Limitations and Restrictions in Cisco IOS XE 3S Releases

This chapter describes the limitations and restrictions applicable to the Cisco ASR 1000 Series Routers and Cisco ASR 903 Series Router for Cisco IOS XE 3S releases:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Limitations and Restrictions in Cisco IOS XE Release 3.5.2S

There are no new limitations and restrictions in Cisco IOS XE Release 3.5.2S.

Limitations and Restrictions in Cisco IOS XE Release 3.5.1S

This section describes limitations and restrictions in Cisco IOS XE Release 3.5.1S and later releases.

Multi-Segment Pseudowire Limitation

- The Cisco ASR 903 Series Router does not support l2vpn Inter-AS.
- VCCV type RA (Router Alert) is not supported with Multi-Segment Pseudowire.
- Multi-Segment Pseudowires are supported only on EVC service instances, as in the following configuration in which the Cisco ASR 903 Series Router acts as the terminating PE (T-PE) router.

```
interface TenGigabitEthernet2/0/0
no ip address
no mls qos trust
service instance 2001 ethernet
encapsulation dot1q 2001
rewrite ingress tag pop 1 symmetric
xconnect 1.1.1.1 2001 encapsulation mpls
```

QoS ACL Restrictions

- QoS ACLs are supported only for IPv4 traffic.
- QoS ACLs are supported only for ingress traffic.
- You can use QoS ACLs to classify traffic based on the following criteria:
  - Source and destination host
  - Source and destination subnet
  - TCP source and destination
  - UDP source and destination
- Named and numbered ACLs are supported.
- You can apply QoS ACLs only to the third level class (bottom-most).
- The following range of numbered access lists are supported:

```
<1-99>       IP standard access list
<100-199>    IP extended access list
<1300-1999>  IP standard access list (expanded range)
<2000-2699>  IP extended access list (expanded range)
```

- You must create an ACL before referencing it within a QoS policy.
- Deny statements within an ACL are ignored for the purposes of classification.
- Classifying traffic based on TCP flags using an ACL is not supported.
- Classifying traffic using multiple mutually exclusive ACLs within a match-all class-map is not supported.
- Classifying traffic on a logical/physical level using an ACL is not supported.
- Applying QoS ACLs to MAC addresses is not supported.
- The **neq** keyword is not supported with the **access-list permit** and **ip access-list extended** commands.
- This release does not support matching on multiple port numbers in a single ACE, as in the following command: **permit tcp any eq 23 45 80 any**

Resilient Ethernet Protocol Limitations

- Resilient Ethernet Protocol (REP) is supported only on trunk EFP interfaces.
- The **ethernet vlan color-block** command is not supported.
- REP is not supported on cross-connect and local connect EVCs.
- REP is not supported on port-channel interfaces.

Limitations and Restrictions in Cisco IOS XE Release 3.5.0S

This section describes limitations and restrictions in Cisco IOS XE Release 3.5.0S and later releases.

ATM IMA Limitation

You can create a maximum of 16 IMA groups on each T1/E1 interface module.

Clocking and Timing Limitation

Only a single clocking input source can be configured within each group of eight ports (0-7 and 8-15) on the T1/E1 interface module using the **network-clock input-source** command.

Ethernet IM Restrictions

- The Cisco ASR 903 Series Router does not support the Facilities Data Link (FDL) on Ethernet interfaces.

- The Cisco ASR 903 Series Router does not support the **mac-address** command on Gigabit Ethernet interface modules.
- On the Cisco ASR 903 Series Router, 10 Gigabit Ethernet interface modules are not supported in slots 4 and 5.
- When you install a Gigabit Ethernet IM in slot 5, the interface GigabitEthernet0/5/0 is not operational; the port is reserved for internal communication.

Pseudowire/AToM Limitation

Cisco IOS Release 15.2(1)S does not support ATM over MPLS N-to-one cell mode or one-to-one cell mode.

