



New Features in Cisco IOS 12.4

Peter J. Welcher

Introduction

I'm writing this in mid-August. Things have been hot (business, weather). That means its time for my more-or-less annual article about new features in Cisco IOS. I'm going to mainly cover Cisco IOS 12.4. The features in PIX 7.0 are also very interesting, but will have to be another whole article.

My intent here is to call attention to features I think are interesting, amazing, neat, or just plain useful. There is no way this article can be complete (hey, I do have a full-time job, despite what some of you think about consultants, that stuff about living a life of luxury?). So I'll refer the curious to the Cisco online documents for the entire set of new features.

About Release 12.4

The mainline or non-T release accumulates features in the 12.3 T and "letter" releases. New features will be added to the 12.4 T train of releases, whereas 12.4 mainline is for bug fixes. Thus new features for the 12.4 mainline code is really describing features added at some point in 12.3, ones that may be approaching the maturity required for production use. Note that I am not implying you should be running 12.4 code in production yet, just anticipating that you will probably be doing so at some point, after more of the bugs are fixed. I do have a customer already running 12.4 code in production -- due to a need for hardware support. Most sites will probably wait a while.

The cumulative new features list can be found at http://www.cisco.com/en/US/products/ps6350/prod_release_notes_list.html as a Release Note. Or off the <http://www.cisco.com/go/ios> page, aka <http://www.cisco.com/warp/public/732/>. If you click on "Cisco IOS Software Major Release 12.4" you'll see links to the new features Bulletin.

New Features Rolled into 12.4 Mainline

The Bulletin at http://www.cisco.com/en/US/products/ps6350/prod_bulletin09186a0080457b39.html provides the info about new features rolled up into 12.4. The following attempts to summarize and call attention to items that have caught my eye. To find the details that were necessarily omitted below, consult this document!

The 12.4 new features document lists the following broad areas of new features:

- 1 Hardware support
- 1 Broadband
- 1 High availability
- 1 Infrastructure
- 1 IP Mobility
- 1 IP Multicast
- 1 IP Routing
- 1 IP Services
- 1 IPv6
- 1 Management Instrumentation
- 1 MPLS
- 1 QoS

- 1 Security and VPN
- 1 Voice

Let's take a look at some of the new features in these categories.

The list of new **hardware support** accumulated into 12.4 is impressive. It includes NAM for modular routers, the new ISR routers, Cisco Unity Express, IDS Network Module. The engineers have stayed busy!

Broadband encompasses DSL aggregation features, ties to MPLS, enhanced dial-like features, that sort of thing. Interesting but a bit specialized?

High availability is two features: Cisco IOS Warm Upgrade, Cisco IOS IPsec stateful Failover. In Warm Upgrade, you decompress and load IOS to memory, greatly speeding the boot process in switching over. The new image need not be burned to flash to do this. You do need sufficient RAM to decompress the new image.

Infrastructure is two items: Cisco IOS Embedded Event Manager 2.1, and Embedded Resource Manager (ERM). The former is the surrounding framework for TCL in IOS. See also my previous article <http://www.netcraftsmen.net/welcher/papers/iostcl01.html>. The idea is to detect events and then trigger local actions within the router, namely any CLI command(s). ERM allows monitoring of internal resources, plus the "ability to perform actions to improve performance and availability of the device", and "yields information to allow better understanding of scalability requirements" (resource consumption). They even say those IBM words, "autonomic computing".

IP Mobility: support for Mobile IP through NAT (RFC 3519), some other Mobile IP enhancements, and Dynamic Security Associations and Key Distribution (i.e. Mobile IP SA's no longer have to be statically configured in advance).

IP Multicast includes some IPv6 multicast features, MSDP enhancements per IETF MSDP Draft 20, and PIM Dense Mode Fallback Prevention after RP Loss. I'll skip over IPv6 as not being of general interest (with apologies to those in DoD or government agencies). The PIM-DM Fallback Prevention feature I like, since my feeling for quite a while has been that one should engineer multicast to avoid PIM-DM even with RP loss. RP-of-last-resort and other techniques have allowed this for a while, but it will be nice as a safety measure to be able to tell the router to never revert to Dense Mode.

One would expect **IP Routing** to be an area with many new features. One minor goodie is that routemap display via show commands now includes more ACL details.

