

Cisco IOS Software Release 12.0

New Features Overview

This product bulletin describes the new features and functionality introduced in Cisco IOS[®] software Release 12.0. Cisco IOS 12.0 will become a General Deployment release (refer to Product Bulletin 537 for information on the types of IOS releases) and as such, the major emphasis has focused on delivering the very highest quality, stable software platform. Therefore, IOS 12.0 has concentrated more on integrating previous, time-proven Early Deployment releases (such as IOS 11.3T, 11.CT, 11.1CC, 11.1CA) rather than the delivery of new leading-edge functionality. Product feature information on these releases has been included below in this 12.0 Product Bulletin. Customers requiring the latest IOS services should consider the parallel IOS 12.0T (technology) release which represents those capabilities inherent to IOS 12.0 as well as the latest features and functionality.

Quality of Service

Committed Access Rate

Description

The committed access rate (CAR) feature performs both packet classification and bandwidth management functionality. The packet classification features let users partition network traffic into multiple priority levels or classes of service (CoSs). The operator can then use the other QoS features to assign appropriate traffic handling policies, including congestion management, bandwidth allocation, and delay bounds for each traffic class.

Packets are classified based on policies specified by the network operator, including those concerning physical port, IP address, application port, IP protocol type, or other criteria specifiable by access lists or extended access lists. Packets can also be classified by external sources (for example, by a customer or by a downstream network provider) and have the classification either accepted by the network or overridden and reclassified according to a specified policy.

The bandwidth management or rate limiting functionality of CAR lets the network operator define aggregate or granular rate limits. The network operator can also specify traffic-handling policies when the traffic either conforms to or exceeds the specified rate limits.

Benefits

Committed access rate will enable customers to deploy and operate large-scale IP networks, that efficiently handle both bandwidth-hungry multimedia/Web and business-critical applications. It allows application-based rate limiting, subrate IP services, and exchange-point traffic control.

Considerations

CAR and dCAR (distributed CAR, available in VIB-based platforms) can be used only with IP traffic. Non-IP traffic is not rate-limited. CAR or dCAR can be configured on an interface or subinterface. However, CAR and dCAR are not supported on the following:

- Fast EtherChannel[®] interfaces
- Tunnel interfaces
- Primary Rate Interfaces (PRIs)
- Any interface that does not support Cisco Express Forwarding (dCEF)

Platform

This feature is supported across Cisco IOS-based: C2600, C36x0, C4x00, RSM 5000 and C7x00 platforms. dCAR is available in VIP (VIP 2-20 and later)-based platforms.

IOS Product Marketing contact: Sanjay Kalra

Weighted Random Early Detection

Description

The Random Early Detection (RED) and Weighted Random Early Detection (wRED) features provide network operators with powerful congestion-control capabilities designed to provide preferential treatment for premium-class traffic under congestion situations while concurrently maximizing network throughput and capacity utilization and minimizing packet loss and delay.

Current router and switch behavior allows output buffers to fill during periods of congestion followed by tail drop—a potentially large number of packets from numerous TCP connections are discarded because of oversubscription. This behavior can lead to global synchronization.

RED handles this situation by providing congestion avoidance—instead of waiting for buffers to fill and incurring the tail-drop situation, the router monitors the buffer depth and performs early discards on selected packets (and selected connections) to avoid dropping large numbers of packets because of full buffers.

Thus, RED works with TCP to increase aggregate network throughput via carefully managed packet discard. Cisco has extended RED to multiclass Internets with wRED, which specifies a RED policy per traffic class based on IP Precedence. Premium traffic receives preferential treatment during congestion situations as standard traffic is discarded earlier and, potentially, more aggressively.

Benefits

wRED is a congestion avoidance mechanism and is useful especially in high-speed transit networks.

Platforms/Considerations

In order to use Distributed wRED (dwRED), Distributed Cisco Express Forwarding (dCEF) switching must be enabled on the interface. wRED is available all IOS-based platforms. dwRED is available in VIP (VIP 2-20 and later)-based platforms.

IOS Product Marketing contact: Sanjay Kalra


QoS Policy Propagation via BGP

Description

The QoS policy propagation via Border Gateway Protocol (BGP) feature allows you to classify packets based on access lists, BGP community lists, and BGP autonomous system (AS) paths. The supported classification policies include IP Precedence setting and the ability to tag the packet with a QoS class identifier (QoS group ID) internal to the router. After a packet has been classified, you can use other QoS features such as CAR and wRED to specify and enforce business policies to fit your business model.

Benefits

Network operators don't have to provision, deploy, and update complex access lists at numerous routers while they benefit from offering value-added premium services.



Considerations

For the QoS policy propagation via BGP feature to work, you must enable BGP and dCEF/dCEF on the router.

Platform

This feature is supported across the Cisco IOS-based C1700, C2x00, C3x00, C4x00, RSM 5000, C7x00 and C12000 platforms.

IOS Product Marketing contact: Sanjay Kalra

Distributed Weighted Fair Queueing

Description

Distributed Weighted Fair Queueing (dWFQ), is a special high-speed version of WFQ. dWFQ has two forms:

- *Flow-based dWFQ*—With flow-based WFQ, packets are classified by flow. Packets with the same source IP address, destination IP address, source TCP or User Datagram Protocol (UDP) ports, destination TCP or UDP port, protocol, and type of service (ToS) field belong to the same flow.

Each flow corresponds to a separate output queue. When a packet is assigned to a flow, it is placed in the queue for that flow. During periods of congestion, WFQ allocates an equal share of the bandwidth to each active queue. Flow-based dWFQ is also called Fair Queueing (FQ) because all flows are equally weighted.

- *Class-based dWFQ*—In class-based dWFQ, packets are assigned to different queues based on their QoS group or the IP Precedence in the ToS field. QoS groups allow you to customize your QoS policy. A QoS group is an internal classification of packets used by the router to determine how certain QoS features, such as WFQ and CAR, treat packets. Use a CAR policy or QoS policy propagation via BGP to assign packets to QoS groups. If you want to classify packets based only on the two low-order IP Precedence bits, use ToS-based dWFQ.

Benefits

dWFQ provides bandwidth allocations and delay bounds to specified IP traffic sources by segregating the traffic into flows or classes and then providing non-first-in, first-out (FIFO) service to the various queues according to their assigned weights.

Considerations

In order to use dWFQ, dCEF switching must be enabled on the interface.

Platform

dWFQ is available on VIP (VIP 2-20 and later)-based platforms.

IOS Product Marketing Contact

Sanjay Kalra

GRE Precedence

Description

This IOS feature integrates IP based Virtual Private Networking (VPN) technology with Layer 3 Quality-of-Service techniques.

VPNs implemented via Generic Route Encapsulation (GRE) tunneling enable overlay topologies to be defined across a common backbone network such as the Internet. This typically allows Enterprises to cost-effectively and securely communicate with other member sites as shown:

And since traffic between sites is fully encapsulated, this VPN mechanism allows Enterprises the flexibility to use registered or unregistered IP addressing ranges for traffic transiting the backbone. GRE is defined in RFC1701 and RFC1702.

However in order to ensure that business critical traffic is expedited or that real-time applications receive predictable performance across the common backbone, QoS is required and in large network environments this is best delivered at Layer 3 via an enhanced IP transport since it inherently provides an end-2-end service and can be configured to differentiate between the needs of different applications and/or users. Cisco's comprehensive IOS Quality-of-Service architecture encompasses prioritized switching, smart queuing, traffic shaping and sophisticated congestion management. These mechanisms are influenced via the "IP Precedence" values associated with the Type-of-Service field in the IP header:

Therefore in order to have the QoS benefits apply to traffic flows transported across a GRE VPN tunnel the IOS now also carries the IP Precedence associated with received traffic flows in the GRE encapsulation. Optionally, the IOS router initiating the tunnel can classify ingress traffic and set the appropriate Precedence value to drive upstream QoS mechanisms as shown:

And setting the Precedence bits can be achieved via complementary IOS functionality such as Policy Routing, Committed Access Rate or BGP Policy Propagation.

