



# Cisco IOS 12.3 Features

Peter J. Welcher

## Introduction

This month's article is for all those readers who are maintaining Cisco routers. Cisco has just released Cisco IOS version 12.3. I'd like to take a look at what's in it for us.

## Why Cisco IOS 12.3?

Cisco IOS Release 12.3 is an expected step in Cisco's normal code process. Every once in a while, Cisco engineers gather together all the new features in the T and X Early Deployment (ED) releases. These form the next major release. At this point, development then takes two paths. New features are added via the 12.3 (number) T or X\* releases, and bug fixes are applied to the 12.3 (number) (no following letters) releases. The releases without a letter are Limited Deployment (LD) releases until there are few important bugs turning up and until Cisco engineers feel the code deserves to be labeled General Deployment (GD).

Why you care about this: if you need to support a new router or router hardware, you may have to use a T or X release in it. You almost certainly should **not** use that code in your other routers. It might have bugs, and is probably less reliable than older more mature code. That's what the euphemism "Early Deployment" means. The code contains version 1.0 of those new features! Finding a "T" in the name means the new features are generally supporting all routers (or will eventually be). Finding an "X" in the name means the feature was introduced to support specific new hardware (router or card for a router).

Some organizations try to only use GD ("General Deployment") releases. These are usually 1 to 2 major versions back, and are usually up around minor release 10 or more. They receive extensive regression testing as well. They are generally rather stable and free of known major bugs.

For example, I just checked CCO. I see that 12.2 (17) or 12.2.17 is marked LD. 12.1.13 onwards are GD. All the 12.2.17 T, S, and X\* releases are marked ED. As I would have expected.

[http://www.cisco.com/cgi-bin/Software/iosplanner/Planner-tool/iosplanner.cgi?get\\_crypto=&data\\_from=&hardware\\_name=&software\\_name=&release\\_name=&majorRel=12.3&state=&type=](http://www.cisco.com/cgi-bin/Software/iosplanner/Planner-tool/iosplanner.cgi?get_crypto=&data_from=&hardware_name=&software_name=&release_name=&majorRel=12.3&state=&type=)

To sum that up: those with new hardware, those with a craving for adventure or the latest new features, and those who don't mind less stable networks, can run ED code. Those who want recent features and don't mind some risk, run LD code. And the risk averse and those who like very stable networks run GD code.

## Supported Devices for 12.3

The official list: Cisco 800, 1700, 2600, 3600, 3700 and 7000 Series Routers. I see a 2500 image on CCO as well (above link).

New platforms supported: 3700 series (3725 and 3745), 1760, 7200 NPE-G1, 7500 series RSP-16.

Other boxes, especially in the Service Provider space, may require 12.2 S or earlier releases.

