Rapid memory leak in ompd after ISE integration with vManage |
| CSCwu49029 | Unexpected reload on CGM (Class-Group Manager) when updated |
| CSCwu51162 | Unexpected reload on router in SDWAN CCE (Classifier and Classification Engine) |
| CSCwv41407 | Device: BGP updates that should be suppressed are advertised with incorrect attribute after RPSO |
| CSCwv97208 | LISP xTR may retain a stale Registering ETR session after dual-WAN failback, delaying Map-Register update to the Map-Server for 6–7 minutes |
| CSCwt88212 | Untagged packets dropped with non-default native VLAN on device |
| CSCwq98154 | Multicast traffic not forwarded over P2P DMVPN phase 1 tunnel |
| CSCwr24042 | Traffic going to all CEDGES without receivers where Replicator stuck in P MDT |
| CSCwu99434 | Unexpected device reload during Rapid Trustpoint Deletion and Creation Events Resulting in core file generation |
| CSCwv25890 | Support for GRE+MPLS on tunnel transport mode |

## Open Bugs for Cisco IOS XE 17.18.5

All open bugs for this release are available in the Cisco Bug Search Tool.

| Identifier | Headline |
|---|---|
| CSCwv71880 | SD-WAN redirect-dns Destination NAT session collides with SIG tunnel IKEv2 control plane traffic |
| CSCws94603 | Crashes During CRL Fetch Failure due memory reallocation |
| CSCwv68329 | Static NAT DIA routes intermittently withdrawn/not reinstalled after transport tracker/TLOC flap |
| CSCwv60786 | Intermittent issue with RRI being lost on the Flex Hub |
| CSCwv73701 | Packet reordering observed when application performance-monitor service policy enabled |
| CSCwq26818 | Device: Link May Stay Down After Swapping 10G To 1G Optics |
| CSCwu02842 | Unexpected reload due to race condition in QoS service group configuration |
| CSCwt63505 | Device crashed while authenticating trustpoint with DNAC |

## Resolved Bugs - Cisco IOS XE 17.18.4

All resolved bugs for this release are available in the Cisco Bug Search Tool.

| Identifier | Headline |
|---|---|
| CSCwt76906 | C9K: Continuous increase in holding memory for CTS CORE |
| CSCwt47516 | WLC crash due to corrupted length field during AAA processing |
| CSCwt94106 | Pubd core generated for C9300 |
| CSCwu04279 | System instability and potential service disruption after invalid GPM load |
| CSCwu03804 | C9000: Randomly during operation - Interface VLAN / SVI go missing from "show run" but remain up. Configs are lost upon reload. |
| CSCwu21451 | C9250/C9350 : Cluster manager crash for stacked devices with specific mac address combination |
| CSCwt51443 | Controller crashed due to CPUHOG under DBAL_EVENTS |
| CSCwt86654 | IOS-XE: IKEv2 process crash caused by stack buffer overflow during AnyConnect EAP credential parsing |
| CSCwu02602 | DBAL EVENTS crash seen while trying to push config group to C8570-G2/C8500-12x4QC in SDWAN and SD-Routing |
| CSCwn80721 | Unexpected Reboot in Process Sessmgrd |
| CSCwt87294 | mDNS Cache-Flush behavior not consistent |

## Open Bugs - Cisco IOS XE 17.18.4

There are no customer impacting bugs that were identified in this release.

## Resolved Bugs for Cisco IOS XE 17.18.3a

| Identifier | Headline |
|---|---|
| CSCwr79336 | Device with POST, multiple MACSEC BFD down seen with peer events |
| CSCws33718 | Unicast packets dropped ingress on port-channel sent from Nexus vpc after clearing vpc inconsistency |
| CSCwt07792 | IPSec packets dropped on device when FP switchover with ESP100x/200x |
| CSCws89172 | Crash @cft_engine_handle_vrf_associate_if_needed on device platform with IPv6 traffic |
| CSCws92228 | PS device shown as "Cisco ASR1000 Unknown Power Supply" "ASR1000-PWR-UNKNOWN" in Inventory |
| CSCws36615 | Device experiences an unexpected reload, generating a IOSd core file |

## Open Bugs for Cisco IOS XE 17.18.3a

All open bugs for this release are available in the Cisco Bug Search Tool.

| Identifier | Headline |
|---|---|
| CSCwq96185 | SD-WAN: High memory usage and unexpected reload due to a vDaemon memory leak |
| CSCwt25957 | Issue with editing security policy after controller upgrade. |

## Resolved Bugs for Cisco IOS XE 17.18.2

| Bug ID | Description |
|---|---|
| CSCwq53150 | Tunnel key/protection do not work together for VPLS multipoint connections. |
| CSCwr42950 | SDWAN On-Demand Tunnels Do Not Expire When UMTS Is Enabled |
| CSCwq51935 | NAT64 static entry removed when command to delete non-existent entry is applied. |
| CSCwe19394 | cEdge: device may boot up into prev_packages.conf due to power outage. |
| CSCwr77958 | NWPI not capturing self-generated syslog traffic. |
| CSCwj61730 | Router crash when removing SGT caching on an interface. |
| CSCwq77322 | Router sending a 2 Byte packet of FLOW_SAMPLER_RANDOM_INTERVAL instead of a 4-Byte packet. |
| CSCwr24031 | After upgrade to 17.15 for earlier releases sd-wan service-tracker in vrf selects source IP address from GRT when MPLS Inter-AS VPN option B configured. |

| Bug ID | Description |
|---|---|
| CSCwr49794 | ISR exporters with ETA enabled are generating invalid template data errors in SN. |
| CSCwq98206 | EPBR set interface action get missing after reboot. |
| CSCwr25077 | vDaemon crash when initializing DNS channels. |