QoS Limitations

- QoS policies are not supported on Link Aggregation (LAG) bundle interfaces or port-channel interfaces configured with Ethernet Flow Points (EFPs).
- QoS policies are not supported on physical interfaces configured with an EFP.
- The Cisco ASR 903 Series Router supports up to 64 unique QoS classification service instances in a given bridge domain. QoS service instances refer to ports, VLAN classes, and EFPs associated with a QoS classification policy.
- Modification of policy-map and class-map definitions while applied to an interface or EFP is not supported.
- Policy validation—Some QoS policy configurations are not validated until you apply the policy-map to an interface or EFP.
- If a QoS configuration is invalid, the router rejects the configuration when you apply it to an interface. In some cases, a QoS configuration may be rejected due to hardware resource exhaustion or limitations. If you receive such an error message, detach the policy and adjust your QoS configuration.
- The **match-all** keyword is supported only for QinQ classification.
- QoS is not supported on Time Division Multiplexing (TDM) interfaces.
- The class-based QoS MIB is not supported.

Subinterfaces Limitation

The Cisco ASR 903 router does not support subinterface configurations in Cisco IOS XE Release 3.5.0S.

T1/E1 IM Limitations

- Serial interfaces are not supported—The current software release does not support serial interfaces or features applied to serial interfaces. It is recommended that you use a configuration with circuit emulation (CEM) or Inverse Multiplexing over ATM (ATM IMA) as a workaround.
- Channel groups is not supported—The current software release does not support configuration of an EtherChannel group using the **channel-group interface** command.

IP addresses are not supported—The current software release does not support specifying an IP address on a T1/E1 interface. You can specify an address on the interface by configuring it as a part of a CEM group using the **cem-group** command or as a part of an ATM IMA **ima-group** command. For more details, see the *Cisco ASR 903 Series Aggregation Services Router Chassis Software Configuration Guide*.

- Configuring encapsulation is not supported—The current software release does not support configuration of Layer 2 encapsulation using the **encapsulation interface** command.
- T1/E1 CRC size is not supported—The current software release does not support configuration of a T1 or E1 CRC size using the **crc** command.
- Inverting data on the T1/E1 interface is not supported—Inverting the data stream using the **invert data interface** command is not supported.
- Bit error rate test (BERT) patterns have limited support—Currently, only the 2^11, 2^15, 2^20-O153, and 2^20-QRSS patterns are supported for BERT.

Limitations and Restrictions in Cisco IOS XE Release 3.4.6S

There are no new limitations and restrictions in Cisco IOS XE Release 3.4.6S.

Limitations and Restrictions in Cisco IOS XE Release 3.4.5S

There are no new limitations and restrictions in Cisco IOS XE Release 3.4.5S.

Limitations and Restrictions in Cisco IOS XE Release 3.4.4S

There are no new limitations and restrictions in Cisco IOS XE Release 3.4.4S.

Limitations and Restrictions in Cisco IOS XE Release 3.4.3S

There are no new limitations and restrictions in Cisco IOS XE Release 3.4.3S.

Limitations and Restrictions in Cisco IOS XE Release 3.4.2S

There are no new limitations and restrictions in Cisco IOS XE Release 3.4.2S.

Limitations and Restrictions in Cisco IOS XE Release 3.4.1S

This section describes limitations and restrictions in Cisco IOS XE Release 3.4.1S and later releases.

sVTI and GRE Tunnel Protection Limitation

The limitations and restrictions on sVTI and GRE tunnel protection in Cisco IOS XE Release 3.4.1S are as follows:

- When using static VTI-based IPSec on a Cisco ASR 1000 Router, if there are multiple remote IPSec endpoints behind the same NAT device, their peer sVTI tunnels must not share the same tunnel source and tunnel destination addresses.
- When using GRE tunnel protection on a Cisco ASR 1000 Router, if there are multiple remote IPSec endpoints behind the same NAT device, their peer GRE Tunnel protection tunnels must not share the same tunnel source and tunnel destination addresses, at the same time, the IPSec mode must be set to transport mode when configuring the corresponding IPSec transform-set.