## New Packaging in Cisco IOS 12.3

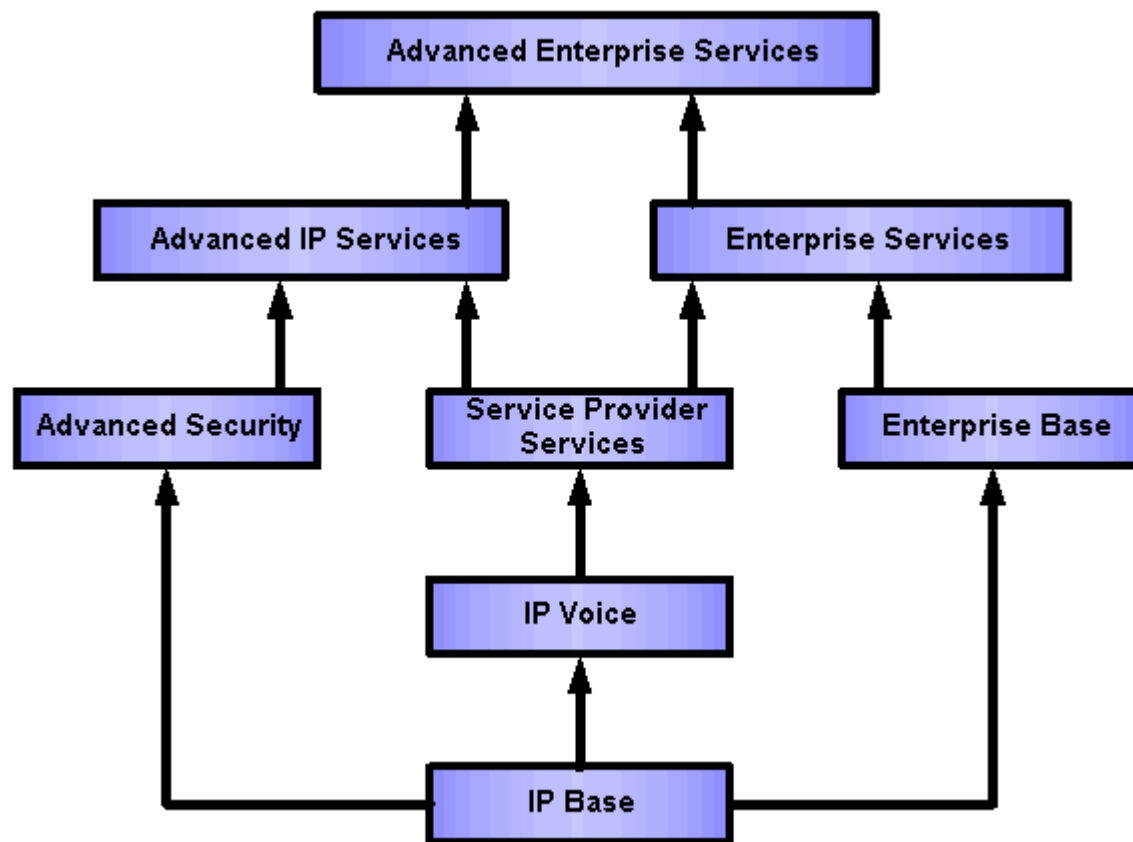
In an attempt to reduce the proliferation of feature sets in prior release, Cisco has re-designed its approach to device packaging. This helps them reduce engineering and support costs. It helps us reduce confusion.

The following section describes the broad outlines of the program.

Be aware that there are exceptions. For example, only 3 packages are available for the 1721 and 1751 routers. The 1720, 2600 non-XM, and the Cisco 3600 routers are not supported via these packages. The following platforms do not support Cisco IOS Packaging in Release 12.3: Cisco 1720, Cisco 2600 non-XM, and the Cisco 3600 Router Series. I checked the Software Planner page, and the feature sets for the 3640 do look similar to the older feature sets.

See also <http://www.cisco.com/warp/public/732/releases/packaging/docs/pb.pdf> .

The new scheme is intended to be hierarchical, with more comprehensive feature sets including all the features in the less comprehensive ones. In the diagram below, the smallest image is at the bottom. The ones above inherit features as indicated by the arrows. This is my version of the diagram in the above document.



The eight (8) current Cisco IOS packages (shown above) are:

- IP Base
- IP Voice
- Enterprise Base
- Advanced Security
- SP Services
- Advanced IP Services
- Enterprise Services
- Advanced Enterprise Services

Some specifics about each of these follow. The quotations are from the above document. The overall recommendation is that if you're in doubt, consult the online Feature Navigator to double-check that a given package contains the features you need. The bottom line appears to be that you need to move up the diagram for each of security, multiple protocols, or ATM or combinations of them that you need. The price also rises as you move up in the diagram.

## IP Base

"IP Base is a baseline set of Cisco IOS Software services required to operate a Cisco IOS Router in a data environment. It includes technologies such as DSL connectivity, Ethernet Switching modules, 802.1q routing, and trunking on Ethernet interfaces. IP Base will be the default image for most Cisco IOS Routers."

## IP Voice

IP Voice adds voice features, including support for VoIP or VoFR. It also includes support for all existing voice interfaces and signaling protocols such as H.323, MGCP Signaling. And it includes key Cisco capabilities such as Cisco IOS Telephony Services and Survivable Remote Site Telephony (SRST).

## Advanced Security

"Advanced Security combines Security and VPN with data connectivity. Additional functionality includes Cisco IOS Firewall, Intrusion Detection Systems (IDS), Secure Shell (SSHv1), and support for Cisco Easy VPN Client and Server. All encryption technologies (3DES and AES as applicable) will be provided in a single feature set."

