

GGSN 12.3(8)XU Product Bulletin No. 2539

Cisco GGSN 12.3(8)XU Release Product Bulletin

Introduction

This Product Bulletin describes the content and delivery information concerning Cisco IOS™ software release 12.3(8)XU.

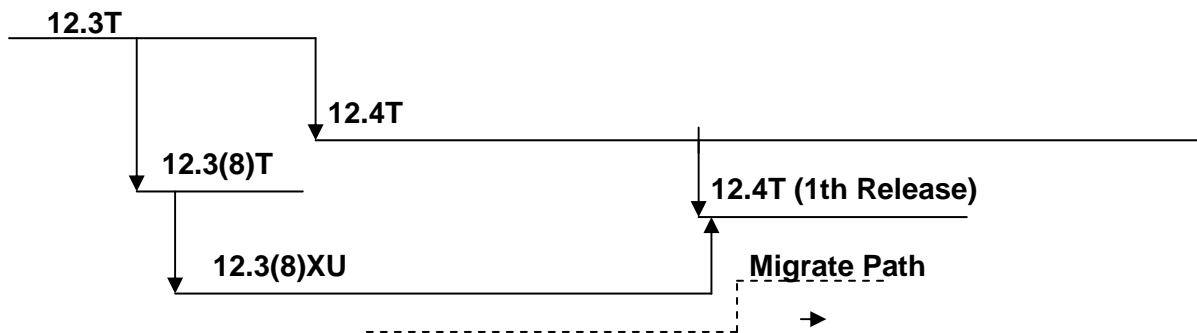
It should be used in conjunction with Product Bulletin titles, Cisco IOS Software Release 12.3(8). The 12.3(8)XU release is supported on:

- Multi-Processor WAN Application Module Card on Cisco 7600 Internet Router and Catalyst 6500 platforms and in future it will be supported on Cisco 7206VXR/NPE-400 Platform with 512MB memory

This release contains all the features supported in the earlier GGSN release 12.3(8)T.

Given below is the release migration diagram depicting the collapse of 12.3(8)XU into the mainline T train:

Figure 1. Migration Diagram



Features in Cisco IOS Release 12.3(8)XU

The following features will be delivered in 12.3(8)XU. Release 5.0 supports the GGSN 3G/UMTS.



Table 1. Cisco IOS Release 12.3(8)XU Features:

Features	MWAM on Cat6000/7600
3GPP standards upgrade: 3GPP standards upgrade compliance is to R98/R99/R4 Dec 2002 level and selected CRs for R5	X
Local/Third Charging GW Support: Support of a third CGW for back up purposes.	X
Time Based Triggers and Charging Characteristics: Enabling Charging per APN	X
Enable Charging per APN: Part of Charging enhancements to enable charging per APN	X
Identification/Differentiation of Regular and Duplicate CDRs	X
Configurable RADIUS attributes for MSISDN and Account Session ID for backward	X
Session timeout from RADIUS	X
Mapping of Multiple APNs to a single VRF	X
Support of Multiple Trusted PLMN Ids	X
Maintenance Mode for APN config during active PDPs: (a) Stop generating CDRs even	X
MIB Enhancements for 5.0 Features	X
Session Timeout from RADIUS	X
Rate (Bandwidth) Limit per PDP: Part of CAC and per PDP policing	X
UMTS Call Admission Control and per PDP Policing: Rate (bandwidth) limit per PDP;	X

*VRF functionality, Overlapping IP Address and Tunnel support will be per image on the MWAM. VRF and Tunnel Aggregation at the SUP level will be supported in SUP720 in Tetons release.

Detailed Information

3GPP Standards/CR Compliance

GGSN 5.0 needs to be fully compliant with 3GPP R98/R99/R4 release and also with R5 release in terms of charging CRs. The compliance level of CRs needed is up to 3GPP TSG 18 (Dec 2002). Specific CRs that GGSN 5.0 is compliant with need to be listed in the SFS and also the level of compliance needs to be documented.

