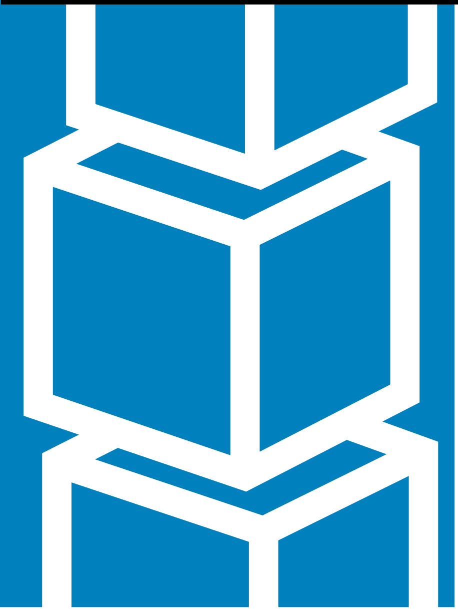
CISCO SYSTEMS

CISCO IOS LEARNING SERVICES



# The ABCs of Cisco IOS Software

# Networking the Enterprise

ABCs of Cisco IOS®

Understanding the Essentials Series

**Please direct comments to abcios@cisco.com**

**Take a quiz and find more information @ http://www.cisco.com/go/abc**

# Table of Contents

## Preface

Cisco IOS® Software, the industry-leading and most widely deployed network system software, delivers intelligent network services on a flexible networking infrastructure that enables the rapid deployment of Internet applications.

Developed and maintained by global engineering workforce, Cisco IOS Software constantly expands in capability and use. Customer requirements drive the capabilities of Cisco IOS Software.

To help customers choose and deploy the appropriate networking infrastructure, you must be familiar with the latest developments. To keep current, you need a broad, basic understanding of what Cisco IOS Software is, how it benefits customers, how it enables Internet business solutions, what it does, and how it is packaged and released.

This document is ideal for anyone seeking to understand the basics of Cisco IOS Software, but it is primarily targeted for technical audience within the enterprise market segment. If you have limited familiarity with this sophisticated, feature-rich software, or would just like a review, then The ABCs of Cisco IOS Software: Networking the Enterprise is for you.

You should read this document sequentially because each topic builds upon the preceding topics. This guide should not be considered the definitive guide for the network technologies that are part of Cisco IOS Software. Please refer to the reference section for further information.

## Cisco IOS Software for Enterprises

Today's new business requirements are network requirements. An e-commerce solution, for example, streamlines a vast array of transactions - ordering, pricing, billing, payment, and customer support - and brings them together into an integrated system. Similarly, a supply-chain solution integrates a business and its suppliers and partners into a single virtual enterprise.

To stay competitive, more and more businesses are using sophisticated Internet applications that rely on the advanced capabilities of Cisco IOS Software.

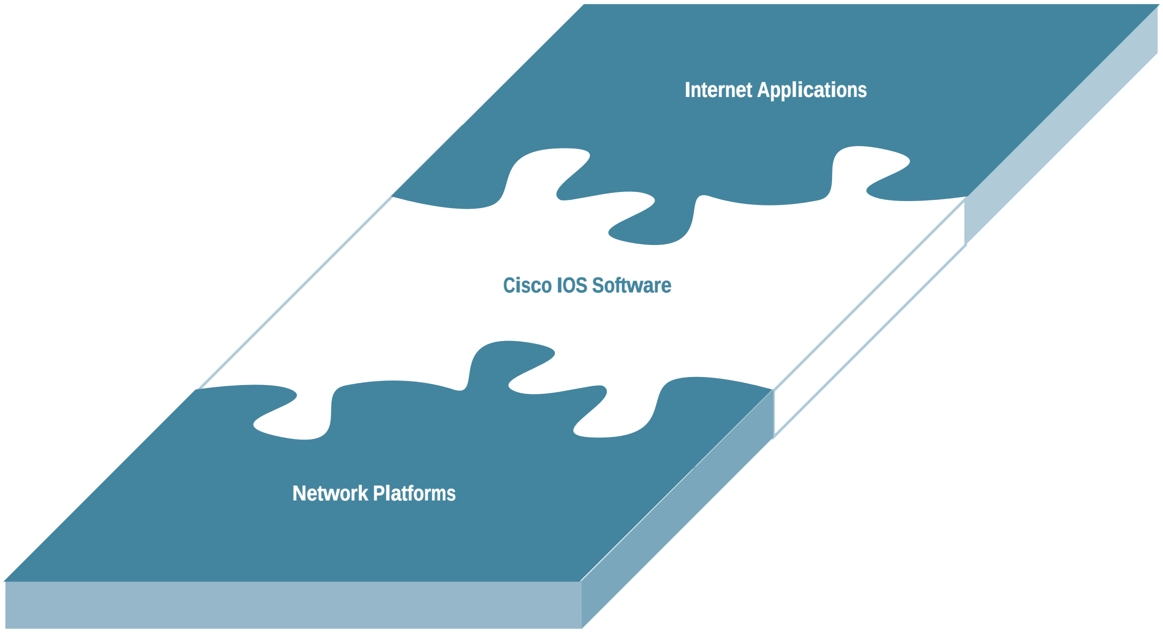
Cisco IOS Software provides a wide range of functionality from basic connectivity, security, and network management to technically advanced services that enable businesses to deploy applications such as real-time trading, interactive support, on-demand media, and unified messaging.

The functionality of Cisco IOS Software is the result of an evolution. First-generation networking devices could only store and forward data packets. Today, Cisco IOS Software can recognize, classify, and prioritize network traffic, optimize routing, support voice and video applications, and much more.

Cisco IOS Software runs on most Cisco routers and, increasingly, on Cisco switches. These network devices carry most of the Internet traffic today.

As shown in figure 1, Cisco network platforms and the Cisco IOS Software running on them are a unified system-one that is a firm foundation for building Internet applications.

Figure 1: Intelligent Network Services



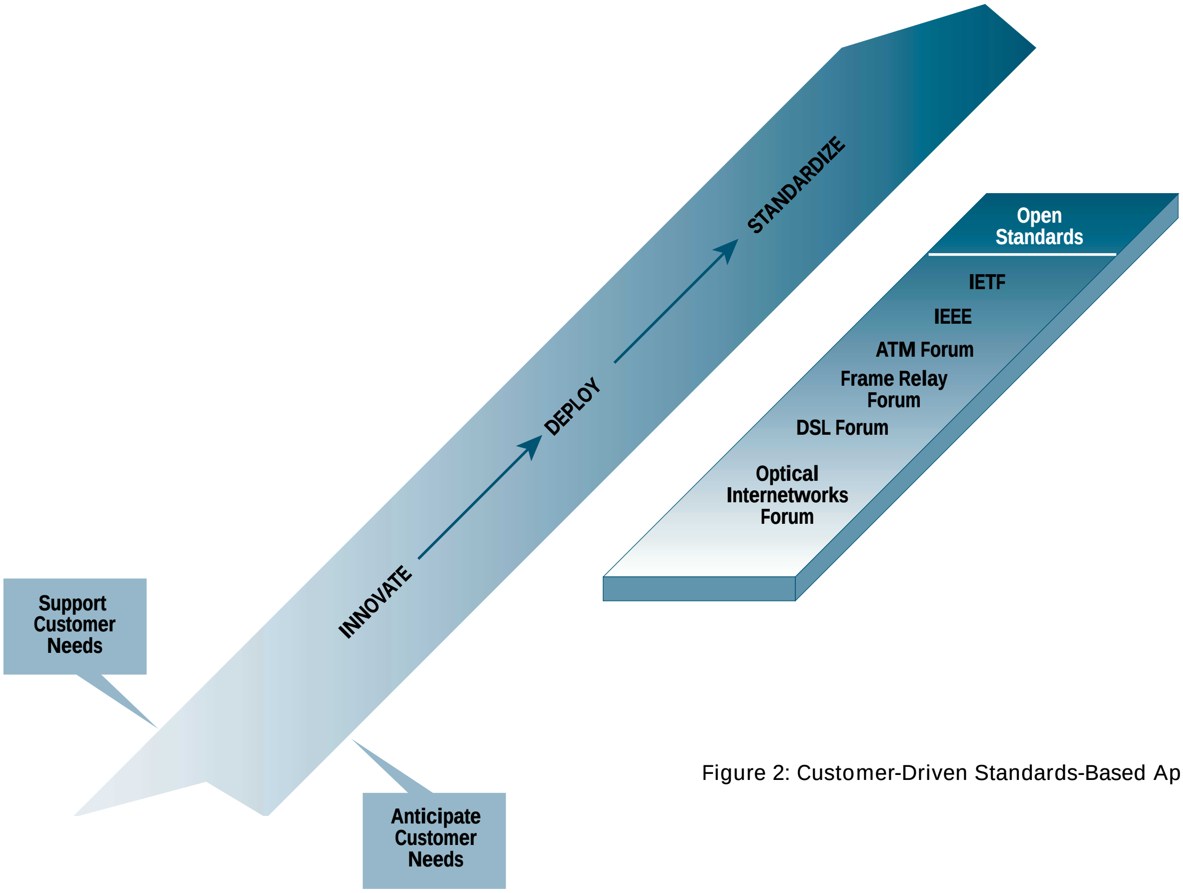


Figure 2: Customer-Driven Standards-Based Approach

Innovation usually starts by helping customers push the boundaries of networking technologies. As shown in figure 2, new and better ways of doing things shortly become open standards of the industry.

Cisco has a strong commitment to the spirit of openness, seen in its participation in virtually every industry group concerned with networking standards and in its willingness to share innovations with others. Cisco innovations often become new standards.

An outstanding example is the Border Gateway Protocol (BGP). Invented by a Cisco IOS Software engineer, it enables networks to integrate into a single Internet, scaling a network to millions of computers without breaking.

An innovative approach to packet forwarding, called Multiprotocol Label Switching (MPLS) has recently become an industry standard and is now making a major impact on networking. Pioneered by Cisco IOS Software engineers in 1997, it (like BGP) was introduced to improve real, complex customer networks.

Cisco IOS Software is based on open standards. More than 200 standards are implemented in Cisco IOS Release 12 alone. Please refer to the “References” section for information on the standards supported.

## Broadest Range of Platforms

One of the unique positions that Cisco enjoys in the industry is that Cisco IOS Software spans one connected world-from service providers to small and medium-sized businesses to enterprises to consumers. Because of the broad range of platforms that run Cisco IOS Software, customers can expect consistent network behavior and uniform delivery of applications and services.

In addition, customers have a lower cost of ownership. Because the Cisco IOS command-line interface (CLI) is consistent, it does not create a training burden when different hardware platforms are introduced into a company’s network.

### Multiprotocol Support

Cisco IOS Software is well-known for supporting many networking protocols, such as IP, Internetwork Packet Exchange (IPX), AppleTalk, DECnet, Systems Network Architecture (SNA), and so on, giving customers choices. Customers can use Cisco IOS Software with any kind of host and operating system environment, transitioning from one to another without changing Cisco networking devices. Multiprotocol support provides a future-proof solution, because new protocols such as IPv6 may have to be integrated in existing infrastructure.

### Broadest Industry Deployment

Cisco IOS Software runs on most of the Internet backbone. It is widely deployed by most of the enterprises and service providers worldwide.

### Global Pool of Cisco IOS Knowledge

A great many experienced technical people, partners, and a growing workforce worldwide are devoted to developing and deploying Cisco IOS Software.

As of June 2000, throughout the world there are more than 5000 Cisco Certified Internetworking Expert (CCIE™) certified professionals, more than 22,000 resellers, more than 1300 solutions partners, and 3700 Cisco Networking Academies in 64 countries.

## The IP Fabric of Cisco IOS Software

### What Is the Cisco IP Fabric?

Modern businesses depend on Internet Protocol (IP) technologies to deliver critical information to partners, suppliers, and customers. E-business relies on IP because IP is fault tolerant (self-healing) and it has proven scalability and broad reach.

The Internet Protocol (IP) fabric is the fundamental element in the Cisco IOS Software that delivers the availability, scalability, and connectivity that enterprises and service providers alike require for today's business applications.

The Internet protocols are the world's most popular open-system protocol suite because they can be used to communicate across any set of interconnected networks and are equally well suited for LAN and WAN communications. The Internet protocols consist of a suite of communication protocols: the Transmission Control Protocol (TCP) and IP.

The Internet Protocol is designed for use in interconnected systems of  packet-switched computer communication networks. (RFC 791). IP provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses. The internet protocol also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through "small packet" networks.

Cisco IOS software IP fabric improves open and efficiently processes IP headers to move traffic around the network. In other words, the IP fabric provides the basis for the advanced capabilities of Cisco IOS software, such as classifying and prioritizing network traffic.

Routing is the process of forwarding packets from one location to another. A routing protocol is a network layer protocol that interprets information in a network layer address to allow a packet to be forwarded to the destination address. Routing protocols are used between routers to determine paths and maintain routing tables.

### Benefits of Cisco IOS IP Routing

- Fast failure recovery (redundancy)
- Best-path routing
- Load balancing/sharing
- Scalability of hierarchical networks
- Address space aggregations and summarization

Please refer to the appendix for a brief discussion of Cisco IOS IP routing.

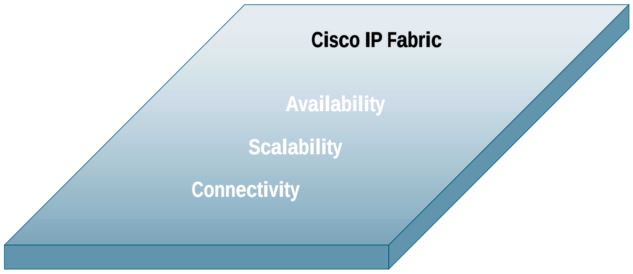


Figure 3: The Cisco IOS Software IP Fabric

### How Is Cisco IOS Software Increasing the Availability of Networks?

Today, when network downtime can cost millions of dollars per hour in lost revenue, high availability is essential. Availability is the proportion of total operating time that a network resource can be accessed successfully.

Ensuring availability depends on good design and providing redundant systems and links. If network traffic has at least one alternate route around any possible point of failure, then no single failure will prevent access to an application. Moreover, if traffic quickly finds an alternate route, the user won't notice any interruption in service.

In addition, given redundant systems and links, network devices can be taken off line one at a time without disrupting service. Consequently, network maintenance requires much less downtime.

Meanwhile, by means of load balancing, network traffic efficiently utilizes all available, alternate routes. Thus, even though redundant, all systems and links are fully used.

Cisco IOS Software includes many features that strengthen network availability. For example, Hot Standby Router Protocol (HSRP) (RFC 2281) brings resilience to the critical junction between hosts and backbone links. The HSRP features built in to Cisco IOS Software offer compelling nonstop networking by providing seamless fail-over.

Enhanced Interior Gateway Routing Protocol (EIGRP) provides superior convergence properties and operating efficiency for Layer 3 load balancing and backup across redundant links and Cisco IOS devices to minimize congestion.

### What about Increasing the Scalability of Networks?

Scalability refers to the ease with which the size of a network can be increased without fundamental changes in the architecture.

Cisco IOS Software includes several features that enhance scalability. Three that deserve special mention are Multi Protocol Label Switching (MPLS), Cisco Express Forwarding (CEF), and NetFlow.

MPLS uses labels to forward packets. Routers at the ingress edge attach a label to each packet after performing a conventional longest-match lookup on the IP header and then forward the packet. The labels indicate routes and service attributes. Core routers merely read the labels, perform appropriate services, and forward the packets according to the labels.

MPLS significantly decreases the cost of expanding a network because core routers forward data without doing Layer 3 table lookups. MPLS enables service providers and large enterprise customers to deploy a scalable IP-based solution for new services such as virtual private networks (VPNs), quality of service (QoS), and traffic engineering. MPLS fuses the intelligence of routing with the performance of switching to scale existing networks to meet future growth demands. With this technology, networks can handle more traffic, users, media-rich data, or bandwidth-intensive applications.

CEF increases performance by adopting a new caching mechanism that optimizes today's Internet traffic and enhances network scalability.

Although previous approaches to switching used the first packet in a flow to build an IP destination cache for subsequent packets to the same destination, CEF uses all available routing information to build an IP Forwarding Information Base (FIB). This allows a router to make a deterministic switching decision for any packet, even the first to a new destination, a scenario that is especially important because traffic flows in the Internet and enterprise intranets are becoming ever shorter and more dispersed.

Rapid growth in Internet and intranet deployment and usage has created a major shift in both corporate and consumer computing paradigms. The need has emerged for measurement technology to support this growth by efficiently providing the information required to record network and application resource utilization. Cisco NetFlow services provide solutions for each of these challenges.