Limitations and Restrictions in Cisco IOS XE Release 3.4.0aS

There are no new limitations and restrictions in Cisco IOS XE Release 3.4.0aS.

Limitations and Restrictions in Cisco IOS XE Release 3.4.0S

The limitations and restrictions for using SPA-24CHT1-CE-ATM in Cisco IOS XE Release 3.4.0S are as follows:

- The SPA-24CHT1-CE-ATM is not supported on the Cisco ASR 1001 Router (1 RU chassis), but supported on all other ASR 1000 chassis.
- The SPA-24CHT1-CE-ATM supports only the CEM mode and not the ATM in Cisco IOS XE Release 3.4.0S.
- The SPA-24CHT1-CE-ATM is supported on Cisco IOS XE Release 3.4.0S and later releases only with these software images: ADVANCED ENTERPRISE SERVICES, ADVANCED ENTERPRISE W/O CRYPTO, ADVANCED IP SERVICES, or ADVANCED IP SERVICES W/O CRYPTO.
- The SPA-24CHT1-CE-ATM is not supported with these software images: IP BASE and IP BASE W/O CRYPTO.
- SPA-24CHT1-CE-ATM does not support ATM and IMA.
- CESoPSN over L2TPv3 is not supported.
- SAToP over L2TPv3 is not supported.
- CEM Access Circuit Redundancy is not supported.

The limitations and restrictions for using SPA-2CHT3-CE-ATM in Cisco IOS XE Release 3.4.0 are as follows:

- The SPA-2CHT3-CE-ATM is supported on Cisco IOS XE Release 3.4.0S and later releases.
- The SPA-2CHT3-CE-ATM is not supported on the Cisco ASR 1001 Router (1 RU chassis), but supported on all other ASR 1000 chassis.

  However, the SPA-2CHT3-CE-ATM supports only the ATM mode in Cisco IOS XE Release 3.4.0 and not the Circuit Emulation (CEM) mode.
- Maximum virtual circuits: 1,000
- Per-virtual circuit and per-virtual path traffic shaping is not supported.

- Switched virtual circuits (SVCs) is not supported.
- Interim Local Management Interface (ILMI) 1.0 is not supported.
- IETF RFC 2364 and 2516 for Point-to-Point Protocol (PPP) over ATM is not supported.
- IETF RFC 1577 support for classical IP and Address Resolution Protocol (ARP) over ATM is not supported.
- ATM Forum UNI 3.0, 3.1, and 4.0 is not supported.
- SPA-2CHT3-CE-ATM SPA does not support port channelization for ATM.
- NLPID encapsulation type is not supported.
- Maximum virtual circuits supported are 1,000.
- The SPA-2CHT3-CE-ATM does not support the CBIT Physical Layer Convergence Protocol (PLCP) framing.
- Only the Clear T3 mode is supported.
- The IMA mode is not supported on SPA-2CHT3-CE-ATM CEoP in Cisco IOS XE Release 3.4.0.
- POS and HDLC capabilities are not supported.
- Inverse Multiplexing over ATM (IMA) is not supported.
- ATM Local Switching is not supported.

The limitations and restrictions for using RTCP service on SPA-DSP in the Cisco IOS XE Release 3.4.0 are as follows:

- The length of the CNAME in the RTCP packets sent by endpoints should not exceed 40 bytes.
- If one endpoint does not send the RTP packets, the SPA-DSP neither generates the RTCP packets nor sends the RTCP packets to the other side.

The following is a limitation related to configuring an IPv6 over IPv4 GRE tunnel:

- In the context of an IPv6 over IPv4 GRE tunnel, if you want to configure the keepalive feature, an IPv4 address must be configured on the tunnel.

