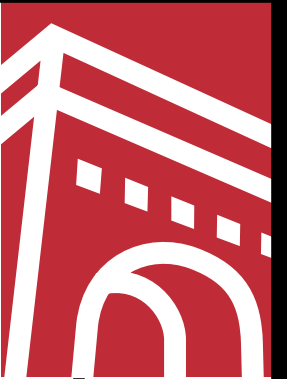


Cisco IOS X-Release 12.2DX



This Product Bulletin describes the content and delivery information concerning Cisco IOS™ software release 12.2DX. It should be used in conjunction with Product Bulletin titled, Cisco IOS Software Release 12.2T. 12.2DX is a short lived Early Deployment (ED) release parented to 12.2(1)DD and supporting Cisco 7200 and 7400 Series platforms. This release contains all new features delivered in 12.2T and 12.2DD up to 12.2(1)T and 12.2(1)DD respectively.

The platform and features delivered in 12.2DX will be immediately incorporated into Cisco IOS 12.2(1)DD and subsequent Cisco IOS 12.2DD releases.

New Features in Cisco IOS Release 12.2(1)DX

The following features will be delivered in the initial release of 12.2(1)DX.

Table 1 Cisco IOS Release 12.2(1)DX New Features

Feature	7200	7200 VXR	7400
7401ASR	No	No	Yes
PA-2FE	Yes	Yes	Yes
PA-8PRI	No	Yes	Yes
Per VRF AAA	Yes	Yes	Yes
PPPoE over Gigabit	Yes	Yes	Yes
PPPoE Session Limit	Yes	Yes	Yes
Quality of Service Features for Parallel Express Forwarding (PXF)	No	Yes	Yes
RADIUS Attribute Screening	Yes	Yes	Yes
Virtual Private Dial-up Network Extended Fail-over Conditions	Yes	Yes	Yes
VPDN Group Session Limiting	Yes	Yes	Yes



Please see the next section for documents that address details on these new features. Any ED release of software should be utilized first in a test network before being deployed in a production network.

New Hardware Features in Cisco IOS Release 12.2(1)DX

The following new hardware features are supported by the Cisco 7200 and 7400 Series platforms for Cisco IOS Release 12.2(1)DX:

Cisco 7400

The Cisco 7400 delivers exceptional price/performance to meet the requirements of both enterprise and service providers. With its combination of scalable performance, density, and low per-port pricing, the Cisco 7400 allows network-layer capabilities to be extended to a much wider range of network configurations and environments. Customers can now gain the advantages of high-performance network-layer switching and services, including security, QoS, and traffic management to more locations throughout the network.

- Form Factor (Stackable 1 rack unit, low power (under 50W), front to back airflow)
- Hardware accelerated network application service with PXF processing
- Cost effective GE to GE Layer 2- 7 network services
- Ideal new world CPE with full MPLS and MPLS VPN support
- Flexible WAN connectivity with over 40 interfaces
- (Serial, Channelized, ISDN, Frame, ATM, IP, 64K to OC3)

The Cisco 7400 delivers the full suite of Cisco IOS software services for managing network security, allocating QoS among applications or users, and providing value-added services such as NetFlow accounting and encryption. QoS applications such as committed access rate (CAR), Weighted Random Early Detection (WRED), and Weighted Fair Queuing (WFQ) can be flexibly applied to provide precedence across IP addresses, applications, or specific users with a high level of granularity.

The Cisco 7400 offers scalable density with a very wide range of interfaces including:

- Ethernet, Fast Ethernet, and Gigabit Ethernet
- Serial and Multi-channel
- OC3 POS, OC3 ATM
- SDN Primary Rate Interface (PRI), Basic Rate Interface (BRI), High-Speed Serial Interface (HSSI), packet over T3/E3, multichannel T1/E1/T3, and ATM

The Cisco 7400 uses the same port adapters as the Cisco 7200 Versatile Interface Processor (VIP), thus protecting customer investment in interfaces and simplifying sparing.

The Cisco 7400 sets new standards in price/performance/ rack density, meeting requirements for high-performance Layer 3 services at an affordable price. The NSE-1 engine powers the Cisco 7400. Network Services Engine (NSE-1) takes advantage of parallel processing in order to offer unprecedented price/performance. NSE-1 delivers wire rate OC3 throughput while running concurrent high-touch WAN edge services. It is the first Cisco processing engine to offer integrated hardware acceleration increasing Cisco 7400 system performance by 50-300% for combined "high touch" edge services. NSE-1 takes advantage of a new technology called Parallel eXpress Forwarding (PXF).

For more information on PXF processing on the Cisco 7400 Series, refer to <http://www.cisco.com/warp/public/cc/pd/ifaa/prossor/nse1/>



PA-2FE

The PA-2FE provides two 10/100-Mbps, 10/100BaseT Fast Ethernet/Inter-Switch Link (ISL) interfaces and supports both full-duplex and half-duplex operation. The PA-2FE comes in two models, the PA-2FE-TX and the PA-2FE-FX).