NetFlow services in Cisco routing and switching platforms provide network traffic-accounting capabilities built in to the fast, optimum, and CEF switching paths. NetFlow Services capitalizes on the flow nature of traffic (unidirectional stream of packets between a given source and a destination---both being defined by network- layer (IP) address and transport-layer port number) in the network to provide detailed traffic accounting information with minimal impact on router/switch performance. NetFlow also efficiently processes access lists for packet filtering and security services. NetFlow data can be used for a variety of purposes, including network management and planning, enterprise accounting, departmental chargeback, usage-based billing, data warehousing/mining for marketing purposes, etc.

### How Is Connectivity Improved?

Connectivity refers to the degree to which users can access network applications, regardless of the locations of the users or the transmission media being used.

Cisco IOS Software supports every major protocol and type of physical medium, for end-to-end connectivity across IP and legacy networks. Cisco IOS WAN and dial connectivity software offers support for ATM, Frame Relay, X.25, ISDN, digital subscriber line (xDSL), cable, wireless, dial, Point-to-Point Protocol (PPP), VPN, and virtual private dialup network (VPDN) services. Within each technology area, Cisco has developed numerous value-added features to assist real-world customers. This breadth and depth of functionality provides a rich base of technology solutions. The major benefits of the Cisco IOS WAN technology include:

- Allowing networking connectivity over a variety of media and topologies
- Optimizing bandwidth utilization
- Providing scalability for large numbers of end users
- Interfacing with Cisco network-layer protocols
- Utilizing QoS  for voice/video/data integration
- Upgrading capability for network evolution so that users can easily scale or evolve their networks to a different WAN technology by installing new Cisco IOS Software releases.

Cisco has fully integrated all the Cisco IOS WAN Software features with network-layer protocols, providing seamless LAN-to-WAN connectivity and powerful bandwidth-optimization features that help customers reduce WAN costs—among the highest recurring costs of operating a WAN.

Cisco continues to maintain and improve Cisco IOS Software. New features to optimize cable technology, DSL, and wireless are among many emerging technologies that Cisco is integrating into Cisco IOS Software.

The major WAN technologies in Cisco IOS Software are discussed in the appendix.

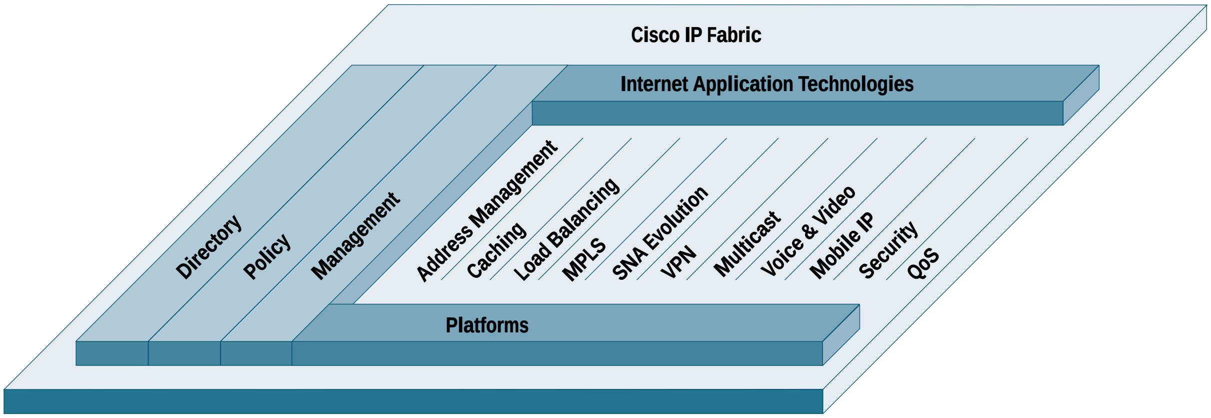
## Cisco IOS Software Intelligent Network Services

### What Are Intelligent Network Services?

Cisco IOS Software goes far beyond increasing the availability, scalability, and connectivity of IP-based networks.

Today’s Internet business solutions, such as e-commerce and workforce optimization, are propelling a major change in networking technology. Availability, scalability, and connectivity-vital as they are-are no longer enough. Now network traffic must be classified and the classes of traffic treated differently.

Figure 4: Cisco IOS Software Intelligent Network Services



Cisco IOS Software performs sophisticated classification, encoding, prioritization, and route selection of network traffic. Moreover, it recognizes a particular application as it requests network resources and ensures that the resources are provided.

We call these capabilities **intelligent network services**. By doing such things as handling voice or video over IP, integrating legacy systems, and ensuring privacy, they make today's demanding business applications possible.

As shown in figure 4, Cisco intelligent network services, the most comprehensive suite of network services available, run on the IP fabric and across a range of networking platforms.

Advanced policy systems, network directories, and management interfaces translate high-level business objectives into network configurations. A well-controlled and -managed network is functionally predictable and secure.

With Cisco intelligent network services in place, businesses can deploy next-generation Internet applications.

## Internet Applications

### What New Uses for the Internet Are Emerging?

As shown in figure 5, Cisco intelligent network services combine in various ways to support new Internet applications that make Internet business solutions possible.

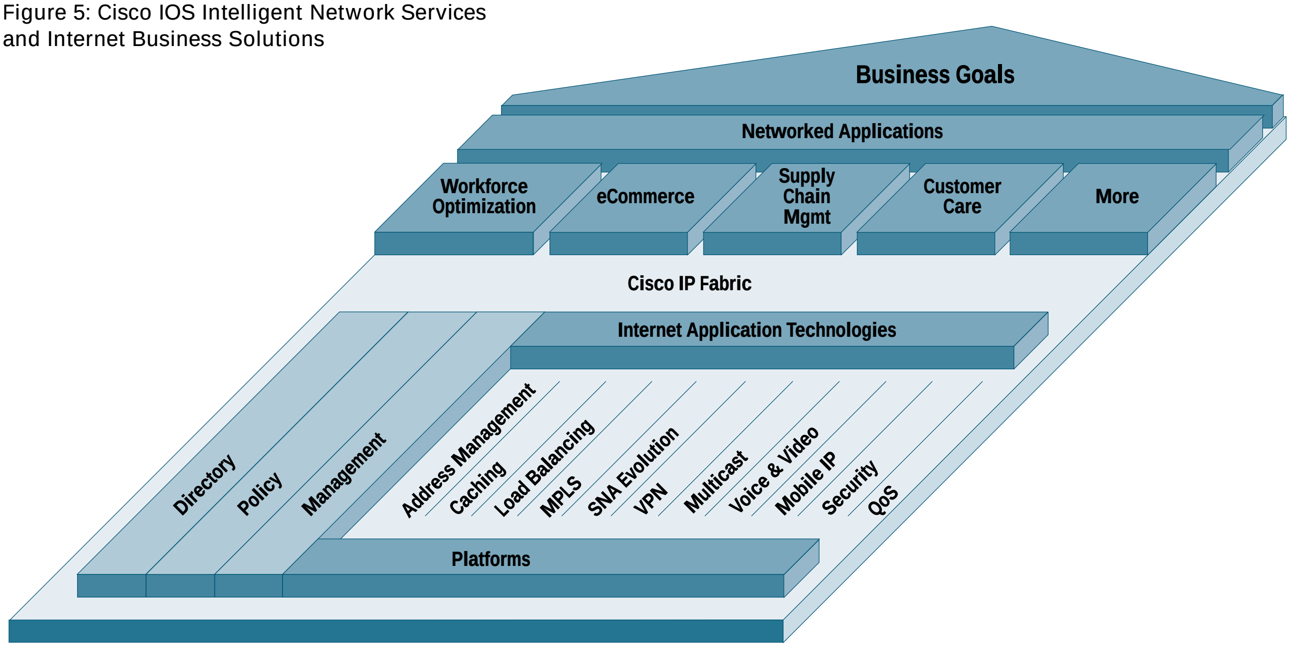
Examples of such applications include:

- Secure, cost-effective, multisite networking which is vital to the operations of many enterprises today, as they decentralize, expand globally, and implement supply-chain management systems.
- Secure real-time transactions that are critical for business solutions such as e-commerce and supply-chain management.
- Unified messaging, in which voice, video, and data traffic coexist in the network, contributes especially to workforce optimization, as well as customer-care solutions.
- Media on demand, the streaming of audio and video content over the Internet, plays a significant role in workforce optimization and e-learning.

To illustrate the power of Cisco IOS Software, the following paragraphs examine how Cisco intelligent network services support these emerging uses for the Internet. The "Internet Applications" section is followed by the key services that Cisco IOS Software provides.

Note: The mapping of intelligent network services to Internet applications is to show the relationship between the two. Network services categorized under certain Internet applications can be relevant to other Internet applications as well.

Figure 5: Cisco IOS Intelligent Network Services
and Internet Business Solutions



### Supply Chain Management

Supply-chain management (SCM) is the planning and control of the flow of goods and services, information, and money electronically back and forth through the supply chain. SCM allows the sharing of deep levels of inventory, forecasting, and logistical information to enable business partners to respond quickly and collectively to changing market conditions. Companies seeking to maintain or increase competitive advantage are looking for this greater depth of integration with their supply-chain partners.

Networked supply chains include everyone from the customer through all suppliers, and incorporate aspects of order fulfillment, product life cycle, and product service. The network infrastructure that connects the supply-chain constituents is the glue that holds the SCM system together. A successful SCM implementation requires the availability of several key network characteristics, including the following:

- **Interoperability**—SCM requires support for disparate network, application, and database assets.
- **Reliability**—Timely event routing requires fault tolerance and resiliency on the part of networks and servers.
- **Scalability**—A successful SCM implementation yields unprecedented growth in sales volume, orders, and deliveries across additional manufacturers, distribution centers, and retail outlets. At each point, the infrastructure must offer flexibility and scalability to support this growth.
- **Connectivity**—Are the suppliers connected via the Internet? If so, extranets and VPNs that support QoS, security, and manageability are paramount. Mobile users can access SCM applications via a number of Cisco IOS Software-based technologies.
- **Performance**—SCM applications analyze and process large volumes of data, so the interaction between the application server(s) and the remote database management system is highly intensive. Employing Cisco load-balancing solutions is crucial for SCM applications. Because SCM requires near-real-time decision making, the network must be instrumented with sophisticated QoS mechanisms. QoS mechanisms should be used to ensure that other application traffic does not negatively impact business-critical SCM transactions.
- **Manageability**—QoS and application performance must be monitored regularly. This requires network monitoring and analysis tools along with the ability to manage traffic flows.
- **Security**—Increased usage of the Internet for SCM functions requires comprehensive encryption and authentication mechanisms. SCM security demands confidentiality, authentication, and nonrepudiation.

As the SCM implementation matures, it expands from the organization's internal value chain to the external supplier, distribution channel, and buyer value systems. To effectively share with partners to create a networked supply chain, companies need a scalable, standards-based infrastructure, including network and integration packages.

### Customer Care

The New Internet Economy is not just about marketing Web sites or selling goods and services on line. It's about a totally revolutionized approach to interacting with customers: complete, consistent care for all customer needs throughout the relationship life cycle across all business functions, all contact points, and all communications media.

Because the cost of acquiring new customers greatly exceeds the cost of retaining even the best customers, enterprises must aggressively target and retain their most attractive customers. This requires them to shift focus away from simply gaining market share (product-centric view) or increasing share of the customer wallet (customer-centric view) to a new business paradigm: one focused on a relationship-centric view measured by the customer lifetime value.

In the face of these business and application challenges, one point emerges clearly: the network must become a utility. The concept of value over time, which is inherent in Customer Relationship Management, implies creating excellent and constantly improving customer service. To support this goal, the network infrastructure must be constantly available, flexible, and secure.

When customer needs change, business software must adapt to the new environment. The network must, therefore, be able to support, or adapt to support, new application demands. Intelligent Network Services such as QoS, VPNs, security options, caching, voice, and video services and load balancing increases the flexibility, adaptability, and overall availability of the network.

### E-Learning

The ability to use corporate networks to teach, train, collaborate, and communicate—any time, anyplace—is changing the way companies learn, operate, and compete. Sometimes called distributed training or e-learning, these applications have helped leading organizations achieve quantifiable, bottom-line business benefits: reduced cycle times, more rapid product introductions, increased operating efficiency, rapid acquisition of new competencies and skills for employees and even customers or business partners, and better relationships with customers.

E-learning is one of the most prominent applications benefiting from the convergence of network technologies. Convergence is a term used to describe the integration of many types of information—voice, video, text, graphics, images, and traditional alphanumeric data—onto the same network. The simplest e-learning application may be nothing more than a set of PowerPoint slides, viewed with audio explanations, that is accessed on the World Wide Web. Here, simple graphical data in the form of slides is augmented by a modest low-bandwidth audio stream of a few kilobits per second (kbps). At the high end, e-learning applications may be based on two-way, full-motion video and voice streams interconnecting several remote locations and corporate desktops. With each video stream consuming between a few hundred kilobits and several megabits per second (Mbps), this application places special requirements on the network.

An e-learning solution requires an environment with a solid network foundation that is scalable to address the growth of users, highly available to meet their demands, and secure to ensure confidentiality when necessary. To meet these requirements, Cisco IOS Software provides intelligent network services such as the following:

- **IP multicast**—The use of multicast technology enables a single video stream to be delivered to multiple recipients, and thus conserve network bandwidth. This is especially important across bandwidth-limited wide-area network links.
- **Voice and video**—These services allow enterprises to deliver e-learning applications over a single networking infrastructure.
- **QoS**—Using more sophisticated QoS mechanisms ensures that the important voice and video data gets through the WAN with as few problems as possible.

### Workforce Optimization

Workforce optimization is all about taking advantage of Internet technologies to maximize people's time so they can focus on the core value of their job. A truly optimized workforce has all the information needed to do the job, as well as the tools required to get the job done most efficiently.

Workforce-optimization applications streamline processes to reduce or eliminate time-consuming administration. At the same time, workforce-optimization applications also provide the right information at the right time to enable the "learning organization," one that can quickly influence employees and react to market conditions.

Cisco IOS intelligent network services that supports workforce optimization-related applications include mobile IP, VPN, caching, and voice and video services.

## Cisco IOS Security Services

### What Are Security Services?

The ability to take advantage of the security services of Cisco IOS Software is crucial to running a highly effective and robust Cisco network. Security services enforce an organization's policies and safeguard networks against misuse. Following are the key security services provided by Cisco IOS Software:

#### Access Control Lists

As the name implies, access control lists (ACLs) are commonly used as security filters to block traffic from entering or exiting parts of the network. The access list is a key Cisco IOS feature whose programming syntax is used across many Cisco features. Cisco has extended the ACL syntax to other features such as routing and routing filters, packet classification for QoS  and queuing, encryption, and dial-on-demand routing.

The most popular use of ACL is for filtering traffic on a router interface. ACL allows defining the traffic that one wants to permit or deny through an interface. The router inspects the traffic flowing through the interface and rejects the packets that are denied by the access list. For IP there are two types of access lists. Standard IP ACL filters packets based on their source address. Extended IP ACL enables one to build more elaborate rules for filtering than do standard access lists. Extended access lists can match on source address, destination addresses, protocol (TCP, User Datagram Protocol [UDP], EIGRP, Open Shortest Path First [OSPF], and so on), protocol-specific options (Telnet, File Transfer Protocol ([FTP], HTTP, SNMP and so on), precedence level and type of service (TOS). Besides access list for IP, there are access list for filtering such protocols as IPX, AppleTalk, DECnet and so on).

### Authentication, Authorization, and Accounting

Authentication validates a user's identity. Authorization limits what a user is allowed to do on the network, usually defined by a profile for the user or a group to which the user belongs. Accounting tracks what a user is doing or has done on the network. Authentication, authorization, and accounting (AAA) plays an important role in providing services to road warriors, telecommuters, and other remote users to access the network from anywhere and at anytime.

Security software on servers and clients work in conjunction with Cisco IOS Software to deliver the AAA capabilities. In the Cisco IOS network, the following popular services are supported by AAA:

- Connectivity (dialup, Internet, wireless) for remote users who want to join the private network with functionality similar to what is available in the office; as an example, a user who dials the private network with a modem to run e-mail and Web applications
- Logins for networking personnel who need to access the Cisco IOS command prompt (EXEC prompt) and monitor or configure Cisco devices

The AAA server and the router converse over the network with a protocol specially designed for exchanging security information. The two most prevalent security protocols are Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System (TACACS+). Cisco IOS Software supports both protocols.