Charging Enhancements

- Local/Tertiary Charging GW support: This is to support a third CGW in addition to the two (primary and secondary) that Cisco GGSN already supports. The third CGW can be deployed locally so that if the access to the primary and secondary CGW which are remote fails, then the GGSN can as backup, send the CDRs to the local (third) CGW till one of both of the remote CGWs become operational. Then the GGSN switches back to the primary and/or secondary.
- Time Based Triggers: GGSN 5.0 needs to support time based triggers for generation of G-CDRs in addition to the volume based triggers that are already supported by the Cisco GGSN. These should be able to be enabled per GGSN or APN or per PDP context.
- Enabling Charging per APN: GGSN 5.0 should allow enabling/ disabling of generation of CDRs per APN.



RADIUS Support

Configurable Radius Attribute for Backward Compatibility: GGSN needs to allow configuration of the RADIUS attributes for MSISDN and the Account Session ID for a user to be able to support backward compatibility with WAP.

APN Based Features

- Mapping Multiple APNs to a Single VRF: GGSN 5.0 needs to support more than one APN per VRF. The maximum number of APNs per VRF need to be clearly documented in the SFS and the product bulletin and other customer documentation.
- Enabling Charging per APN: GGSN 5.0 should allow enabling/ disabling of generation of CDRs per APN. This is the same feature which is part of the Charging enhancements.
- Rate Limit for users per APN: This feature should allow a controlled distribution of bandwidth per APN. Some APNs may be recognized as those used for bandwidth intensive applications such as music mp3 hosts or others where image files or large file sizes are involved. The GGSN is configurable on a per APN basis to restrict the transfer rate per subscriber to an operator defined limit that would reduce the chance of a GGSN from being congested and thereby increase its availability. This is also part of the CAC and per PDP policing feature suite.

Security Enhancements

Support of Multiple Trusted PLMN IDs: Access to certain partner roaming MSs should be allowed and by default other roamers should be blocked on an APN basis. This allows the operators to provision access based on partner agreements. GGSN needs to allow more than one trusted PLMN Id. This is for operators forming multiple alliances and they do not want the MSs from their partners to be blocked because they do not belong to the home PLMN that the GGSN belongs to. This feature should allow the operator to configure multiple trusted MCC/MNCs.

Operation, Maintenance Features

- Maintenance Mode: GGSN needs to allow key APN configuration when there are active PDP contexts. GGSN should allow the operators to change the APN configuration in real-time, without tearing down any active PDP contexts on that APN. Example: This is a big issue for VF, Spain, for Parking meters where new PDP requests keep coming in even as the old ones are being torn down for maintenance purposes. They have 400 parking machines that use an APN, to change the APN, they must delete all PDP contexts, but as soon as they delete them the machines restart the PDP contexts, so there is a very short time they can change the APN, they end up having to unplug the cable or reboot, which is equivalent to loss of revenue.
- Prevent Generation of CDRs for active PDP contexts: This was a request from Amena, Spain. Deactivation of generation of G-CDRs for an active PDP context. Customers should be able to stop generation of G-CDRs when a PDP context is active without tearing down the PDP context to be able to do this. This is related to the above maintenance mode feature for allowing key APN configuration for active PDP contexts.

Policy Enforcement/IMS Enabling Features

- UMTS CAC: UMTS Call Admission Control is used by the GGSN admission decisions based on the network resource availability and the policy set by the PDF in case of IMS subsystem implementation. It can also downgrade a service if the policy parameters from PDF do not match those from the SGSN. CAC is based on the parameters configured in the APN, such as max activated PDP, max bitrate, guaranteed bitrate, etc., and bandwidth allocated to a particular traffic class the PDP belongs to.



- Per PDP Policing: GGSN will support Per-PDP policing to limit downlink traffic at Gi interface. If the bandwidth is exceeded on a PDP context, packets may be dropped or assigned a higher drop precedence value.
- Rate Limit for PDPs per APN: GGSN 5.0 should allow operators to configure rate (bandwidth) thresholds per APN. This is also mentioned above in the APN Based Features.

Backward Compatibility

All GGSN R4.0 features supported in 12.3(8)T will be supported in 12.3(8)XU on MWAM. The VRF functionality, Overlapping IP Address and Tunnel support will be per image on the MWAM. VRF and Tunnel Aggregation at the SUP level will be supported in SUP720 in Tetons release.