Each Fast Ethernet port on the PA-2FE-TX has an RJ-45 connector to attach to Category 5 unshielded twisted-pair (UTP) cable for 100BaseTX. Each Fast Ethernet port on the PA-2FE-FX has an SC-type fiber-optic connector for 100BaseFX.

PA-8PRI

The multichannel E1/PRI port adapters (PA-MC-2E1 and PA-MC-8E1) integrate data service unit (DSU) functionality and E1 channel support into the Cisco router. The PA-MC-2E1 or PA-MC-8E1 port adapter provides two or eight independent E1 (120-ohm) connections via RJ-48C connectors. (See Figure 1-1 and Figure 1-2.) The PA-MC-8E1 port adapter can provide up to 128 separate full-duplex High-Level Data Link Control (HDLC) channelized E1, fractional E1, full E1, or unframed E1 interfaces and the PA-MC-2E1 port adapter can provide up to 62 separate full-duplex HDLC channelized E1, fractional E1, full E1, or unframed E1 interfaces.

New Software Features in Cisco IOS Release 12.2(1)DX

The following new software features are supported by the Cisco 7200 and 7400 Series platform for Cisco IOS Release 12.2(1)DX.

Per VRF AAA

Using the Per VRF AAA feature Internet Service Providers (ISPs) can partition authentication, authorization, and accounting (AAA) services based on Virtual Route Forwarding (VRF). This permits the Virtual Home Gateway (VHG) to communicate directly with the customer RADIUS server associated with the customer VPN, without having to go through a RADIUS proxy. Thus, ISPs can scale their VPN offerings more efficiently because they no longer need to proxy AAA to provide their customers the flexibility demanded.

To support per VRF AAA, AAA must be VRF aware. ISPs must be able to define multiple instances of the same operational parameters—such as AAA server groups, method lists, system accounting, and protocol specific parameters—and secure the parameters to the VRF partitions.

If an AAA configuration, such as a method list, is uniquely defined many times across the network access server (NAS), the specification of the AAA server, which is based on IP addresses and port numbers, may create an overlapping of private addresses between VRFs. Securing AAA method lists to a VRF can be accomplished from one or more of the following sources:

Virtual Template—used as a generic interface configuration

Service Provider AAA server—used to associate a remote user with a specific VPN based on the domain name or DNS. The server then provides the VPN-specific configuration for the virtual access interface, which includes the IP address and port number of the customer's AAA server.

Customer VPN AAA server—used to authenticate the remote user and to provide user-specific configurations for the virtual access interface.

Global AAA accounting configurations and some AAA protocol-specific parameters cannot be logically grouped under the Virtual Template configuration.



PPPoE over Gigabit Ethernet

The PPPoE over Gigabit Ethernet feature enhances PPP over Ethernet (PPPoE) functionality by adding support for PPPoE and PPPoE over IEEE 802.1Q VLANs on Gigabit Ethernet interfaces. The PPPoE over Gigabit Ethernet feature is supported on Cisco 7200 series routers with Gigabit Ethernet line cards.

PPPoE Session Limit

The PPPoE Session Limit feature enables you to limit the number of PPPoE sessions that can be created on a router or on an ATM PVC, PVC range, or VC class.

Before the introduction of this feature, there was no way to limit the number of PPPoE sessions that could be created on a router. Not having a limit was potentially a problem because it was possible that the router could create so many PPPoE sessions that it would run out of memory.

To prevent the router from using too much memory for virtual access, the PPPoE Session Limit feature introduces a new command and a modification to an existing command that enable you to specify the maximum number of PPPoE sessions that can be created. The new `pppoe limit max-sessions` command limits the number of PPPoE sessions that can be created on the router. The modified `pppoe max-sessions` command limits the number of PPPoE sessions that can be created on an ATM PVC, PVC range, VC class, or Ethernet subinterface.

Quality of Service Features for Parallel Express Forwarding (PXF)

The Modular Quality of Service Command-Line Interface (Modular QoS CLI) and many of the associated class-based QoS features are now available on PXF.

The following class-based QoS features are being introduced for PXF:

- Traffic Policing —the `police` command in policy map class configuration mode.
- Class-Based Weighted Fair Queueing (CBWFQ) —the `bandwidth` and `fair-queue` commands in policy map class configuration mode.
- Low Latency Queueing (LLQ) —the `priority` command used in policy map class configuration mode.
- Class-Based Weighted Random Early Detection (CBWRED) and Differentiated Services- Compliant Weighted Random Early Detection (DiffServ-Compliant WRED)—the `random-detect` command used simultaneously with the `bandwidth` command in policy map class configuration mode.
- Flow-Based Weighted Random Early Detection—the `random-detect` command used simultaneously with the `bandwidth` command in policy map class configuration mode.
- Class-Based Marking —the `set` command used in policy map class configuration mode. Class-Based Marking support is limited to 32 traffic classes per traffic policy, and the QoS group marking (`set qos-group`) is not supported.