### IP Security

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

IPSec provides security services such as confidentiality, integrity, origin authentication, and antireplay. IPSec is a fairly large collection of technologies that encompasses network and security protocols, cryptographic algorithms, and recommendations. In particular, IPSec uses:

- Diffie-Hellman key exchange for deriving key material between peers on a public network
- Public key cryptography for signing the Diffie-Hellman exchanges to guarantee the identity of the two parties and avoid man-in-the-middle attacks
- Bulk encryption algorithms, such as Data Encryption Standard (DES), for encrypting the data
- Keyed hash algorithms, such as HMAC, combined with traditional hash algorithms such as Message Digest 5 (MD5) or secure hash algorithm (SHA) for providing packet authentication
- Digital certificates signed by a certificate authority to act as digital ID cards

Cisco IOS Software provides an extensive implementation IPSec.

### Cisco IOS Firewall

A firewall is a set of hardware and software implemented at a particular spot on a network infrastructure to enforce the organization's security policy.

The Cisco IOS Firewall adds practical, state-of-the-art firewall technology to Cisco IOS Software-based routers. As an integrated solution, it takes advantage of what a customer already owns (a perimeter router) and understands (Cisco IOS Software), to simplify ownership and management considerations. As software, it is inexpensive, readily configurable, and easily upgraded. The Cisco IOS Firewall Feature Set is an optional, add-on software license for Cisco routers that provides firewall functionality integrated in an Cisco IOS Router.

The Cisco IOS Firewall Software incorporates a multitude of powerful security features, including:

- **Context-based access control (CBAC)**—secure, per-application-based access control for all traffic across perimeters such as those between private enterprise networks and the Internet; CBAC thwarts most attempts at "port scanning"

- **Intrusion detection**—real-time monitoring, interception, and response to network misuse; a broad set of the most common attack and information-gathering intrusion-detection signatures
- **Authentication prox**y—dynamic, per-user authentication and authorization for LAN-based and dial-in communications
- **Denial-of-service detection and prevention**—defends and protects router resources against common attacks (packet headers are checked; suspicious packets are dropped)
- **Dynamic port mapping**—network administrators can run CBAC-supported applications on nonstandard ports
- **Java applet blocking**—protects against unidentified, malicious Java applets
- **VPNs, IPSec encryption, and QoS support:**
  - Operates with Cisco IOS Software encryption, tunneling, and QoS features to secure VPNs
  - Provides scalable encrypted tunnels on the router while integrating strong perimeter security, advanced bandwidth management, intrusion detection, and service-level validation
  - Based on standards for interoperability
- **Real-time alerts**—logs alerts for denial-of-service attacks or other preconfigured conditions; now configurable on a per-application, per-feature basis
- **Audit trail**—details transactions; records time stamp, source host, destination host, ports, duration, and total number of bytes transmitted for detailed reporting; now configurable on a per-application, per-feature basis
- **Event logging**—enables administrators to track potential security breaches or other nonstandard activities in real time by logging system error message output to a console terminal or syslog server, setting severity levels, and recording other parameters
- **Firewall management**—wizard-based network configuration tool that offers step-by-step guidance through network design, addressing, and Cisco IOS Firewall security policy configuration; also supports Network Address Translation (NAT) and IPSec configurations
- **Integration with Cisco IOS Software**—inter-operates with Cisco IOS features, integrating security policy enforcement into the network
- **Basic and advanced traffic filtering:**
  - Standard and extended ACLs apply access controls to specific network segments and define which traffic passes through a network segment.
  - Lock and Key dynamic ACLs grant temporary access through firewalls upon user identification (username/password).
- **Policy-based multi-interface support**—provides ability to control user access by IP address and interface as determined by the security policy
- **Network Address Translation**—hides internal network from the outside for enhanced security
- **Time-based access lists**—defines security policy by time of day and day of week
- **Peer router authentication**—ensures that routers receive reliable routing information from trusted sources

### Cisco IOS Firewall Feature Set and Cisco PIX Firewall

At many points in the network design, choices need to be made between using integrated functionality in a network device (Cisco IOS Firewall feature set) versus using a specialized functional appliance (PIX™ Firewall). The integrated functionality is often attractive because it can be implemented on existing equipment or because the features can inter-operate with the rest of the device, thereby providing a better functional solution. Appliances are often used when the depth of functionality required is very advanced or when performance requirements dictate the use of specialized hardware. Choices must be made each time based on the capacity and functionality of the appliance versus the integration advantage of the device.

## Cisco IOS Quality of Service

A communication network forms the backbone of any successful organization. These networks transport a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. The bandwidth-intensive applications stretch network capabilities and resources, but also complement, add value, and enhance every business process. Networks must provide secure, predictable, measurable, and sometimes guaran-

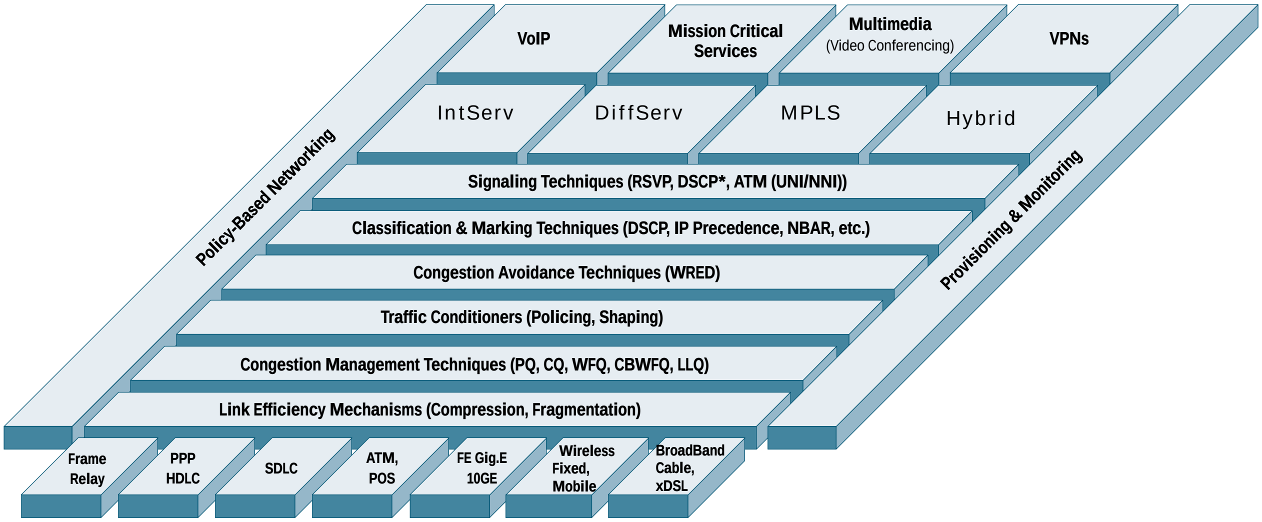

VoIP
Mission Critical Services
Multimedia (Video Conferencing)
VPNs
IntServ
DiffServ
MPLS
Hybrid
Policy-Based Networking
Provisioning & Monitoring
Signaling Techniques (RSVP, DSCP*, ATM (UNI/NNI))
Classification & Marking Techniques (DSCP, IP Precedence, NBAR, etc.)
Congestion Avoidance Techniques (WRED)
Traffic Conditioners (Policing, Shaping)
Congestion Management Techniques (PQ, CQ, WFQ, CBWFQ, LLQ)
Link Efficiency Mechanisms (Compression, Fragmentation)
Frame Relay
PPP HDLC
SDLC
ATM, POS
FE Gig.E 10GE
Wireless Fixed, Mobile
BroadBand Cable, xDSL

Figure 6: End-to-End Quality of Service Framework

teed services to support business processes. Achieving the required QoS by managing the delay, jitter, bandwidth, and packet-loss parameters on a network becomes the secret to a successful end-to-end business solution. (Latency is the delay that traffic experiences as it travels across the network;  jitter is the variation in latency over time.)

Different applications have different requirements with respect to bandwidth, latency, and jitter. Time-sensitive applications, such as online transactions or voice transmission (over IP), may not require high bandwidth, but they are sensitive to delay and jitter. Alternatively, an FTP file transfer may require considerable bandwidth, while easily tolerating delay. Certain mission-critical applications may require high bandwidth with little delay.

QoS refers to the ability of a network to provide better service to selected network traffic over various underlying technologies including Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, Synchronous Optical Network (SONET), and IP-routed networks that may use any or all of these underlying technologies.

## End-to-End QoS Models

As shown in figure 6, end-to-end QoS is the ability of the network to deliver service required by specific network traffic from one end of the network to another. Cisco IOS QoS supports the following types of service models:

- **Integrated service or IntServ**—An IETF standard, in this model the application requests a specific kind of service from the network before sending data.
- **Differentiated service or DiffServ**—Also an IETF standard, in this model the network tries to deliver a particular kind of service based on the QoS specified by each packet. Typically, this service model is appropriate for aggregate flows because it performs a relatively coarse level of traffic classification.

## Key Benefits of QoS

- **Manage network resources**-One can have control over which resources (bandwidth, equipment, wide-area facilities, and so on) are being used. For example, limit bandwidth consumed over a backbone link by FTP transfers or give priority to an important database access. QoS allows networks to be more predictable and use the network resources in a manner that benefits business processes.

- **Tailored services**—The control and visibility provided by QoS enables Internet service providers (ISPs) to offer carefully tailored grades of service differentiation to their customers.

- **Coexistence of mission-critical applications**—Cisco QoS features ensure that WAN links are used efficiently by mission-critical applications that are most important to the business; that bandwidth and minimum delays required by time-sensitive multimedia and voice applications are available; and that other applications using the link get their fair service without interfering with mission-critical traffic.

### Cisco IOS QoS Technology

The Cisco IOS QoS tools are divided into six main categories:

- **Classification and Marking**—Packet classification features allow traffic to be partitioned into multiple priority levels or classes of service. Packets can be classified based on the incoming interface, source or destination addresses, IP protocol type and port, application type (network-based application recognition [NBAR]), IP Precedence or differentiated-service-code-point (DSCP) value, 802.1p priority, MPLS EXP field, and other criteria. Marking is the QoS feature component that 'colors' a packet (frame) so it can be identified and distinguished from other packets (frames) in QoS treatment. Policies can then be associated with these classes to perform traffic shaping, rate-limiting/policing, priority transmission, and other operations to achieve the desired end-to-end QoS for the particular application or class.
- **Congestion management**—Congestion-management features operate to control congestion after it occurs. Queuing algorithms are used to sort the traffic and then determine some method of prioritizing it onto an output link. Congestion-management techniques include, Weighted Fair Queuing (WFQ), Class-Based Weighted Fair Queuing (CBWFQ), Low-Latency Queuing (LLQ), which is especially suited for voice over IP (VoIP), and the high-performance Modified Deficit Round Robin (MDRR) available on the Cisco 12000.
- **Congestion avoidance**—Congestion-avoidance techniques monitor network traffic loads in an effort to anticipate and avoid congestion at common network and inter-network bottlenecks before it becomes a problem. A Weighted Random Early Detection (WRED) algorithm avoids congestion and controls latency at a coarse level by establishing control over buffer depths on both low- and high-speed data links.
- **Traffic conditioning**—Traffic entering a network can be conditioned (operated upon for QoS purposes), by using a policer or shaper. Traffic shaping involves smoothing traffic to a specified rate by the use of buffers. A policer, on the other hand, does not smooth/buffer traffic. It simply remarks (IP Precedence/DSCP), transmits, or drops the packets, depending on the configured policy. Committed access rate (CAR, the Cisco implementation of a policer) lets network operators define bandwidth limits and specify actions to perform when traffic conforms to, exceeds, or completely violates the rate limits. Generic traffic shaping (GTS, the Cisco implementation of a shaper) provides for a mechanism to control traffic by buffering it and transmitting at a specified rate. Frame Relay traffic shaping (FRTS) provides mechanisms for shaping traffic based on Frame Relay service parameters such as the committed information rate (CIR) and the backward explicit congestion notification (BECN) provided by the Frame Relay switch.
- **Signaling**—End stations or network nodes can use Resource Reservation Protocol (RSVP) to request special handling of certain traffic. Cisco QoS supports both controlled-load and guaranteed-rate signaling in full conformance with the IETF standards. This capability in routers and switches allows the efficient construction of VoIP and video-over-IP services. Cisco RSVP adds further value by performing robust admission control and synchronization with H.323 signaling for VoIP. A call is completed only if the resources are available for it, ensuring that a call coming into a network does not bump or affect the quality of existing calls.
- **Link efficiency mechanisms**—Two-link efficiency mechanisms work in conjunction with other QoS features to maximize bandwidth utilization. Newer multimedia application traffic such as packetized audio and videos are in Real-Time Transport Protocol (RTP) packets, and Cisco IOS Software saves on link bandwidth by compressing the RTP header (Compressed Real-Time Protocol [cRTP]). To decrease latency and jitter for interactive traffic, link fragmentation and interleaving (LFI) breaks up large datagrams and interleaves delay-sensitive interactive traffic with the resulting smaller packets.

### Cisco IOS VPN Service

Enterprises often connect remote, branch, and main offices by using private, leased-line networks with Frame Relay or ATM. Although these networks are secure and easily managed, they are expensive.

A secure, scalable, and more cost-effective alternative is to use a VPN. By making encrypted connections ("tunnels") between two points over the Internet, a public network, a VPN provides the same security and performance as a private, leased-line network-without the high cost. Site-to-site VPNs are best constructed by using Cisco VPN-optimized routers at each site.

Critical Cisco IOS VPN services include:

- **Tunneling**—Some key features are Layer 2 Tunneling Protocol (L2TP), IPSec, Layer 2 Forwarding (L2F), Point-to-Point Tunneling Protocol (PPTP), generic routing encapsulation (GRE), and MPLS.
- **Encryption and security**—Key features include IPSec (DES and Triple DES [3DES]) and MPPE encryption.
- **VPN resiliency**—Cisco IOS Software provides tunnel keepalives, tunnel endpoint discovery (TED), and dynamic route discovery (via GRE tunnels) for unsurpassed dynamic recovery.

By delivering a comprehensive VPN solution in a single device, Cisco VPN-optimized routers ensure greater interoperability of different services such as security, QoS, and tunneling/encryption than multidevice solutions offered by competitors.

### Cisco IOS Address-Management Services

Mobility in the workforce-telecommuters coming aboard, moving, or leaving and many mobile workers-raises another problem: keeping track of who is doing what on the corporate network. IT organizations everywhere are struggling to meet this ballooning demand for remote connectivity and to deal with the resulting increases in network complexity and end-user support costs. At the same time, IT must support growing branch-office connectivity. Particularly in organizations growing through acquisition or merger, the ability to rapidly integrate separate and frequently incompatible infrastructures can be critical to the success of business relationships. Meanwhile, regional registries as well as ISPs exercise a strict control on address allocation, making it difficult to obtain a large block of registered IP addresses. So, there is a clear need for address-management services that conserve addresses and simplify their management.

These services allow network administrators to build self-configuring addressing systems and to bind users to network addresses in a dynamic fashion.

One such service of Cisco IOS Software is Network Address Translation (NAT).

On its own network, an organization might have private IP addresses, invalid Internet addresses, or even addresses that “belong” to another organization. NAT, functioning on a router that connects the organization’s internal network to the external Internet, translates the organization’s addresses into valid, routable Internet addresses and vice versa. NAT is one-to-one IP address mapping.

Closely related to NAT, Port Address Translation (PAT) provides a means to reduce the number of registered IP addresses an organization may require. PAT can associate a large number of internal addresses to a single external address and distinguish between them by associating each with a unique port number on the external address. PAT is many-to-one address mapping.

Another important Cisco IOS feature, Dynamic Host Configuration Protocol (DHCP) server, supports both DHCP and BOOTP clients. In addition, it supports automatic and manual address allocation, as well as finite and infinite address lease periods. Cisco IOS Software also supports intelligent DHCP relay functionality. Generally speaking, a DHCP relay agent is any host that forwards DHCP packets between clients and servers. A DHCP relay agent enables the client and server to reside on separate subnets. If the Cisco IOS DHCP server cannot satisfy a DHCP request from its own database, it can forward the DHCP request to one or more secondary DHCP servers defined by the network administrator via standard Cisco IOS “ip helper-address” functionality.

Cisco IOS Easy IP enables transparent and dynamic IP address allocation for hosts in remote environments via DHCP, reduces router configuration tasks via dynamic PPP/Internet Protocol Control Protocol (IPCP) address negotiation, conserves IP addresses via PAT, and minimizes Internet access costs for remote offices.

IP version 6 (IPv6) architecture (RFC 2460), also known as IP Next-Generation (“IPng”), by greatly increasing the availability of network addresses, is intended to scale the Internet. IPv6 increases the IP address size from 32 bits to 128 bits, to introduce some levels of addressing hierarchy, a much greater number of addressable nodes, and simpler auto-configuration of addresses.