Benefits

Leverages existing IOS Quality-of-Service technology, e.g. Committed Access Rate, Weighted Fair Queuing, Policy Routing, Weighted Random Early Detection etc.

- IP addressing flexibility with Layer3 GRE VPNs.
- Security—IOS Network Layer Encryption can be used in conjunction with GRE Precedence to provide data confidentiality between VPN tunnel endpoints.
- QoS Policy granularity, e.g. per network, per user, per application etc.
- Deployment flexibility, i.e. applicable at Enterprise CPE or Service Provider ingress point.

Platforms/Considerations

GRE Precedence is available across the Cisco IOS-based C1600, C1700, C2500, C2600, C3600, C4x000, AS5x00, RSM 5000, C7x00 and C8500 platforms.

Product Marketing Contact

Martin McNealis

LightStream 1010 FC-PFQ

Description

The LightStream 1010 per-flow queuing feature card, Private Network-Network Interface (PNNI) hierarchy, signaling features, ATM tag switching router.

Benefits

Per flow queuing is critical to the LightStream 1010 from a fairness and represents a valuable competitive advantage over other ATM switches. PNNI hierarchy is critical from the scalability of the LightStream 1010 networks, given that some customers already have about 100 node networks. Other features, (for example, ATM soft restart, permanent virtual circuit [PVC] accounting, E.164 autoconversion, closed user groups, and so on) have been requested by specific customers.

Product Marketing Contact: David Benham

IP and Routing

Multiprotocol over ATM

Description

Multiprotocol over ATM (MPOA) over Ethernet LAN Emulation (LANE user-networks interface [UNI] v2.0) on the Catalyst® 5000/5500 switches, Cisco 7500/7200, and Cisco 4500/4700 routers. Specifically, the Catalyst 5000/5500 will support the MPOA client (MPC) function and the Catalyst 5000/5500 route switch module (RSM), Cisco 7500/7200, and Cisco 4500/4700 routers support the MPOA server (MPS) function.

Benefits

MPOA is an extension to LANE that allows LANE clients to forward unicast packets between subnets to other LANE clients. Thus, MPOA allows LANE clients to perform internetwork layer forwarding and establish direct communications without requiring that the LANE edge devices be full functioning routers, all while utilizing installed Cisco routers for scalability and redundancy of the MPS function via Cisco's Hot Standby Router Protocol (HSRP) and providing backward compatibility with LANE only clients and Cisco's Single Server Redundancy Protocol (SSRP) provide standards-based LANE services redundancy.

Platforms/Considerations

MPOA is supported on Cisco 4x00, 72xx, 75xx routers and Catalyst route switch module (RSM) and ATM uplink modules.

Product Marketing
Contact: David Benham

NHRP Enhancements

Description

This feature builds on the IOS support for the Next Hop Resolution Protocol (NHRP) by adding the ability to set thresholds on the setup and teardown of dynamic switched virtual circuits. In addition it enables the Cisco IOS platform to function only as an NHRP server.

Benefits

The ability to determine the traffic load at which NHRP establish as a direct connection across an NBMA backbone provides much improved granularity, control, and overall protocol scalability.

Platforms/Considerations

This NHRP enhancement feature is supported on C4x00, RSM 5000, C7x00 platforms.

Product Marketing Contact
Martin McNealis

IPX Infrastructure Enhancements

Description

The Internetwork Packet Exchange (IPX) infrastructure enhancements feature intends to address diagnostic-related issues by accepting and processing unicast or broadcast diagnostic packets and to make enhancements to the current IPX ping command to ping other stations using the diagnostic packets and displaying the configuration information in the response packet.

Benefits

This feature will:

- Improve IPX (SAP) handling code to be more robust
 - a. Decouple the SAP process code from IPX, NLSP, and EIGRP
 - b. Convert SAP to use chunk manager
 - c. Allow IPX Enhanced Internet Group Management Protocol (EIGRP) split horizon to be enabled per interface
 - d. Improve SAP table handling
 - e. Improve IPX EIGRP display commands and memory handling
- Add traceroute and diagnostic ping debug capabilities

Platforms/Considerations

Currently IOS software supports traceroute for IP, Connectionless Network Service (CLNS), AppleTalk, and Vines, but not IPX. This feature will implement IPX traceroute. IOS software also ignores IPX diagnostic ping request packets.

Product Marketing Contact
Martin McNealis

Protocol-Independent Multicast (PIM) Version 2

Description

Protocol-Independent Multicast (PIM) Version 2 offers many improvements over PIM Version 1. PIM v2 offers a single, active rendezvous point (RP) exists per multicast group, with multiple backup Raps. This compares to multiple active Raps for the same group in PIM Version 1. Also, bootstrap router (BSR) provides a fault-tolerant, automated RP discovery and distribution mechanism. Thus, routers dynamically learn the group-to-RP mappings. Furthermore, sparse mode and dense mode are properties of a group, as opposed to an interface. We strongly recommend sparse-dense mode, as opposed to either sparse mode or dense mode only. PIM Join and Prune messages also have more flexible encodings for multiple address families. A more flexible Hello packet

format replaces the Query packet to encode current and future capability options. Further, register messages to an RP indicate whether they were sent by a border router or a designated router. Finally, PIM packets are no longer inside IGMP packets; they are stand-alone packets.

PIM Version 1, together with the Auto-RP feature, can perform the same tasks as the PIM Version 2 BSR. However, Auto-RP is a standalone protocol, separate from PIM Version 1, and is Cisco proprietary. PIM Version 2 is a standards track protocol in the Internet Engineering Task Force (IETF).

Cisco's PIM Version 2 implementation allows good interoperability and transition between Version 1 and Version 2. You can upgrade to PIM Version 2 incrementally. PIM Versions 1 and 2 can be configured on different routers within one network. Internally, all routers on a shared media network must run the same PIM version. Therefore, if a PIM Version 2 router detects a PIM Version 1 router, the Version 2 router downgrades itself to Version 1 until all Version 1 routers have been shutdown or upgraded.

PIM uses the BSR to discover and announce RP-set information for each group prefix to all the routers in a PIM domain. This is the same function accomplished by Auto-RP, but the BSR is part of the PIM Version 2 specification. The BSR mechanism interoperates with Auto-RP on Cisco routers.

To avoid a single point of failure, you can configure several candidate Basra in a PIM domain. A BSR is elected among the candidate BSRs automatically; they use bootstrap messages to discover which BSR has the highest priority. This router then announces to all PIM routers in the PIM domain that it is the BSR.

Routers that are configured as candidate RPs then unicast to the BSR the group range for which they are responsible. The BSR includes this information in its bootstrap messages and disseminates it to all PIM routers in the domain. Based on this information, all routers will be able to map multicast groups to specific RPs. As long as a router is receiving the bootstrap message, it has a current RP map.

Benefits

PIM Version 2 is a standards track protocol in the IETF.

Platforms/Considerations

This feature is supported across Cisco IOS-based C100X, C1600, C2x00, C36x0, C3800, C 4x00, C5x00, C7200, RSM 5000, C 7500, and the C12000 platforms.