The features of 12.3(8)XU which will be the same as in 12.3(8)T are described below:

L2TP Extension on Gi for PPP PDP Type

GPRS Tunneling Protocol (GTP) is the protocol used between SGSN and GGSN to tunnel various data protocols through the GPRS backbone. The PPP PDP type traffic from MS is processed at the GGSN, where the PPP sessions are terminated. The GGSN then transports the traffic over L2TP and then routes over Gi, to their destination. This feature requires the MS to support PPP PDP type.

PPP PDP Type terminated in GGSN

GPRS Tunneling Protocol (GTP) is the protocol used between SGSN and GGSN to tunnel various data protocols through the GPRS backbone. The MS can send IP traffic encapsulated as PPP sessions all the way to GGSN, where the PPP sessions are terminated, and the IP packets are routed as IP Packets over Gi, by GGSN to their destination. This feature requires the MS to support PPP PDP type.

QoS Mapping per standards for GTPv0

In addition to new full QoS support for UMTS, GGSN 4.0 also supports for GTPv0, mapping of GPRS QoS classes to IP QoS classes (air to wireline). New QoS mapping based on delay class (compliant to UMTS) is supported. Resulting QoS classes mapped to Diffserv classes. The canonical QoS mapping supported in GGSN 3.0 is still supported for GTPv0 in GGSN 4.0.

Duplicate IP Address Protection (also known as PLMN Address Protection)

This feature also known as PLMN address protection, allows the GGSN to be configured with a specific address range (i.e. the PLMN IP addressing plan), and the GGSN will reject the PDP creation if the MS address belongs to the specified range.

Dynamic Echo Timer

In the previous releases, the retransmission scheme used for the GTP Echo messages is using the usual T3-timer and N3-Request. However according to the standard if a path failure is detected (i.e. no Echo Response after N3 Echo Request) on the Echo Request message, all PDP context related to this path shall be deleted. This feature allows the GGSN to use a dynamic timer for the Echo Request message. To avoid having a large number of PDP contexts to be deleted because of a network congestion between the GSNs, the dynamic echo timer takes into account the Round Trip Time (RTT) between GSNs.

PPP Regeneration (L2TP on Gi)

This feature allows the GGSN to regenerate a PPP session and forward the PPP frames within L2TP tunnels on Gi. Targeted for corporate users, the GGSN can be seamlessly integrated in a VPDN L2TP infrastructure.



Virtual APN Support

The virtual APN concept allows provisioning of one APN per type of access, one for corporate, one for ISP, etc. The selection of the "real" network is made using a structured username entered by the users. As an example, for corporate access the user will enter as username "login@domain". Where domain indicates the corporate (e.g. cisco.com). Upon PDP context activation the GGSN will select the target corporate using this username and not the APN.

Enhanced Security Feature Support

- Source IP spoofing protection (also called Anti-spoofing feature): This feature allows the operator to prevent source IP address spoofing and protects the network from malicious attacks by unauthorized users.
- PLMN Network Protection from MSs: This feature allows the operator to protect their PLMN by dis-allowing MS traffic to the destination IP address range that falls within or coincides with the PLMN's IP address range.
- Steer MS to MS traffic: This feature allows steering of MS to MS traffic to a specific external network element instead of allowing the traffic to loop through the GGSN. This is for firewall filtering and to enable external billing.

Route Aggregation

In GPRS release 1.4 a static route for the MS was created in the GGSN after each PDP context activation. Each route, has indeed an impact on the capacity of the GGSN. In GGSN 4.0 release, to scale and support more PDP contexts, an aggregate route can be used to handle user data packets for multiple PDP contexts (instead of a host route for each PDP context). Using this feature, MS host routes with the same prefix will be aggregated into one route.

CEF Switching

This feature adds Cisco Express Forwarding enhanced Layer 3 switching technique to the GGSN. Basically, CEF switch is to switch the packet out in the receive handler, it will avoid the delay incurred due to enqueueing/ dequeueing. CEF avoids the potential overhead of continuous cache churn by instead using a Forwarding Information Base (FIB) for the destination switching decision which mirrors the entire contents of the IP routing table. i.e. there is a one-to-one correspondence between FIB table entries and routing table prefixes; therefore no need to maintain a route-cache.