Cisco IOS IPv6 supports the stateless address auto-configuration mechanisms such as defined in RFC 2462. A Cisco router configured with IPv6 will advertise its IPv6 prefix(es) on one or more interfaces, allowing IPv6 clients to auto-configure their address(es).

Cisco is taking a leadership role in delivering comprehensive IPv6 services that integrate features based on experience gained from the current IP, Version 4. Integration and coexistence of the IPv6 protocols in today’s IPv4 Internet are keys to building the new generation of network appliances.

### Cisco IOS Mobile IP Services

The mobile workforce needs the ability to communicate with customers, partners, and fellow workers anywhere, anytime and have access to relevant business applications, tools to carryout business effectively. Enterprise mobility is about providing ubiquitous connectivity to the mobile user, independent of the devices and access technologies.

Mobile IP, an IETF standard (RFC 2002), allows a host device to be identified by a single IP address even though the device may move its physical point of attachment from one network to another.

Regardless of movement between different networks, connectivity at the different points is achieved seamlessly without user intervention. Roaming from a wired network to a wireless or wide-area network is also done with ease. Mobile IP provides ubiquitous connectivity for users-whether they are within their enterprise networks or away from home. Mobile IP is part of both IPv4 and IPv6 standards. Cisco Systems has been supporting mobile IP in Cisco IOS Software Releases 12.0(1)T and beyond.

Mobile IP is the first protocol to offer such transparent mobility.

### Cisco IOS Legacy and SNA Integration Service

Even today—in this time of personal computers and the Internet-vast amounts of business data are stored and processed by mainframe computers.

For many organizations (such as stock markets), legacy systems are vital to their business operations. In deploying an Internet application, these businesses must integrate their legacy systems with IP networks, for two main reasons:

- The business logic in the mainframe applications is not easily divorced from how the raw data is stored.
- The information in the legacy systems is useful to a broader audience, in a wider set of circumstances, than when the mainframe applications were created.

Implemented in more than half a million routers, Cisco Data-Link Switching Plus (DLSw+) is the leading solution for integrating SNA and IP networks. Moreover, DLSw+ enables SNA or NetBIOS systems to communicate regardless of the underlying physical media.

Fully compliant with RFCs 1795 and 2166, DLSw+ includes Cisco extensions to guarantee QoS, enhance availability, and improve scalability. It also offers extensive Management Information Bases (MIBs) and easy-to-use management tools.

### Cisco IOS Load-Balancing Service

Enterprises that rely on the Internet for real-time transactions or mission-critical business functions demand the highest levels of availability. Availability is closely tied to network capacity.

Increasing content-delivery capacity is typically achieved by clustering servers—connecting them together to work as if they were one. Load-balancing capabilities in Cisco IOS Software make the most efficient use of available capacity by directing network traffic to clusters of servers or single servers, depending on the load on each system.

Clustering servers and balancing the traffic load offer major advantages:

- **Scalability**—Clustering servers is especially scalable because any particular user's working session, when linked to a cluster, is bound to one machine. There is little need to share resources within a cluster.
- **Nondisruptive growth**—Machines can be added to a cluster without disrupting work that is executing on the other machines.
- **Load distribution**—Directing network traffic to systems by accounting for the present load on those systems avoids wasting capacity on some systems while overloading others.
- **Continuous availability**—An instance of an application or an individual machine can fail (or be taken down for maintenance) without shutting down service to end users. Users are unaware of a failure because they are simply reconnected to an alternate image.

Various mechanisms are currently available to achieve the above advantages; some of them are running on specific hardware devices such as Cisco CSS1100 or Local Director, and some of them have been fully or partially integrated into Cisco IOS Software.

MultiNode Load Balancing (MNLB) is an IP server load-balancing solution that distributes load-balancing capabilities across any number of routers, enabling the highest levels of availability, scalability, and performance for server applications. MNLB consists of software running on Cisco routers and switches, Cisco Local Director, and application server platforms.

Using server load balancing (SLB), a network administrator defines a virtual server to represent a group of real servers. Clients are configured to connect to the IP address of the virtual server. That address is configured as a loopback address, or secondary IP address, on each of the real servers. When a client initiates a connection to the virtual server, the Cisco IOS SLB function chooses a real server for the connection based on a configurable load-balancing algorithm.

Servers provide input into the IP load-balancing decisions by means of the Dynamic Feedback Protocol (DFP), indicating the level of CPU utilization, application, and user identity.

### Cisco IOS Voice and Video Services

Cisco IOS Software provides the technologies that enable the consolidation of voice and video over data onto a single IP network. This convergence of voice, video, and data allows enterprises and service providers to create a single, powerful network that is far easier and less expensive to manage and operate than individual networks for different media types.

Cisco AVVID (Architecture for Voice, Video and Integrated Data) provides customers with the tools required to evolve their disparate data, voice, and video networks into a single converged infrastructure. The primary goal of this evolution is to enable customers to benefit from next-generation New World applications such as unified messaging, virtual contact centers, and virtual intelligent assistants.

A combination of different Cisco products-hardware and software and ecosystem partner applications together provide the Cisco AVVID solution to the customers. Cisco IOS Software plays the major role of providing the IP fabric and the intelligent network services such as QoS, to prioritize mission-critical and voice traffic and voice features such as the various signaling protocols.

Cisco IOS Software intelligent services that make VoIP possible include:

- Compression/decompression algorithms (codecs) that allow voice data to be squeezed into a fraction of the space used by traffic in traditional telephone circuits
- Standards-based protocols for call control such as H.323, the Simple Gateway Control Protocol (SGCP), the Media Gateway Control Protocol (MGCP), and the Session Initiation Protocol (SIP)
- QoS functionality such as LLQ, which provides priority queuing for voice traffic to reduce delay and jitter (voice-bearer traffic is transported by the RTP); CBWFQ, cRTP, and LFI are additional features that provide QoS that voice requires

Cisco IOS voice services also includes voice-over-Frame Relay (VoFR) features such as FRF.11 and FRF.12 and voice-over-ATM (VoATM) features such as ATM adaptation layer 5 (AAL5).

Cisco IOS Software also supports a rich set of PBX/Public Switched Telephone Network (PSTN) signaling protocols that allow Cisco IOS gateways to connect to the Old World time-division multiplexing (TDM) networks. These signaling protocols include foreign exchange station (FXS), foreign exchange office (FXO), receive and transmit (E&M), Basic Rate Interface (BRI), T1/E1 Primary Rate Interface (PRI), T1/E1 QSIG, E1 R2, analog direct inward dial (DID), T1 channel-associated signaling (CAS), E1 CAS, and so on. Cisco IOS Software provides features that supports the Signaling System 7 (SS7) voice solution.

As with VoIP, transmitting video traffic relies on codecs and enhanced QoS services.

The Cisco Multimedia Conference Manager (MCM) is a Cisco IOS Software feature set that enables IP networks to support secure, reliable H.323 videoconferencing, with advanced QoS capabilities. The MCM functions as a high-performance H.323 gatekeeper and proxy, allowing network managers to control bandwidth and priority setting for H.323 videoconferencing services based on individual network configurations and capacities. These capabilities ensure appropriate allocation of network resources for videoconferencing as well as other critical applications running simultaneously on the network. The Cisco MCM combines H.323 gatekeeper/proxy with packet routing on a single hardware platform to support reduced costs, ease of management, and integrated IP services for video and voice.

Video traffic consumes much more network capacity than voice traffic, and it does so for longer periods of time. On the other hand, unlike voice traffic, which is mostly real-time and conversational, most video traffic is stored and then viewed on demand.

### Cisco IOS IP Multicast Services

Frequently, in a media-on-demand environment, media are streamed to a group of individuals, all receiving the same content at the same time. How can this be done most efficiently?

Unicast transmission sends one copy of each packet to each member of the group. This is inefficient because the same information must be carried multiple times, requiring extra bandwidth. During a broadcast transmission, each host on the network, even if not interested in the information, must process the broadcast packets. Consequently, network resources are significantly burdened.

The best approach is to use IP multicast, a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients and homes.

Multicast opens a world of possibilities and real advantages:

- **New distributed applications**—Multicast routing makes multimedia applications on the Internet (such as distance learning and videoconferencing) scalable, reliable, and efficient.
- **Network cost savings**—Utilizing IP multicast conserves bandwidth and reduces server and network processing.
- **Increased workforce productivity**—Employees who are separated by large distances from each other find new ways to collaborate by videoconferencing rather than traveling, thus saving time and money.
- **Increased competitivenes**s—IP multicast enables enterprises and ISPs to offer new services-such as streaming media-that are not feasible with unicast transport.
- **Very high scalability**—The number of participants can grow without a corresponding increase in the load on the server that originates the transmission.
- **Increased availabilit**y—Because multicast transmission is much more efficient than unicast or broadcast transmission, much less network congestion occurs and many more users have simultaneous access to applications.

### What Are the General Kinds of Multicast Applications?

There are three general categories of multicast applications:

- **One to many**—A single host sends data to two or more receivers. Examples are database updates, finance applications, live concerts, news feeds, push-media, caching, and training and corporate communications.
- **Many to one**—Two or more receivers send data back to a sender (a source). Examples include auctions, polling, and data collection.
- **Many to many**—Also called N-way multicast, it consists of any number of hosts sending to the same multicast group address, as well as receiving from it. Examples are distance learning, collaboration, multimedia conferencing, multiplayer games, and chat groups.

### What Are the Multicast Technologies?

Multicast is based on the concept of a group. An arbitrary group of receivers expresses an interest in receiving a particular data stream. This group does not have any physical or geographical boundaries—the hosts can be located anywhere on the Internet. Hosts that are interested in receiving data flowing to a particular group must join the group using Internet Group Management Protocol (IGMP). Hosts must be a member of the group to receive the data stream.

To support IP multicast, the sending and receiving nodes intermediate routers and the network infrastructure between them must be multicast enabled. In deploying IP multicast as an end-to-end solution, the following areas need to be considered:

**Addressing**—Multicast addresses specify an arbitrary group of IP hosts that have joined the group and wish to receive traffic sent to this group. In addition, there must be a way of mapping this address onto Layer 2 multicast addresses of the underlying physical networks. For IP networks, Class D addresses have been set aside for multicast addressing. This address range is only for the group address or destination address of IP multicast traffic. The source address for multicast datagrams is always the unicast source address. The IEEE LAN specification (802.3 standard) makes provisions for the transmission of broadcasts or multicast packets. For mapping IP multicast addresses to Ethernet addresses, the lower 23 bits of the Class D address are mapped into a block of Ethernet addresses that have been reserved for multicast.

**Dynamic registration**—There must be a mechanism that informs the network that the computer is a member of a particular group. Without this information, the network would be forced to flood rather than multicast the transmissions for each group. For IP networks, the IGMP is an IP datagram protocol between routers and hosts that allows group membership lists to be dynamically maintained. The host sends an IGMP "report," or join, to the router to join the group. Periodically, the router sends a "query" to learn which hosts are still part of a group. If a host wants to continue its group membership, it responds to the query with a report. If the host sends no report, the router prunes the group list to minimize unnecessary transmissions. With IGMP v2, a host may send a "leave" message to inform the router that it no longer is participating in a multicast group. This allows the router to prune the group list before the next query is scheduled, minimizing the time period in which wasted transmissions are forwarded to the network.

### Multicast in the Layer 2 Switching Environment

The default behavior for a Layer 2 switch would be to forward all multicast traffic to every port that belongs to the destination LAN on the switch. This would defeat the purpose of the switch, which is to limit traffic to the ports that need to receive the data. There are two methods to deal with multicast in a Layer 2 switching environment efficiently—Cisco Group Management Protocol (CGMP) and IGMP Snooping. CGMP is a Cisco developed protocol that allows Catalyst® Switches to take advantage of IGMP information on Cisco routers to make Layer 2 forwarding decisions. CGMP has to be configured both on the multicast routers and the Layer 2 switches. The net result is that with CGMP, IP multicast traffic is delivered only to those Catalyst Switch ports that are interested in the traffic. All other ports that have not explicitly requested the traffic will not receive it. IGMP Snooping requires the LAN switch to examine, or "snoop" some Layer 3 information in the IGMP packets sent between the hosts and the router. When the switch hears the IGMP Host Report from a host for a particular multicast group, the switch adds the host port number to the associated multicast table entry. When the switch hears the IGMP Leave Group message from a host, it removes the host port from the table entry.

### Multicast Distribution Trees

Multicast-capable routers create distribution trees that control the path that IP multicast traffic takes through the network in order to deliver traffic to all receivers. The two basic types of multicast distribution trees are source trees and shared trees.

The simplest form of a multicast distribution tree is a source tree with its root at the source and branches forming a spanning tree through the network to the receivers. Because this tree uses the shortest path through the network, it is also referred to as a shortest-path tree (SPT).

Unlike source trees that have their root at the source, shared trees use a single common root placed at some chosen point in the network. This shared root is called a rendezvous point (RP).

Both SPTs and shared trees are loop free. Messages are replicated only where the tree branches.

### Multicast Forwarding

In multicast routing, the source is sending traffic to an arbitrary group of hosts that are represented by a multicast group address. The multicast router must determine which direction is upstream (toward the source) and which direction (or directions) is downstream. If there are multiple downstream paths, the router will replicate the packet and forward it down the appropriate downstream paths—which are not necessarily all paths. The concept of forwarding multicast traffic away from the source, rather than to the receiver, is called Reverse Path Forwarding.

Multicast routing protocols fall into two categories: dense mode (DM) and sparse mode (SM). DM protocols assume that almost all routers in the network will need to distribute multicast traffic for each multicast group (for example, almost all hosts on the network belong to each multicast group). Accordingly, DM protocols build distribution trees by initially flooding the entire network and then pruning back the small number of paths without receivers. SM protocols assume that relatively few routers in the network will be involved in each multicast. The hosts belonging to the group are widely dispersed, as might be the case for most multicasts in the Internet. Therefore, SM protocols begin with an empty distribution tree and add branches only as the result of explicit requests to join the distribution.

There are several standards for routing IP multicast traffic. The solution recommended by Cisco is Protocol Independent Multicast (PIM), a multicast protocol that can be used with any unicast IP routing protocols to build data distribution trees. PIM can support both DM and SM groups. PIM can service both shared trees and SPTs.

PIM can also support bidirectional trees. In bidirectional mode, traffic is routed only along a bidirectional shared tree that is rooted at the RP for the group. PIM-SM was originally described in RFC 2362 (revised version in progress). PIM-DM is an IETF draft. PIM is the only multicast routing protocol deployed on the Internet to distribute multicast data natively and not over a bandwidth-limited, tunneled topology.

### Multicast Applications

End-node hosts must have IP multicast application software such as videoconferencing and must be able to support IP multicast transmission and reception in the TCP/IP protocol stack.

IP multicast is based on UDP, in which no acknowledgments are returned to the sender. The sender, therefore, does not know if the data it sends is being received, and the receiver cannot request that lost or corrupted packets be retransmitted. Cisco currently delivers Pragmatic General Multicast (PGM) as the reliable multicast solution.

PGM guarantees that a receiver in the group either receives all data packets from transmissions and retransmissions, or is able to detect unrecoverable data packet loss. PGM is specifically intended as a workable solution for multicast applications with basic reliability requirements.

The Source-Specific Multicast (SSM) feature is an extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. When SSM is used in a network, only source-specific multicast distribution trees (no shared trees) are created.

The multicast routing monitor (MRM) feature is a management diagnostic tool that provides network fault detection and isolation in a large multicast routing infrastructure. It is designed to notify a network administrator of multicast routing problems in near real time.

## Cisco IOS Caching Services

When making requests to listen to or view content, users of content-on-demand applications expect a level of responsiveness that is comparable to what they have become accustomed to for getting a dial tone when picking up the phone.

How can that high level of performance be provided for content on demand across the Internet, where traffic is doubling every 100 days?

One of the solutions deployed by ISPs and corporations is to cache frequently requested content (or content for which requests are anticipated) as close as possible to the user. The Cisco network caching solution combines the Cisco IOS Software industry-leading Web Cache Control Protocol (WCCP)-with a network-caching device-the Cisco Content Engine. WCCP is submitted to the IETF Web Replication and Caching (WREC) working group.

When a user requests data from a Web server, a WCCP-enabled router on the path of this request sends the request to a Cisco Content Engine. If the content engine has the data already stored, the engine sends the data to the user. If not, the content engine gets the data from the Web server, stores the data, and forwards a copy to the user.

Content engines are frequently deployed nearby clients to ensure faster network response time and minimal WAN bandwidth usage. Thus, the content engines are caching the clients' most frequently accessed content. In addition, content engines can also be deployed in front of Web server farms to increase the server-farm capacity and improve Web-site performance. This configuration is called reverse proxy caching because the content engines are caching content from only the servers for which they are acting as a front end.