Product Marketing Contact

Martin McNealis

Fast-Switched Fragmented IP Packets

- IP fast fragmentation is available on Cisco 7200 series routers

Web Cache Control Protocol


- The Web Cache Control Protocol feature transparently redirects HTTP requests from the intended server to a Cisco Cache Engine. When the Cisco Cache Engine receives the request, it attempts to service the request from its own cache. If the requested information is not present, the Cisco Cache Engine then makes a request to the web server to get the required information. After receiving the required information from the web server, the Cisco Cache Engine passes the information back to the client and possibly caches it to fill future requests.

Connectivity and Scalability

IOS Scalability

Description

Cisco IOS scalability enables Cisco IOS to support an increased number of interfaces, particularly on platforms such as the Cisco 5800, by adding functionality including:

- 
- Enhanced debugging (or per-port debugging)
 - Expression Management Information Base (MIB)
 - Entity MIB
 - Simple Network Management Protocol (SNMP) bulk transfer
 - IOS file system
 - Open Shortest Path First (OSPF) point-to-multipoint support

Benefits

IOS scalability significantly enhances the ability of Cisco IOS platforms to scale to large numbers of interfaces.

Platforms/Considerations

This feature is supported across the Cisco IOS-based C100X, C1600, C2x00, C2500, C36x0, C38xx, C4x00, C7x00, LS1010, and C8500 platforms.

Product Marketing Contact

Douglas Frosst

PPP over Frame Relay (rfc 1973)

Description

RFC 1973 defines a standardized method for transporting Point-to-Point Protocol (PPP) packets over a Frame Relay infrastructure.

This feature is especially important to the Cisco 90i IDSL product. This product accepts either a PPP or a Frame Relay connection over IDSL from a router or TA which supports leased line mode ISDN. The 90I resides in a D4 Channel bank in a CO environment with a Frame Relay backhaul to an ISP or corporate customers network. If the customer requires PPP services such as authentication, compression or encryption then it is a requirement that the router which terminates the Frame Relay link supports standards based PPP over Frame Relay.

Benefits

Service providers offering IDSL services would prefer to use PPP access as most of their corporate customers wish to take advantage of the standardized facilities PPP offers in terms of authentication, compression etc.

It is also true that the majority of low-cost customer premises equipment which can be used with IDSL services supports PPP but not Frame Relay. Support for PPP over Frame Relay at the head-end of the network increases the market opportunity for service providers dramatically.

Considerations/Platforms

Only Frame Relay PVC's are supported

- IP is the only supported protocol
- Fast-switching must be used
- The only queuing method supported is FIFO

PPP over Frame Relay is supported on the C4x00, C7200 and C7500 platforms.

Product Marketing Contact

Kevin Dickson

Always On/Dynamic ISDN (AO/DI)

Description

Always On/Dynamic ISDN (AO/DI) is a new access connectivity solution which draws on the strengths (and tariff structures) of both packet and circuit switched networks in order to provide more efficient dial-up connectivity. Both D and B-Channel ISDN connections are used depending on the bandwidth requirements of the data being transferred at any time. The initial connection with this service is always a D-Channel X.25 long-hold switched virtual circuit call. However it is important to recognize that this

X.25 connection is only a transport mechanism for the first PPP link in a Multilink Protocol (MP) bundle. When extra bandwidth is required a circuit-switched B-Channel call is made and this becomes the second link in the MP bundle. When traffic falls back to low levels the B-Channel call will be dropped and traffic will once again only use the Always On D-Channel connection.

Note that whilst circuit-switched calls are up MP will not load share over the D-Channel link. This link remains up but is “idled” out of use. Traffic will once again use this link once all circuit-switched calls have ended.

Benefits

A good proportion of Internet traffic is still low speed in nature. For example, downloading email in most instances does not require the full bandwidth of an ISDN B-Channel. Using an AO/DI service may provide cost savings over regular ISDN services in areas where B-Channel connection tariffing is based on per-minute charging. AO/DI reduces costs by increasing NAS port efficiencies.

Although this is a potential new service there are no new management or security considerations. All existing AAA functions in place for regular dial-up services can be utilized with AO/DI.

Platforms/Considerations

AO/DI services are still in their infancy. Many telcos do not have a tariffed offering for X.25 on the D-Channel.

Where ISDN Tariffing is flat rate there is no benefit to the consumer and only minor benefit to the owner of the Network Access Server pool. In this instance AO/DI may not be an appropriate solution to pitch.

Product Marketing Contact

Kevin Dickson

Multiple ISDN Switch Types

Description


The Multiple ISDN Switch Types feature allows you to configure more than one ISDN switch type per router. You can apply an ISDN switch type on a per interface basis, thus extending the existing global ISDN switch-type command to the interface level. This allows Basic Rate Interfaces (BRI) and Primary Rate Interfaces (PRI) to run simultaneously on platforms that support both interface types.

Table 1 ISDN Switch Types Summary

Vendor	Signaling	Software	Country
Lucent 4ESS	PRI	Custom	North America
Nortel DMS 250	PRI	Custom	North America
Nortel DMS 100	PRI	Custom	North America
Nortel DMS 100	BRI	NI	North America
Lucent 5ESS	PRI & BRI	Custom & NI	North America
AGCS GTD-5	PRI	NI	North America
	BRI	NET 3	Asia, Europe, New Zealand, Australia
	PRI	NET 5	Asia, Europe, New Zealand, Australia
	PRI & BRI	NTT	Japan
	BRI	1TR6	Germany
	BRI	TS013	Australia
	PRI	TS014	Australia

Benefits

Multiple ISDN Switch Types provides the following advantages:

- 
- Allows you to use ISDN BRI and PRI simultaneously on the same Cisco platform.
 - Allows you to add ISDN switch types per interface.
 - Allows you to change the ISDN switch type without reloading the router.
 - Allows you to use existing ISDN global configuration commands. The first time a switch type is added to an interface, the new value is read in and propagated to the interface level.

Platforms/Considerations

The Multiple ISDN Switch Types feature is supported on the following platforms: C36x0, C4x00, C5x00, and C7x00.

The following restrictions apply to Multiple ISDN Switch Types:

You must configure a global ISDN switch type using the existing `isdn switch-type` global configuration command before you can configure the ISDN switch type on an interface.

Product Marketing Contact

Anita Freeman

National ISDN Switch Type for Primary Rate Interfaces

Description

National ISDN Switch Type for Primary Rate Interfaces introduces changes to ISDN switch types for Primary Rate Interfaces (PRI) by adding a new switch type for PRI interfaces, National ISDN Primary Rate Interface (Bellcore SR3887, November, 1996). This feature also adds the ability to configure outgoing PRI B channel selection for the T1 controller in ascending order (channel 1 to channel 23) or descending order (channel 23 to channel 1). Previously, the router selected a B channel for outgoing calls from the highest free channel in descending order. The E1 controller channel selection for ascending order is channel 1 to 31, and 31 to 1 for descending order.

Benefits

National ISDN Switch Types for Primary Rate Interfaces provides the following benefits:

- Unlike previous custom implementations, such as `primary-5ess`, and `primary-dms100`, the National ISDN specification is designed to be switch independent. This increases flexibility in adapting to evolving standards and future enhancements.
- The National ISDN for PRI feature addition completes Cisco IOS support for the complement of switch types for ISDN PRI deployed in the United States public switched network. The Cisco IOS implementation of National ISDN PRI was certified by Bellcore to National ISDN Primary Rate Interface, SR3887, Issue 1, November 1996.
- Included in this feature is the highly demanded support of National ISDN PRI on the Lucent 5ESS and the AGCS GTD-5 switches.
- The ability to select PRI B channel order election for outgoing calls allows extended flexibility and compatibility with a variety of ISDN switch type service implementations. Additionally, this ability reduces ISDN switch misconfigurations, which can delay initial service activation.