Optimized Edge Routing (OER) is an interesting new feature that may be the subject of a future whole article in itself. OER is technology for determining best outbound route, usually when one has two or more ISP's. It is based on NetFlow and SAA. OER can dynamically detect path failures at the WAN edge. "... Cisco OER is unique in that it can make instant routing adjustments based on criteria other than static routing metrics: response time, packet loss, path availability, traffic load distribution, and financial cost minimization policies."

The newest features added to OER are (monetary) cost optimization and traceroute reporting. Another new OER feature is support for policy-rules configuration, whereby you can configure policies and then switch between them. Yet another: support for prefix learning based on protocol ports of interest.

For the details of OER (at least until I write that future article), see:

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a008046460e.html

Policy Based Routing now supports a recursive next hop, i.e. one that is not directly connected. That makes it much easier to deploy consistent PBR across multiple routers, without creating a routing loop.

IGMPv3 Host Stack means the router can now act like a host, also do Source Specific Multicast. This helps with Music on Hold, also multicast troubleshooting.

There are routing protocol protections, to prevent Denial of Service via routing protocol (accidental or deliberate). EIGRP has configurable prefix limits and OSPF has database overload protection, to protect against exhausting CPU or memory. You can similarly limit mroute state per-interface. This prevents for example home users from creating a multicast-based Denial of Service situation, for example.

Historically, OSPF was enabled on interfaces using the network command in router mode. OSPF can now be enabled on interfaces in interface mode, for consistency with OSPFv3.

There are a number of other routing enhancements I won't list here (minor or more specialized).

The category **IP Services** encompasses a variety of items. Among these: DHCP and NAT features, many for VRF and MPLS VPN support.

The feature titled "First Hop Routing Protocols—Object Tracking List Support" allows you to use object tracking to trigger HSRP, VRRP, or GLBP failover. But not just for single objects, but tracking a list of things. Boolean operations, thresholds, and weighting can also be applied for complex failover logic. See my "The Missing Link" article for an explanation of single object tracking. It is at <http://www.netcraftsmen.net/welcher/papers/missinglink.html>.

"Rate Based Satellite Control Protocol (RBSCP)" provides optimizations for satellite links, intended to replace Performance Enhancing Proxies (PEPs) and some related problems.

IP Access Lists now support filtering on IP Options if you wish. You can choose to drop selected packets, or any packets that use IP Options. You can now also filter on TCP flags.

There are a large number of new features relating to **IPv6** and **MPLS**, not necessarily grouped into those sections. As I consider these somewhat specialized, I'm not going to list them here. I will note that SNMP with IPv6 transport is among the new features.

Under **Management Instrumentation** are a number of new SNMP MIBs, as one might expect. One new feature is locking of configuration sessions, preventing others from changes during the lock. Another is fine-grained control over which subsystems can be configured via HTTP.

The feature "Bandwidth Estimation via Corvil Technology" is rather intriguing to me, as a practitioner of QoS. This is patented technology you license for selected routers. You then configure SLAs for desired packet loss and delay bounds or characteristics, on a per-class basis. The QoS command "show policy interface" then displays recommended bandwidth levels. The Corvil management software (or other applications) can pull in this info via the updated CBQoS MIB, to recommend QoS class bandwidth levels and link bandwidth. The claim is this takes into account the bursty nature of applications. For the data sheet, see http://www.cisco.com/en/US/tech/tk543/tk759/tech_brief0900aecd8024d5ff.html.

The new name for SAA is "IP Service Level Agreements" or "IP SLA". The bottom line is, this whole area seems to be getting a lot of emphasis lately. The IP SLA capabilities now support measuring VoIP Call Setup and VoIP Gateway delay. One way synthetic voice measurements are now available, as well MOS calculation. The CLI is being migrated to a new simpler set of commands, while retaining support for the older rtr commands. The accuracy has been improved from one millisecond to one-tenth of a millisecond. More efficient time stamping adds to greater accuracy of measurements. A feature called "SAA Multiple Operation Scheduling" allows you to easily set up and schedule performance measurements to a group of destinations from a source router, one SNMP set or CLI command.

Egress NetFlow provides tracking of packets as they leave (e.g. after QoS or NAT changes). It can be used with IP and MPLS.

NetFlow information (and configuration) is now accessible via an SNMP MIB. This includes a Top N Talkers and Conversations facility, also supported with a show command.