This feature is particularly important when content engines are acting as front ends for server farms in which certain content is dramatically more popular than other content on the servers. Using reverse-proxy caching allows administrators to prevent a small number of high-demand Universal Resource Locators (URLs) from impacting overall server performance. Better yet, this means the high-demand URLs do not have to be identified, manually replicated, or independently managed from the bulk of the URLs on the servers.

Cisco caching services provide the following benefits:

- **Accelerated content delivery**—If a client requests content that is already stored, the request and the data have to travel only between the Cisco Content Engine and the client. Without a Web cache, the request and the reply must travel over the Internet or a wide-area links of the intranet/extranet.
- **Scalability and performance**—The Cisco caching solution is architected to enable network administrators to

easily cluster content engines to scale high traffic loads. This design approach allows customers to linearly scale performance and storage as content engines are added. This linear scalability is achieved because of the manner in which WCCP-enabled routers redirect traffic to content engines. The Catalyst 6000 Family of switches equipped with multilayer switch feature cards (MSFCs) provide transparent Web cache redirection using Cisco WCCP v2.

- **Optimized WAN bandwidth usage**—Redundant WAN traffic is minimized. As a result, WAN bandwidth costs either decrease or grow less quickly. This bandwidth optimization increases network capacity for additional users and traffic and for new services such as voice. Typical bandwidth savings range from 25 to 60 percent.

### Cisco IOS Network-Management Services

Network management requires a variety of tools and capabilities. Cisco IOS Software incorporates numerous network-management features and capabilities that are common to all Cisco IOS devices; some of these capabilities are discussed below.

### Cisco Service Assurance Agent

The Cisco IOS Software service assurance agent (SAA) is an application-aware synthetic operations agent that monitors network performance by measuring key service-level-agreement (SLA) metrics such as response time, availability, jitter (interpacket delay variance), connect time, throughput, packet loss, and application performance.

With the increasing importance of mission-critical applications and networks linking global enterprises, customers are demanding SLAs that guarantee minimum acceptable levels of service. The challenge for the network operators is to create a reliable mechanism for accurately monitoring and ensuring contractual levels of service. Measurement features of the SAA built into Cisco IOS Software enable customers to provide assurances for the managed or delivered services.

The SAA allows users to monitor network performance between a Cisco router and a remote device, which can be another Cisco router, an IP host, or a multiple virtual storage (MVS) host. This feature enables users to perform troubleshooting, problem analysis, and notification based on the statistics collected by the SAA.

The SAA was previously known as the response time reporter (RTR). The response-time and availability-monitoring capabilities of RTR have been extended to include support for VoIP, QoS, and the Web, and thus RTR has evolved into the SAA, starting with Cisco IOS 12.0(5)T.

### SNMP

The Simple Network Management Protocol (SNMP system consists of the following three parts:

- An SNMP manager
- An SNMP agent
- A Management Information Base MIB

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. The SNMP manager can be part of a network management system (NMS) such as CiscoWorks. An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can indicate improper user authentication, restarts, link status (up or down), closing of a TCP connection, loss of connection to a neighbor router, or other significant events. The MIB is a virtual information storage area for network-management information, which consists of collections of managed objects. The agent and MIB reside on the router.

Cisco IOS Release 12.1 Software supports the following versions of SNMP:

- **SNMPv1**—A full Internet standard, defined in RFC 1157 (RFC 1157 replaces the earlier versions that were published as RFCs 1067 and 1098); security is based on community strings

- **SNMPv2c**—The community-string-based administrative framework for SNMPv2; SNMPv2c (the “C” stands for “community”) is an experimental Internet Protocol defined in RFCs 1901, 1905, and 1906; SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 Classic), and uses the community-based security model of SNMPv1

- **SNMPv3**—Version 3 of the SNMP; SNMPv3 is an interoperable standards-based protocol defined in RFCs 2273-2275; SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network

### RMON

Remote Monitoring (RMON) identifies activity on individual nodes and allows one to monitor all nodes and their interaction on a LAN segment. Used in conjunction with the SNMP agent in a router, RMON allows one to view both traffic that flows through the router and segment traffic not necessarily destined for the router. Combining RMON alarms and events (classes of messages that indicate traffic violations and various unusual occurrences over a network) with existing MIBs allows one to choose where proactive monitoring will occur.

Cisco IOS Software provides a series of protocols for end-to-end configuration management. The Cisco Discovery Protocol (CDP) advertises device-type information to its neighbors. Network-management applications can use this information to build a topology map, for example. The Virtual LAN Trunk Protocol (VTP) provides network-wide virtual LAN (VLAN) information, which automates the assignment of VLANs and ensures VLAN configuration consistency across the network. The Dynamic InterSwitch Link (DISL) protocol is used by two adjacent switches to automatically negotiate VLAN trunk configuration parameters. DISL enables a switch that is being plugged into a network to automatically and appropriately configure its trunks to support protocols such as ISL or 802.1q.

### Network Time Protocol

The Network Time Protocol (NTP) is a protocol designed to time-synchronize a network of machines. NTP runs over UDP, which in turn runs over IP. NTP is documented in RFC 1305.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a timeserver. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of each other.

To provide information about system processes, the Cisco IOS Software includes an extensive list of EXEC commands that begin with the word show, which, when executed, display detailed tables of system information.

The router includes hardware and software to aid in tracking down internal problems and problems with other hosts on the network. The privileged debug EXEC commands start the console display of several classes of network events.

## Cisco IOS Software Releases

A release works across many platforms. Each platform supports many feature sets, and  each feature set contains many features.

Releases are packaged as combinations of features—depending on hardware platforms and the needs of customers. Consequently, the number of different packages may be quite large.

Cisco IOS Software releases are packaged in “feature sets” (also called “software images”). Many different feature sets are available, and each feature set contains a specific subset of Cisco IOS features. Not all feature sets are available on all platforms. Also, some feature sets support different features when run on different platforms. Examples of feature-set categories include:

- **Basic**—a basic feature set for the hardware platform; for example IP, IP/FW
- **Plus**—a basic feature set plus additional features such as IP Plus, IP/FW Plus, and Enterprise Plus
- **Encryption**—the addition of the 56-bit (Example: Plus 56) data encryption feature sets to either a basic or plus feature set;  examples include IP/ATM PLUS IPSEC 56 or Enterprise Plus 56. From Cisco IOS Release 12.2 onwards, the encryption designators are k8/k9:
  k8: less than or equal to 64-bit encryption (on 12.2 and up)
  k9: greater than 64-bit encryption (on 12.2 and up)

### What Are the Different Types of Cisco IOS Releases?

- An early-deployment (ED) release, as its name implies, focuses on the timely introduction of innovative internetworking technologies.
- A major release takes the new functions introduced in several ED releases and extends them to more platforms and ensures that reliability is achieved over a long period of time.
- A general-deployment release is a major release that has had extensive market exposure in a wide range of network environments. In addition, it has been qualified through extensive analysis of stability and bug trends, as well as customer-satisfaction surveys.

### What Is a Major Release?

Major releases are the primary deployment vehicles for Cisco IOS Software products. Major releases consolidate features, platforms, functionality, technology, and host proliferation from the previous ED releases. The goal of a major release is to deliver stable, high-quality software for general deployment in customers' production networks. To ensure stability, no new feature or platform support is added to a major release after its first commercial shipment (FCS). (FCS is the date of first shipment to customers through any channel.)

Major releases have scheduled maintenance updates-called maintenance releases-that are fully regression tested, incorporate the most recent bug fixes, and support no new platforms or features.

### How Is a Major Release Identified?

The release number of a major release identifies the major release and its maintenance level. In figure 7 below, 12.1 is the number of the major release, and 7 is its maintenance level. The complete release number is 12.1(7).

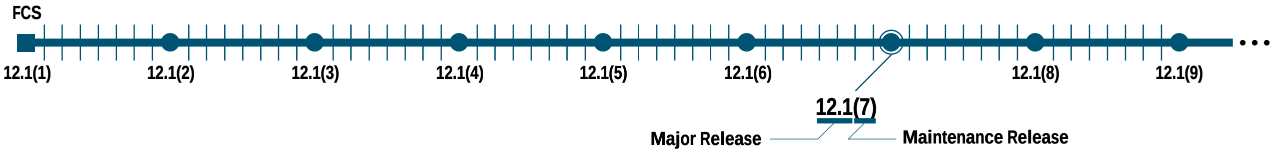


Figure 7: Major-Release Numbering Scheme

### What Is General-Deployment Certification?

At some point during the release life cycle, Cisco will declare a major release to be ready for general-deployment (GD) certification. Only a major release can achieve GD status. It meets the GD certification milestone when Cisco is satisfied that the release has been:

- Proven through extensive market exposure in diverse networks
- Qualified by metrics analyzed for stability and bug trends
- Qualified through customer-satisfaction surveys

GD is achieved by a particular maintenance version. Subsequent maintenance updates for that release are also GD releases. For example, 12.0 got the GD certification at 12.0(8). Thus, 12.0(9), 12.0(10), and so on are GD releases.

Cross-functional teams are formed by bringing together key personnel from Customer Advocacy, the Technical Assistance Center (TAC), Global Support, Network Supported Accounts, System Test Engineering, and Cisco IOS Engineering to evaluate every outstanding defect of the release. Only such a team can certify GD status.

### What Is an Early-Deployment Release?

Based on a major release, an ED release  is a vehicle to quickly deliver new functionality, addressing the need for early availability of product.

ED releases, subjected to the same testing as major releases, have regular maintenance releases. Each maintenance update includes new features, additional platform support, and bug fixes. If a bug originated in the "parent" major release, it is fixed in both the major release and the ED release. Bugs found in a ED release are analyzed to determine whether they originated in that ED release or in the underlying major release. ED releases do not obtain GD certification because the intent is to introduce new functions.

There are two types of ED releases:

- **T Release**—A T (technology) release uses the current major release as its foundation to provide new features and platform support. These releases are easily identifiable by their name, which always ends with a "T." An example is Cisco IOS Release 12.1T.
- **X Release**—An X release normally is based on a T release (such as 12.1T); it supports only a limited number of platforms. An X release normally has an "X" in its name, such as 12.1(1)XB.

  X releases don't usually go through maintenance releases. However, the new functionality in an X release is incorporated into a subsequent update of its "parent" technology release, to  provide ongoing maintenance releases. For example, 12.1(1)XB introduced new platforms and features. As a result, ongoing support for these platforms and features is available in 12.1(3)T and subsequent maintenance releases of 12.1T.

In addition to the T and X releases, other ED releases are aimed at specific targets:

- **Technology or market theaters**—Released on specific platforms and solely under the supervision of a Cisco business unit (BU), these releases are identified by two letters appended to the major release version. An example is Cisco IOS Software Release 12.1(1)DC, which supports the Cisco 6400 Universal Access Concentrator and should be used only for customers who are using the Cisco 6400.

- **Market segments (ISPs, telcos, enterprises, and so on)—** These releases transcend specific technology barriers to achieve business solutions for a given market segment. In addition, they are built for only specific platforms of relevance to the targeted market. Such releases are identified by one alphabetic character appended to the major release version. For example, Cisco IOS 12.0S (for the ISP market) delivers an array of cross-business-unit technology solutions that are of primary interest to service providers. Cisco IOS Release 12.1E focuses on adding new features and functionality for the enterprise market segment.

### How Is an ED Release Distinguished from a Major Release?

One can tell a major release from an ED release by looking at the name. A major release has a numerical name such as 12.0, whereas an ED release has a name that ends with one or more letters such as 12.0T or 12.0XE.

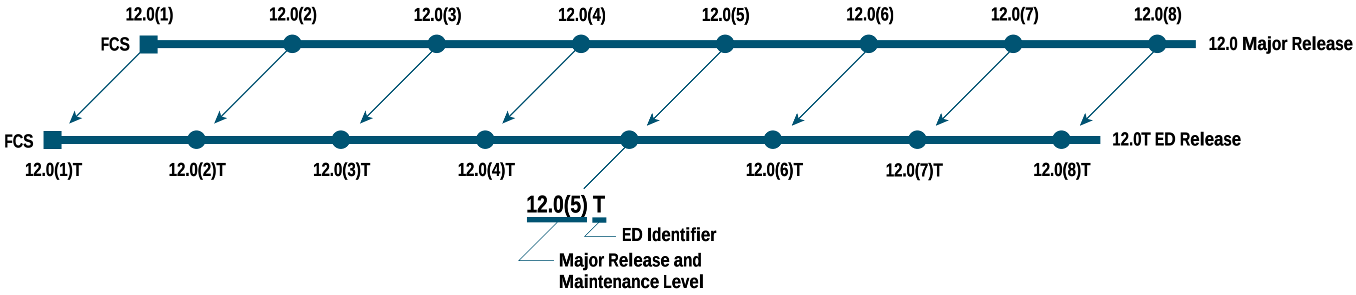
### How Is an ED Release Number Interpreted?

The ED release number identifies the “parent” major release and its maintenance level, in addition to information unique to the ED release.

In the above figure, 12.0(5)T indicates the following:

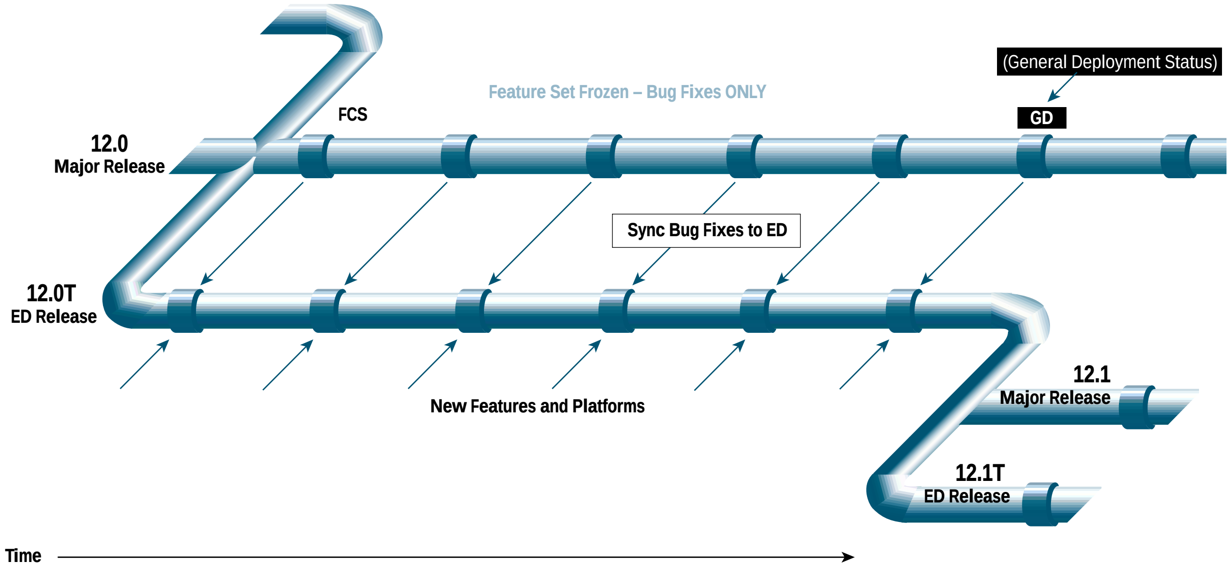
- The ED Release 12.0(5)T is based on the major Release 12.0.
- Release 12.0(5)T is a maintenance release. It incorporates all bug fixes that have been made to the 12.0 release through its fifth maintenance release-12.0(5).
- Release 12.0(5)T is a maintenance release that includes any additional functionality and bug fixes introduced on previous maintenance releases of the 12.0T release.
- Release 12.0(5)T is a maintenance release that may include new functionality not previously introduced in maintenance releases of Release 12.0T.

Figure 8: ED Release Numbering Example-The 12.0(5)T Release



## What Is the Cisco IOS Software Major and T Release Development Process?

Figure 9: Major and T Release Development Process



Major releases and ED releases are closely related in the Cisco IOS Software development process.

Major Release 12.0, as shown above, had its feature content frozen at its FCS. Major Release 12.0 is a consolidation of previous ED releases.

Maintenance updates are provided typically every eight weeks until GD status is achieved. Cisco IOS Release 12.0 attained GD at 12.0(8).

An ED Release 12.0T is also kicked off at the same time as the major release. It contains the same functionality as the major release, plus new features that are continually added at maintenance updates.

Bug fixes in Release 12.0 are also applied to 12.0T.

The final maintenance release of 12.0T is used as the basis of the next major release. In this illustration, it is 12.1. At the same time, a new technology release, 12.1T, is created.

Thus, the process begins again.