Platforms/Considerations

The National ISDN Switch Types for Primary Rate Interfaces feature is supported on the following platforms: Cisco IOS-based C36x0, C4x00, C5x00, C7x00.

The following restriction applies to National ISDN Switch Types for Primary Rate Interfaces:

The Nx64 multirate feature in National ISDN Primary Rate Interface, SR3887, Issue 1, November, 1996 is not supported.

Product Marketing Contact

Anita Freeman

NFAS with D Channel Back Up

Description

The Nortel DMS250, Nortel DMS100 and National ISDN switch types have been added to the existing Non-Facility Associated Signaling (NFAS) with D Channel Backup feature.

ISDN NFAS allows a single D channel to control multiple PRI interfaces. A backup D channel is configured for use when the primary NFAS D channel fails.

An NFAS group is a PRI channel group (the group of interfaces) under control of a single D channel. The channel group can include all the ISDN channels on multiple T1 controllers. Cisco IOS supports ten PRI interfaces in an NFAS group with a primary D channel and a backup D channel. Five NFAS groups are supported in a single chassis.

Table 2 NFAS Summary

Switch Type	Type of NFAS	Release
Lucent 4ESS	Custom	11.3
Nortel DMS 250	Custom	11.3
Nortel DMS 100	Customer	11.3
Lucent 5ESS	Custom-Does not support FNAS	
Lucent 5ESS	National ISDN	11.3(3)T
AGCS GTD-5	National ISDN	11.3(3)T

Benefits

- Use of a single D channel to control multiple PRI interfaces can free one B channel on each PRI interface to carry other traffic.
- On the Nortel DMS100, when the single D channel is shared, multiple PRI interfaces may be configured in a single trunk group. The additional use of alternate route indexing, a DMS100 feature that provides a rotary from one trunk group to another, enables the capability of building large trunk groups in the public switched network.
- Any hard failure causes a switchover to the backup D channel and currently connected calls remain connected.

Platforms/Considerations

The NFAS with D Channel Backup feature is supported on these IOS-based platforms: Cisco 3600 series, Cisco 4000 series, Cisco 5200, Cisco 5300, Cisco 7200 series, Cisco 7500 series

NFAS is supported when there is an ISDN PRI capable channelized T1 controller. The router must connect to Lucent 4ESS, Nortel DMS250, Nortel DMS100, or National ISDN PRI switches.

Product Marketing Contact

Anita Freeman

Dialer Watch


Description

Dialer Watch is a backup feature that integrates dial backup with routing capabilities. Prior dial backup implementations used the following conditions to trigger backup:

- Interesting packets were defined at central and remote routers using Dial on Demand routing (DDR).
- Connection loss occurred on a primary interface using a back up interface with floating static routes.
- Traffic thresholds were exceeded using a dialer load threshold.

Prior backup implementations may not have supplied optimum performance on some networks, such as those using Frame Relay multipoint subinterfaces or Frame Relay connections that do not support end-to-end LMI.

Dialer Watch provides reliable connectivity without relying solely on defining interesting traffic to trigger outgoing calls at the central router. Dialer Watch uses the convergence times and characteristics of dynamic routing protocols. Integrating backup and routing features enables Dialer Watch to monitor every deleted route. By configuring a set of watched routes that define the primary interface, you are able to monitor and track the status of the primary interface as watched routes are added and deleted. Monitoring the watched routes is done in the following sequence:

- 
1. Whenever a watched route is deleted, Dialer Watch checks to see if there is at least one valid route for any of the watched IP addresses defined.
 2. If there is no valid route, the primary line is considered down and unusable.
 3. If there is a valid route for at least one of the defined watched IP addresses, and if the route is pointing to an interface other than the backup interface configured for Dialer Watch, the primary link is considered up.
 4. In the event that the primary link goes down, Dialer Watch is immediately notified by the routing protocol and the secondary link is brought up.
 5. Once the secondary link is up, at the expiration of each idle timeout, the primary link is rechecked.
 6. If the primary link remains down, the idle timer is indefinitely reset.
 7. If the primary link is up, the secondary backup link is disconnected. Additionally, a disable timer can be set to create a delay for the secondary link to disconnect, after the primary link is reestablished.

Benefits

Dialer Watch provides the following advantages:

- *Routing*—Backup initialization is linked to the dynamic routing protocol, rather than a specific interface or static route entry. Therefore, both primary and backup interfaces can be any interface type, and they can be used across multiple interfaces and multiple routers. Likewise, Dialer Watch relies on convergence, which is sometimes preferred over traditional DDR links.
- *Nonpacket semantics*—Dialer Watch does not exclusively rely on interesting packets to trigger dialing. The link is automatically brought up when the primary line goes down without postponing dialing.
- *Dial backup reliability*—DDR redial functionality is extended to dial indefinitely in the event that secondary backup lines are not initiated. Typically, DDR redial attempts are affected by enable-timeouts and wait-for-carrier time values. Intermittent media difficulties or flapping interfaces can cause problems for traditional DDR links. However, Dialer Watch automatically reestablishes the secondary backup line on ISDN, synchronous, and asynchronous serial links.

Considerations/Platforms

This feature is supported on these platforms Cisco IOS-based: Cisco 100x, Cisco 160x, C2x00, C 36x0, C4x00, C 4x00, C5x00, and C7x00.

Product Marketing Manger

April Chou

L2F Stacking Home Gateways

Description

The feature permits Multilink PPP links from a single client to terminate physically at different Home Gateways while logically appearing to terminate at a single Home Gateway. This feature is a superset of the L2F load sharing feature which was available in 11.3. If the B channel calls are tunnel across different L2F tunnels and terminating at different Home Gateways, these fragmented packets are reassembled at the Home Gateway which was determined via Stack Group Bidding Protocol (SGBP).

Benefits

Organizations can scale access bandwidth by adding new devices to the MMP pool. Home Gateway Load sharing is now possible with Multilink PPP.

Platforms/Considerations

This feature is supported on the Cisco IOS-based C100x, C1600, C2x00,C 36x0,C 4x00, C4x00,C 4700,C 5x00, C7x00. The Configuration of L2F load sharing must be done on the AAA server.

Product Marketing Contact

April Chou

L2F Multihop Support

Description

This feature will allow an extension of a L2F tunnel from a Home Gateway (tunnel termination point) to another Home Gateway. PPP is forwarded from the first Home Gateway to the Home Gateways where the tunnel is extended, in this sense the intermediate Home Gateway can be considered as an IP forwarder.

Benefits

A service provider has the ability to provide wholesale dial service to another service provider who then provides VPDN service to an Enterprise Corporation. For example, a Telco is providing wholesale dial services to an ISP. The ISP provides the virtual private dial-up network to an Enterprise Corporation. In this case, a L2F tunnel will be built to the ISP Home Gateway. This L2F tunnel will be extended to the Enterprise Corporation's Home Gateway, when remote users are trying to reach their Enterprise headquarters.

The benefit for the Telco is creating a new source of revenue in wholesale dial services while benefiting from the result of redirecting data traffic from a voice network, thus reducing network congestion. The benefits for ISPs are lowering the continuous investment in remote access equipment and concentrate on providing value-added services such as VPN services. The Enterprise Corporation also benefits by receiving the virtual private network services from an ISP.

Platforms/Considerations

This feature is supported on the Cisco IOS-based C100x, C1600, C2x00, C36x0, C4x00, C5x00, C7x00 platforms. The maximum tunnel extension is 4. This number is set to 4 in order to avoid recursive routing loops as well as to prevent a PPP time-out condition. Multihop or tunnel extension within the same stackgroup is not allowed. The VPDN tunnel configuration is also required on the intermediate Home Gateway either locally or via RADIUS server.