VRF Based VPN Switching

Virtual Routing Function feature allows traffic to be switched to a destination VPN. This will enable GGSN with true VPN support with redundant interfaces. This feature supports routing protocols per APN. Each VRF is a virtual router in GGSN and can map to an APN. This provides flexibility to connect to a corporate network, and still satisfy the destination networks that are unique to each corporate. Benefits of using VRF also include:

- Security (traffic separation and isolation)
- Reliability and Scalability (multiple interfaces can be supported in one VRF)
- Flexibility (can use policy and address space independently)

Charging for Roamers

This feature enables the operators to charge the roamers based on the matching of MNC/MCC id and the IMSI/MSISDN address.



GTP SLB Support for GTPv0 and GTPv1

The GTP Server Load Balancing (SLB) features allows to truly distribute the PDP context creation between multiple GGSNs. The load-balancing mechanism actually uses the load of each GGSN to do the load balancing.

GTP SLB for MWAM Based GGSNs:

For MWAM GGSNs on 7600 Internet Router and Cat6500 platforms, the GTP SLB will be supported on the SUP2. The GTP SLB functionality is supported in 12.2(14)ZA release.

The most current release notes for 12.2(14)ZA on the Catalyst 6500 series switches and Cisco 7600 Series Internet Routers are available on Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_3827.htm

Network Initiated PDP Context Support

GGSN R4.0 supports GTP Location Management Messages for Network-Requested PDP Context Activation procedure via a GTP-MAP protocol-converting GSN. Static PDP context information for IP address to IMSI mapping need to be configured on GGSN for the support.

RADIUS Support/Enhancements

The following Radius features are supported in GGSN 4.0:

- Complete 3GPP attribute support as per 29.061 specification
- Per PDP Accounting for GTPv1 sessions including accounting for Secondary PDPs
- Suppression of Radius attributes
 - 3GPP-IMSI
 - 3GPP-SGSN-Address
 - 3GPP-QoS-Negotiated
- Support Anonymous access
- Support of VRF aware Radius groups
- RADIUS Class Attribute
- Session idle timer (on top of session idle timer per APN)
- Wait Accounting

Miscellaneous

Brief explanation of key Radius features from the above list is provided below:

Support anonymous access

Allow to support RADIUS authentication when only handset are used (e.g. GPRS WAP phones). Default username and password configured per APN on the GGSN



RADIUS Class Attribute

GGSN R3.0 supports the RADIUS Class attribute (#25). This attribute is sent upon authentication, within the Access-Response message by the RADIUS server to the GGSN. The Class attribute received in the authentication response of Primary PDP context is sent in all the accounting messages of Secondary PDP context.

Session Idle Timeout Timer (configurable per APN)

GGSN support for radius attributes for session/ idle timeout on a per session basis. In GGSN 1.4 the idle timer granularity is at the GGSN level. Idling PDP contexts are deleted when the timer expires GGSN 4.0 provides a per session idle timer. The granularity of support is:

- per session based on RADIUS attribute
- configurable, per APN
- configurable, per GGSN

Wait Accounting

Another key Radius enhancement supported is the 'Wait-accounting' feature which enables GGSN to wait for the accounting response from Radius server before sending back Create PDP Context Response message.

Miscellaneous

Other Radius enhancements were made in the GGSN release 3.0 will be supported in GGSN 4.0 also, such as supporting new CLI, and allowing authentication and accounting using the new server group commands, and also have the ability to enable accounting in the transparent mode.