## SP Services

"SP Services is a comprehensive set of data connectivity with voice encapsulation and transport services, in addition to SSHv1. It provides full support for Voice and data over IP and ATM. SP Services also provides NetFlow and IPv6. "

## Enterprise Base

"Enterprise Base integrates support for data connectivity, QoS features, and other routed and IBM services (i.e.: Appletalk, Novell, and IPX)."

## Advanced IP Services

"Advanced IP Services combines support for data and voice with Security and VPN capabilities. It supports all features and hardware supported in the SP Services feature set, and adds support for the VPN, IDS, and Cisco IOS Firewall services in the Advanced Security feature set."

## Enterprise Services

"Enterprise Services combines support for IPX, Apple Talk and IBM services with voice and/or ATM services. It supports all features and hardware supported in the SP Services feature set, and adds support for L3 routed protocols introduced in the Enterprise Base feature set. It fully meets the requirements of customers who wish to integrate full IBM support and voice services."

## Advanced Enterprise Services

"Advanced Enterprise Services merge support for all routed protocols (i.e.: Appletalk, Novell, IPX, and DECnet) with voice, security (i.e.: Cisco IOS Firewall and IDS), VPN, and other premium features (i.e.: IPv6, Netflow). It is the most premium and services rich feature set."

## Let's Talk Technical

This section is based on two Cisco documents:

- <http://www.cisco.com/warp/public/732/releases/release123/docs/techshowcase.ppt>
- <http://www.cisco.com/warp/public/732/releases/release123/docs/pb.pdf>

I'm going to try to summarize them for you in what space remains.

## AutoSecure

The idea of AutoSecure is "one touch device lockdown". The one command acts as a macro, causing the router to automatically configure itself with a wide variety of security features, implementing "best practices for router security". I'm sure you'll want to look into this as 12.3 matures. Things to be aware of: AutoSecure disables CDP and NTP. You can re-enable them. It also does introduce anti-spoofing source address access lists, which may need modification for your site. There's enough here that I may write a follow-on article about AutoSecure.

- Brief data sheet: <http://www.cisco.com/warp/public/732/Tech/security/docs/autosecure.pdf> .
- AutoSecure technical documentation: [http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123\\_1/ftatosec.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123_1/ftatosec.htm)

## Easy VPN Remote

Easy VPN Remote is server support for the Cisco VPN client (software and hardware). This is intended to make it easier to use the Cisco IPSec with any of the VPN gateways. The IPSec policy for the client is centrally managed, pushed to the client by the server. (Let's see, there's the VPN client product called Unity, there's also the unified email/vmail product already named Unity. Couldn't the folks at Cisco have chosen different names for the products, to reduce the confusion?).

## AES Support

Advanced Encryption Standard (AES) encryption support is available in software and selected hardware encryption.

## GLBP

Gateway Load Balancing Protocol (GLBP) is included in Cisco IOS 12.3. I've been thinking of GLBP as HSRP on steroids for WAN routers. I'm seeing more and more sites with dual WAN routers, even at remote offices (except for the smallest offices). It is highly desirable in most cases to use both WAN links out of a site -- you've already paid for them. You can do this with HSRP on some of the routers, by creating two virtual routers, and varying the default gateway on the PC's. GLBP is a simpler alternative, at least administratively.

With GLBP, the routers work together to assign each a different virtual MAC address, accompanying the IP address of the virtual router. When clients ARP for their default gateway, i.e. the virtual router's IP, one of the real routers responds with the appropriate MAC address. Different routers respond to different clients. Hence traffic is randomly distributed across the WAN links. Should a GLBP participating router fail, one of the other routers assumes responsibility for forwarding frames sent to the MAC address of the failed router, in addition to those sent to the router's own MAC. Like HSRP, GLBP allows tracking of WAN link status, so it can be smart about not using a router when the attached WAN link is down. Pretty nifty idea!

## Stateful NAT Failover

Stateful NAT works with HSRP so that NAT routers can track state and maintain services should one of the routers fail.

## CPE Nonstop Forwarding Awareness for CPE

The idea of Nonstop Forwarding (NSF) is to support dual Route Processor failover. When a routing neighbor sees a dual-RP router fail in a known way, it can continue to forward packets using old routing information. When the dual-RP failover brings up an active RP, it re-establishes adjacencies and exchanges routing information. Normally, the peers would detect the failure and flush routes. With NSF, some packets may be lost, but the time period until resumption of service may be much shorter.