Limitations and Restrictions in Cisco IOS XE Release 3.3.2S

There are no new limitations and restrictions in Cisco IOS XE Release 3.3.2S.

Limitations and Restrictions in Cisco IOS XE Release 3.3.1S

There are no new limitations and restrictions in Cisco IOS XE Release 3.3.1S.

Limitations and Restrictions in Cisco IOS XE Release 3.3.0S

The following are the limitations and restrictions in Cisco IOS XE Release 3.3.0S and later releases:

- The SPA-1CHOC3-CE-ATM is not supported on the Cisco ASR 1001 Router, but is supported on all the other Cisco ASR 1000 Series Routers.
- All the other ASR 1000 Routers support the SPA-1CHOC3-CE-ATM for Circuit Emulation applications, but not ATM applications.

- The SPA-1CHOC3-CE-ATM is supported on Cisco IOS XE Release 3.3.0S and later releases only with these software images: ADVANCED ENTERPRISE SERVICES, ADVANCED ENTERPRISE W/O CRYPTO, ADVANCED IP SERVICES, and ADVANCED IP SERVICES W/O CRYPTO.
- The SPA-1CHOC3-CE-ATM is not supported with these software images: IP BASE and IP BASE W/O CRYPTO.

Limitations and Restrictions in Cisco IOS XE Release 3.2.2S

There are no new limitations and restrictions in Cisco IOS XE Release 3.2.2S.

Limitations and Restrictions in Cisco IOS XE Release 3.2.1S

The following are the limitations and restrictions in Cisco IOS XE Release 3.2.1S and later releases:

- On the standby RP, auto service level-initiated sessions containing IPv6 ACLs do not follow the template. This condition is observed consistently in the context of ACLs that can follow IPv6 templates. As a workaround, you can use the user level setting per-user avpair to define ACLs externally.

  However, IPv4-initiated sessions with the auto service level setting follow the template correctly.
- An IPv6 traffic filter cannot be configured under the policy map type service. Due to this, Service Logon profiles cannot be defined locally. As a workaround, you can use RADIUS to define Service Logon profiles.

Limitations and Restrictions in Cisco IOS XE Release 3.2.0S

This section describes limitations and restrictions in Cisco IOS XE Release 3.2.0S and later releases.

IPSec on Cisco ASR 1000 Routers

The following limitations and restrictions are related to the use of IPSec on Cisco ASR 1000 Routers:

- In the context of an IPSec DVTI Connection, the Cisco ASR 1000 Router does not support dynamic download ACL rule (per-user attribute) from the AAA server.

  For example, the following configurations are not supported:

  cisco-avpair += "ip:inacl#1=permit ip any 2.2.2.0 0.0.0.255"

  cisco-avpair += "ip:outacl#1=permit ip 2.2.2.0 0.0.0.255 any"
- The Cisco ASR 1000 Router does not support the **if-state nhrp** command in configuring the tunnel.
- The Cisco ASR 1000 Router Dead Peer Detection behavior is different than the pre-defined behavior (i.e. when there is no traffic to be sent, no DPD is sent, while if any traffic to be sent, DPD is sent). A Cisco ASR 1000 Router DPD is sent out regardless there is outbound traffic needs to be sent out.
- The Cisco ASR 1000 Router does not support SA Path MTU on data path.
- The Cisco ASR 1000 Router does not support double ACL in dynamic crypto map.