For more detailed information about the platform and features being delivered in 12.3(8)XU release, please reference the following release notes documents:

For 12.3(8)XU on MWAM Release Notes, please refer to the following link:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123reInt/cat6000/index.htm>

Support

Cisco IOS software release 12.3(8)XU follows the standard Cisco support policy as indicated in the following link:

<http://www.cisco.com/en/US/support/index.html>



Product Numbers

Product Numbers for MWAM (cat6500 and 7600 platforms) based 12.3(8)XU Release are as follows:

Table 2. MWAM Cisco IOS Release 12.3(8)XU Feature Sets, Images and Descriptions:



Platform	Product Code	Software Description	Image	Flash	DRAM
7600/6500 MWAM	SC-SVC-GG50B	Cisco MWAM Series IOS GGSN 5.0 Base	c6svc-mwam-g8is-b1.123-8.XU.bin	48 MB	512MB
7600/6500 MWAM	SC-SVC-GG50B=	Cisco MWAM Series IOS GGSN 5.0 Base	c6svc-mwam-g8is-b1.123-8.XU.bin	48 MB	512MB
7600/6500 MWAM	SC-SVC-GG50P	Cisco MWAM Series IOS GGSN 5.0 Premium	c6svc-mwam-g8is-b1.123-8.XU.bin	48 MB	512MB
7600/6500 MWAM	SC-SVC-GG50P=	Cisco MWAM Series IOS GGSN 5.0 Premium	c6svc-mwam-g8is-b1.123-8.XU.bin	48 MB	512MB
7600/6500 MWAM	SC-SVC-GG50UP=	Cisco MWAM Series IOS GGSN 5.0 Base to Premium Upgrade	c6svc-mwam-g8is-b1.123-8.XU.bin	48 MB	512MB
7600/6500 MWAM	SC-SVC-GG50UBB=	Cisco MWAM Series IOS GGSN Upgrade from 4.0 to 5.0 Base	c6svc-mwam-g8is-b1.123-8.XU.bin	48 MB	512MB
7600/6500 MWAM	SC-SVC-GG50UBP=	Cisco MWAM Series IOS GGSN Upgrade from 4.0 to 5.0 Premium	c6svc-mwam-g8is-b1.123-8.XU.bin	48 MB	512MB
7600/6500 MWAM	SC-SVC-GG50BIM	Cisco MWAM Series IOS GGSN 5.0 Base (Single IM)	c6svc-mwam-g8is-b1.123-8.XU.bin	48 MB	512MB
7600/6500 MWAM	SC-SVC-GG50BIM=	Cisco MWAM Series IOS GGSN 5.0 Base (Single IM)	c6svc-mwam-g8is-b1.123-8.XU.bin	48 MB	512MB
7600/6500 MWAM	SC-SVC-GG50PIM	Cisco MWAM Series IOS GGSN 5.0 Premium (Single IM)	c6svc-mwam-g8is-b1.123-8.XU.bin	48 MB	512MB
7600/6500 MWAM	SC-SVC-GG50PIM=	Cisco MWAM Series IOS GGSN 5.0 Premium (Single IM)	c6svc-mwam-g8is-b1.123-8.XU.bin	48 MB	512MB
7600/6500 MWAM	SC-SVC-GG50UPIM=	Cisco MWAM Series IOS GGSN 5.0 Bs to Prm Upg (Single IM)	c6svc-mwam-g8is-b1.123-8.XU.bin	48 MB	512MB
7600/6500 MWAM	SC-SVC-GG50UBBIM=	Cisco MWAM Series IOS GGSN Upg-4.0 to 5.0 Bs (Sngle IM)	c6svc-mwam-g8is-b1.123-8.XU.bin	48 MB	512MB
7600/6500 MWAM	SC-SVC-GG50UBPIM=	Cisco MWAM Series IOS GGSN Upg-4.0 to 5.0 Prm (Sngle IM)	c6svc-mwam-g8is-b1.123-8.XU.bin	48 MB	512MB
7600/6500 MWAM	WS-SVC-MWGG50- BDL	Cisco MWAM Series GGSN 5.0 Premium 2 Unit Bundle	c6svc-mwam-g8is-b1.123-8.XU.bin	48 MB	512MB
7600/6500 MWAM	WS-SVC-MWGG50- BDL=	Cisco MWAM Series GGSN 5.0 Premium 2 Unit Bundle	c6svc-mwam-g8is-b1.123-8.XU.bin	48 MB	512MB

Download Information

Customers can download Cisco IOS Software Release 12.3(8)XU software from Cisco.com in the software image library:

<http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml>.

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International
BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright 2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site 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. (0301R)