Cisco IOS 12.3 adds support for NSF to EIGRP, BGP, OSPF, and IS-IS routing protocols.

## IPv6

Cisco has been adding IPv6 support and features for quite a while now. With Cisco IOS 12.3, Cisco is emphasizing the ability to put IPv6 services into production, and to use the various transition mechanisms, with broad-based support in widely deployable images.

## Multicast Subsecond Convergence

The claim is that new algorithms and processes reduce the time for IP multicast convergence by a factor of ten! This improves service availability for large multicast networks. Multicast paths are recovered almost immediately after unicast routing convergence.

## SRST

Survivable Remote Site Telephony has been in ED and LD images for a while now. SRST provides for continuing basic Cisco IP Phone services even if a remote CallManager becomes unreachable over the WAN. Lucent/Avaya and Nortel's approaches require a backup server (IP PBX) at each remote site instead. The attraction of SRST is that of having a centralized PBX with simpler hardware and maintenance costs, while having survivability at the remote sites.

## SIP

Cisco IOS Firewall supports SIP. SIP state awareness mitigates potential Denial of Service attacks.

## AutoQoS

AutoQoS is intended to provide initial VoIP QoS configuration of routers (and switches) via one or two commands. AutoQoS keys off interface bandwidth and "does the right thing". AutoQoS looks like a great way to get started on QoS and not have it slow down your initial VoIP deployment. You can later go back and tune the QoS configuration. With the Modular QoS CLI, you can easily and incrementally add QoS classes and new policy rules as to handle those classes of traffic.

See also my online note about AutoQoS, at <http://www.netcraftsmen.net/welcher/papers/autoqos01.htm> . This may become a full article someday. There is more information at the following URL's:

- [http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/autoq\\_pg.ppt](http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/autoq_pg.ppt)
- [http://cco-stage.cisco.com/warp/public/732/Tech/qos/docs/autoqos\\_wp.pdf](http://cco-stage.cisco.com/warp/public/732/Tech/qos/docs/autoqos_wp.pdf)

## Modular QoS CLI Enhancements

The short list of incremental enhancements:

- Frame Relay DLCI classification
- Three-level hierarchical policing and policies
- Enhanced set policies via table mapping, including simpler CoS to Precedence/DSCP mapping
- MQC class-based header compression, simpler classification of CRTP packets

## NetFlow Version 9

NetFlow has become popular for traffic accounting. Cisco has enhanced NetFlow to provide for new needs with an extensible template-based approach. NetFlow is being enhanced to support BGP next-hop and IP multicast, also to be MPLS aware. By the way, there is now more router based aggregation of NetFlow for TOS, Type of Service -- think QoS reporting! And Cisco is working with the IETF to standardize NetFlow to permit reporting across vendors.

For more information, see [http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/nflov\\_pg.ppt](http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/nflov_pg.ppt) . (Thanks, Marty!)

## SAA for FR and ATM

For those who have been reading my articles on network management, you already know SAA is Service Assurance Agent. SAA provides all sorts of round-trip delay and jitter statistics, which can be useful for troubleshooting and for QoS management.

My interpretation of this new feature: Cisco has teamed with Visual Networks to include reporting of the information gathered by Visual Networks probes into the Cisco IOS. So for the cost of a router IOS upgrade, you can get Layer 1 and 2 statistics on selected FR and ATM interfaces. Models supported include 1600, 1700, 2600, 3600, 7200, 3810.

I know the Visual Networks software and CSU/DSU probes are heavily used by Service Providers, and that many enterprises also like the reporting. This new features cuts costs, since now separate CSU/DSU probes need not be purchased. This new feature also may help Visual Networks sell software, since the hefty investment in probes is no longer required. And Cisco is marketing a relabeled version of the Visual Networks software as "WAPS", Cisco WAN Access Performance Management System. For more information, see <http://www.cisco.com/en/US/products/sw/netmgtsw/ps4884/index.html> .