- VRF without crypto map configured on a physical interface causes dual esp reload on a Cisco ASR 1000 Router.
- The command: **show crypto ipsec sa identity** does not log send and receive error counts.
- The commands: **clear crypto** and **show crypto** on Standby RP are inconsistent with Active RP. At present most of other features disable 'clear commands' from Standby RP, but IPSec still allows to clear sa, session etc. from the standby.
- The Cisco ASR 1000 Router does not support Cisco AAA av-pair "**cisco-avpair += ip:sub-policy-In=policy1**".
- CLI allows both ikev1 and ikev2 profile configured under the same crypto map, even though it is not supported internally on the ASR 1000 Router.
- For a Cisco ASR 1000 Router, the tunnel protection should be removed first before changing any configuration for tunnel protection.
- On a Cisco ASR 1000 Router, when an EzVPN session is ended, the EzVPN server sends out the STOP accounting message. This message does not contain the Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets, and Acct-Output-Packets fields. It might cause a disruption in the accounting process.
- When using dynamic VTI-based IPSec on a Cisco ASR 1000 Router, if there are multiple remote IPSec endpoints behind the same NAT device, only one of the endpoints has connectivity. In other words, multiple endpoints cannot have connectivity at the same time.

TCP Failover in the Hardware High-Availability Mode

TCP failover is not supported in the Hardware High Availability mode. If the active node fails in the Hardware High Availability mode and if the network is then restored, it may take 5 to 10 minutes for the standby node to become the active node. This is because of the reboot and the peer negotiation delay. If the network is not restored, only the switched-over active peer is available. Failover is not possible in this state.

Tunneling on Cisco ASR 1000 Routers

The Cisco ASR 1000 Router does not support multi-VRF selection by the PBR feature on the tunnel interfaces on which the **ip vrf receive** setting has been configured.

Limitations and Restrictions in Cisco IOS XE Release 3.1.4aS

There are no new limitations and restrictions in Cisco IOS XE Release 3.1.4aS.

Limitations and Restrictions in Cisco IOS XE Release 3.1.4S

There are no new limitations and restrictions in Cisco IOS XE Release 3.1.4S.

Limitations and Restrictions in Cisco IOS XE Release 3.1.3S

There are no new limitations and restrictions in Cisco IOS XE Release 3.1.3S.

Limitations and Restrictions in Cisco IOS XE Release 3.1.2S

There are no new limitations and restrictions in Cisco IOS XE Release 3.1.2S.

Limitations and Restrictions in Cisco IOS XE Release 3.1.1S

This section describes the limitations and restrictions in Cisco IOS XE Release 3.1.1S and later releases.

Flexible NetFlow (FNF)

This section describes limits and restrictions related to Cisco Flexible Netflow features in Cisco IOS XE Release 3.1.1S on the Cisco ASR 1000 Series Router.

- V5 (old style) export with any user-defined flow record format is not supported. This applies even when the user-defined format is a subset of a supported v5 format. For more details, see CSCti69232.
- NetFlow on BB sessions is not supported. For more details, see CSCsx24985.

Note CSCsx24985 applies to both Cisco tNF and Cisco FNF features.

- v6 FNF is not supported. For more details, see CSCsx24985.
- MPLS netflow is not supported. For more details, see CSCtf39723.
- FNF ISSU/SSO is not supported. For more details, see CSCth71187.

For more information, see *Cisco IOS XE Flexible NetFlow Overview* at the following location:

http://www.cisco.com/en/US/docs/ios/ios_xe/fnetflow/configuration/guide/fnetflow_overview_xe.html

Limitations and Restrictions in Cisco IOS XE Release 3.1.0S

This section describes limitations and restrictions in Cisco IOS XE Release 3.1.0S and later releases.

SIP-40G:SPA-4XT-SERIAL

SIP-40G:SPA-4XT-SERIAL was not supported in Release 3.1.0S when plugged into a Cisco ASR1000 Series Router with SIP-40 linecard. This SPA is supported in Release 3.1.1S on a SIP-40 linecard.

FNF

The Cisco FNF feature is not supported in Cisco IOS XE Release 3.1.0S on the Cisco ASR 1000 Series Router.

SDH support on 1xCHOC12/DS0 SPA

SDH framing is not supported in Cisco IOS XE Release 3.1.0S for the 1xCHOC12/DS0 SPA. SONET is the only supported in framing mode.