## Open Bugs for Cisco IOS XE 17.18.2

| Bug ID | Description |
|---|---|
| CSCws30834 | Cedge ignore the keepalive command under the SIG tunnel interface pushed by the SD-WAN Manager. |
| CSCws13857 | Incorrect NAT translation from service-vrf to global for self-generated ICMP 11 (Time Exceeded) packets. |
| CSCwq77458 | fman crash after FNF config changes. |
| CSCwr87083 | Not able to onboard sd-routing devices using generic bootstrap file stored in USB. |
| CSCws12946 | Cedge port forward issue with multiple ISP. |
| CSCws18137 | Out of sync when CLI Template was attached. |
| CSCwr76580 | Strange behavior with the Cisco Umbrella SIG tunnels configured from vManage to Umbrella. |
| CSCwr30573 | TLOC Extension unable to program due to module boot up timing. |
| CSCws25557 | Cipher Suites TLS 1.2 for control connections. |
| CSCwr95551 | Router crashes when configuring SSL VPN with Policy-Based Routing (PBR) and NAT. |
| CSCwr08462 | There seems to be an issue where the NAT router is not responding to ARP requests. |
| CSCwr44921 | SDWAN C-Edge Router Crashes - CPU Usage due to Memory Pressure exceeds threshold. |
| CSCwr97784 | Slow performance on Netconf RPC on 17.15.2a on stateless static NAT translation. |
| CSCwr88206 | FIB table routes: Next Hop (NH) ID 0 is getting corrupted and assigned to a value other than Blackhole. |
| CSCwr84985 | dmiauthd process crashes, due to which the configuration does not sync between startup-config and the running-config. |
| CSCwm97460 | 17.9 cEdges - Control Connection to vManage is only Attempted over Highest Priority TLOC. |
| CSCwr00088 | Add CLI to change per MPLS label CEF statistics query interval on FMAN FP. |
| CSCwr55240 | Router experienced Critical process ompd fault on rp_0_0. |

| Bug ID | Description |
|---|---|
| CSCwr72709 | Router crash in TDM-TDM call when debug voip fpi enabled. |
| CSCwq98154 | [XE MCAST] Multicast traffic not forwarded over P2P DMVPN phase 1 tunnel. |
| CSCwr49475 | BFD sessions flapping and not recovering - SYMNAT port not updating to data-plane. |
| CSCwo42664 | SD-WAN Edge: Periodic Service Restart May Generate Crash Files. |
| CSCwr64257 | Unexpected reload on ftmd SDWAN device. |
| CSCws26373 | cEdge experiences an unexpected reboot due to NAT in the data-plane after a policy push |
| CSCwp97178 | v1718/polaris: flapping nat will casue bfd session down with ipsec session shown. |
| CSCwr76176 | BFD SD-WAN PMTUD: PMTU Converges Unexpectedly to 970 Bytes After dbg2:1 Event |
| CSCwr77083 | Router crashed in crypto library. |

### Resolved Bugs for Cisco IOS XE 17.18.1a

| Bug ID | Description |
|---|---|
| CSCwo05703 | VFR is not dynamically disabled after ZBFW removal. |
| CSCwm27749 | Speed test download / Throughput issue on router seen with IPSEC ESP-NULL transform using Zscaler. |
| CSCwp23487 | SGW offline with SSH error Unable to open socket while establishing NETCONF session. |

### Open Bugs for Cisco IOS XE 17.18.1a

| Bug ID | Description |
|---|---|
| CSCwo42664 | 17.12 - keyman core files on router. |

## ROMmon Release Requirements

For more information on ROMmon support for Route Processors (RPs), Embedded Services Processors (ESPs), Modular Interface Processors (MIPs), and Shared Port Adapter Interface Processors (SIPs) on Cisco ASR 1000 Series Aggregation Services Routers, see https://www.cisco.com/c/en/us/td/docs/routers/asr1000/rommon/asr1000-rommon-upg-guide.html.

## Related Documentation

- Release Notes for Previous Versions of ASR 1000 Series Aggregation Services Routers
- Hardware Guides for Cisco ASR 1000 Series Aggregation Services Routers

- Configuration Guides for ASR 1000 Series Aggregation Services Routers
- Product Landing Page for ASR 1000 Series Aggregation Services Routers
- Datasheet for ASR 1000 Series Aggregation Services Routers
- Upgrading Field Programmable Hardware Devices for Cisco ASR 1000 Series Routers
- Cisco ASR 1000 Series Aggregation Services Routers ROMmon Upgrade Guide
- Field Notices
- Cisco Bulletins

## Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

### Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

## Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

## Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at https://www.cisco.com/en/US/support/index.html.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.