## MPLS: VRF-Aware IPsec, AToM

VRF-Aware IPsec means that the Service Provider can easily map IPsec tunnels to MPLS VPN's, based on the IKE authentication. This means that IPsec VPDN's can terminate in the customer's MPLS VPN, so remote and mobile users can appear to be connected internally to the corporate customer network. This simplifies life and reduces costs for the Service Provider, since they can now do all this in their PE inside one box.

AToM is Anything Over MPLS. This feature allows MPLS "circuits" to be set up, transport Ethernet, FR, ATM, etc. over an MPLS network. This is initially mostly of interest to Service Providers. But I expect a certain amount of interest in Ethernet over MPLS among large enterprise/governmental networks running MPLS, since EoMPLS is a lot more manageable and scalable than trying to provide VLAN connectivity across a large core network.

For more about AToM including links, see <http://www.netcraftsmen.net/welcher/papers/mpls4.html> .

In addition, EoMPLS has the potential as I see it to reduce router counts. Designing flat Layer 2 bridged/switched networks at large scale alarms me. But having a point-point link terminating in a router interface doesn't alarm me. For example, perhaps district schools connect back to a local fiber hub site via FastEthernet over fiber. This could be over a managed MPLS network or over a county/state MPLS network. Each school is then connected from the local fiber hub site via EoMPLS to a VLAN on a central hub 6500. The school support staff then only has one or two central routers to maintain, the MSFC's in the central 6500 switches.

## Other Technical Features

We're out of space, so I'm going to have to refer you to the Product Bulletin listing all the technical features rolled up in Cisco IOS 12.3. The link is in the following table.

## Conclusion and Links

The following is where to go to start reading about Cisco IOS 12.3. Note that there are documents on AutoSecure and AutoQoS off the main page listed below. There are also links concerning SRST.

Cisco IOS 12.3 overall page	<a href="http://www.cisco.com/warp/public/732/releases/release123/major/">http://www.cisco.com/warp/public/732/releases/release123/major/</a>
Cisco IOS 12.3 technical presentation	<a href="http://www.cisco.com/warp/public/732/releases/release123/docs/techshowcase.ppt">http://www.cisco.com/warp/public/732/releases/release123/docs/techshowcase.ppt</a>
Cisco IOS 12.3 technical product bulletin	<a href="http://www.cisco.com/warp/public/732/releases/release123/docs/pb.pdf">http://www.cisco.com/warp/public/732/releases/release123/docs/pb.pdf</a>
Cisco IOS 12.3 packaging document	<a href="http://www.cisco.com/warp/public/732/releases/packaging/docs/pb.pdf">http://www.cisco.com/warp/public/732/releases/packaging/docs/pb.pdf</a>

I've posted several new seminars on my web page. See <http://www.netcraftsmen.net/welcher/seminars/index.htm> . The new seminars include IP Telephony Readiness, Introduction to IPsec VPN, Voice and Video Enabled IPsec VPN (V3PN), and High Availability Campus Design -- Best Practices. We're making an effort to post other company seminars at <http://www.netcraftsmen.net/Seminars.htm> . And we're working to try to bring the seminars to various locations, especially on the East Coast. Check our News link for any scheduled seminars.

At this point, I have no idea what next month will bring. I've got a bunch of interesting topics in mind. One is MPLS for large enterprise and government (Federal, state, county). Another is WLAN Security and/or WLAN Design. Something about Intrusion Detection Systems (IDS's) also seems like a good idea.

If you have ideas or suggestions for articles, please let me know! If you have an interesting network design or

troubleshooting case study that you don't mind exposing in public to some degree, by all means, please get in touch!

---

Dr. Peter J. Welcher (CCIE #1773, CCSI #94014, CCIP) is a Senior Consultant with Chesapeake NetCraftsmen. NetCraftsmen is a high-end consulting firm and Cisco Premier Partner dedicated to quality consulting and knowledge transfer. NetCraftsmen has eight CCIE's, with expertise including large network high-availability routing/switching and design, VoIP, QoS, MPLS, network management, security, IP multicast, and other areas. See <http://www.netcraftsmen.net> for more information about NetCraftsmen. Pete's links start at <http://www.netcraftsmen.net/welcher> . New articles will be posted under the Articles link. Questions, suggestions for articles, etc. can be sent to [pjw@netcraftsmen.net](mailto:pjw@netcraftsmen.net) .

6/3/2003

Copyright (C) 2003 Peter J. Welcher