SDH framing support will be supported, starting in Cisco IOS XE Release 3.1.1S on 1xCHOC12/DS0 SPA.

uRPF ACL

The Cisco ASR 1000 Series Routers do not support uRPF ACL.

Interchassis and Intrachassis Support

Coexistence of interchassis high availability and intrachassis high availability is not supported.

In the Cisco ASR 1001 Router, Cisco ASR 1002 Router, and Cisco ASR 1004 Router, interchassis redundancy is not supported with software redundancy.

In the Cisco ASR 1006 Router and Cisco ASR 1013 Router, interchassis redundancy is not supported with intrachassis redundancy. It is supported with only a single RP and ESP in the chassis.

GRE Keepalive with Tunnel Protection

The Cisco ASR 1000 Series Router supports GRE keepalive with tunnel protection. However, the keepalive packet that is returned is not encrypted.

Limitations and Restrictions in Cisco IOS XE Release 2.3.0

This section describes limitations and restrictions in Cisco IOS XE Release 2.3.0 and later releases.

User-Defined Parent Class Limitation (for Hierarchical QoS)

On a Cisco ASR 1000 Series Router with hierarchical QoS and user-defined parent classes applied, each child policy must be a unique policy map. The use of a single child policy map in multiple instances in the definition of a user-defined parent class is not supported in Cisco IOS XE Release 2.3.0. For more details, see CSCsr56079.

Note The User-Defined Parent Class Limitation (for Hierarchical QoS) is no longer applicable in Cisco IOS XE Release 2.3.1 and later releases. The use of a single child policy map in multiple instances in the definition of a user-defined parent class is supported in these later releases.

User-Defined Parent Class Limitation (for Conditional Policer)

On a Cisco ASR 1000 Series Router with hierarchical QoS and user-defined parent classes applied, each child policy must use an unconditional policer (priority + policer). The use of conditional policers (priority x kbps) is not supported in these configurations in Cisco IOS XE Release 2.3.0. For more details, see CSCsy99583.

Deny ACL Limitation for GET VPN

No more than 8 deny access control lists (ACLs) (a total of Key Server downloaded and group member local) are supported for Group Encrypted Transport VPN (GET VPN) in Cisco IOS XE Release 2.3.0. For more details, see CSCsy24144.

Limitation Related to the Use of Deny Statements in QoS Classification

Large numbers of **deny** statements should not be used as access control entries (ACEs) in access control lists (ACLs) used for Quality of Service (QoS) classification in Cisco IOS XE Release 2.3.0. The number of **deny** statements and the order of these statements with other **permit** statements in an ACL determines the amount of content-addressable memory (TCAM) used, and there is no fixed number quantified as a limit for this configuration. For more details, see CSCsx16234.

Limitations and Restrictions in Cisco IOS XE Release 2.2.3

This section describes limitations and restrictions in Cisco IOS XE Release 2.2.3 and later releases.

DMVPN Limitation

In a very large Dynamic Multipoint VPN (DMVPN) network (for example, 1500 spokes connecting to a single hub), some of the tunnels may not be fully reflected in the hardware and may cause traffic drop on those tunnels. This condition is more likely to happen when users configure a very large number of spokes and toggle the interfaces between **shut** and **no shut** multiple times. When this condition occurs, perform **shut/no shut** on the specific spoke for which the hub does not have the entry in the hardware.

Scaling Limits for MLP

The supported scaling limits for Multilink PPP (MLP) for Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.2.3 and later releases are as follows:

- 123 10-link bundles

- 245 5-link bundles
- 616 2-link bundles

The maximum scaling limit for LFI is 1232 single-link bundles.

If either the maximum number of bundles or maximum number of links are exceeded, the interface line rate may not be maintained. This limitation is especially applicable for configurations that have a high number of links per bundle and a high number of features enabled.