Product Marketing Contact

April Chou

Switching

Cisco Express Forwarding

Description

Cisco Express Forwarding (dCEF) is an advanced Layer 3 IP forwarding technology designed to optimize network performance and scalability. This new switching paradigm is what's termed a full topology-driven architecture because, unlike previous switching mechanisms, used the first packet in a flow to build an IP destination cache that subsequent packets to the same network destination would use (a technique known as "demand-caching"). dCEF uses all available routing information to build an IP Forwarding Information Base (FIB) so that a deterministic switching decision can be made, even for the first packet to a new destination. This capability is significant, given the changing traffic dynamics on the Internet and within enterprise intranets, where flows are increasingly of shorter duration and more topologically dispersed (for example, Web traffic).

Benefits

- *Improved system performance*—dCEF implements an expedited IP lookup and forwarding algorithm to deliver maximum Layer 3 switching performance. It is also less CPU intensive than route caching; therefore, more CPU processing power can be applied to Layer 3 services such as quality of service (QoS), NetFlow, and security.
- *Scalability*—Cisco's Express Forwarding technology is optimized for information distribution, allowing it to take advantage of the distributed architecture of the high-end Cisco IOS routers such as the Cisco 7500 and the gigabit switch router (GSR). Thus Distributed dCEF (dCEF) delivers scalable switching capacity by providing each line card with an identical on-card copy of the FIB table, enabling them to independently perform Express Forwarding and therefore significantly increase aggregate throughput.
- *Resilience*—dCEF offers an unprecedented level of switching consistency and stability in large dynamic networks because the FIB table contains all known routes that exist in the routing table and routing updates are conveyed and processed autonomously.

- **Load balancing**—Load balancing can be performed with negligible performance impact on either a per-destination or per-packet basis over up to six equal/unequal cost links.

Platforms/Considerations

Cisco Express Forwarding is supported across the Cisco IOS-based C2600, C36x0, C4x00, RSM5000, AS5800, C7x00, C85x0 and C12000 platforms.

Product Marketing Contact

Martin McNealis

Tag Switching

Tag Switching is an innovative new technique for high-performance packet forwarding that assigns “tags” to multiprotocol frames for transport across packet or cell-based networks. It is based on the concept of “label swapping,” in which units of data (e.g., a packet or a cell) carry a short, fixed length label that tells switching nodes how to process the data.

Specifically Cisco’s Tag Switching delivers the following features, functions, and benefits:

Feature	Function	Benefit
Tag Switch Path Tunnels (TSP Tunnel)	Create alternative path(s) or connection(s) between source and destination.	Lower cost - through higher network utilization
Traffic Engineering	Define traffic that will traverse a TSP Tunnel.	Lower cost through higher network utilization
Ships in the Night	Support ATM and Tag Switching services simultaneously on the same ATM backbone	Lower cost through higher network utilization
Tag Distribution Protocol (TDP)	Assign tags to routes and communicate assignments to peers. Runs in conjunction with Layer 3 routing protocols.	Supports the creation of a Tag Switching network.
Dynamic Tag Switching	Allocate and distribute tags based on routing topology discovered by Layer 3 protocols. Runs in conjunction with Layer 3 routing protocols.	Supports the creation of a Tag Switching network.
Static Tag Switching	Allocate and distribute tags based on RSVP signaling.	Supports the creation of TSP tunnels.
Support for OSPF, IS-IS, RIP, and EIGRP	Build routing topology used by the Tag Distribution Protocol	Flexibility to support multiple Layer 3 routing protocols
Tag Switch Controller	Enables BPX 8620 and 8650 to participate in a Tag Switching network.	Supports scalable integration of IP and ATM.

- **Tag Distribution Protocol (TDP)**—Tag Distribution Protocol (TDP) is the protocol responsible for binding tags to routes and distributing tags between neighboring routers. TDP runs in parallel with native Layer 3 protocols using them to discover the routing topology of the network. TDP is an incremental protocol thereby limiting TDP traffic between Tag Switch Routers (TSRs) to changes in the routing topology.

Dynamic Tag Switching
When a Tag Switching network is in the dynamic mode, tags are allocated and distributed based on the routing topology. This is in contrast to the static mode where tags are allocated based on a configured path using RSVP signaling (see Tag Switched Path Tunnels). The TDP protocol, running in parallel with native Layer 3 routing protocols, is used to distribute tags. As new routes are discovered, tags are assigned and TDP is used to distribute them with no modification of the routing protocols required. So Tag Switching can be run in conjunction with any routing protocol. In Tag Switching phase 1 OSPF, IS-IS, RIP, and EIGRP are all supported on Cisco’s 7xxx family of routers and Cisco’s BPX 8620 and 8650 with OSPF support on the Cisco LightStream 1010.

- **Tag Switched Path (TSP) Tunnels**—In conventional layer 3 routing, network topologies frequently include multiple paths between two points, but the normal routing procedures typically select a single path as the Layer 3 route between two points regardless of the load on the links that implement the path. As a consequence, some links are congested while some are underused. TSP Tunnels provide a way to override routing protocols across multiple routers. It gives you the ability to direct selected traffic over specific paths in the network in order to efficiently use network resources and provide different levels of service.

RSVP, with some extensions, is the signaling protocol used to set up TSP tunnels. Within a Tag Switching network the RSVP tunnel set-up is initiated at the source Tag Switch Router (TSR) or ATM-TSR at the head of the tunnel. The forward message carries a complete source routed path with all intermediate hops identified. The reply message carries the tags that build the tunnel. A rapid tear down mechanism has been added, via an extension, in the event of link failure. Thus we can immediately stop using a tunnel rather than relying on the standard RSVP time-out.

- *Traffic Engineering*—Traffic Engineering is the set of mechanisms by which an administrator can specify what traffic should enter a TSP tunnel. This is accomplished by defining a filter that specifies the traffic you are interested in engineering and then mapping that filter to the appropriate TSP tunnel. Several options exist when mapping a filter onto a TSP tunnel, such as, mapping a filter to a specific tunnel, mapping a filter to multiple tunnels, or load balancing between multiple tunnels. When mapping to multiple tunnels it is possible to rank the various tunnels by attractiveness (e.g. number of hops) with the default option of normal IP routing if no tunnel is available.
- *Ships in the Night*—ATM Tag Switched Routers (ATM-TSR), such as Cisco's LightStream 1010 or BPX 8620 or BPX 8650, can simultaneously support ATM and Tag Switching Virtual Paths (VPs) on the same switch allowing Service Providers to deliver ATM and IP services on the same ATM network.
- *Tag Switch Controller (TSC)*—The Tag Switch Controller (TSC) is a tag switch router (TSR) that controls the operation of a separate ATM switch. Together, the router and ATM switch function as a single ATM Tag Switching router (ATM-TSR). A Cisco 7200 or 7500 series router acts as the TSC, and a Cisco BPX 8600 Service Node (8620 wide area switch or 8650 IP+ATM switch) or a partner's switch acts as the VSI-controlled ATM switch. The TSC controls the ATM switch using the Cisco Virtual Switch Interface (VSI), which runs over an ATM link connecting the two.

xDigital Subscriber Line Bridge Support

Description

This feature enables an IOS platform acting as a Local Access Concentrator in a DSL environment to apply selective forwarding policy to traffic between subscribers. Typically it is deployed in conjunction with IOS Integrated Routing and Bridging (IRB) (refer to Product Bulletin 487) in an upstream routing/downstream bridging paradigm.