Configuration Rollback/Replace is a big deal! It allows you to send out a full configuration. The router then generates differences, which can be viewed, and applies them to its running state. This allows you to revert to a "last known good" configuration. The "Contextual Configuration Diff Utility" allows you to do diff comparisons of any two config files, e.g. in flash or any Cisco file system. These features are aware of order-sensitive commands as well!

Embedded Syslog Manager (ESM) allows correlation, augmentation, filtering, and routing of syslog messages. You can customize messages, send certain messages to a specific syslog receiver, correlate events within one device to limit event storms, and send SMTP notifications from the Cisco IOS device.

Several interesting new features are listed under the heading **QoS**. As noted above, the Corvil feature is instrumentation useful for QoS. Several of the QoS features refine AutoQoS. The "show auto discovery qos" displays the recommended autoqos configuration that "auto qos" would apply. "AutoQoS for the Enterprise" records statistics for observed traffic using NBAR, then generates a recommended QoS configuration from that. This feature only works on PPP, Frame Relay, and ATM WAN interfaces. For more info, see the following URL: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_feature_guide09186a00802000a7.html

NBAR is now enhanced to detect HTTP on ports other than 80 ("NBAR Extended Inspection for HTTP Traffic"). The feature "NBAR User-Defined Custom Application Classification" now allows you to define your own match criteria, based on string or byte at specific offset within the packet payload. Source and destination ports or ranges of ports can also be used. You can define more than 30 custom application classifications this way. Finally, turbo ACL's can be used on the 7200 to enhance performance where turbo ACL's and QoS are both in use.

The **Security and VPN** category of new IOS features is large enough I'll have to leave it for another article. It contains 62 new features!

The **Voice** category of new features includes only Call Manager Express (a big inclusion). Consider however that a large number of the other features discussed above or bypassed also relate to voice.

Switches: L2 Traceroute

I hadn't noticed this switch feature until somebody mentioned it in passing. I mention it here since you may not have noticed it either.

Layer 2 traceroute works within a VLAN to show the switches and ports used to reach the destination device (MAC address). The command is "traceroute mac" or "traceroute mac ip".

Layer 2 traceroute has been around for a while! Layer 2 traceroute is in release 12.2(18) SXE for the 6500, CatOS 6.2.1 for the 4000, 12.1(13) EW for Cat4500 SupIII/IV, and 12.1(14)EA1 for Catalyst 3750, 3550, 2970, 2955, 2950, and 2950-LRE. For details, see one of the following.

- 1 http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a00804357b3.html
- 1 http://www.cisco.com/en/US/products/hw/switches/ps663/prod_bulletin09186a008008886f.html
- 1 http://www.cisco.com/en/US/products/hw/switches/ps4916/prod_bulletin09186a00801a759a.html

Even Newer New Features

Going to the "old" documentation, I found the New Features page where it traditionally has been. See http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124_x/index.htm. Listed there:

- 1 Support for two hardware modules
- 1 L2TP IPsec Support for NAT/PAT Windows Clients
- 1 MPLS LDP (default is now LDP not TDP)
- 1 NBAR (all platforms)
- 1 Scalability for Stateful NAT (holds HSRP changeover until state information is fully exchanged)

These are also the "Feature Guides" on the TAC documentation pages at http://www.cisco.com/en/US/products/ps6350/products_feature_guides_list.html. They represent features added in 12.4(1) and (3).

For the adventurous, new features in the 12.4 T trains can be found at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t2/index.htm>. Or as "Feature Guides" in the new documentation pages for 12.4 T.

Summary

I hope this article has been useful, if for no other reason than to remind you that it's time once again to look at all the features the Cisco engineers have put into the Cisco IOS. We did skip some of the "gap-filling" features that were necessary but not so exciting, at least not until the day you need them.

I plan to write an article about QoS in the 7600, since I've recently spent some time clarifying bits and pieces of the documentation, with some help from various folks.

Your comments, questions, and suggestions for future articles are of course welcome! See below to decipher my email

address.

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 ten CCIE's, with expertise including large network high-availability routing/switching and design, VoIP, QoS, MPLS, IPSec VPN, wireless LAN and bridging, 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 <at> netcraftsmen <dot> net](mailto:pjw@netcraftsmen.net) (formatted this way to fool email harvesting software).

8/15/2005

Copyright (C) 2005 Peter J. Welcher