Limitations and Restrictions in Cisco IOS XE Release 2.2.1

This section describes limitations and restrictions in Cisco IOS XE Release 2.2.1 and later releases.

Cisco Firewall and WAAS Inter-Op Limitations and Restrictions

The Cisco Firewall and WAAS Interoperability feature is subject to the following limitations and restrictions in Cisco IOS XE Release 2.2.1:

- Only Generic Routing Encapsulation (GRE) redirect and return is supported. Layer 2 redirect and return is not supported.
- Certain platforms, such as the Cisco 2800 series, support an inbox network service module (WAAS-NM) that provides WAAS services. The Cisco ASR 1000 Series Routers do not support inbox network service modules; thus, the router will not support WAAS-NM.

Control Plane Policing (CoPP) Limitations and Restrictions

Control Plane Policing (CoPP) does not support **match protocol l2tp** and **match protocol dhcp** for Cisco IOS XE Release 2.2.1. However, because CoPP supports packet matching with access lists, you can police Layer 2.

L2TP and DHCP packets can be matched by access lists. For example, L2TP and DHCP packets can be matched with access lists that check UDP packet port number (1701 for L2TP, 67 and 68 for DHCP).

Flexible Packet Matching (FPM) Limitations and Restrictions

Flexible Packet Matching (FPM) support is subject to the following limitations and restrictions in Cisco IOS XE Release 2.2.1:

- Table 1 describes the functionality supported in the Raw FPM and Basic FPM (Raw FPM+) modes in Cisco IOS XE Release 2.2.1.

Table 1 FPM Functionality Support by Mode

Mode	Supported Functionality
Raw FPM	• Supports Raw offset and bit pattern matching from L2 or L3 start • Protocol unaware • Match string pattern up to 32 bytes • Regular expression matching • Packet inspection depth: 256 bytes • Maximum 32 classes are supported in a policy-map; 8 entries per class map
Basic FPM (Raw FPM+)	• PHDF nomenclature (for fixed length fields) • Support for building protocol stacks (for static header length only)

- Although Cisco IOS XE Release 2.2.1 does not support the traffic classification description file (TCDF), bittorrent, iis-unicode, ios-http-vuln and skype can be configured manually.

L2TP AAA Accounting Include NAS-PORT (VPI/VCI) Limitation

In Cisco IOS XE Release 2.2.1, the L2TP AAA Accounting Include NAS-PORT feature does not support the asynchronous transfer mode (ATM) virtual path identifier/virtual channel identifier (VPI/VCI) pair.

Limitations and Restrictions in Cisco IOS XE Release 2.1.1

This section describes the limitations and restrictions in Cisco IOS XE Release 2.1.1 and later releases.

Maximum Number of Broadband Tunnels Limitation

Up to 16K broadband tunnels are supported in Cisco IOS XE Release 2.1.1.

Maximum Number of IPSec Tunnels Limitation

Up to 4K IPSec tunnels are supported in Cisco IOS XE Release 2.1.1.

Limitations and Restrictions in Cisco IOS XE Release 2.1.0

This section describes limitations and restrictions in Cisco IOS XE Release 2.1.0 and later releases.

IPv6 Source Address of ICMPv6 Error Message

Note This limitation has been removed in Release 3.4.0 and later releases.

When all the interface related to ICMPv6 error message generation or forwarding have only the IPv6 link-local address in place, link-local is set as the source address of generation ICMPv6 error mesages.

The interface types related to ICMPv6 error message generation or forwarding are:

1. The interface by which the original packet is received. The original packet refers to the packet triggering the ICMPv6 error message.
2. The interface by which the original packet should be sent out there is no incident to trigger an ICMPv6 error message.
3. The interface by which the ICMPv6 error message is sent out. To perform asymmetric routing, the interfaces described in the pervious items are different, otherwise, the interfaces are identical.