Benefits

This provides security and enhanced performance since it contains the flooding of traffic at Layer2 between subscribers that are members of the same "*Subscriber Group*" and in particular the default subscriber policy behavior is to apply filtering intelligence to common traffic types such as ARP, Unknown Unicast, Multicast, Broadcasts etc.

Platforms/Considerations

DSL Subscriber Bridging support is available across C100x,C1600,C 2x00,C 36x0,C 4x00, C5x00,C 7x00 and C7x00 platforms.

Product Marketing Contact

Martin McNealis

Optimized VIP Local Switching

Description

If is traffic coming in on an VIP2 interface configured for distributed forwarding and the outgoing interface resides on the same VIP2 the packet is switched directly to the outgoing interface without interrupting the RSP. Previously some resources on the RSP were used although the forwarding process was done by the VIP2.

Benefits

Reduces CyBus load and saves memory resources on the RSP.

Distributed Switching Support for Fast EtherChannel (FEC)

Description

Support for distributed dCEF switching for IP is added to Fast EtherChannel interfaces



Benefits

Distributed switching reduces the load on the RSP. Previously all IP traffic for Fast EtherChannel interfaces was forwarded by the RSP.

Distributed Switching for LANE

In LAN Emulation (LANE) networks, distributed switching for LANE is a new Cisco 7500 series feature that allows a LAN Emulation Client (LEC) to be distributed from the RSP to one or more VIP2 interfaces. In doing so, the VIP2 distributed switching capability can now provide switching between each emulated LAN connected to each VIP2 independently. This ability provides increased aggregate IP switching performance across the 7500 architecture for LANE networks versus centralized RSP switching. The inter-ELAN switching performance provided by the VIP2 modules is additive across the 7500 series routers and increases with each new VIP2/ATM port adapter. This ability also minimizes the utilization of the RSP—freeing the RSP for other functions including low-level routing and routing updates.

The other components of LANE, such as LAN Emulation Servers (LES), broadcast and unknown server (BUS), and LAN Emulation Configuration Servers (LECS), are functions used primarily during network initialization for address look-ups. These functions are not in the data flow, and distributing these functions does not provide any performance gain. Therefore, the LES, BUS, and LECS functions continue to reside on the RSP with this feature.

Distributed switching for LANE for the Cisco 7500 series is completely ATM Forum compliant. It is intended for any Enterprise or ISP ATM applications where multiple VIP2/ATM port adapter combinations are installed in the same 7500 series router, or for any ATM applications where the performance can be optimized by dedicating the RSP to other routing functions.

This capability only supports the IP protocol for Ethernet LANE in a distributed manner. Token Ring LANE is not supported via distributed switching; however, it is supported within the RSP.

Security

IP Security (IPSec)

Description

IPSec is a framework of open standards for ensuring secure private communications over the Internet. Based on standards developed by the Internet Engineering Task Force (IETF), IPSec ensures confidentiality, integrity and authenticity of data communications across a public network. IPSec provides a necessary component of a standards-based, flexible solution for deploying a network-wide security policy.

Benefits

Customers that use Cisco's IPSec will be able to secure their network infrastructure without costly changes to each and every computer. If a customer deploys IPSec in their network, applications gain privacy, integrity, and authenticity controls without affecting individual users or applications. Application modifications are not required, eliminating the need to deploy and coordinate security on a per application, per computer, basis. This provides great cost savings, as only the infrastructure needs to be changed.

IPSec provides an excellent remote user solution. Remote clients will be able to use an IPSec client on their PC in combination with L2TP to connect back to the enterprise network. The cost of remote access is decreased dramatically, and the security of the connection actually improves over that of dial-up lines.

Platforms/Considerations/Caveats

This feature is supported across Cisco's IOS-based C1600, C 2x00, C36x0, C4x00, C 4x00, C 5x00, and C 7x00 platforms.

IPSec will not work with distributed switching on a VIP on a 7500 router. With a VIP installed, all IPSec processing will be done by the RSP.

The Encryption Service Adapter (ESA) does not support IPSec. The ESA supports Cisco Encryption Technology. A new hardware acceleration option for IPSec will be available later.

Product Marketing Contact
Terry Bernstein

Cisco IOS Firewall Feature Set

Cisco IOS security services include an array of features that enable managers to configure a Cisco router as a firewall. The Cisco IOS Firewall feature set adds greater depth and flexibility to existing Cisco IOS security solutions.

New Firewall Features:

- *Context-based access control (CBAC)*—Provides internal users secure, per-application-based access control for all traffic across perimeters, e.g. between private enterprise networks and the Internet
- *Java blocking*—Protects against unidentified, malicious Java applets
- *Denial of Service detection/prevention*—Defends and protects router resources against common attacks; checks packet headers and drops suspicious packets
- *RealTime alerts*—Logs alerts in case of denial-of-service attacks or other pre-configured conditions.
- *Audit trail*—Details transactions; records time stamp, source host, destination host, ports, duration and total number of bytes transmitted
- *ConfigMaker support*—A Windows95/WindowsNT-Wizard based network configuration tool that offers step-by-step guidance through network design, addressing and Firewall feature set implementation.

Benefits

- *Flexibility*—All-in-one solution can perform routing, provide secure Internet connectivity, and apply distinct security characteristics according to a user-defined policy to each interface on a per-user or per-application basis.
- *Investment Protection*—Integrating firewall functionality into a multiprotocol router leverages an existing router investment.
- Routers are usually deployed to separate sensitive network segments and manage private/public network interfaces. The incremental change saves costs and management training associated with learning a new platform.
- *Easier management*—With remote management capabilities, a network administrator can implement security features from a central console over the network.
- *Seamless interoperability*—Use with other Cisco IOS software features, optimize, WAN utilization, provide robust, scalable routing, and interoperate with existing Cisco IOS-based networks (such as the Internet).

Platforms/Considerations

This feature is supported on the Cisco IOS-based C1600, C1700, and C2500 series routers.

Product Marketing Contact
Jocelyne Okrent

Voice

Voice over IP

Description

Voice over IP enables a Cisco router to carry live voice traffic (for example, telephone calls and faxes) over an IP network.


Benefits

Toll bypass, Remote PBX presence over WAN's, Unified voice/data trunking, POTS-Internet telephony gateways.

Platforms/Considerations

This feature is supported on the Cisco IOS-based 36x0.

Product Marketing Contact
Mark Monday



Reliability

Hot Standby Router Protocol (HSRP) Support on Fast EtherChannel (FEC)

Description

Support for Hot Standby Router Protocol (HSRP) is added to Fast EtherChannel interfaces. This feature is only available on the Cisco 7500.

Benefits

HSRP increases network availability by providing protection against router failures.

Automatic Protection Switching for POS interfaces

Description

The automatic protection switching (APS) feature is supported on Cisco 7500 series routers. This feature allows switchover of Packet-Over-SONET (POS) circuits between cards or systems and is often required when connecting SONET equipment to Telco equipment. APS refers to the mechanism of bringing a “protected” POS interface into the SONET network as the “working” POS interface on a circuit from the intervening SONET equipment.

Benefits

Increased resilience against failures within the Sonet/SDH infrastructure or failure of a POS interface or router.

MS Callback

Description

The MS Callback feature provides client-server callback services for Microsoft Windows 95 and Microsoft Windows NT clients. MS Callback supports the Microsoft Callback Control Protocol (MSCB). MSCB is Microsoft’s proprietary protocol that is used by Windows 95 and Windows NT clients. MS Callback supports negotiated PPP Link Control Protocol (LCP) extensions initiated and agreed upon by the Microsoft client. MS Callback is added to existing PPP Callback functionality. Therefore, if you configure your Cisco access server to perform PPP Callback using Cisco IOS Release 11.3(2)T or later, MS Callback is automatically available.