The Committed Access Rate (CAR) feature configured to use an access list with rate-limiting policies (the `access-list rate-limit` command in interface configuration mode) is also now available on PXF. If you wish to rate-limit traffic without using an ACL, use the Modular QoS CLI to configure the Traffic Policing feature.

Because of the addition of the Modular QoS CLI, traditional WRED (the `random-detect` command in interface configuration mode) and Fair Queueing (the `fair-queue` command in interface configuration mode) are no longer configurable. If you would like to configure WRED or Fair Queueing, you can use the Modular QoS CLI to configure Class-Based WRED or Class-Based Weighted Fair Queueing on a per-class rather than a per-interface basis.



The Modular QoS CLI on PXF does not currently support the following match criteria that are available on other Modular QoS CLI-supported platforms:

- Destination address
- Input Interface
- Internet Protocol (IP) values
- Multi Protocol Label Switching (MPLS) values
- Protocol
- Quality of Service (QoS) group values
- Source address

For additional information on the Modular QoS CLI, see the Modular Quality of Service Command-Line Interface doc.

RADIUS Attribute Screening

The RADIUS Attribute Screening feature allows users to configure a list of "accept" or "reject" RADIUS attributes on the network access server (NAS) for purposes such as authorization or accounting.

If a NAS accepts and processes all RADIUS attributes received in an Access-Accept packet, unwanted attributes may be processed, creating a problem for wholesale providers who do not control their customers' authentication, authorization, and accounting (AAA) servers. For example, there may be attributes that specify services to which the customer has not subscribed, or there may be attributes that may degrade service for other wholesale dial users. The ability to configure the NAS to restrict the use of specific attributes has therefore become a requirement for many users.

The RADIUS Attribute Screening feature should be implemented in one of the following ways:

- To allow the NAS to accept and process all standard RADIUS attributes for a particular purpose, except for those on a configured reject list
- To allow the NAS to reject (filter out) all standard RADIUS attributes for a particular purpose, except for those on a configured accept list

Virtual Private Dial-up Network Extended Fail-over Conditions

The Virtual Private Dial-up Network (VPDN) failover has been extended to occur in instances where the receiving node sends an error message to the transmitting node. Before this feature, the failover mechanism would only occur when the transmitting node did not receive a response from the receiving node.

This feature occurs automatically when failover is configured, so this feature has no new command. Failover is configured in the VPDN group by using the `initiate-to` command.

VPDN Group Session Limiting

Before the introduction of the VPDN Group Session Limiting feature, you could only globally limit the number of VPDN sessions on a router with limits applied equally to all VPDN groups. Using the VPDN Group session limiting feature, you can limit the number of VPDN sessions allowed per VPDN group. This feature is implemented with the introduction of the `session-limit` number command in VPDN configuration mode. VPDN group session limiting is applied after the global VPDN session limiting (which is configured via the `vpdn session-limit` session command in configuration mode) is enforced.

Product Numbers

Table 2 Cisco IOS 12.2(1)DX Feature Sets, Images, and Memory Recommendations

Platform	Software Feature Set	Product Code	Image	Flash	DRAM
Cisco 7200 Series	Enterprise	S72A-12201DX	c7200-js-mz	16 MB	128 MB
Cisco 7400 Series	Enterprise	S74A-12201DX	c7400-js-mz	16 MB	128 MB

Download Information

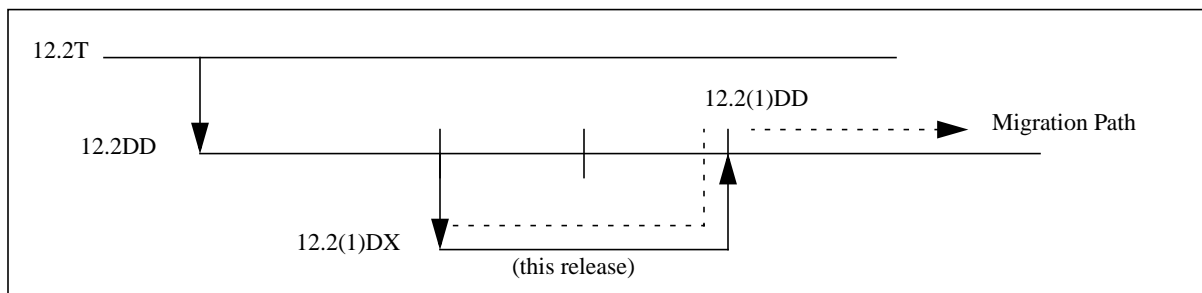
Customers can download Cisco IOS Release 12.2(1)DX software from Cisco Connection Online (CCO) in the Software Image Library.

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

Migration Path

It is important to note that there are no planned maintenance releases for 12.2DX. In addition, please note the migration path to the latest DD release. Customers should prepare to upgrade using this migration path.

Diagram 1: Cisco IOS Release 12.2(1)DX Release Train and Migration Guide





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 Europe
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
www.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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 Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco.com 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

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement. Printed in the USA. AccessPath, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco Net *Works* logo, the Cisco Powered Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Discover All That's Possible, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, PIX, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Voice LAN, Wavelength Router, WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or 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. (0101R)