IPv6 Address Support on ASR1000 Hardware Interfaces

On the Cisco ASR 1000 Series Router, only one IPv6 IP address exists for each interface. Even if, several IPv6 IP addresses are configured on an interface, only the lowest IPv6 IP address is downloaded to the hardware.

The Cisco ASR 1000 Router hardware, supports only one IPv6 address for each interface. Therefore, even if several IPv6 IP addresses are configured on an interface, in Cisco IOS, only the lowest IPv6 address is downloaded to the hardware.

Note When IPv6 is enabled in the interface mode (config-if), and if global unicast and anycast IPv6 addresses are not configured, the link-local address is downloaded to the hardware. Otherwise, the lowest IPv6 address is downloaded to hardware.

Conditional Policing Feature of QoS Limitation

The Conditional Policing feature of Quality of Service (QoS) is not supported in Cisco IOS XE Release 2.1.0

Note Beginning with Cisco IOS XE Release 2.1.1 and later releases, the Conditional Policing feature of Quality of Service (QoS) is supported. This limitation does not apply to these later releases.

IPSec Anti-Replay Window Size Limitation

The maximum IPSec anti-replay window size supported in Cisco IOS XE Release 2.1.0 is 512.

Maximum Number of IPSec Tunnels Limitation

Up to 2k IPSec tunnels are supported in Cisco IOS XE Release 2.1.0.

Note From Cisco IOS XE Release 2.1.1, up to 4K IPSec tunnels are supported. This 2K limitation does not apply to these later releases.

NBAR Protocol Support Limitation

Note Later releases of NBAR in Cisco IOS XE include support for additional protocols. For information about the NBAR protocol support per Cisco IOS XE release, see the following document: http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/clsfy_traffic_nbar_xe.html

Network Based Application Recognition (NBAR) can only match the following protocols in Cisco IOS XE Release 2.1.0:

- CU-SeeMe
- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS)
- Post Office Protocol (POP3)
- Telnet
- Secure HTTP
- Real Time Streaming Protocol (RTSP)
- Session Initiation Protocol (SIP)
- Skype (TCP-only)
- HTTP (no options including url and host)
- File Transfer Protocol (FTP)
- H.323

police Command Limitation

When using a policer for service policies configured on Multilink PPP (MLP) bundles, the **percent** version of the **police** command should be used in Cisco IOS XE Release 2.1.0.

Scaling Limits for MLP

The supported scaling limits for Multilink PPP (MLP) in Cisco IOS XE Release 2.1.0 are as follows:

- 16 10 link T1 bundles
- 27 7 link T1 bundles
- 40 5 link T1 bundles

- 500 single link T1 bundles with LFI

Note From Cisco IOS XE Release 2.2.3, the MLP scaling limits have been revised. For information about the revised scaling limits for Cisco IOS XE Release 2.2.3 and later releases, see the "Scaling Limits for MLP" section on page 34.

Router Advertisement and Neighbor Solicitation Processing Limitation

Router advertisements and neighbor solicitation messages are not processed if IPv6 unicast routing is not configured.

sVTI, DMVPN, and GRE Tunnel Protection Limitation

The Cisco ASR 1000 Series Routers do not support sVTI, DMVPN, and GRE tunnel protection with NAT traversal.

Note From Cisco IOS XE Release 3.4.1S, the limitation on sVTI and GRE tunnel protection has been revised. For information about the revised limitation for Cisco IOS XE Release 3.4.1S and later releases, see the "Limitations and Restrictions in Cisco IOS XE Release 3.4.1S" section on page 27.

Limitation Related to the Handling of Link-Layer Broadcasts

According to RFC 1812, a packet must be dropped if the L2 address is a broadcast address and the L3 address is not a multicast address or if the broadcast address is not a valid broadcast address. At present, this is not implemented. Note that a valid broadcast address is defined as one of the following:

- 255.255.255.255
- Subnet broadcast address of the incoming interface
- Subnet network address of the incoming interface