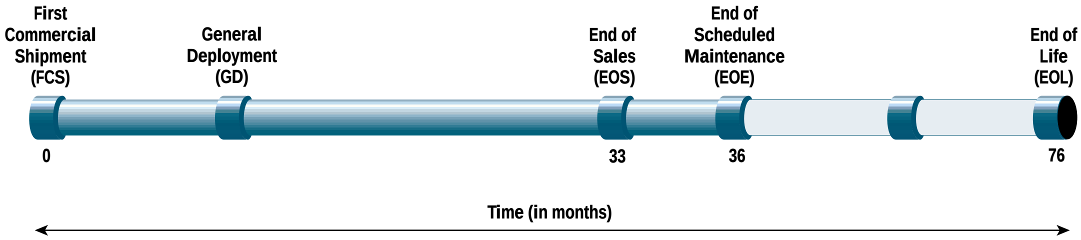
### What Are the Major and T Release Life Cycle Milestones?

Cisco IOS Software uses a time-based release strategy, allowing Cisco to quickly and predictably provide new functions or bug fixes. By tracking the release life-cycle milestones and the migration paths of the releases, a customer can better plan upgrades while the release is actively supported.

FCS corresponds to the first maintenance update of a major release. Each major release receives regular maintenance at eight-week intervals during the early part of the life cycle and at 13-week intervals during the later part of the life cycle. Remember that no functionality is added during the major release life cycle.

End of sale (EOS) is the final date that the product can be ordered through customer service or manufacturing. Until they reach end of life (EOL), releases that reach this milestone are still available through field support offices (FSOs) and CCO to customers under maintenance contract or to Engineering (CSE) support.

Figure 10: Major and T Release Life Cycle Milestone



**Note:** Timeline is a guideline.

Customer Service End of scheduled maintenance or end of engineering (EOE) is the last scheduled engineering maintenance release. Engineering no longer actively applies any defect repairs to the release, regardless of origin or severity (except for security and Y2K defects). The product continues to be available through FSO and CCO.

EOL is the final stage of support and engineering of the release. After this date, the software release is no longer officially supported by Cisco personnel and is removed from CCO.

### Which Release Should a Customer Use?

- A Cisco IOS ED release provides new features as soon as they are available. It is for the customer who is developing strategic network initiatives or leading-edge applications or simply looking for a competitive advantage.

- A Cisco IOS major release is appropriate for a network that requires new technology with continuously improving quality and maturity. It is for the customer who wants to obtain the advanced, consolidated technology introduced in previous ED releases and to benefit from the greater maturity of the major release.

- A GD release is appropriate for a network that requires mature, proven technology with the highest levels of reliability. It is for the customer running major, business-critical applications.

In conclusion, Cisco IOS Software is the industry-leading and most widely deployed network system software that delivers intelligent network services on a flexible networking infrastructure that enables the rapid deployment of Internet applications.

## Cisco IOS IP Routing

**Routing protocols can be classified in many ways, including operational characteristics, such as their field of use and the number of redundant routes to each supported destination. Dynamic routing protocols are categorized as Interior Gateway Protocols (IGPs) and Exterior Gateway Protocols (EGPs). IGPs are used within an autonomous system, in other words, within a single controlling entity, whereas EGPs are used between autonomous systems.**

### Cisco IOS Supported Interior Gateway Protocols: Key Features

### Distance-Vector Protocols

- Interior Gateway Routing Protocol (IGRP)
  - Classful addressing (Class A, B, C)
  - Single subnet mask
  - Metric parameters (bandwidth, cost, load, and others)
  - Full routing-table updates
- Enhanced Interior Gateway Routing Protocol (EIGRP)
  - Classless addressing (prefix based)
  - Variable length subnet mask (VLSM)
  - Address summarization
  - Route filtering
  - Periodic and incremental updates
- Routing Information Protocol (RIP v1)
  - Classful addressing (Class A, B, C)
  - Single subnet mask
  - Hop count (max. 16)
  - Periodic updates
  - Full routing-table updates
- RIP v2:
  - Classless addressing (prefix based)
  - VLSM
  - Triggered updates
  - Full routing-table updates

### Link-State Protocols:

- Open Shortest Path First (OSPF):
  - Hierarchical scaling (two levels)
  - VLSM
  - Address summarization
  - Stub areas
  - Incremental updates
  - Per-area topology database
  - Dijkstra’s shortest path first algorithm (SPF)
- Integrated Intermediate System-to-Intermediate System (IS-IS):
  - Support for both IP and Connectionless Network Protocol (CLNP)
  - Hierarchical scaling (two levels)
  - VLSM
  - Address summarization
  - Incremental updates
  - Per-area topology database
  - Dijkstra’s SPF algorithm

### Key Features of Cisco IOS Supported Exterior Gateway Protocols

### Path-Vector Protocols

- Border Gateway Protocol (BGP)
  - Classless addressing (prefix based)
  - Address aggregation
  - Extensive routing policy filtering
  - Incremental updates
  - Internal scaling:
  - Full mesh
  - Route reflectors
  - Confederations

Depending on the IP routing requirements of the network, Cisco IOS Software offers routing solutions with a wide array of features and functionality for each routing protocol. Whether the choice is a single protocol as a solution or a combination of protocols, to meet individual routing needs, Cisco IOS Software provides an ideal infrastructure for deploying applications and services across the network.

## Major WAN Technologies in Cisco IOS Software

The major WAN technologies in Cisco IOS Software include ATM, Frame Relay, X.25, ISDN, xDSL, cable, wireless, dial, PPP, VPN, VPDN, and so on. This section lists some key features offered by the Cisco IOS Software. For a complete description of all Cisco IOS Software features, please refer to the current Cisco IOS Software release note at http://www.cisco.com/univercd/cc/td/doc/product/software/index.htm

### ATM

- **Permanent virtual circuits (PVCs) and switched virtual circuits (SVCs)**—Cisco IOS Software includes a range of tools for configuring and optimizing PVCs and SVCs.
- **Inverse multiplexing over ATM (IMA)**—IMA enables users to aggregate separate physical channels so that PVCs go across a virtual interface and provides load balancing of data traffic across the channels.
- **PPP over ATM**—This feature allows ATM infrastructure to support newer technologies such as xDSL. Using asymmetric DSL (ADSL termination, for example, DSL users can establish PPP connections through an ATM switch to a Cisco 7200 Series for connection to an IP network.
- **Voice applications—**Voice applications support the transport of voice traffic across ATM adaption layer 2 (AAL2).

### Frame Relay

- **Frame Relay switching**—Frame Relay switching allows users to build a switched Frame Relay network, enabling the router to operate as a central switch and to deliver very high throughput.
- **Compression techniques**—Compression techniques provide powerful functionality for compressing data files such as TCP/IP header compression, which reduces bandwidth costs. It also provides standards-based FRF.9 for payload compression.
- **Traffic shaping and prioritizatio**n—Traffic shaping and prioritization provides traffic-management functionality to shape and police data traffic, allowing multiple classes of service.
- **Standards supported**—Frame Relay supports a wide range of the Frame Relay Forum standards. Among others, FRF.5 allows connection between two different Frame Relay end stations over an ATM cloud; FRF.8 allows connection of a Frame Relay end user with an ATM end user; FRF.11 allows voice applications; FRF.12 allows packet fragmentation; FRF.4 provides for Frame Relay SVCs.

### X.25

- **X.25 over Frame Relay**—X.25 over Frame Relay supports Annex G, which allows encapsulation of X.25 traffic within a Frame Relay network.
- **X.25 over TCP (XOT)**—X.25 over TCP (XOT) encapsulates the X.25 packet inside a TCP connection, allowing X.25 equipment to be connected via a TCP/IP-based network.
- **X.25 over ISDN B and D Channels**—This feature allows X.25 packets to be transported over ISDN B and D channels.
- **X.25 payload compression**—Using the LZS (lossless) data-compression algorithm,  Cisco IOS Software can compress the payload by an average ratio of 2:1. This improves the network performance.
- **Packet assembler and disassembler**—The Cisco X.28 packet assembler/disassembler (PAD) supports all eight X.28 ITU-T 1988 standard commands. This allows a user to review and modify X.3 parameters and place calls. Cisco has also implemented several extended X.28 commands that enhance the functionality of the PAD.

### Dial Services

- **Terminal services**—Terminal services provide many options for supporting dial access, including ISDN modems, PPP, dial-on-demand routing, and dial backup. With dial backup, if a line fails in Frame Relay or ATM, you can use a dial backup line to ensure a connection.
- **Bandwidth optimization**—Bandwidth optimization provides many dialup features that optimize bandwidth and lower costs, including snapshot routing, asynchronous callback, and dial-on-demand routing. For example, snapshot routing preserves a periodic “picture” of the settings of a router so that bandwidth on WAN lines are not consumed by routing updates; dial-on-demand routing dials a connection only when data is to be sent, minimizing control messages during connection establishment.

- **Virtual private networks**—VPNs support L2F, L2TP, and dial ISDN for packet encapsulation and AAA services for security. For AAA, both RADIUS and TACACS are supported.

### ISDN

- **Multiple ISDN switch types**—This feature allows the configuration of multiple ISDN switch types per router. It allows users to add ISDN switch types per interface, change the ISDN switch type without reloading the router, and use PRI and BRI simultaneously on the same Cisco platform.

- **Dynamic multiple encapsulations over ISDN**—Using dynamic encapsulation, it allows the transport of different protocols such as X.25, Frame Relay, ISDN Link Access Procedure, Balanced - terminal adapter [IS THIS CORRECT?] (LAPB-TA), and PPP over multiple B channels on a PRI or BRI. This reduces channel assignment and management effort and increases flexibility.

- **ISDN special signaling support**—This feature supports a list of ISDN special signaling such as ISDN advice of charge (AOC), ISDN nonfacility-associated signaling (NFAS), and ISDN BRI for leased line.

- **Virtual asynchronous traffic over ISDN**—The Cisco IOS Software offers two solutions to send virtual asynchronous traffic over ISDN: ITU-T V.120 and ITU X.75. A virtual asynchronous interface (also known as vty-async) is created on demand to support calls that enter the router through a nonphysical interface.

### Broadband Technologies

- **Service selection gateway (SSG)**—SSG enables subscribers to selectively access different services based on their Layer 2 or Layer 3 connectivity to their service provider.

- **PPP over ATM (PPPoA)**—PPPoA allows users to run PPP traffic over an ATM infrastructure, combining the benefits of PPP and ATM.

- **PPP over Ethernet (PPPoE)**—PPPoE allows PPP traffic to run over Ethernet, providing the ability to connect a network of hosts over a simple bridging access device to an access concentrator.

- **Route bridge encapsulation (RBE)**—This feature seamlessly integrates routing and bridging to achieve high scalability, performance, and security.

## Open Networking Standards and Why We Need Them

In a network, data flows freely from device to device (a computer, an IP phone, a router, a printer, and so on) and to and from physical links. For that to happen, the different devices and the software components (responsible for different functions, such as network addressing or segmenting and reassembling data) must be able to “talk to each other.”

Most large networks, such as wide-area networks (WANs) that interconnect local-area networks (LANs), and the Internet have always consisted of hardware and software built by different vendors. For a long time now (since at least the release of the well-known Open System Interconnection [OSI] reference model in 1984), the networking industry has recognized a need for certain agreed-upon standards to forestall potential incompatibility among these products.

These standards take the form of protocols—a “common language” for networking. As such, they are sets of rules that govern how networking devices and various software components send and receive data. By adhering to these open, public standards—published by official bodies such as the IETF-the industry has achieved interoperability across the Internet and laid the foundation for its phenomenal growth.

In addition to interoperability, other distinct benefits come from maintaining open standards:

- Reduced costs to customers

- Greater innovation

Compare the cost (price per seat) of a proprietary product, the PBX, to that of an “open” product, the LAN switch. In the last five years, the cost of a PBX has not decreased at all, while the cost of a LAN switch has dropped dramatically.

Although one might think that conformance to standards stifles innovation, the opposite is true. By ensuring interoperability, the open standards foster competition. Customers can purchase new, innovative products, and be confident that these products will be compatible with other devices or software in their networks.

Moreover, often the needs of customers drive innovations that become translated into new standards. Open standards, by promoting interoperability, innovation, and reduced costs, have been in large measure the basis for the decision of so many enterprises to integrate the Internet fully into their way of doing business.

## The Cisco IOS Software Binary Image Naming Convention

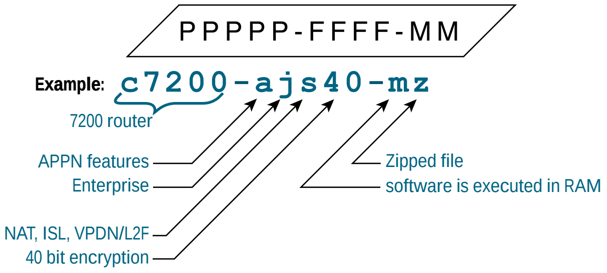
Cisco has a Cisco IOS image naming convention for identifying the platform or board for which the binary software is built, the package feature content of the image, and the area of memory used by the image at run time. As shown in figure 11, the image name follows a three-part format, where:

PPPPP = Platform

FFFF = Features

MM = Run-time memory and compression format

Figure 11: Cisco IOS Image Naming Convention



**Platform Identifiers:**

PPPP indicates the platform for this image is a Cisco 7200 Series Router.

Cisco IOS images that run on boards are named according to a scheme that identifies the board and the platform that supports the board. The names have three parts, separated by dashes (BBB-PPPP-MM). Example: dsc-as5800-mz.

**Feature Content of Cisco IOS Images:**

FFFF identifies the feature content of the image (also referred to as the Cisco IOS feature set). Example: c7200-ajs56-mz.

Here "a" stands for Advanced Peer-to-Peer Networking (APPN) features, "j" is for enterprise features (desktop plus all routing protocols), "s" is for the plus features such as NAT, Inter-Switch Link (ISL), L2F, and VPDN, and "56" stands for 56-bit encryption.

**Cisco IOS Run-Time Memory Space:**

MM in figure 11 is composed of two letters. The first letter identifies the memory area where the Cisco IOS image is executed at run time. The second letter indicates the method used to compress the Cisco IOS binary image.

**Cisco IOS Execution Area:**

| | |
|---|---|
| F | Image runs in Flash |
| m | Image runs in RAM |
| R | Image runs in ROM |
| L | Image will be relocated at run time |

**Cisco IOS Image Compression Identifiers:**

| | |
|---|---|
| Z | Image is Zip compressed |
| x | Image is Mzip compressed |
| w | Image is "Stac" compressed |

As far as users are concerned, they only need to get the image into the router Flash or ROM. At run time, the image automatically unzips itself and relocates to the area of memory from where it is intended to run.

For more information, refer to the white paper at: http://www.cisco.com/warp/public/620/4.html#image

## Identifying a Cisco IOS Release on a Running Router

The show version command issued on any Cisco IOS Router generates the Cisco IOS banner that contains a wealth of information.

Cisco IOS image banners are strings that display information regarding the type of build from which the Cisco IOS image was produced, the release name, and whether it is an interim build, a maintenance build, or a rebuild. The Cisco IOS banner syntax is as follows:

Cisco IOS® <platform_series> Software (<image_name>), Version <version>[, <release_type>]

Copyright (c) 2000-<year> by Cisco Systems, Inc.

Compiled <day> <date> <time> by <user>

Show Version Output Field Definitions

| | |
|---|---|
| Platform_series | Series number of the platform |
| Image_name | Formal image name, as defined by Cisco IOS image naming conventions |

| | |
|---|---|
| Version | Release version number |
| Release_type | Type of build and release vehicle |

Cisco IOS image banners usually contain an “fc1” or “fc2” designator following the “release-type” field. The fc2 designator is an internal rebuild of the fc1 build. The fc2 designator is usually created to fix a specific defect found in the fc1 build. When an fc2 build occurs, all necessary precautions are taken to avoid the distribution of the sister fc1 build.

## Upgrading Cisco IOS Software

### What Is an Upgrade?

An upgrade is an order placed for a Cisco IOS feature set that contains more functionality than the one being replaced. Upgrade is not an “update;” an update consists of installing a more recent version of the same feature set.

Exception: If a feature set is outdated, the next, closest feature set, on a more recent release, will be considered an update.

### What Is the Cisco IOS Software Release Product Number?

A product number, also known as a stock-keeping unit (SKU), is an alphanumeric software product designation indicating a specific model and feature set. Product numbers appear in Cisco price lists as well as Cisco and Cisco partners’ Internet commerce ordering tools.

### What Is the Product Numbering Format?

A product number comprises several parts.