- MS Callback supports AAA security models using a local database or AAA server.
- MSCB uses LCP callback options with sub-option type 6. The Cisco MS Callback feature supports clients with a user-specified callback number and server specified (preconfigured) callback number.
- MS Callback does not affect non-Microsoft machines that implement standard PPP LCP extensions as described in RFC 1570. In this scenario, MS Callback is transparent.

Platforms/Considerations

This feature is supported on these platforms: C100x, C1600, C2x00, C 36x0, C 4x00, C 4x00, C5x00, C 7x00.

Product Marketing Manger

April Chou

Management

ATM PVC Management

Description

The ATM PVC Management feature set includes new and enhanced capabilities that allow you to create and manage ATM PVCs and SVCs with more ease and improved integrity. This feature set includes the following five subfeatures:

- *New VC Configuration*—The New VC Configuration subfeature allows you to create ATM permanent virtual circuits (PVCs), switched virtual circuits (SVCs), static maps, and associated virtual circuit (VC) parameters more easily and with fewer errors using new ATM commands in new VC command modes.
- *VC Integrity Management*—The VC Integrity Management subfeature allows you to manage your ATM PVCs and SVCs so that you receive immediate notification of when these VCs come down in your network. Upon notification, protocols can reroute ATM packets and prevent unpredictable and relatively long timeout periods.

- *PVC Discovery*—The PVC Discovery subfeature allows you to enable your router to automatically assign or ‘discover’ PVCs on an ATM interface or subinterface using information from an attached adjacent switch.
- *Multiprotocol Inverse ARP*—The Multiprotocol Inverse ARP subfeature allows you to enable a dynamic protocol mapping between an ATM PVC and a network addresses by configuring Inverse Address Resolution Protocol (Inverse ARP) on ATM PVCs running IP or IPX.
- *Rate Queue Tolerance*—The Rate Queue Tolerance subfeature allows you to configure a range of peak rates on a single rate queue, thereby improving ATM rate queue usage.

Benefits

Use the ATM PVC Management feature set to simplify and expedite PVC and SVC configurations and improve the management of PVC and SVC integrity. The benefits of this feature set include:

- Simplified ATM PVC, SVC, and static map configuration.
- VC management that detects connections and disconnections of PVCs and SVCs immediately, so that ATM packets are rerouted upon notification.
- Automatic assignment or ‘discovery’ of ATM PVCs on an ATM interface or subinterface using information from an attached adjacent switch.
- Dynamic protocol mapping between a PVC and a network address so that you no longer have to manually configure an ATM static map.
- Improved rate queue usage when you configure a range of peak rates on a single rate queue.

Platforms/Considerations

This feature is supported on the following IOS-based platforms: Cisco 4500 and 4700, Cisco 7200 series, and the Cisco 7500 series. ATM rate queue tolerance is not supported on the Cisco 7200 series.

Product Marketing Manger

Kevin Dickson

SNMP Inform Requests

Description

The SNMP Inform Requests feature allows routers to send inform requests to SNMP managers.

Benefits

Informs are held in memory until a response is received or the request times out. They are more reliable than traps.

Platforms/Considerations

Informs consume more memory than traps. Feature supported on the C2x00,C 36x0,C 3800, 38xx, C4x00,C 5x00 and C 7x00

Product Marketing Contact

Peter Long

SNMP Manager

Description

The SNMP Manager feature allows a router to server as a SNMP manager. As a SNMP manager, the router can send SNMP requests to agents and receive SNMP responses and notifications from agents.

Product Marketing Contact

Peter Long

VPDN MIB and Syslog Facility

Description

The VPDN MIB and Syslog Facility feature provides the SNMP-based networking management support and the Syslog messages for Cisco’s VPDN feature set, specifically the L2F tunneling technology and will later apply to the L2TP emerging standard.



The VPDN MIB includes four groups of objects:

- System wide information and statistics regarding VPDN (cvpdnSystemInfo)
- Information and statistics regarding active VPDN tunnels (cvpdnTunnelInfo)
- Information and statistics regarding active user sessions in active VPDN tunnels (cvpdnTunnelUserInfo)
- Information regarding failure history per user name (cvpdnUserToFailHisInfo)

The VPDN syslog mechanism provides a generic logging output for VPDN use, L2F or L2TP. The syslog messages are generated to inform of an authentication or authorization error, resource issues, including IDB's, and time-out events.

IP MAC Accounting

Description

Provides switching statistics per MAC address for IP hosts.

Benefits

Provides accounting for IP hosts on a per MAC address basis.

IBM

Cisco Database Connection

Description

Cisco Database Connection turns a Cisco router into a high-speed, data-access device by enabling client-based, Open Database Connectivity (ODBC) applications using TCP/IP to connect to IBM's family of DB2 relational databases.

Benefits

This standards-based solution is easy to manage, provides complete fault tolerance, reduces expensive CPU utilization on the host, and maximizes users' IT investments by taking advantage of distributed processing and standard communication protocols.

Furthermore, it offers the following benefits:

- *Leverages existing TCP/IP network*—Because Database Connection converts DRDA packets over TCP/IP to DRDA packets over APPC (LU 6.2) you can leverage TCP/IP in your enterprise.
- *Improves manageability*—You can manage enterprise-wide access to DB2 from a single centralized location within the data center.
- *Maximizes computer resources*—Database Connection takes advantage of distributed processing and standard communication protocols and reduces CPU utilization on the host.
- *Eliminates special software*—Database Connection works on your router without the need for any special software on the IBM host. It allows ODBC clients to connect to IBM's DB2 relational databases using TCP/IP without the need for communication packages on the desktop. Database Connection supports ODBC on client systems, allowing you to use applications of your choice that are enabled with ODBC. Some examples of applications that utilize ODBC are Microsoft Excel, Microsoft Access, Lotus 1-2-3, Visual Basic, Visual C++, and PowerBuilder.
- *Increases data speed access*—Cisco routers enable high-speed connections to DB2 on hosts, and these connections are faster than native host TCP/IP.

Platforms/Considerations

This feature is supported across Cisco IOS-based: C 4x00, C 4x00, C7x00, and C 7x00 platforms.

New Feature Hardware Support

Packet-over-Sonet Port Adapter

Descriptions

The packet-over-SONET port adapter (PA) is a single-port, single-wide OC-3c/Synchronous Transport Module level 1 (STM-1) port adapter. The packet-over-SONET PA is specifically designed to provide high-performance Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) connectivity with increased port density and flexibility for the Cisco 7200 and 7500. The packet-over-SONET PA is available in three physical interfaces: OC-3c/STM-1 multimode, OC-3c/STM-1 single-mode intermediate reach, or OC-3c/STM-1 single-mode long reach.

Benefits

The packet-over-SONET port adapter provides the same level of high switching performance as the existing packet-over-SONET/SDH interface processor in a single-wide port adapter design. Furthermore, the packet-over-SONET PA extends the benefits of packet-over-SONET connectivity to the Cisco 7200 series router. Providing tremendous network flexibility, the packet-over-SONET PA can be deployed on the Cisco 7200 in SONET/SDH networks that require a large number of distributed, multiservice edge routers.

Platforms/Considerations

Packet-over-SONET PA is supported on the Cisco 7200 with network processing engine (NPE)-150 or NPE-200 and the Cisco 7500 with Versatile Interface Processor (VIP)2-50.

Product Marketing Contact

Bill Clark

PA-A3-DS3/E3 Support

Description

Support for the PA-A3-DS/E3 port adapters is added. These high performance PAs support traffic shaping and ABR.