For more information, please refer to Product Bulletin 1087:

Cisco IOS® Software Product Numbering Change Announcement
http://www.cisco.com/cpropart/salestools/cc/pd/iosw/iore/prodlit/1087_pb.htm

### How Do I Order an Upgrade?

Please refer to Product Bulletin 957:

Cisco IOS Upgrade Ordering Instructions
http://www.cisco.com/cpropart/salestools/cc/pd/iosw/prodlit/957_pp.htm

## Useful Cisco IOS Tools

### Cisco IOS Feature Navigator

http://www.cisco.com/go/fn

Cisco IOS Feature Navigator is a fast, easy, and accurate Web-based tool to help users to determine which Cisco IOS images support a particular set of features, or which features are supported in a particular Cisco IOS image.

### Cisco IOS DocGen

http://www.cisco.com/go/doc/docgen

Cisco IOS DocGEn is a web-based tool that allows one to quickly and accurately produce customized command reference documents for Major Release 12.0.

### Cisco IOS Software Roadmap

http://www.cisco.com/warp/customer/620/roadmap.shtml

This roadmap has information about individual releases, target markets, migration path, new features descriptions, and so on.

### Hardware/Software Compatibility Matrix

http://www.cisco.com/cgibin/front.x/Support/HWSWmatrix/hwswmatrix.cgi

Use the hardware/software compatibility matrix to find the minimum required software release for a product family.

Note: The minimum supported release may not necessarily be the recommended release. To determine the best maintenance release for your Cisco product, search for bugs listed by product component in the Bug Navigator. In addition, the hardware documentation reflects the current Cisco IOS requirements.

### Cisco IOS Upgrade Planner

http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi?majorRel=12.0

Cisco IOS Upgrade Planner allows more flexibility to browse for the preferred software. You are no longer limited to seeing just one major release at a time or forced to make choices in a certain order. You can now view all major releases, all platforms, and all software features from a single interface.

### Bug Toolkit:

http://www.cisco.com/support/bugtools/

The Bug Toolkit is a set of integrated applications that can be used to identify and evaluate status defects.

The Bug Toolkit consists of three tools: Bug Navigator, Bug Watcher, and Watcher Agents. Together these tools allow you to locate (Navigator, ID Search) and subscribe to either specific defects (Watcher) or defects matching a network profile that you create (Alerts).

Bug Navigator allows you to search for defects and, in addition, allows you to create the alert agents and watcher bins to constantly monitor your specific network situation.

Bug Watcher allows you to create collections or bins of defects that you can use to monitor the status of specific defects. When the status of a defect changes (for example, when its fix is integrated into a software release), you can view the status of that defect in real time, or you can opt to receive e-mail or fax notifications of those changes.

Bug Watcher Agents are linked with watcher bins to feed new defects that match your agent profile to the bins. Using agents, you can stay continuously updated on any new defect issues critical to your successful network operations.

## Acronyms

### A

**AAA**

Authentication, authorization, and accounting

AAL2:

ATM Adaptation Layer

**AAL5**

ATM adaptation layer 5æOne of four ATM adaption layers (AALs) recommended by the ITU-T. AAL5 supports connection-oriented, variable-bit-rate (VBR) services, and is used predominantly for the transfer of classical IP over ATM and LAN emulation (LANE) traffic.

**ACL**

Access control list—A roster of users and groups of users kept by routers to control access to or from the router for a number of services.

**AppleTalk**

Aproprietary local area network protocol developed by Apple Computer, Inc. for communication between Apple products (e.g. Macintosh) and other computers.

**AS:**

Autonomous System

**ATM**

Asynchronous Transfer Mode—International standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. An internationally standardized implementation of cell-relay technology, ATM represents the first worldwide standard to be embraced by the computer, communications, and entertainment industry. ATM is a high-bandwidth, low-delay, connection-oriented, packet-like switching and multiplexing technique for data transmission that communicates all types of information (traditionally data, burst data, voice, video, image, and cell) over a common backbone using fixed cell lengths. ATM uses a 53-byte cell format that includes a 5-byte header and 48 bytes of payload. Because of the architecture, ATM has the capability to run from 45 Mbps using a DS3 to 2.5 Gbps using an OC-48.

**AVVID:**

Architecture for Voice and Video Integrated with Data

**B**

**BECN**

Backward explicit congestion notification—Bit set by a Frame Relay network in frames traveling in the opposite direction of frames encountering a congested path.

**BGP**

Border Gateway Protocol—Interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). BGP exchanges reachability information with other BGP systems. It is defined by RFC 1163.

**BOOTP**

Bootstrap Protocol—A protocol used by a network node to determine the IP address of its Ethernet interfaces, in order to affect network booting.

**BRI**

Basic Rate Interface

**C**

**CAR**

Committed access rate—A tool for managing bandwidth by controlling transmission rates into the network when traffic is congested. Using CAR, the network operator allocates minimum and maximum bandwidth values to categories of traffic such as voice grade, premium IP data, best effort, and so on.

**CAS**

Channel-associated signaling—CAS voice switching allows PBXs with T1 trunks the ability to have their voice calls routed over the company's Frame Relay/ATM data network.

**CBAC**

Context-Based Access Control—A method for managing different types of traffic on a single network. CBAC allows an intelligent network to recognize a given type of traffic and prioritize its movement over the network. For example, voice will have greater priority over data because voice is more sensitive to delays and dropouts.

**CBWFQ**

Class-Based Weighted Fair Queuing—Allows the user to define traffic classes based on customer-defined match criteria such as access control lists (ACLs), input interfaces, protocol, and quality-of-service (QoS) label. For example, a class might consist of a team working on a certain project or a class can be created for the important mission-critical applications; for example, enterprise resource planning (ERP). When the traffic classes have been defined, they can be assigned a bandwidth, queue limit, or drop policy such as Weighted Random Early Detection (WRED).

**CCIE®:**

Cisco Certified Internetwork Expert

**CDP**

Cisco Discovery Protocol (CDP)—Used primarily to obtain protocol addresses of neighboring devices and discover the platform of those devices. CDP can also be used to show information about the interfaces the router uses. CDP is media and protocol independent, and runs on all Cisco manufactured equipment including routers, bridges, access servers, and switches.

**CEF**

Cisco Express Forwarding—Increases performance by adopting a new caching mechanism that optimizes Internet traffic and enhances network scalability.

**CGMP**

Cisco Group Management Protocol—A Cisco developed protocol that allows Catalyst Switches to take advantage of Internet Group Management Protocol (IGMP) information on Cisco routers to make Layer 2 Forwarding decisions. Cisco Group Management Protocol (CGMP) has to be configured both on the multicast routers and the Layer 2 switches. The net result is that with CGMP, IP multicast traffic is delivered only to those Catalyst Switch ports that are interested in the traffic. All other ports that have not explicitly requested the traffic will not receive it.

### CHAP

Challenge Handshake Authentication Protocol—A security feature supported on lines using Point-to-Point Protocol (PPP) encapsulation that prevents unauthorized access. CHAP does not itself prevent unauthorized access; it merely identifies the remote end. The router or access server then determines whether that user is allowed access.

### CIR

Committed information rate—The rate at which a Frame Relay network agrees to transfer information under normal conditions, averaged over a minimum increment of time. Measured in bits per second, CIR is one of the key negotiated tariff metrics.

### Cisco IOS Software

Cisco IOS Software, the leading and most widely deployed network system software, delivers intelligent network services on a flexible networking infrastructure that enables the rapid deployment of Internet applications.

### CLI

Command-line interface—Interface that allows the user to interact with the operating system by entering commands and optional arguments.

### Codec

Coder/decoder. A software algorithm used to compress/decompress speech or audio signals.

### CPU

Central Processing Unit.

### CRTP

Compressed Real-Time Protocol—Compressed RTP (CRTP), or Real-Time Protocol (RTP) header compression, is a method for making the voice-over-IP (VoIP) packet headers smaller to regain some of the "lost" bandwidth. CRTP compresses the IP/UDP/RTP header in an RTP data packet from 40 bytes to approximately 2 to 5 bytes.

### CCO:

Cisco Connection Online

### CLNP:

Connectionless Network Protocol

### CSE:

Customer Support Engineering

### D

### DECnet

Digital Equipment Corporation Network—Group of communications products (including a protocol suite) developed and supported by Digital Equipment Corporation.

### DES

Data Encryption Standard—Standard cryptographic algorithm for virtual private networks (VPNs).

### DFP

Dynamic Feedback Protocol—The protocol that allows servers to provide input into IP load-balancing decisions. Input includes the level of CPU utilization, the application, and the identity of the user.

### DHCP

Dynamic Host Configuration Protocol—A protocol that allows a server to dynamically assign IP addresses to nodes (workstations) on the fly so that addresses can be reused when hosts no longer need them.

### DLSw+

Data-Link Switching Plus—Cisco implementation of the data-link switching (DLSw) standard for Systems Network Architecture (SNA) and NetBIOS traffic forwarding. DLSW+ goes beyond the standard to include the advanced features of the current method of bridging, and provides additional functionality to increase the overall scalability of data-link switching.

### DSL

Digital subscriber line—Another term denoting xDSL; a family of technologies transmitting digital information (and sometimes plain old telephone service [POTS]) over existing copper-wire pairs for limited distances or over fiber-optic cables. The "x" in xDSL stands for any number of letters denoting the xDSL family members, commonly ISDN DSL (IDSL), single-line DSL (SDSL), high-data-rate DSL (HDSL), asymmetric DSL (ADSL), and very-high-data-rate DSL (VDSL).

**DSCP**

Differentiated service code point—Six bits in the type-of-service (ToS) field.

**DID:**

Direct Inward Dialing

**DiffServ:**

Differentiated Services

**DISL:**

Dynamic InterSwitch Link

**DM:**

Dense Mode

### E

**E1**

Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 2.048 Mbps. E1 lines can be leased for private use from common carriers.

**EIGRP**

Enhanced Interior Gateway Routing Protocol—Advanced version of Interior Gateway Routing Protocol (IGRP) developed by Cisco. Provides superior convergence properties and operating efficiency, and combines the advantages of link-state protocols with those of distance-vector protocols.

**E&M**

Receive and transmit—E&M is a common trunk-signaling technique used on telephony switches and PBXs. The signaling and voice trunks in E&M are separated.

**ED:**

Early Deployment

**EGP:**

Exterior Gateway Protocol

**EOL:**

End of Life

**EOS:**

End of Sales

### F

**FIB**

Forwarding Information Base

**FRF.11**

Frame Relay Fragmentation.11—FRF.11-based voice over Frame Relay (VoFR) allows for vendor interoperability by specifying the frame format and coder types to use when transmitting voice traffic through a Frame Relay network. FRF.11 allows up to 255 subchannels to be multiplexed onto a single Frame Relay data-link connection identifier (DLCI).

**FRF.12**

Frame Relay Fragmentation.12—Frame Relay Fragmentation based upon FRF.12 was developed in conjunction with FRF.11 (voice over Frame Relay) to allow long data frames to be fragmented into smaller pieces and interleaved with real-time voice frames or other delay-sensitive traffic. In this way, real-time traffic, such as voice, and non-real-time data traffic can be carried together on shared permanent-virtial-circuit (PVC) connections without causing excessive delay to the real-time traffic. FRF.12 can be used in conjunction with FRF.11 or it can be used independently. It enables end-to-end fragmentation on a per-PVC basis and allows fragment size to be configurable on a per-PVC basis. FRF.12 currently uses Weighted Fair Queuing (WFQ). Voice over Frame Relay frames cannot be fragmented, but voice-over-IP frames may be fragmented because they are treated as data frames at the Frame Relay level.

**FRTS**

Frame Relay Traffic Shaping (FRTS)—Provides parameters that are useful for managing network traffic congestion. These include committed information rate (CIR), forward and backward explicit congestion notification (FECN/BECN), and the discard-eligibility (DE) bit.

**F-SSRP**
Fast Simple Server Redundancy Protocol

**FTP**
File Transfer Protocol—An application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes.

**FXS**
Foreign exchange station

**FXO**
Foreign exchange office

**FCS:**
First Commercial Shipment

**FRF.9:**
Frame Relay Fragmentation 9

**G**

**GRE**
Generic routing encapsulation—Tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP network.

**GTS**
Generic traffic shaping (GTS)—Provides a mechanism to control the traffic flow on a particular interface. It reduces outbound traffic flow to avoid congestion by constraining specified traffic to a particular bit rate (also known as the token bucket approach), while queuing bursts of the specified traffic. Thus, traffic adhering to a particular profile can be shaped to meet downstream requirements, eliminating bottlenecks in topologies with data-rate mismatches.

**GD:**
General Deployment

**H**

**H.323**
An extension of International Telecommunication Union Telecommunication Standardization Sector (ITU-T) standard H.320; H.323 is a specification for transmitting audio, video, and data across an IP network, including the Internet.

**HSRP**
Hot Standby Router Protocol—Provides high network availability and transparent network topology changes. HSRP creates a hot standby router group with a lead router that services all packets sent to the hot standby address. Other routers in the group monitor the lead router, and if it fails, one of these standby routers inherits the lead position and the hot standby address.

**HTTP**
Hypertext Transfer Protocol

**HMAC:**
Hashing Message Authentication

**I**

**IETF**
Internet Engineering Task Force—A task force consisting of over 80 working groups responsible for developing Internet standards.

**IEEE**
Institute of Electrical and Electronics Engineers—Professional organization whose activities include the development of communications and network standards. IEEE LAN standards are the predominant LAN standards today.

**IGMP**
Internet Group Management Protocol—Used by IP hosts to report their multicast group memberships to an adjacent multicast router.

**IGMP Snooping**
Internet Group Management Protocol Snooping—Requires the LAN switch to examine, or “snoop” some Layer 3 information in the Internet Group Management Protocol (IGMP) packets sent between the hosts and the router. When the switch hears the IGMP Host Report from a host for a particular multicast group, the switch adds the host port number to the associated multicast table entry. When the switch hears the IGMP Leave

Group message from a host, it removes the host port from the table entry. Because IGMP control messages are transmitted as multicast packets, they are indistinguishable from multicast data at Layer 2. A switch running IGMP snooping must examine every multicast data packet to see if it contains any pertinent IGMP control information.

**IP**

Internet Protocol—Network-layer protocol in the TCP/IP stack offering a connectionless internetwork service.  IP provides features for addressing, type of service specification, fragmentation and reassembly, and security.

**IPCP**

IP Control Protocol—A protocol for transporting IP traffic over a Point-to-Point Protocol (PPP) connection.

**IPv6**

IP Version 6

**IPX**

Internet Packet Exchange—NetWare network-layer (Layer 3) protocol used for transferring data from servers to workstations.

**ISDN**

Integrated Services Digital Network—A communication protocol, offered by telephone companies, that permits telephone networks to carry data, voice, and other source traffic.

**IGP:**

Interior Gateway Protocol

**IMA:**

Inverse Multiplexing over ATM

**Ipng:**

Internet Protocol v6

**IPSec:**

IP Security

**IPv4:**

Internet Protocol Version 4

**ISP:**

Internet Service Provider

**IntServ:**

Integrated Services

**L**

L2FLayer 2 Forwarding—A protocol that supports the creation of secure virtual private dialup networks (VPDNs) over the Internet.

**L2TP**

Layer 2 Tunneling Protocol—This Internet Engineering Task Force standard (RFC 2661) is a means of providing secure, high-priority, temporary paths through the Internet.

**LFI**

Link fragmentation and interleaving (LFI)—Reduces delay and jitter on slower-speed links by breaking up large datagrams and interleaving low-delay traffic packets with the resulting smaller packets.

**LLQ**

Low--latency queuing (LLQ) —Brings strict priority queuing to Class-Based Weighted Fair Queuing (CBWFQ). Strict priority queuing allows delay-sensitive data such as voice to be de-queued and sent first (before packets in other queues are de-queued), giving delay-sensitive data preferential treatment over other traffic.

**LAN:**

Local Area Network

**M**

**MDRR**

Modified Deficit Round Robin (MDRR) —A variant of Deficit Round Robin (DRR). Regular DRR selects packets from each virtual output queue in a regular round-robin mechanism, thus providing every class-of-service (CoS) queue equal scheduling into the fabric. In MDRR, all queues are also serviced in a round-robin fashion, with the exception of one of the queues.

**MGCP**

Media Gateway Control Protocol—A protocol designed to bridge between current circuit-based Public Switched Telephone Networks (PSTNs) and emerging IP technology-based networks.

**MIB**

Management Information Base—A database of network-management information that is used and maintained by a network-management protocol such as Simple Network Management Protocol (SNMP) or Common Management Information Protocol (CMIP).

**MNLB**

MultiNode Load Balancing—A forwarding agent that redirects traffic to the load balancer. MNLB distributes load-balancing decisions across any number of routers and switches, making possible the highest levels of availability of server applications.

**MPLS**

Multiprotocol Label Switching (MPLS)—Provides the mechanisms to perform "label switching," which is an innovative new technique for high-performance packet forwarding that assigns "labels" to packets for transport across packet- or cell-based networks. It is based on the concept of "label swapping," in which units of data (for example, a packet or a cell) carry a short, fixed-length label that tells switching nodes how to process the data.

**MPPE**

Microsoft Point-to-Point Encryption

**MTU**

Maximum transmission unit—Maximum packet size, in bytes, that a particular interface can handle.

**MCM:**

Multimedia Conference Manager

**MD5:**

Message Digest 5

**MRM:**

Multicast Routing Monitor

**MSFC:**

Multilayer Switch Feature Card

**MVS:**

Multiple Virtual Storage

## N

**NAT**

Network Address Translation (NAT)—Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space.

**NBAR**

Network-based application recognition (NBAR) —A new classification engine that can recognize a wide variety of application-level protocols, including HTTP via Universal Resource Locator/Multipurpose Internet Mail Extensions (URL/MIME) type and protocols that utilize dynamic port assignments. When the traffic is classified by NBAR, appropriate quality-of-service (QoS) policies can be applied to the traffic classes using existing Cisco IOS QoS features.

**NetBIOS**

Network Basic Input/Output System—An application programming interface (API) used by applications on an IBM LAN to request services from lower-level network processes. These services can include session establishment and termination, and information transfer.

**Network Time Protocol**

Network Time Protocol (NTP)—A protocol designed to time-synchronize a network of machines.

**NFAS:**

Nonfacility Associated Signaling

## O

**OSPF**

Open Shortest Path First—Link-state, hierarchical Interior Gateway Protocol (IGP) routing algorithm proposed as a successor to Routing Information Protocol (RIP) in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing.

**OSI:**
Open Systems Interconnection

## P

**PAT**
Port Address Translation—A feature that lets you number a local-area network (LAN) with inside local addresses and filter them through one globally routable IP address.

**PBR**
Policy-based routing—Routing scheme that forwards packets to specific interfaces based on user-configured policies. Such policies might specify that traffic sent from a particular network should be forwarded out one interface, while all other traffic should be forwarded out another interface.

**PBX**
Private branch exchange—Digital or analog telephone switchboard located on the subscriber premises and used to connect private and public telephone networks.

**PIM**
Protocol Independent Multicast (PIM)—PIM gets its name from the fact that it is IP routing protocol independent. PIM can take advantage of whichever unicast routing protocols are used to populate the unicast routing table, including Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), or static routes. PIM uses this unicast routing information to perform the multicast forwarding function; therefore, it is IP protocol independent. Although PIM is called a multicast routing protocol, it actually uses the unicast routing table to perform the Reverse-Path-Forwarding  (RPF) check function instead of building up a completely unrelated multicast routing table. PIM does not send and receive multicast routing updates between routers like other routing protocols.

**PPP**
Point-to-Point Protocol—A protocol that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits.  A successor to Serial Line Internet Protocol (SLIP), which was designed to work with IP, PPP is designed to work with several network-layer protocols such as IP and Internetwork Packet Exchange (IPX).

**PPTP**
Point-to-Point Tunneling Protocol—A protocol that enables virtual private networking by providing secure remote access to corporate networks over the Internet.

**PGM:**
Pragmatic

**PRI:**
Primary Rate Interface

**PSTN:**
Public Switched Telephone Network

**PVC:**
Permanent Virtual Circuits

## Q

**QoS**
Quality of service (QoS)—The goal of QoS is to provide better and more predictable network service by providing dedicated bandwidth, controlled jitter and latency, and improved loss characteristics. QoS achieves these goals by providing tools for managing network congestion, shaping network traffic, using expensive wide-area links more efficiently, and setting traffic policies across the network.

**QPPB**
QoS Policy Propagation over BGP

**QSIG**
QSIG, a European Computer Manufacturers Association (ECMA) telephony signaling standard, provides an enabling technology to fuel the migration of legacy voice systems to intelligent "multiservice" networks. Originally standardized in the European Integrated Digital Services Network (ISDN) market, QSIG has quickly found worldwide acceptance for private and public applications.

## R

### RADIUS

Remote Authentication Dial-In User Service—A popular security system that has become an accepted standard. RADIUS, a client/server-based authentication software system, supports remote-access applications that allow an organization to maintain user profiles in a centralized database. This database resides on an authentication server that can be shared by multiple remote-access servers.

### RED

Random Early Detection—This class of algorithms is designed to avoid congestion in internetworks before it becomes a problem. RED works by monitoring traffic load at points in the network and stochastically discarding packets if the congestion begins to increase. The result of the drop is that the source detects the dropped traffic and slows its transmission. RED is designed to work primarily with TCP in IP internetwork environments.

### RFC

Request for Comment—A document series used as the primary means for communicating information about the Internet, such as industry standards and protocol specifications. An RFC progresses through several development stages, under the control of the Internet Engineering Task Force (IETF), until it is finalized or discarded.

### RPF

Reverse Path Forwarding—A fundamental concept in multicast routing that enables routers to correctly forward multicast traffic down the distribution tree. RPF makes use of the existing unicast routing table to determine the upstream and downstream neighbors. A router will forward a multicast packet only if it is received on the upstream interface. This RPF check helps to guarantee that the distribution tree will be loop free.

### RMON

Remote Monitoring (RMON)—Identifies activity on individual nodes and allows one to monitor all nodes and their interaction on a LAN segment. Used in conjunction with the Simple Network Management Protocol (SNMP) agent in a router, RMON allows one to view both traffic that flows through the router and segment traffic not necessarily destined for the router.

### RSVP

Resource Reservation Protocol (also known as Resource Reservation Setup Protocol)—A protocol that supports the reservation of resources across an IP network.

### RTP

Real-Time Transport Protocol—A host-to-host protocol used for carrying newer multimedia application traffic, including packetized audio and video, over an IP network. RTP provides end-to-end network transport functions intended for applications transmitting real-time requirements, such as audio, video, or simulation data over multicast or unicast network services. RTP header compression increases efficiency for many of the newer voice-over-IP or multimedia applications that take advantage of Real-Time Transport Protocol (RTP), especially on slow links.

### RBE:

Route Bridge Encapsulation

### RIP v2:

Routing Information Protocol

### RP:

Rendezvous Point

### RTR:

Response Time Reporter

## S

### SAA

Service Assurance Agent or Cisco Service Assurance Agent—The Cisco IOS Software Service Assurance Agent (SAA) is an application-aware synthetic operations agent that monitors network performance by measuring key service-level-agreement (SLA) metrics such as response time, availability, jitter (interpacket delay variance), connect time, throughput, packet loss, and application performance.

### SBM

Subnet Bandwidth Manager

**SGCP**
Simple Gateway Control Protocol—A protocol that Bellcore has created to address the concept of a network that would combine voice and data on a single packet-switched IP network.

**SLA**
Service-level agreement.

**SLB**
Server load balancing—Allows the network administrator to define a virtual server to represent a group of real servers.

**SMTP**
Simple Mail Transfer Protocol—The TCP/IP protocol governing e-mail transmissions and receptions.

**SNA**
Systems Network Architecture—A large, complex, feature-rich network architecture developed in the 1970s by IBM.

**SNMP**
Simple Network Management Protocol—SNMP was designed as the TCP stack network-management protocol. It can now manage virtually any network type and has been extended to include non-TCP devices such as 802.1 Ethernet bridges.

**SONET**
Synchronous Optical Network—A standard of fiber-optic transmission rates that allows interlocking or transmission products from multiple vendors.

**SS7**
Signaling System 7—Used to perform out-of-band signaling in the Public Switched Telephone Network (PSTN).

**SHA:**
Secure Hash Algorithm

**SIP:**
Session Initiation Protocol

**SKU:**
Stock Keeping Unit

**SM:**
Sparse Mode

**SPF:**
Shortest Path First

**SPT:**
Shortest Path Tree

**SSG:**
Service Selection Gateway

**SSM:**
Source Specific Multicast

**SVC:**
Switched Virtual Circuits

## T

**T1**
Digital WAN carrier facility. T1, as used in the United States, is a 1.544-Mbps pulse-code-modulation (PCM) system that supports 24 voice frequency (VF) input channels. On each of the 24 VF channels, a device called a coder/decoder samples the analog input and converts the analog signal into a stream of digital signals called PCM words. A time-division multiplexer (TDM) cycles through the 24 channels and combines a group of 24 PCM words into a frame for transmission over the T1 line.

**TACACS**
Terminal Access Controller Access Control System—Authentication protocol, developed by the Defense Data Network (DDN) community, that provides remote-access authentication and related services, such as event logging.

**TCP**
Transmission Control Protocol

**TED**
Tunnel endpoint discovery

**TOS**
Type of service.

**TAC:**
Technical Assistance Center

**TCP/IP:**
Transmission Control protocol/ Internet Protocol

**TDM:**
Time Division Multiplexing

**U**

**UDP**
User Datagram Protocol—Connectionless transport-layer protocol in the TCP/IP protocol stack. UDP neither guarantees delivery nor does it require a connection. As a result it is lightweight and efficient, but all error processing and retransmission must be taken care of by the application program.

**V**

**VoIP**
Voice over IP—A software feature that enables a router to carry voice traffic (such as telephone calls and faxes) over an IP network.

**VPDN**
Virtual private dialup network—A special type of virtual private network (VPN) that reduces costs by extending a VPN across dialup lines.

**VPN**
Virtual private network—A private communications network that enables traffic to travel securely over a shared public network.

**VLSM:**
Variable Length Subnet Mask

**VoATM:**
Voice over ATM

**VoFR:**
Voice over Frame Relay

**VTP:**
Virtual Terminal Protocol

**W**

**WCCP**
Web Cache Control Protocol—The protocol that provides for Web content caching and retrieval by using a cache engine. This process improves download time for the user and reduces bandwidth use on the network.

**WFQ**
Weighted Fair Queuing—Ensures that queues do not starve for bandwidth, and that traffic gets predictable service. Low-volume traffic streams—which comprise most traffic—receive preferential service, transmitting their entire offered loads in a timely fashion. High-volume traffic streams share the remaining capacity proportionally between them.

**WRED**
Weighted Random Early Detection—Combines the capabilities of the Random Early Detection (RED) algorithm with IP Precedence. This combination provides for preferential traffic handling for higher-priority packets. It can selectively discard lower-priority traffic when the interface starts to get congested and provide differentiated performance characteristics for different classes of service.

**WAN:**
Wide Area Network

**WREC:**
Web Replication and Caching

## References

**Note:** Some pages will require Cisco Connection Online (CCO) login.

Cisco IOS Software on CCOhttp://www.cisco.com/go/ios

Cisco Solutions Pagehttp://www.cisco.com/public/Solutions_root.shtml

Product Bulletin, No. 1189: Standards Supported in Cisco IOS Software Release 12.1/12.1T http://www.cisco.com/warp/public/cc/general/bulletin/software/general/1189_pp.htm

Cisco IOS Software Configurationhttp://www.cisco.com/univercd/cc/td/doc/product/
software/

Cisco IOS IP and IP Routing Configuration Guide
http://www.cisco.com/univercd/cc/td/doc/product/
software/ios121/121cgcr/ip_c/index.htm

### Releases

Cisco IOS Software — Releases
http://www.cisco.com/warp/public/732/releases/

Cisco IOS Releases: The Complete Reference by Mack M. Coulibaly

ISBN: 1578701791, Pages: 308, Pub Date: Apr 2000

White Paper: Cisco IOS Reference Guide
http://www.cisco.com/warp/public/620/1.html

Types of Cisco IOS Software Releases — Product Bulletin 537
http://www.cisco.com/warp/public/cc/pd/iosw/iore/prodlit/
537_pp.htm

Customer Advocacy Cisco IOS Home Page
http://www-tac.cisco.com/Support_Library/Software/Ios/
General/IOS_tools.html

Cisco IOS Software Product Bulletins
http://www.cisco.com/warp/public/cc/general/bulletin/
software/

Product Bulletin, No. 957: Cisco IOS Upgrade Ordering Instructions
http://www.cisco.com/cpropart/salestools/cc/pd/iosw/
prodlit/957_pp.htm

Product Bulletin - No. 1087: Cisco IOS Software Product Numbering Change Announcement
http://www.cisco.com/cpropart/salestools/cc/pd/iosw/iore/
prodlit/1087_pb.htm

### Cisco IOS Intelligent Network Services

Enhanced IP Services for Cisco Networks by Donald C. Lee, CCIE expert
ISBN: 1578701066, Pages: 408, Pub Date: Oct 1999

### Cisco IOS Security Services

Cisco IOS Security Page
http://www.cisco.com/warp/public/732/Tech/security/index.html

Cisco Security Solutions
http://www.cisco.com/go/security

Cisco Security TAC Page
http://www.cisco.com/pcgi-
bin/Support/PSP/index.pl?i=Technologies#Security

Cisco IOS Security Configuration Guide
http://www.cisco.com/univercd/cc/td/doc/product/
software/ios121/121cgcr/secur_c/index.htm

### Cisco IOS Quality of Service

Cisco IOS QoS page
http://www.cisco.com/warp/public/732/Tech/qos/index.html

Cisco IOS 12.1 QoS Configuration Guide
http://www.cisco.com/univercd/cc/td/doc/product/
software/ios121/121cgcr/qos_c/index.htm

QoS Central
http://www-tac.cisco.com/Support_Library/
Internetworking/IP_Routing/QoS/Resources/

### Cisco IOS VPN Service

Cisco VPN Page
http://www.cisco.com/go/vpn

Cisco IOS VPN Page
http://www.cisco.com/warp/public/732/Tech/vpn/index.html

Cisco IOS VPN Documentation
http://www.cisco.com/warp/public/779/largeent/vpne/
vpndocs/vpnsw.html#iosdocset

Cisco TAC VPN Page
http://www.cisco.com/warp/customer/471/top_issues/vpn/vpn_index.shtml

### Cisco IOS Address-Management Service

Cisco IOS Address-Management Page
http://www.cisco.com/warp/public/732/Tech/address/index.html

Cisco IPv6 Page
http://www.cisco.com/go/ipv6

Cisco TAC Page
http://www.cisco.com/pcgi-
bin/Support/PSP/index.pl?i=Technologies#IPRouting_
Protocols

### Cisco IOS Mobile IP

Cisco IOS Mobile IP
http://www.cisco.com/warp/public/cc/pd/iosw/iore/iomjre12/prodlit/817_pb.htm

### Cisco IOS Legacy and SNA Integration Service

Cisco IOS SNA Evolution
http://www.cisco.com/warp/public/732/Tech/sna/index.html

Cisco TAC SNA
http://www.cisco.com/cgibin/Support/PSP/index.pl?i=Technologies#IBM

Cisco IOS Bridging and IBM Networking Command Reference, Vol I
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ibm_r/index.htm

Cisco IOS Bridging and IBM Networking Command Reference, Vol II
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ibm_r2/index.htm

### Cisco IOS Load-Balancing Service

Cisco IOS Load-Balancing Page
http://www.cisco.com/warp/public/732/Tech/load/index.html

Cisco TAC
http://www.cisco.com/pcgi-bin/Support/PSP/index.pl?i=Products#Content_Delivery_Devices

### Cisco IOS Voice and Video Services

Cisco IOS Voice and Video Page
http://www.cisco.com/warp/public/732/Tech/voice/index.html

Cisco IOS Voice and Video Documentation
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/multi_c/index.htm

Cisco TAC Voice and Telephony
http://www.cisco.com/pcgi-bin/Support/PSP/index.pl?i=Technologies#Voice_and_Telephony

Cisco AVVID
http://www.cisco.com/warp/public/788/avvid_index.html

### Cisco IOS Multicast Services

Cisco IOS Multicast Page
http://www.cisco.com/warp/public/732/Tech/multicast/index.html

Internet Broadcast
http://www.cisco.com/go/ib

Developing IP Multicast Networks, Volume I by Beau Williamson, CCIE expert ISBN: 1578700779, Pages: 568, Pub Date: Oct 1999

Cisco IOS 12.1 IP Multicast Documentation
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt3/index.htm

### Cisco IOS Caching Service

Cisco IOS Caching Page
http://www.cisco.com/warp/public/732/Tech/caching/index.html

WCCP
http://www.cisco.com/go/WCCP

### Cisco IOS WAN Connectivity

ATM
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/wan_c/wcdatm.htm

Frame Relay
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/wan_c/wcdfrely.htm

X.25
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/wan_c/wcdx25.htm

Dial Services
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/dialns_c/index.htm

ISDN
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/dialts_c/dtsprt3/index.htm

Broadband Technologies
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/index.htm

### Cisco IOS Management Services

Cisco IOS System Management Documentation
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt3/index.htm

### Cisco IOS NetFlow Services

Cisco IOS NetFlow Page
http://www.cisco.com/warp/public/732/Tech/netflow/index.html

CISCO SYSTEMS

**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
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
http://www-europe.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
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/go/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