Benefits

Granular traffic shaping and Available Bitrate support allow effective use of available bandwidth in the ATM network.

PA-A3-OC3 Support

Description

Support for the PA-A3-OC3 port adapters is added. This high performance PA supports traffic shaping and ABR.

Benefits

Granular traffic shaping and Available Bitrate support allow effective use of available bandwidth in the ATM network.

Second-Generation Fast Ethernet Interface Processors

- The FEIP2-DSW second-generation Fast Ethernet Interface Processor is a replacement for the FEIP2-2TX and FEIP2-2FX, which are available on Cisco 7500 series routers, and on Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

SA-Comp/1 and SA-Comp/4 Data Compression Service Adapters

- Multiple SA-Comp/1 and SA-Comp/4 data compression service adapters (CSA) are available on Cisco 7200 series routers.



Enhanced ATM Port Adapter (PA-A3)

Descriptions

The enhanced ATM port adapter (PA-A3) is a new generation of single-wide, single-port ATM port adapter for the Cisco 7200 and 7500 high-end routers that introduces per-virtual connection (VC) traffic shaping and support for many ATM service classes (non-real time variable bit rate [NRT-VBR], available bit rate [ABR], and unspecified bit rate [UBR]). Supporting DS3, E3, OC-3c/STM-1 multimode, OC-3c/STM-1 single-mode intermediate reach, and OC-3c/STM-1 single-mode long reach interfaces, the enhanced ATM port adapter is designed for many enterprise WAN and service provider applications.

The PA-A3 complements the existing PA-A1, which provides low-cost, high-performance ATM connectivity for the campus and Internet service provider (ISP) point-of-presence (POP), and the ATM circuit emulation services (CES) PA (PA-A2), which provides multiservice (voice and data) integration on the Cisco 7200 for remote enterprise WAN/MAN applications. In addition to supporting all the hardware features of the existing ATM Interface Processor (AIP), the PA-A3 adds several new features in a smaller, lower-cost port adapter design. As a port adapter, the PA-A3 is supported on both the Cisco 7200 and the Cisco 7500. In the Cisco 7500, the PA-A3 leverages the distributed switching capabilities of VIP2 and enables an extensive set of distributed services for scalable, high-performance routing.

Benefits

The PA-A3 allows customers to effectively manage traffic bandwidth at the edges of the ATM network while implementing value-add Layer 3 services. With advanced, per-VC traffic shaping features and support for many ATM service classes (including ABR), the PA-A3 can be widely deployed in all enterprise WAN and service provider backbone.

Platforms/Consideration

The PA-A3 is supported on the Cisco 7200 with NPE-150 or NPE-200 and the Cisco 7500 with VIP2-40 or VIP2-50.

Product Marketing Contact

Bill Clark

PA-MC-E3 Support

Description

Support for the PA-MC-E3 port adapters is added. These PAs support multilevel channelization of a channelized E3 connection, providing access to 2.048 Mbps E1 and further down 64 kbps DS0 connections.

Benefits

This port adapter provides high density connectivity for up to 128 remote sites in a single-wide form factor.

PA-MC-T3 Support

Description

Support for the PA-MC-T3 port adapters is added. This PA supports multilevel channelization of a channelized T3 connection, providing access to 1.544 Mbps T1 and further down 64 kbps DS0 connections.

Benefits

This port adapter provides high density connectivity for up to 128 remote sites in a single-wide form factor.

PA-MC-8T1, PA-MC-4T1, PA-MC-8DSX1, PA-MC-8E1/120 Support

Description

Support for the 4/8 port Multichannel T1/E1 port adapters is added. These PAs support T1, T1DSX and E1 channelized connections. Up to 128 connections can be defined being either full or fractional E1/T1 or carrying multiple nx64 kbps connections.

Benefits

This port adapter provides high density connectivity for up to 128 remote sites in a single-wide form factor at lower speed links up to T1/E1.

- CSA Support Over HSSI-SA-Comp/1 and SA-Comp/4 data compression service adapters (CSA) now operate over High-Speed Serial Interface (HSSI) links available through the PA-2H and PA-H Revision B port adapters. When using compression, limit HSSI speeds to 16 Mbps to ensure no packet loss.

Channelized T3 Dual-Wide Port Adapter

The channelized T3 dual-wide port adapter (PA-CT3/4T1) is available on C7x00 routers.

PA-T3 and PA-2T3 Serial Port Adapter

The PA-T3 and PA-2T3 serial port adapters are available on Cisco 7200 series routers, on Cisco 7500 series routers, and on Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI). For information on interoperability guidelines for T3 serial port adapter DSUs, refer to the *T3 Serial Port Adapter Installation and Configuration* publication that ships with the product.

VIP2-50

The VIP2-50 is available on Cisco 7500 series routers, and on Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI). Although the VIP2-50 is being announced with Release 11.1(15)CA, it is also supported in Release 11.1(14)CA1.

High-Speed Serial Interface Port Adapters

The PA-2H Revision B port adapter is available on Cisco 7200 series routers, Cisco 7500 series routers, and on Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI). This port adapter was revised to improve performance.

Fast EtherChannel

The Fast EtherChannel feature allows multiple Fast Ethernet point-to-point links to be bundled into one logical link to provide bidirectional bandwidth of up to 800 Mbps. Fast EtherChannel can be configured between Cisco 7500 series routers and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI) or between a Cisco 7500 series router or a Cisco 7000 series router with the RSP7000 and RSP7000CI and a Catalyst5000 switch.

PA-E3 and PA-2E3 Serial Port Adapters

The PA-E3 and PA-2E3 serial port adapters are available on Cisco 7200 series routers, on Cisco 7500 series routers, and on Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI). For information on interoperability guidelines for E3 serial port adapter DSUs, refer to the *E3 Serial Port Adapter Installation and Configuration* publication that ships with the product.

High-Speed Serial Interface Port Adapters

The PA-H Revision B port adapter is available on Cisco 7200 series routers, Cisco 7500 series routers, and on Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI). This port adapter was revised to improve performance.

E1-G.703/G.704 Serial Port Adapter

The E1-G.703/G.704 serial port adapters (PA-4E1G-120 and PA-4E1G-75) are available on Cisco 7500 series routers, Cisco 7200 series routers, and on Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

PA-A2 ATM-CES Port Adapter

The PA-A2 ATM-CES port adapters (PA-A2-4T1C-OC3SM, PA-A2-4T1C-T3ATM, PA-A2-4E1XC-OC3SM, PA-A2-4E1XC-E3ATM, PA-A2-4E1YC-OC3SM, and PA-A2-4E1YC-E3ATM) are available on Cisco 7200 series routers.

Channelized T3 Interface Processor Feature Enhancements

- The Channelized T3 Interface Processor (CT3IP) available on Cisco 7500 series routers, and on Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI) now supports the following additional features:
 - SNMP MIB support per RFC 1406 and RFC 1407
 - Performance monitoring via Facility Data Link (FDL) per ANSI T1.403
 - Remote FDL loopbacks
 - Generation of bit error rate testing (BERT) test patterns
 - User configurable yellow alarm processing
- PA-A1-OC3MM and PA-A1-OC3SMI ATM Port Adapters-The Asynchronous Transfer Mode (ATM) port adapters (PA-A1-OC3MM and PA-A1-OC3SMI) are available on Cisco 7200 series routers, on Cisco 7500 series routers, and on Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).



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

European Headquarters
Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtabouef Cedex
France
<http://www-europe.cisco.com>
Tel: 33 1 69 18 61 00
Fax: 33 1 69 28 83 26

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

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
<http://www.cisco.com>
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

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

Cisco Connection Online Web site at <http://www.cisco.com/offices>.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong • 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 • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela