April 2009

Empowering Branch Networks with Value-Added Integrated Services and Solutions

A Cisco Integrated Services Router Technology Primer

Edited by:
Shashi Kiran
Srinivas Kotamraju

Network Systems and Security
Cisco

Table of Contents

1.0 Executive Summary

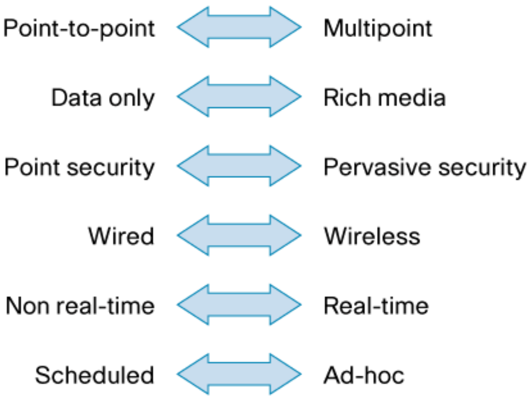
Today's business realities are changing the communications landscape, accelerating convergence and integration. For example, the ubiquitous cell phone is no longer just a phone. It has now morphed into an integrated MP3 player, a camera, a camcorder, web browser, text messaging, email, walkie-talkie, a storage media, an authentication device—the capabilities are endless. Likewise, a computer is no longer just a fast computing machine, but a true multimedia endpoint capable of serving as a DVD player/recorder, a VoIP phone, an audio player, a game machine, and even a TV, as well as a work system. Wherever one looks, the trend is obvious—integrated services and applications are being delivered in a smaller form factor, resulting in enhanced productivity and efficiency to the end user.

Over the past few years, Cisco® has assumed industry leadership in applying this innovative concept to a domain that is considered mission-critical—the branch router. The result is the highly successful Cisco Integrated Services Routers, with over 5 million sold in a little more than three years. This white paper discusses the concept of Integrated Services as they apply to the branch router and how they help to create the empowered branch for small-to-medium business, large enterprises, and service providers offering managed services.

2.0 The Empowered Branch

Yesterday's buzzwords are becoming today's business realities, changing the way networks are designed and run. The communications landscape is rapidly evolving as IP convergence takes hold and accelerates the use of unified applications. Enterprises, small and medium-sized businesses (SMBs), and service providers recognize this trend and are adapting themselves as quality of experience (QoE) becomes paramount (Figure 1).

Figure 1. Business Imperatives and Network Realities Accelerating Branch Infrastructure Upgrades



The emergence of the corporate branch as a major center of business activity has presented both challenges and opportunities to IT organizations. Today, over one-third of all employees work in remote sites.[1] Decision making is becoming localized as branches evolve into "mini-HQs". To be productive in this model, the branch employees demand consistent application and end-user experience, independent of geography and the size of the organization. They also require service coherency and consistency on par with the headquarters. A reliable network infrastructure is vital to deliver on these objectives.

As a result, branches face two challenges today—(i) to embrace technology and deliver collaborative applications and (ii) to achieve the first objective, while focusing on the cost aspects, i.e., return on investment (ROI) and total cost of ownership (TCO). The "empowered branch" concept is a Cisco initiative that describes how organizations can achieve both these goals by adopting integrated services into the network. By doing so, Cisco customers amplify the

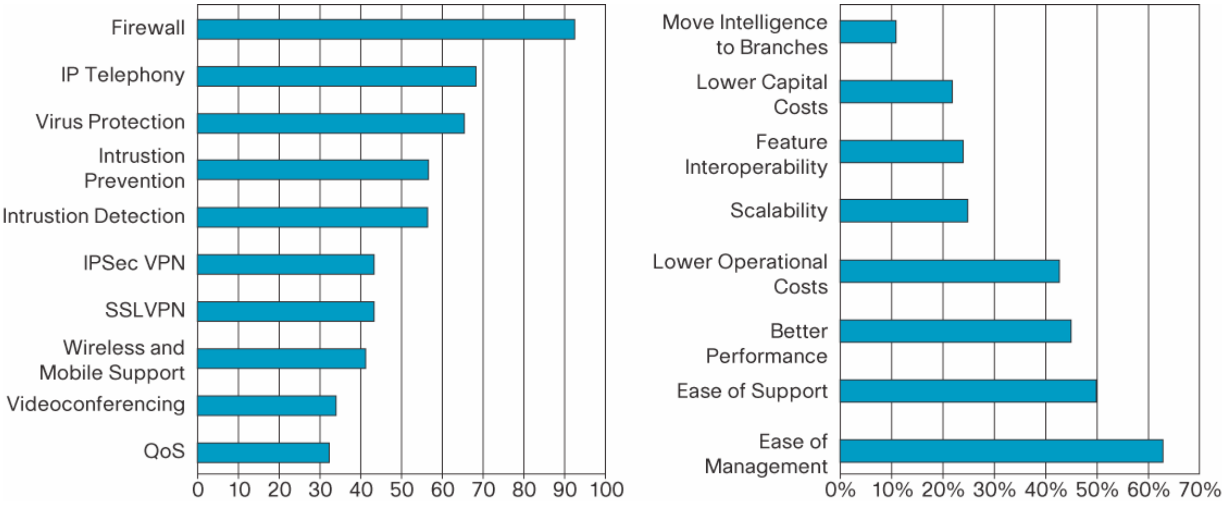
[1] Gartner Group, 2006

business potential of their organization and facilitate secure collaborative applications optimized for “quad play”—i.e., unified voice, video, data, and mobility applications.

3.0 Concept of Integrated Services in a Branch Router

Consider the requirements of a typical branch. The customer premises equipment (CPE) infrastructure in general (and the CPE router in particular) plays an important role in enabling this change and in truly empowering the branch to become more productive and business-efficient. A recent Yankee branch survey indicated that more than 60% of the respondents prefer router-integrated services and listed the features that they would like most to be integrated into their routing platforms:

Figure 2. Preferred Router-Integrated Services and Their Primary Benefits



The reason for such a preference is simple. Services convergence helps companies to protect, optimize and grow their business. In fact, the survey respondents cited manageability as the biggest incentive, along with ease of support, better performance, lower operational costs, and the other factors shown in Figure 2.

These results are in line with the feedback Cisco has received from its own customers and that has been incorporated into its product design. Based on the considerations outlined previously, and Cisco’s own experience, we can infer the requirements for at least the following customer capabilities, irrespective of whether they are offered as an integrated service or as discrete capabilities:

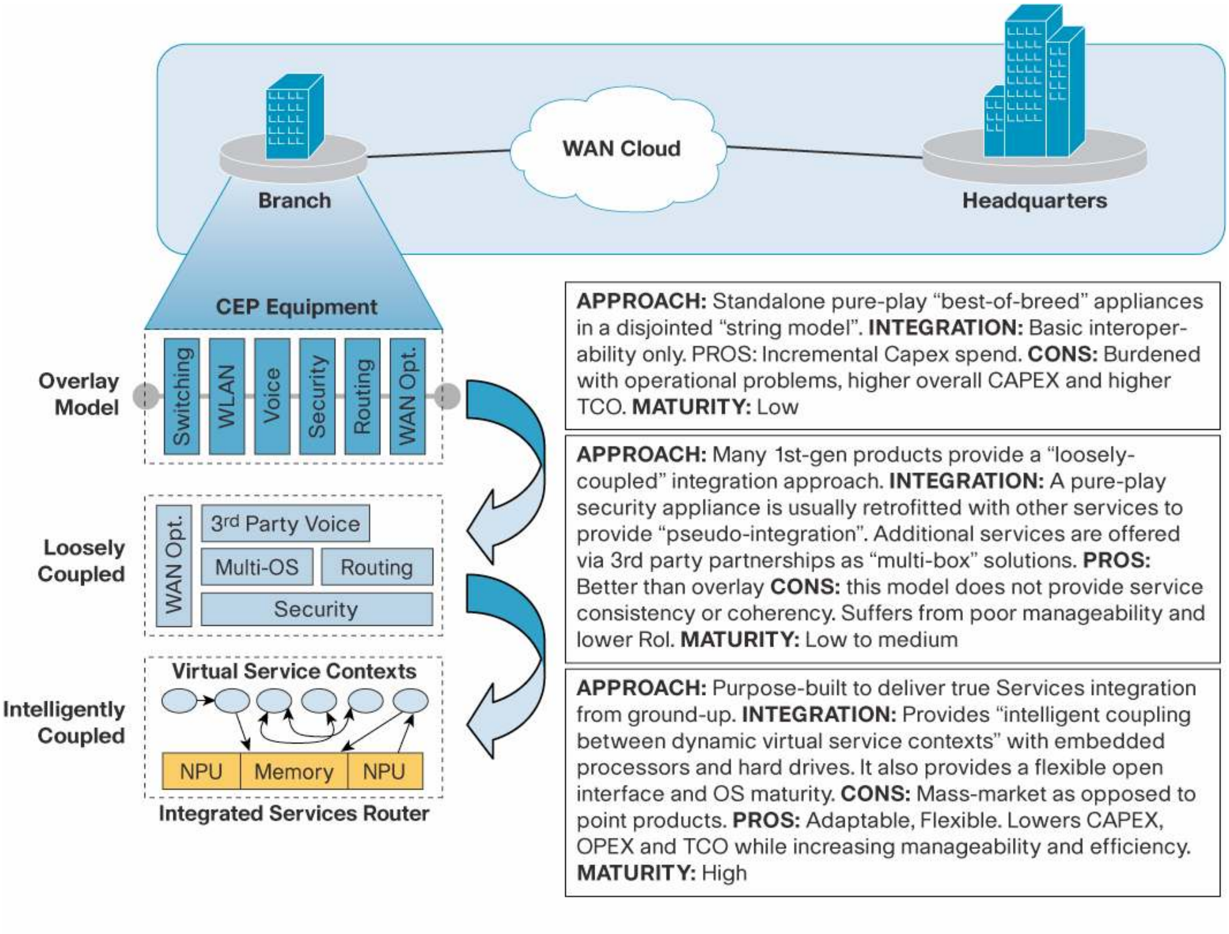
- Routing
- Switching
- Secure connectivity: Flexible VPNs
- High-touch security services: Stateful Firewalls, Intrusion Detection/Prevention Services (IDS/IPS), anti-spoofing, Distributed Denial of Service (DDoS) attack mitigation, virus protection, Network Address Translation (NAT), Network Admission Control (NAC), URL filtering, etc
- Collaborative applications: IP telephony, voice-video integration, video conferencing
- Bandwidth and application optimization: Quality of Service (QoS), Bandwidth, and WAN optimization
- Mobility: Wireless applications

3.1 Approaches to Deliver Integrated Services at the Customer Premises

Now, let’s examine the various options available to deliver some of these services to the customer. In the process, we shall also trace their evolution and examine their relevance to today’s network requirements.

Consider the highly simplified scenario of a typical branch office connected to its headquarters through a “WAN cloud.” For purposes of simplicity, we need not concern ourselves with WAN protocols or even the means of connectivity. We can also combine the requirement for virtual private networks (VPNs) with that of high-touch security services under a generic “security services” category. Using this method, we can classify the different approaches into three distinct areas (Figure 3).

Figure 3. Illustrating the Various Integrated Service Approaches at the CPE



APPROACH: Standalone pure-play “best-of-breed” appliances in a disjointed “string model”. **INTEGRATION:** Basic interoperability only. PROS: Incremental Capex spend. **CONS:** Burdened with operational problems, higher overall CAPEX and higher TCO. **MATURITY:** Low

APPROACH: Many 1st-gen products provide a “loosely-coupled” integration approach. **INTEGRATION:** A pure-play security appliance is usually retrofitted with other services to provide “pseudo-integration”. Additional services are offered via 3rd party partnerships as “multi-box” solutions. **PROS:** Better than overlay **CONS:** this model does not provide service consistency or coherency. Suffers from poor manageability and lower RoI. **MATURITY:** Low to medium

APPROACH: Purpose-built to deliver true Services integration from ground-up. **INTEGRATION:** Provides “intelligent coupling between dynamic virtual service contexts” with embedded processors and hard drives. It also provides a flexible open interface and OS maturity. **CONS:** Mass-market as opposed to point products. **PROS:** Adaptable, Flexible. Lowers CAPEX, OPEX and TCO while increasing manageability and efficiency. **MATURITY:** High

3.1.1 The Overlay Model

In typical “overlay” network architectures, services such as firewalls, intrusion detection and prevention, virtual private networks, voice capability, and network monitoring, are provided by a separate appliance. A single enterprise branch network, therefore, may utilize some six or seven separate devices for fulfilling functions such as routing, switching, helping ensure security, etc. This is because, historically, a majority of budget constrained enterprise IT organizations have functioned in a reactive mode, focusing on helping ensure basic connectivity as more branches and remote sites are added. Many legacy networks existing today were built together in an overlay “string model,” where devices were added to the CPE infrastructure based either on incremental budget allocation or in response to certain “incidents.” For instance, a distributed denial-of-service (DDoS) attack could prompt the addition of a stateful firewall and perhaps an intrusion detection and/or prevention appliance, while a virus outbreak could trigger the addition of an anti-virus application. Similarly, regulatory requirements could lead to the introduction of encryption, resulting in a heterogeneous, multi-vendor chain of overlay point products that suffer from poor integration.

While this model has the benefits of low capital costs to start with, it suffers from severe scalability and integration issues as the network evolves. With training, warranty, software loads, management, and support needs different for each multi-vendor product, the overlay model does not scale to keep pace with network growth.

3.1.2 Loosely Coupled Integration Model

This model advocates an “in-between” approach and is usually promoted by equipment vendors who are delivering first-generation products or are trying to retrofit additional services onto a base functionality. An architecture optimized for delivery of security services could be retrofitted to add routing capabilities, or even collaborative applications, but such integration would result in sub-standard performance for the non-core features.

This model is usually delivered by vendors of point products who have the necessary depth in one or two core areas, but not the breadth. As customer needs grow, additional complex functionalities like IP telephony or advanced routing and application optimization features are added via loosely coupled third-party integration. While this model endeavors to provide some degree of depth and breadth, it becomes unnecessarily complex as the network scales because of multi-vendor interoperability and multi-box manageability issues. Performance also becomes an area of concern.

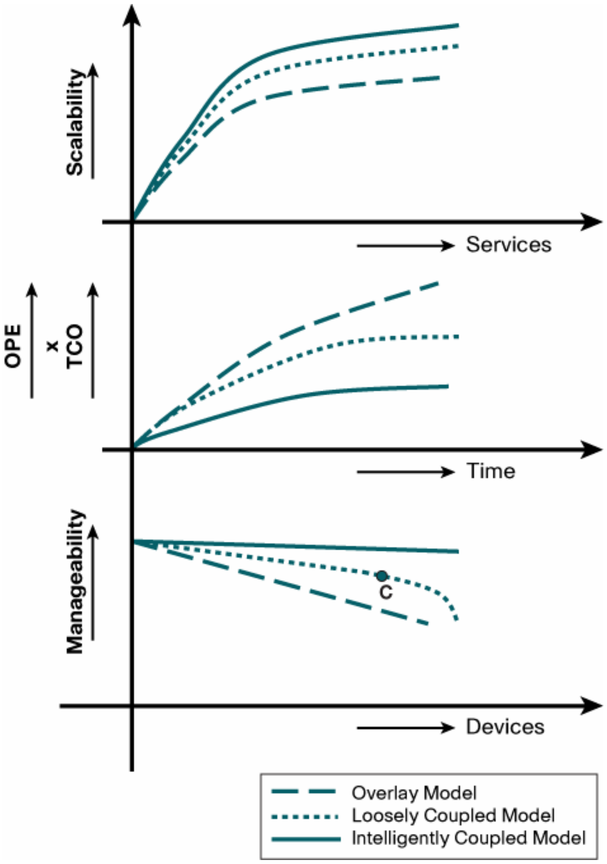
3.1.3 Intelligently Coupled Model

This model advocates a platform purpose-built for flexible services integration and with the capability to evolve as new services and applications emerge. The biggest difference is in the architecture, which is optimized for concurrently delivering tightly coupled services at wire speed through dynamic virtual service contexts on a single system. In its most rudimentary form, they take advantage of the same operating system, memory, and processor. They are fine-tuned to utilize the services chain construct and intelligently deliver on secure collaborative applications.

Minor compromises in performance and sometimes even functionality are acceptable as compared to standalone “best-of-breed” devices because the benefits overwhelmingly outweigh any potential disadvantages. Even these perceived disadvantages are negated as the current generations of integrated services devices utilize embedded processors and hard drives for application performance and scalability. Furthermore, since the various services form part of one device, the manageability, training, support, and software loads are vastly simplified.

Figure 4 conceptually compares the typical behavior exhibited by the three models described previously.

Figure 4. Conceptual Comparison of Service Delivery Models



A system that is intelligently coupled can provide greater scalability (and performance) with concurrent services, as compared to an overlay system or a loosely coupled one. Over time, the return on investment is much higher with an intelligently coupled system because of lower operational costs and a far lower TCO. Manageability, listed as the highest priority for an integrated services router, is also vastly superior with a single system. While the overlay model causes a huge strain on resources because of multiple configuration, provisioning, and troubleshooting requirements, the loosely coupled system begins to experience the same issues when third-party add-ons are used to offset deficiencies in core services. Point “C” represents this inflection point with loosely coupled systems when management becomes a multi-box solution, primarily due to integration of 3rd party capabilities to supplement the capabilities of the base platform

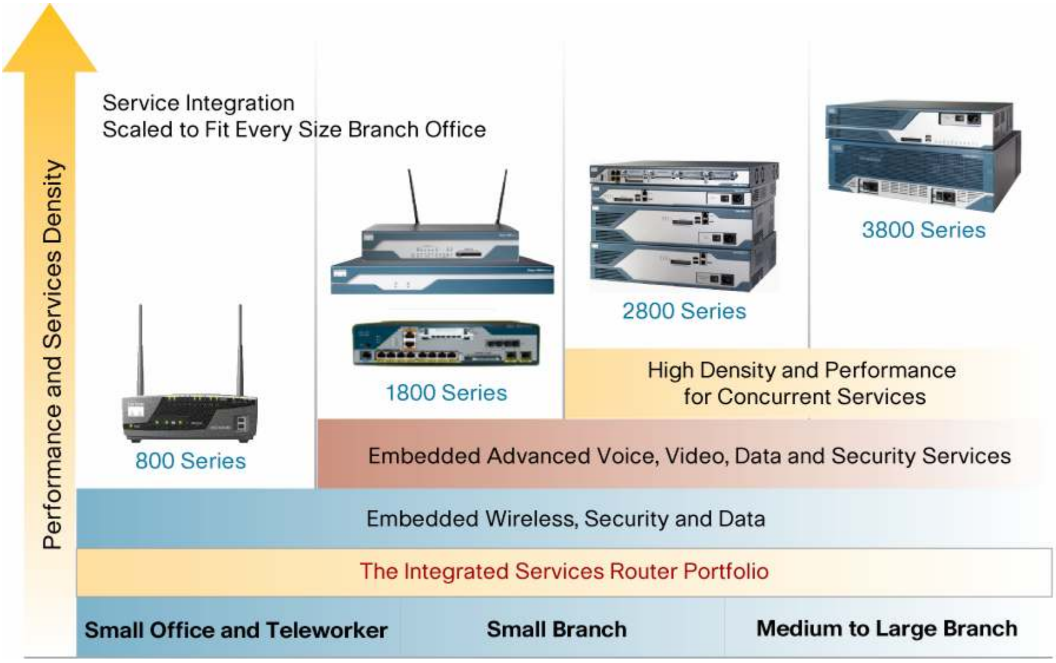
Cisco advocates and delivers on the intelligently coupled model with an advanced architecture through its Integrated Services Router portfolio. Now in their third generation and backed by over 20 years of experience embedded in the Cisco IOS® Software, this is a mature approach that offers the greatest value to customers.

4.0 Introducing the Cisco Integrated Services Router

The Cisco Integrated Services Router portfolio is a family of products that allows Cisco customers to “right-size” their network for a given deployment, while providing the opportunity to future-proof and scale the network evolution based on advanced services, platform density, roadmap, cost, and performance.

With multiple product offerings to meet the varied growth requirements, the Cisco Integrated Services Router offers choice, flexibility and functionality to aid customized network deployment. Cisco IOS Software is the “binding glue” that transcends across different platforms and offers consistency of user experience. Available in fixed-slot and modular configurations, this high-performance architecture is designed and optimized for concurrent service deployment without undue degradation and offers increased default and maximum memory configurations to accommodate future growth (Figure 5).

Figure 5. Cisco Integrated Services Router Portfolio


Performance and Services Density
Service Integration
Scaled to Fit Every Size Branch Office
3800 Series
2800 Series
1800 Series
800 Series
High Density and Performance
for Concurrent Services
Embedded Advanced Voice, Video, Data and Security Services
Embedded Wireless, Security and Data
The Integrated Services Router Portfolio
Small Office and Teleworker
Small Branch
Medium to Large Branch

Cisco 800 Series Routers (Cisco 860, 880, 890, etc.) and Cisco 1800 Series Integrated Services Routers are primarily meant for enterprise SMBs and teleworker deployments. The modular Cisco 1841 and 1861 Integrated Services Routers and Cisco 2800 and 3800 Series Integrated Services Routers are meant for SMBs and enterprise branch offices and deliver integrated unified communications, data, security, and wireless solutions. They offer a variety of LAN and WAN interface modules that provide unmatched flexibility for a variety of media types and access protocols. These modules are field upgradeable, allowing customers to easily change a network interface without affecting the entire branch-office network.

http://www.cisco.com/web/solutions/smb/products/routers_switches/800_series_integrated_services_routers/index.html

4.1 Add-on Modules and Embedded Processors for Enhanced Performance

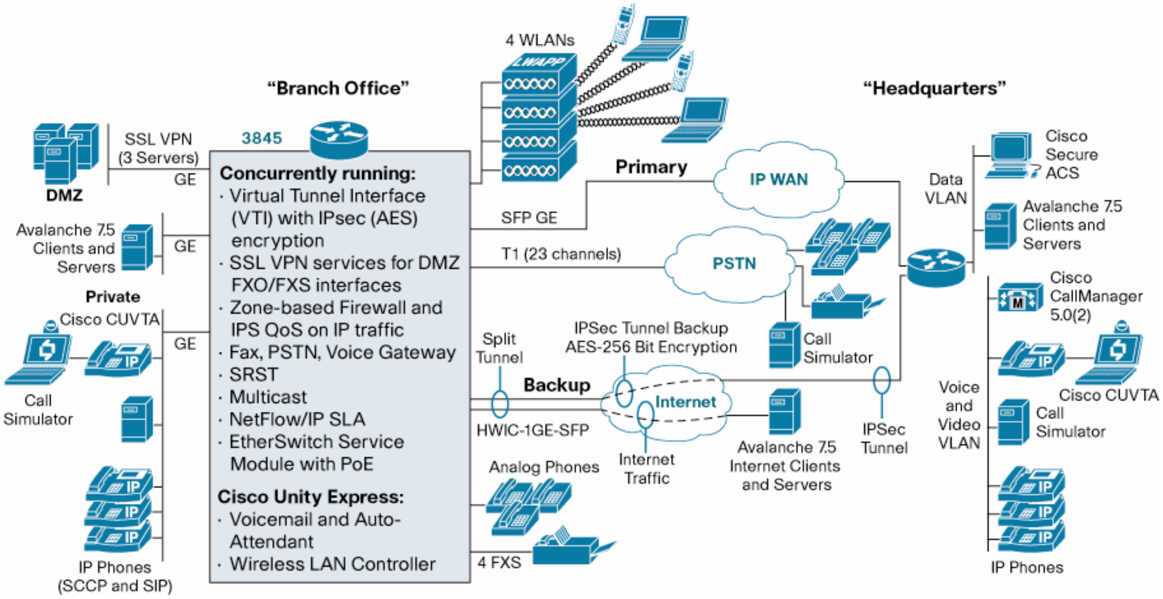
The greatest benefits for integrated services are seen with the higher-end modular routers. For instance, with the optional integration of numerous services modules, Cisco Integrated Services Routers offer the capability to easily integrate the functions of standalone network appliances and components into the chassis itself. Many of these services modules, such as the Cisco Network Analysis Module (NM-NAM), Cisco Unity® Express Extended Capacity Network Module for voicemail and autoattendant (16 ports) (NM-CUE-EC), Cisco Intrusion Prevention System Network Module (NM-CIDS-K9), Cisco Content Engine Network Module (NM-CE-BP-80G-K9), Cisco Wide Area

Application Services (WAAS) Network Module (NM-WAE-522-K9) for WAN optimization, Cisco WLAN Controller Module (NME-AIR-WLC8-K9), and Cisco Application Extension Platform (AXP) service module, have embedded processors and hard drives that allow them to run largely independently of the router, while allowing management from a single management interface. This powerful concept of a "platform within a platform" greatly expands the potential applications of the Cisco 3800 Series beyond traditional routing while maintaining the benefits of integration.

Independent external verifications have consistently provided proof points for the performance and scalability of the Cisco Integrated Services Router architecture running concurrent services.

For example, a December 2006 independent test by Miercom[2] evaluated the Cisco 3845 integrated services router in multiple areas including integrated Layer 2 switching, VPNs, security services and voice capabilities, among others. The Cisco 3845 router ran Cisco IOS Software Release 12.4(9)T1 in the test bed. In the performance test, Miercom verified that, while running a rich set of concurrent services, the Cisco 3845 deployed in the branch office could sustain a high level of bi-directional traffic to the headquarters site. This included feature-testing, performance testing as well as failover scenarios as applicable to the branch office (Figure 6).

Figure 6. Actual Test Bed Set Up by Miercom to Independently Test Performance of Concurrent Services on the Cisco 3845 Integrated Services Router



5.0 Raising the Bar with Integrated Services and Solutions

High-performance, scalable integrated services and solutions are delivered on the Cisco Integrated Services Router via a flexible framework of services building blocks. The entire framework revolves around providing easier manageability independent of the solution being delivered and also on enforcing the three pillars of performance, availability and scalability that are so important to growing businesses needing to be "always on."

Figure 7 depicts a conceptual services framework geared to deliver solutions for voice, video, and data, as well as those related to emerging technologies like Wide Area Application Services or even Cisco TelePresence. This should not be construed as a layered model, but rather a modular one, where different building blocks can be mixed and matched to deliver the best possible solution.

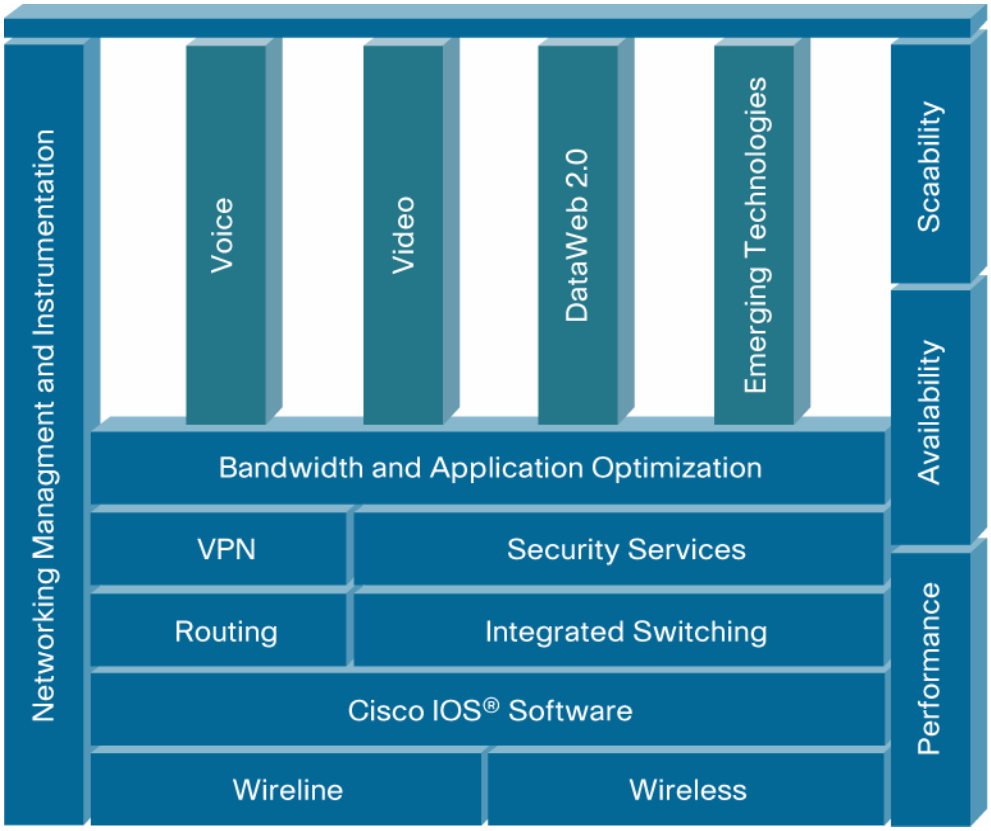
[2] http://www.miercom.com

> “Our most recent independent tests (Dec 2006) showed the Cisco 3845 could sustain over 50 Mbps of concurrent voice, video, wireless and data routing services over a Gigabit Ethernet link and the 3845 processor still had capacity to spare. The AIM crypto-module handled 256-bit AES encryption, IPsec links and clientless SSL VPN connections. The integrated EtherSwitch Service module was able to route near line-rate traffic between 2 switch ports without impacting the 3845’s processor performance. Additionally, with our performance load running, we were able to exercise a full suite of telephony functions including PSTN calls, secure voice calls, conferencing, auto-attendant, a variety of voice mail features and fax.”
>
> **—Rob Smithers, President/CEO, Mier Communications Inc.**

The Cisco Integrated Services Routers support more than 100 different modules for the widest array of deployment options, with new modules being continually introduced. The elegance of the framework helps ensure that each of the optional dedicated modules for advanced capabilities can function with no reliance on other network modules or WAN interface cards (WICs), but transparently integrate with Cisco IOS Software to provide an integrated solution. The Cisco Integrated Services Router further provides the flexibility to implement many services via Cisco IOS Software or with added hardware acceleration.

To address export restrictions, new SKUs such as C3825-NOVPN and C3845-NOVPN have been introduced to the Cisco Integrated Services Router product family. These SKUs are classified for unrestricted export by the U.S Department of Commerce and are available for customers in countries located outside the EU License-Free Zone in Asia-Pacific and Latin American regions. These SKUs exclude VPN payload and secure voice capabilities, in contrast to other Cisco 3800 Series products.

Figure 7. Modular Services Framework on the Cisco Integrated Services



The following sections will highlight some of the key services that can be delivered with the Cisco Integrated Services Router.

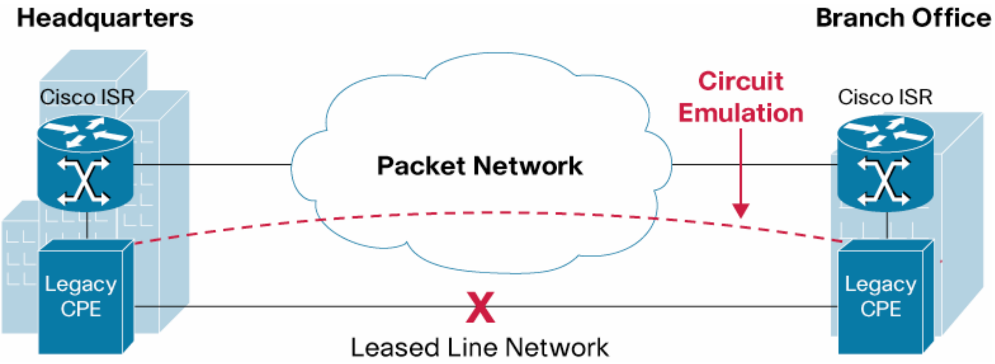
5.1 Routing

The Cisco Integrated Services Router supports the industry's most comprehensive suite of routing protocols using the Cisco IOS Software stack. These include Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Border Gateway Protocol (BGP), and Optimized Edge Routing (OER). Support for both IPv4 and IPv6 capabilities are provided to perform scalable routing.

The Cisco Integrated Services Router also supports Multi-protocol Label Switching (MPLS) Label Edge Routing and customer edge functionality: Layer 3 VPNs, Layer 2 Any Transport over Multi-protocol Label Switching (AToM) pseudowires, and Multi Virtual Route Forwarding (Multi-VRF).

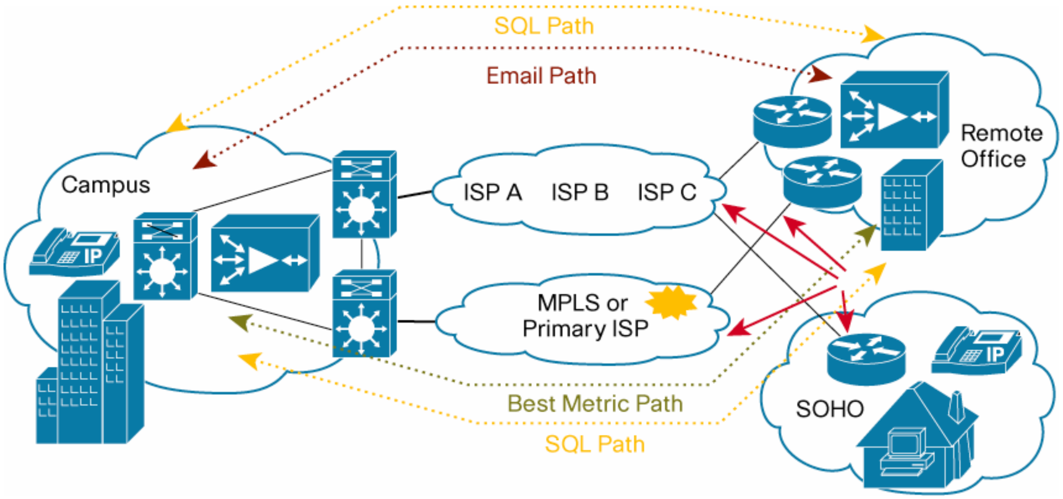
In addition to routing normal IP traffic, the Cisco Integrated Services Router also provides support for legacy non-IP protocols through circuit emulation (Figure 8). Supported through network modules offering circuit emulation, this imitates a protocol-agnostic physical communications link across a packet-based IP network. Circuit emulation offers a huge advantage for large corporations consolidating their legacy networks over IP. It is also ideal for TDM and leased line replacements in a phased manner.

Figure 8. Circuit Emulation over IP



Cisco Integrated Services Routers also support Performance Routing (PfR), which routes data packets through the best IP path between disparate network locations. The router dynamically chooses the optimum route based on variables other than just the shortest path—the criterion used by standard routing algorithms—by correlating real-time data about network latency, jitter, packet loss, link utilization, reachability, throughput, and link cost (Figure 9).

Figure 9. Performance Routing : Routes Packets Through the Best IP Path



5.2 Integrated Switching

The Cisco Integrated Services Router supports integrated switching on the Cisco 2800 and 3800 Series using the Cisco EtherSwitch® Service Modules. These innovative solutions reduce total cost of ownership by optionally integrating switch ports within a router—offering both routing and switching on a single platform and providing fewer points of management for the branch.

Other key features include:

- Support for new features such as IEEE 802.3af Power over Ethernet (PoE)
- Local, robust Layer 3 flexible WAN routing with wire speed full-duplex Layer 2 switching
- Support from IEEE 802.1p, 802.1Q, 802.1D spanning tree
- Voice virtual LAN (VLAN) Feature for IP Phones
- Autosensing on each port, QoS and scalable VLANs
- Cisco Network Assistant and Cisco Emergency Responder

- Cisco StackWise® interfaces (available on select Network modules)
- Software feature parity with highly advanced Cisco Catalyst® 3750 Series Switches

A unique architectural design helps ensure that the Cisco EtherSwitch Module runs an independent Cisco IOS Software image providing feature parity with the Cisco Catalyst 3750 Series Switches that helps ensure that voice calls and data connections can stay up through the switch even when the Cisco IOS Software on the router is being reloaded (including during a Warm reload).

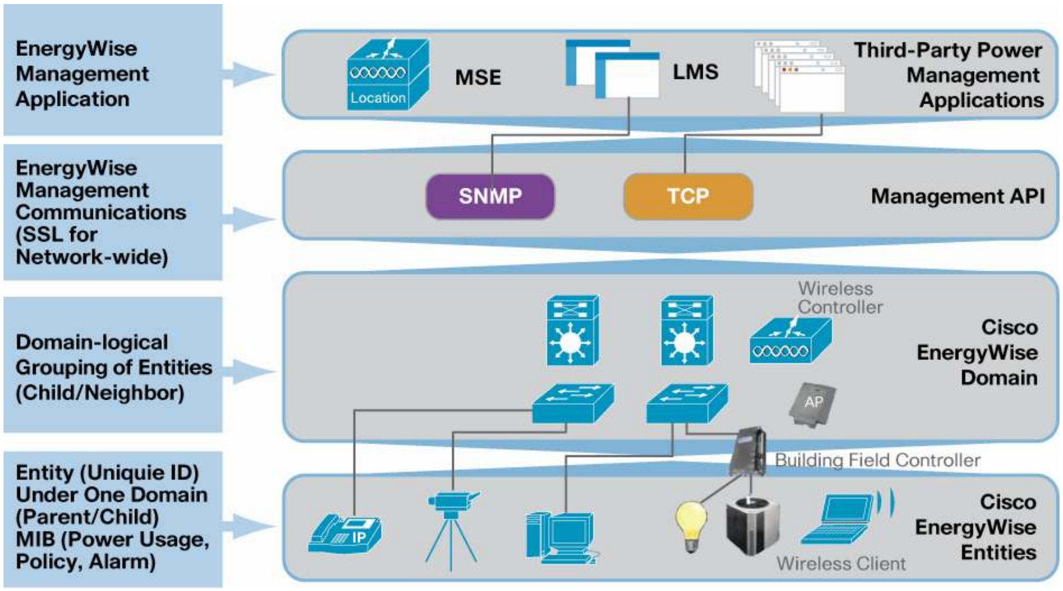
5.2.1 Energy Management Solution

Cisco Integrated Services Routers (selected models) support the recently introduced Cisco EnergyWise solution. This solution monitors the power of all Cisco network-connected devices, from Power-over-Ethernet (PoE) devices to IP-enabled building controllers, and reports aggregate power consumption to provide a clear understanding of an organization’s power habits.

The Cisco EnergyWise solution enables network sustainability by offering a holistic approach to reduce energy costs and greenhouse gas emissions (GHGs), increase overall operating efficiency, and attain sustainable business behavior.

Figure 10 shows a typical Cisco network enabled by the Cisco EnergyWise solution, including the management layer and endpoints.

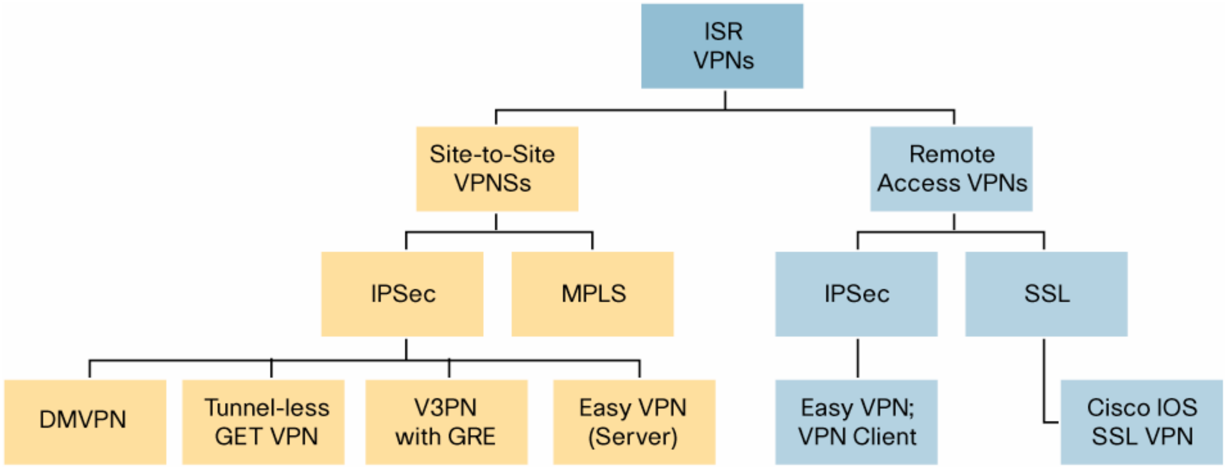
Figure 10. Cisco EnergyWise Components


EnergyWise Management Application
Location
MSE
LMS
Third-Party Power Management Applications
EnergyWise Management Communications (SSL for Network-wide)
SNMP
TCP
Management API
Domain-logical Grouping of Entities (Child/Neighbor)
Wireless Controller
Cisco EnergyWise Domain
AP
Building Field Controller
Entity (Uniquie ID) Under One Domain (Parent/Child) MIB (Power Usage, Policy, Alarm)
IP
Wireless Client
Cisco EnergyWise Entities

5.3 Virtual Private Networks (VPNs)

The Cisco Integrated Services Routers offer a variety of VPN offerings for both site-to-site and remote-access deployments that are among the broadest and most secure in the industry. The site-to-site VPN offerings include a strong suite of IPsec-based VPNs and MPLS-based VPNs, the former being more predominant in the branch routers. Remote-Access VPNs include those based on IPsec, as well as Secure Sockets Layer (SSL) with complementary capabilities. Figure 11 illustrates the categorization of different offerings.

Figure 11. Cisco Integrated Services Router VPN Offerings



A new IPsec and SSL acceleration Advanced Integration Module (AIM) has been introduced for the modular Cisco Integrated Services Routers that encrypts both SSL and IPsec. It accelerates IPsec and is ideal for Group Encrypted Transport (GET) VPN and Dynamic Multipoint VPN (DMVPN). This AIM also doubles the SSL VPN throughput and number of sessions compared to previous modules.

5.3.1 Site-to-Site VPNs

- **Dynamic Multipoint VPN (DMVPN):** DMVPNs is a popular IPsec-based Cisco IOS Software solution that supports hub-and-spoke IPsec + GRE VPN deployments by building secure meshed tunnels. It relies on two proven Cisco technologies, viz., the Next Hop Resolution Protocol (NHRP) and Multipoint Generic Routing Encapsulation (GRE) tunnel interface. The simplicity of configuration with DMVPN has helped ensure its successful deployment in hundreds of customer locations worldwide.

  DMVPN supports scalable hub-spoke and spoke-spoke communication with dynamic routing utilizing GRE. Recent enhancements have included the improved resiliency to hub failures, reduced latency during call setup for spoke-to-spoke tunnels and provision for hierarchical hub design.

- **Tunnel-less VPNs using Group Encrypted Transport (GET):** Newly launched and an industry first from Cisco, Tunnel-less VPNs offer an exciting ground-breaking paradigm shift by building on the benefits of standards-based IPsec with intelligent dynamic QoS-based routing to provide secure any-to-any communication without overlay tunnels (Figure 12). Group Encrypted Transport advocates the concept of “trusted groups” and uses a RFC 3547 Group Domain of Interpretation (GDOI) protocol-based key server to establish security associations among authorized group members.

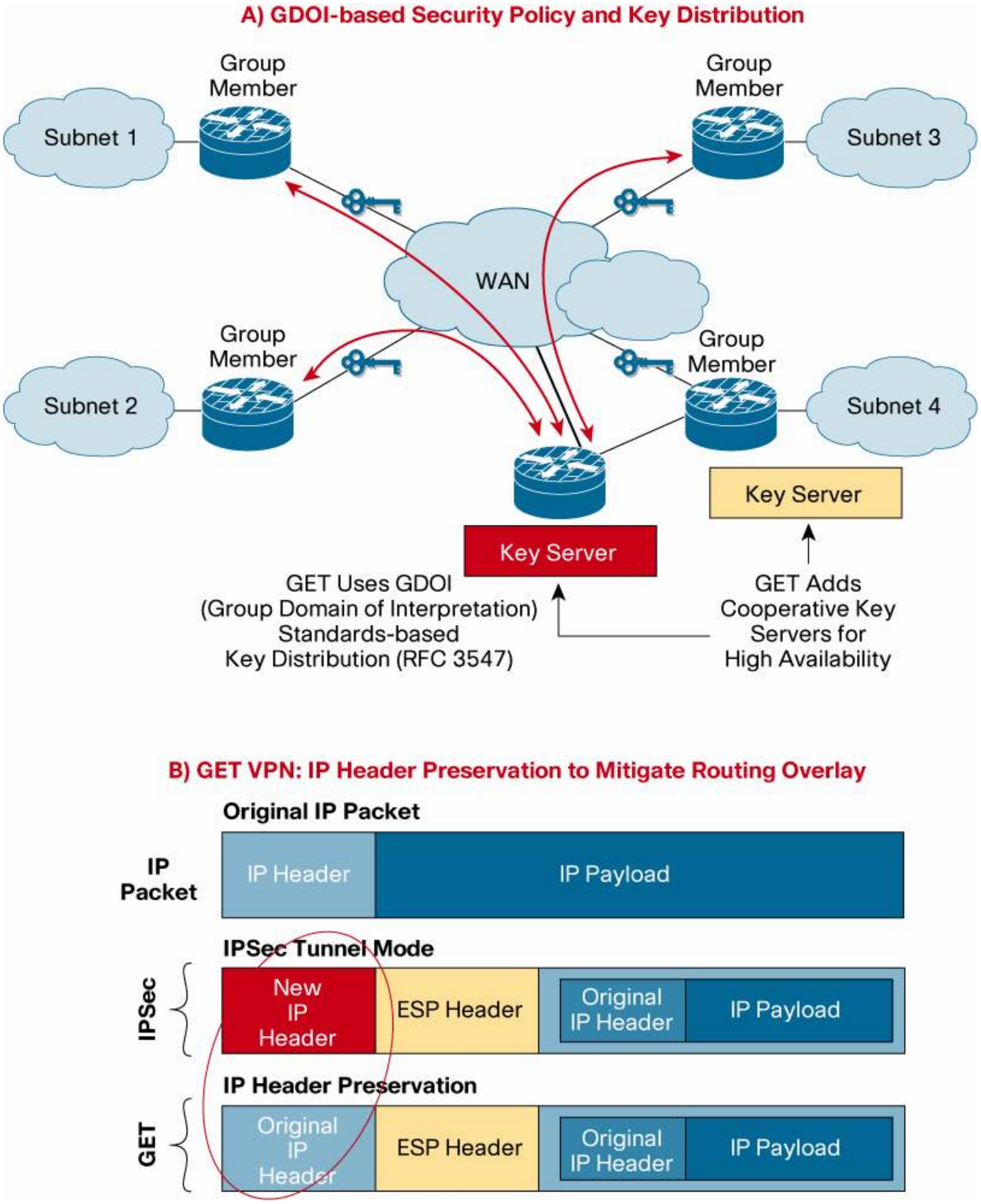
  Group Encrypted Transport uses the existing routing infrastructure while encrypting packets using IPsec. However, unlike traditional Tunnel-mode IPsec encryption, which introduces a new outer-IP header with ESP, the GET VPN security model transposes and attaches the original IP header with ESP, thereby preserving the Layer 3 routing (and inherited QoS) information.

  Dispelling the notion of static mesh and overlay tunnels, this simple but elegant concept helps ensure:

  - Optimized routing over the WAN infrastructure (including traffic-engineering routing over MPLS backbones), especially suited to deliver secure latency-sensitive traffic
  - Higher scalability
  - Better multicast replication
  - Better manageability, especially for large-scale deployments requiring centralized management

- ◦ Secure policy assignment and enforcement, including addressing needs of lawful intercept and mirroring
- ◦ Compliance to regulatory requirements (e.g., HIPAA, PCI) necessitating encrypted traffic independent of WAN connectivity

Figure 12. Fundamental Principles of Tunnel-less VPNs with Group Encrypted Transport



- **Voice- and video-enabled VPN (V3PN):** Since managing separate voice, video, and data networks is costly and inefficient, the Cisco Integrated Services Router has voice- and video- enabled VPN (V3PN) solutions. These integrate cost-effective, secure connectivity provided by site-to-site IPsec VPNs with the IPsec tunnel built over a GRE interface. The network infrastructure enables toll-quality voice and jitter-free video with QoS policies. V3PN also provides bandwidth conservation and LAN and WAN security with encryption, as well as SLA and Multicast support.

- **Cisco Easy VPN Server:** Cisco Easy VPN greatly simplifies virtual private network (VPN) deployment for remote offices and teleworkers. Based on the Cisco Unified Client VPN Framework, the Cisco Easy VPN solution centralizes VPN management across all Cisco VPN devices, reducing the management complexity of VPN deployments. Cisco Easy VPN consists of two components: Cisco Easy VPN Remote and Cisco Easy VPN Server. The Cisco Easy VPN Remote feature allows Cisco IOS Software routers, Cisco PIX® Security Appliances, Cisco VPN 3002 Hardware Clients, and the Cisco VPN Client to receive security policies upon a VPN tunnel connection from a Cisco Easy VPN Server, minimizing configuration requirements at the remote location.

  The Cisco Easy VPN Server allows the Integrated Services Router to act as a headend for site-to-site or remote-access VPNs where the remote-office devices are using the Cisco Easy VPN Remote feature. This feature pushes security policies defined at the central site to the remote VPN device, helping ensure that those connections have up-to-date policies in place before the connection is established. Additionally, a device enabled with the Cisco Easy VPN Server can terminate VPN tunnels initiated by mobile remote workers running the Cisco VPN Client software on PCs. This flexibility allows mobile and remote workers to access critical data and applications on their corporate intranet.

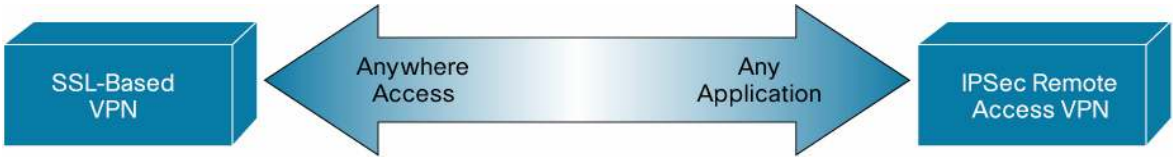
5.3.2 Remote-Access VPNs

Cisco Integrated Services Routers support both the IPsec and SSL VPN flavors for remote access.

- **Easy VPN Remote:** Easy VPN Remote functionality allows the Cisco Integrated Services Routers and other appliances supporting this capability to connect remote offices. It connects to the Easy VPN Server over a VPN tunnel connection and receives security policies, minimizing configuration requirements at the remote location.
- **Cisco VPN Client:** These IPsec thin clients run on desktops and notebooks and terminate on the Cisco Integrated Services Routers, allowing mobile and teleworkers access to corporate infrastructure. The Cisco VPN Clients are supported on a variety of Windows, MAC-OS, Linux, and Solaris operating systems.
- **Cisco IOS SSL VPN:** Formerly known as Cisco IOS WebVPN, this capability allows for secure remote access through standard browsers supporting native SSL encryption. Cisco IOS SSL VPN provides the flexibility to support secure access for all users, regardless of the endpoint host from which they are establishing the connection. If application access requirements are modest, the SSL VPN does not require a VPN client to be preinstalled on the endpoint host.

IPsec and SSL-based VPN offerings are complementary as they solve different problems (Figure 13). They can coexist on the same platform, allowing the Cisco Integrated Services Routers to service different remote-access user requirements.

Figure 13. Solution Space for IPsec and SSL-Based Remote-Access VPNs



5.4 High-Touch Security Services

In addition to secure site-to-site and remote-access VPNs, the Cisco Integrated Services Router is a key part of the Cisco Self-Defending Network (SDN) security strategy, and its comprehensive services enable a single, resilient platform to rapidly deploy and secure networks and applications. All entry points to the network are protected by best-in-class security functions at multiple layers that are streamlined to lower training and manageability costs, providing Adaptive Threat Defense (ATD). Prominent threat defense features include:

- **Stateful firewall:** The Cisco IOS Firewall is an ICSA-certified virtual stateful firewall feature set that helps businesses guarantee network uptime and security by protecting customer networks against network and application layer attacks, viruses, and worms as well as providing effective control on application traffic flowing through the network. Cisco IOS Firewall configuration is supported by an intuitive GUI-based device management application called the Cisco Router and Security Device Manager (SDM), which is provided free of charge as part of all Cisco IOS Software security images. Cisco IOS Firewall configuration is also supported by Cisco Security Manager for larger deployments. Centralized monitoring across distributed firewalls and other security devices is available through Cisco Security Monitoring, Analysis and Response System (MARS).

  Main firewall capabilities include:

  - Zone-based policy framework for intuitive policy management
  - Application firewalling for web, email and other traffic
  - Instant messenger and peer-to-peer application filtering
  - VoIP protocol firewalling
  - Bandwidth usage protection via integration with world-class Cisco IOS QoS
  - Virtualized and VRF firewalling
  - Wireless integration
  - Stateful failover
  - Intuitive device management using Cisco Router and SDM or Cisco Security Manager
  - Firewall monitoring using Cisco Security MARS, SNMP MIB, and Cisco Router and SDM
  - Local URL whitelist and blacklist support
- **Intrusion prevention system (IPS):** The Cisco Integrated Services Router supports dynamic inline intrusion prevention through a dedicated network module or through Cisco IOS Software. The IPS-AIM module on Cisco Integrated Services Routers enables superior performance through hardware acceleration enabled by dedicated CPU and DRAM to offload host CPU. The module provides inline and promiscuous intrusion protection processing and includes strong encryption using the Secure Shell (SSH) Protocol. It has a comprehensive signature database and can dynamically load custom signatures. The IDS network module stores the signature database locally and captures and logs all events. It can send alarms, drop packets, and reset connections.
- **Trust and identity**: Cisco Integrated Services Routers offer a flexible authentication, authorization, and accounting (AAA) mechanism including support for Public Key Infrastructure (PKI) and IEEE802.1.x.
- **Cisco Network Admission Control (NAC):** Cisco Integrated Services Routers support advanced Cisco NAC capabilities by offering the industry’s first full Cisco NAC network module (NME-NAC-K9) that proactively scans and evaluates network activity across all organization for security breaches, allowing network administrators to authenticate, authorize, and evaluate access to network resources and enforce comprehensive admissions policy across all access methods. It assesses all endpoints, including LAN, wireless connectivity, remote access, and WAN, and prevents noncompliant and rogue endpoints from accessing or affecting the network. It proactively protects against worms, viruses, spyware, and malware. Cisco NAC builds on existing endpoint and antivirus investments (with multivendor support) and helps reduce operating costs by enabling easier deployment, troubleshooting, and management of security services and reducing downtime from unplanned outages.

- **DDoS mitigation**: A multi-pronged strategy helps thwart the threat of DDoS attacks.

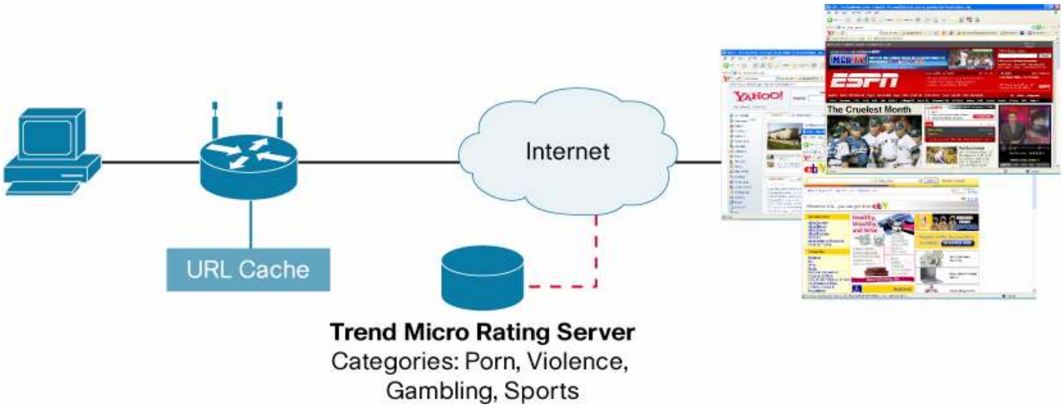
  When combined with other security features such as Network Address Translation (NAT) and VPNs, as well as other Cisco IOS Software features such as Layer 2 Tunneling Protocol (L2TP) and QoS, the Cisco Integrated Services Router provides a secured branch-office environment with branch and perimeter security solutions.

  Many of these security services also adhere to stringent industry certification standards. The VPN and firewall capabilities are constantly tested and conform to FIPS 140-2, ICSA and Common Criteria EAL-4 certifications.

  The same concept is extended to secure management with the support for Secure Shell v2 (SSHv2) Protocol and SNMPv3. To minimize security breaches, the Cisco Integrated Services Routers also support Role-Based CLI Access, which provides a hierarchical configuration and viewing capability based on administrative privileges and profiles.

- **Network-Based Application Recognition (NBAR):** This is a classification engine within Cisco IOS Software that uses deep and stateful packet inspection to recognize a wide variety of applications, including web-based and other difficult-to-classify protocols that utilize dynamic TCP/UDP port assignments. NBAR, when used in a security context, can detect worms based on payload signatures. When an application is recognized and classified by NBAR, a network can invoke services for that specific application. NBAR also helps ensure that network bandwidth is used efficiently by working with QoS features to provide guaranteed bandwidth, bandwidth limits, traffic shaping, and packet coloring. Cisco Router and SDM has an easy-to-use wizard to enable NBAR and also provides a graphical view of application traffic.
- **CPU and memory thresholding:** Cisco IOS Software enables users to set global memory thresholds on memory utilization of the router and generate notifications when the thresholds are hit. By reserving CPU and memory, this feature allows the router to stay operational under high loads, such as those created by attacks.
- **Cisco IOS Content Filtering:** The Cisco IOS Content Filtering solution monitors and regulates all web activities by blocking specific websites or restricting access to certain websites. Cisco IOS Content Filtering is a simple and easy-to-deploy solution. It is scalable, and fully integrated with Cisco IOS Software. The solution provides category-based productivity and security (reputation) ratings to protect against malware, malicious code, phishing attacks, and spyware. This hosted solution uses Trend Micro's global TrendLabs threat database and is closely integrated with Cisco IOS Software. It enforces compliance regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), and Children's Internet Protection Act (CIPA) to mandate reliable content filtering. It also enables an organization to set security policies that limit Internet access and help ensure that employees are productive when accessing the Internet. This feature prevents bandwidth-intensive applications and malware from being downloaded, thereby protecting network resources. Configuration is supported by Cisco Configuration Professional, which that enables rapid deployment of Cisco IOS Content Filtering registration and policies. Support for static black and white lists in Cisco IOS Software as well as keyword blocking is also part of native the Cisco IOS Content Filtering feature set. The feature also supports web redirects to third-party servers such as Websense and Secure Computing (Figure 14).

Figure 14. Cisco IOS Content Filtering



5.4.1 Network Foundation Protection (NFP)

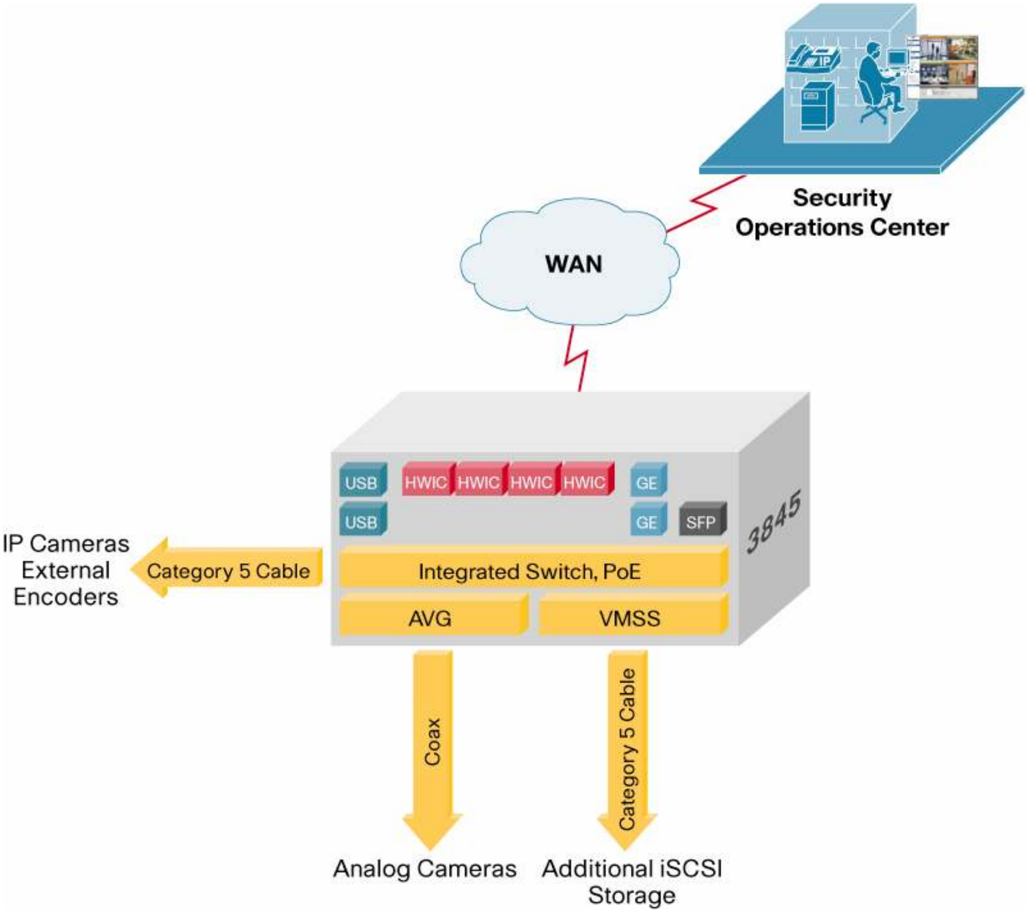
How does one secure a device that is intended to offer security services, and help ensure that the device is not overwhelmed by denial-of-service (DoS) attacks, or by actions originating from unlawful access? Cisco IOS Software offers powerful security features that help ensure continual operation for the Cisco Integrated Services Router.

- **Control-plane policing:** To block DoS attacks and similar threats directed toward the heart of the network, Cisco IOS Software includes programmable policing functionality on routers that limits the rates of, or “polices,” traffic destined for the control plane. This feature can be configured to identify and limit certain traffic types either completely or when above a specified threshold level.
- **AutoSecure:** AutoSecure simplifies router security configuration and reduces the risk of configuration errors with customized approaches for experienced and inexperienced administrators. A single command instantly configures the security posture of routers and disables nonessential system processes and services, eliminating potential network security threats.

5.4.2 Physical Security

By using the IP network, Cisco Integrated Services Routers transform older physical security systems into enabling applications that enhance security and foster multigroup collaboration. The Cisco Video Surveillance Integrated Services Platform combines, on a single platform, the primary functions of an analog video gateway, a video management system, video switching, and inline power for the connected IP cameras and encoders (Figure 15).

Figure 15. Video Surveillance on Cisco Integrated Services Routers



The EVM-IPS-16A module on Cisco Integrated Services Routers aggregates older analog video streams with up to 16 analog ports and migrates to the IP network. The NME-VMSS module provides the interface to manage and monitor video streams, links directly to IP cameras that are connected to PoE-enabled switches, and even locally stores some video footage.

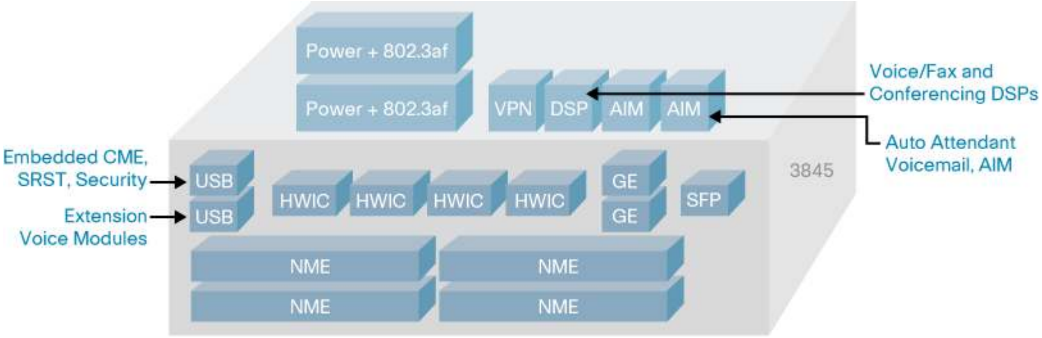
Integrating video switching functions in the platform reduces the complexity and lowers the cost of deploying video surveillance capabilities while the flexibility to design video applications that are customized to unique requirements.

5.5 Voice integration

The Cisco Integrated Services Router delivers affordable and robust IP communications in enterprise branch offices and SMB offices. Through the integration of security, voice gateway, call processing, voicemail, automated attendant, conferencing, and trans-coding capabilities, Cisco Integrated Services Router platforms deliver a complete office IP communications solution.

The platform architecture embeds voice functions directly on the router motherboard enabling customers to deploy advanced telephony services by installing digital signal processors (DSPs) and advanced integration modules (AIMs) for IP telephony conferencing, voice gateways, Cisco Unity Express voice mail and automated attendant in addition to industry-standard security. The advantage with this DSP-based approach is that it frees up the modular slots on the router for other modules or the high-speed WAN interface cards (HWICs). Motherboard packet voice DSP modules (PVDM) modules deliver conferencing, transcoding and voice termination without the need for a network module or AIM. Cisco PVDM2 products installed within the integrated services router provide these services for both voice-over-IP (VoIP) and time-division multiplexed (TDM) traffic (Figure 16).

Figure 16. IP Telephony with Embedded Voice Functions Inside the Cisco 3845 Integrated Services Router



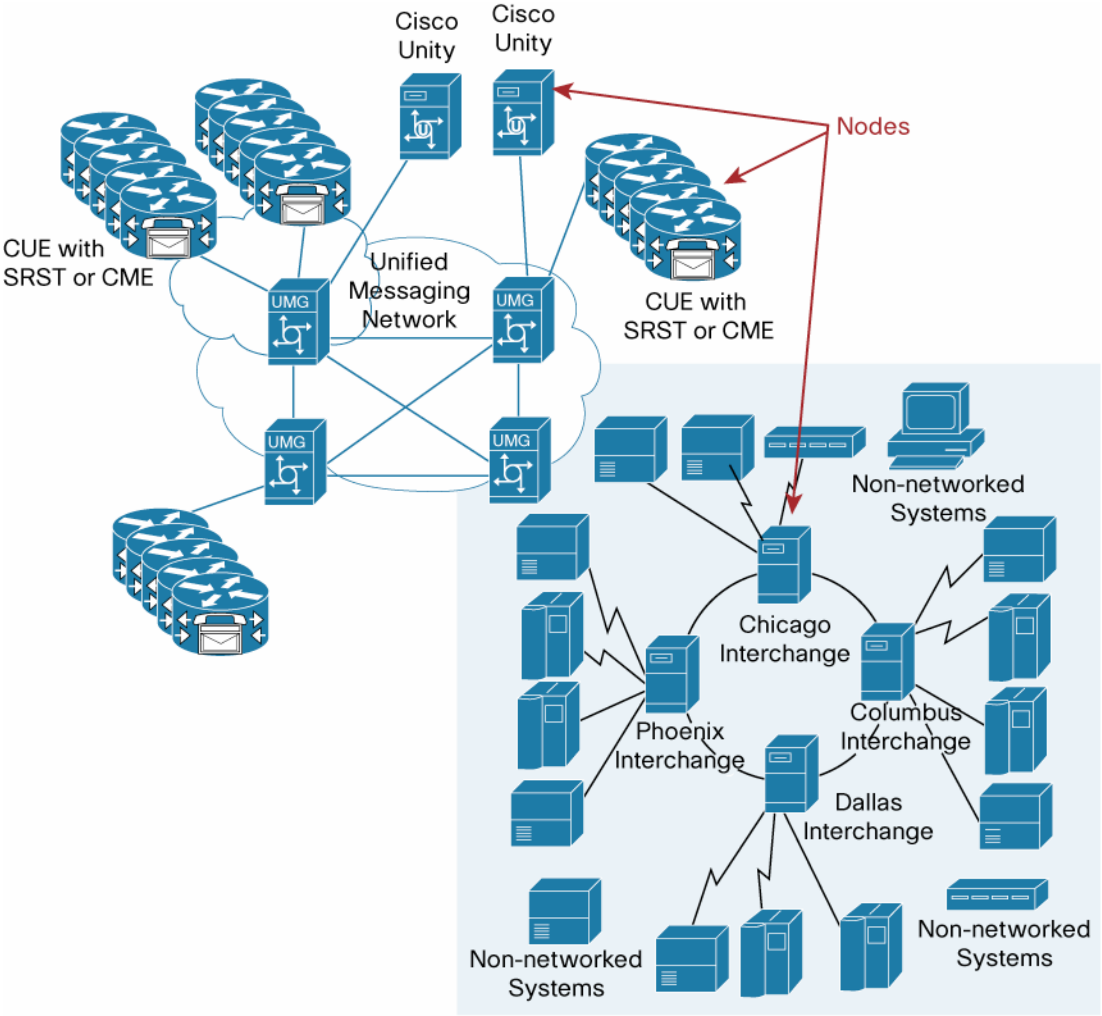
The IP communications component of the Cisco Integrated Services Routers includes the Cisco Unified Communications Manager Express (CME) as part of the Cisco IOS® Software with Cisco Unity Express and Survivable Remote Site Telephony (SRST). The Cisco Integrated Services Router supports industry-standard protocols like Media Gateway Control Protocol (MGCP), Session Initiation Protocol (SIP) and H.323 as well as a variety of high-density analog and digital Network modules to connect to standard telephony equipment such as fax machines, PBXs, key systems and telephones. It can handle localized call processing with Cisco Unified CME while Integrated Switching with the Cisco EtherSwitch Service Module can aid with support for IEEE 802.3af in powering IP phones.

Key voice applications and benefits with the Cisco Integrated Services Router include both mature features and recent innovations:

- **Operation of the routers as toll-bypass gateways:** This operation is accomplished by routing traditional private branch exchange (PBX) traffic across a corporation's IP network.
- **Survivable Remote Site Telephony (SRST):** This mode helps guarantee call quality and preserves communication locally during network outages, promoting higher availability. This complements other availability features like Cisco Unified CME autoregistration and Cisco Unified CME DSP-based conferencing. Here voice mail and automated attendant services can be delivered directly inside the Cisco integrated services router using Cisco Unity Express or delivered centrally using Cisco Unity software. Customers can also implement Secure SRST to enable authentication and encryption support for both signaling and media transmission during a WAN outage
- **Enhanced security**
    - Secure SIP gateways: for encryption and fraud prevention with the ability to act as a Layer 7 device that intelligently allows or disallows traffic between networks
    - Secure SRST for network outages
    - Secure Cisco Unified CME with media encryption and signaling; provides security and helps ensure that voice conversations terminating on either TDM or analog gateway voice ports are protected from eavesdropping by using Secure Real-time Protocol (SRTP) and Transport Layer Security (TLS)
- **Support for VoiceXML**: This feature facilitates advanced IVR and call-center functionality as well as do-not-call registry processing.
- **Integrated messaging system:** The Cisco Integrated Services Routers platform supports Cisco Unity Express messaging and enables a cost-effective voicemail and integrated messaging system. It supports multiple languages with autoattendant and optional interactive voice response (IVR). With advanced features such as live record and live reply, end users can record active phone conversations and be able to reply to voicemail by sending voicemail to the sender or returning the call to the sender's number.

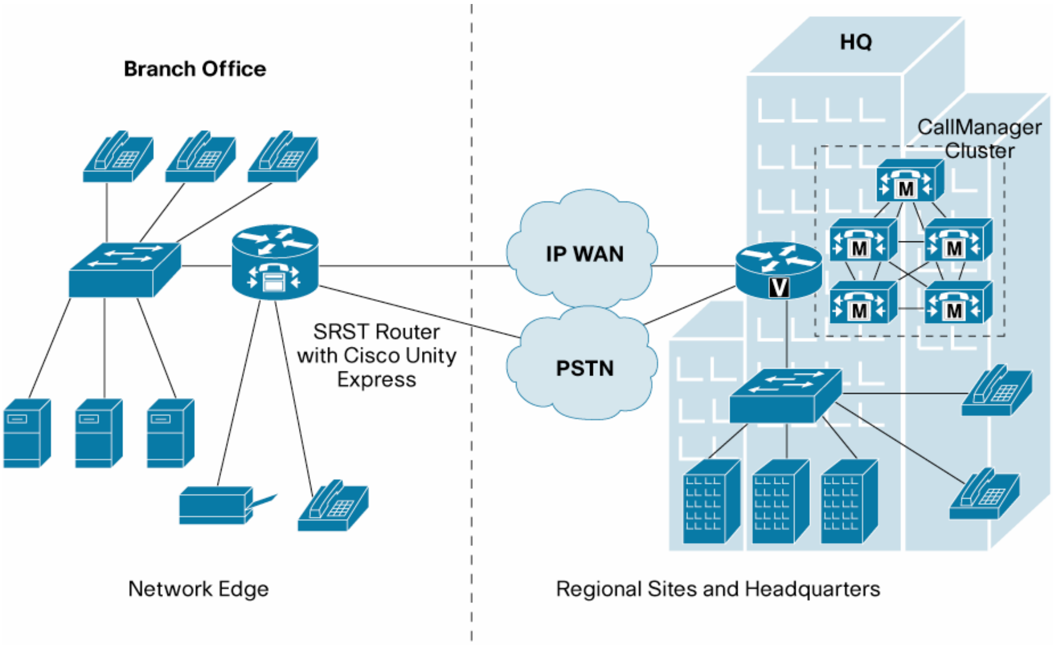
- **Transparent interconnection of IP-based voice networks**: Cisco Integrated Services Routers offer transparent border interconnection services between IP networks through the Cisco Unified Border Element. This solution includes a session border controller (SBC) that facilitates end-to-end IP-based rich-media communication across independent unified communications networks. It transforms communication networks from IP islands by adding the capability to join voice-over-IP (VoIP) and video communications networks without the need to transit through the TDM-based PSTN. Some of the supported features on Cisco Unified Border Element include signaling interworking between H.323 and Session Initiation Protocol (SIP), media interworking (dual-tone multifrequency [DTMF], fax, modem, and codec transcoding), quality of service (QoS), and bandwidth management (QoS marking using type of service [ToS], differentiated services code point [DSCP], and bandwidth enforcement using Resource Reservation Protocol [RSVP] and codec filtering).
- **Voice Security**: Cisco Unity Express supports voice security capabilities such as SFTP for secure backup and restore, support for 160-bit secured hash algorithms, and hack-prevention lockout.
- **Enhanced SIP trunking:** The Cisco Integrated Services Router can provide VoIP and other real-time services based on Session Initiation Protocol (SIP) trunks and integrated SIP capabilities. With the Cisco SIP trunking solution in place, enterprises can quickly and easily implement secure VoIP throughout their organizations. SIP trunking allows provisioning of end-to-end voice, video and data services with the ability for convergence while having easy trunk access and easy management of accounts. From a managed services perspective, this allows for higher quality of service and better customer satisfaction.
- **Centralized and simplified management**: With Cisco Unified Communications Manager, the Cisco Integrated Services Routers deliver next-generation integrated IP telephony, voicemail, and autoattendant functions for all sites of an enterprise, allowing customers to deploy one device to address all their business needs and thereby simplifying management, maintenance, and operations. Features such as SRST provide telephone backup services by automatically detecting failures and initiating call processing redundancy procedures to help ensure that branch offices have uninterrupted telephony service.
- **Scalable voice messaging framework:** The Cisco Unified Messaging Gateway (UMG) solution on Cisco Integrated Services Routers integrates Cisco Unity and Cisco Unity Express capabilities to enable scalable end-to-end networked voice messaging solutions. It supports intelligent voice message routing, management of system directories, interoperability with older voicemail systems, NAT support, and dial-by-name capability. It is available as a network module (NME-UMG) on the Cisco Integrated Services Routers platform. Figure 17 shows a typical UMG deployment.

Figure 17. Cisco Unified Messaging Gateway-Based Network



- **Service consolidation on a single PRI:** Integration of voice, video and data connectivity over a single Primary Rate Interface (PRI) link allows optimal use of existing bandwidth

Figure 18. Cisco Integrated Services Router Platforms Used for IP Telephony in Branch Networks


Branch Office
HQ
CallManager Cluster
M
M
M
M
M
IP WAN
V
SRST Router with Cisco Unity Express
PSTN
Network Edge
Regional Sites and Headquarters

The Cisco Integrated Services Router platforms are ideal platforms for implementing IP Communications in enterprise branch offices and small and medium-sized businesses. Figure 19 shows the use of Cisco ISR for IP Telephone in branch networks. Their ability to deliver wire-speed IP Communications are the result of a high-performing processor, specialized voice silicon, innovative analog and BRI interface capabilities, embedded modularity DSPs, and advanced telephony services such as Cisco Unified CME, Cisco Unity Express, conferencing, and transcoding. With room for services growth and scalable options for integrated modularity, Cisco Integrated Services Router platforms are the platforms for IP Communications that protect future investments.

5.6 Video

Cisco is embracing the medianet by enabling exceptional, reliable, rich media experiences anywhere, anytime, and to any device. Using the same powerful support for QoS, multicast, security, and bandwidth enhancement, Cisco provides video conferencing capability to the branch office. The Cisco Unified MeetingPlace® conferencing solution is a complete multimedia conferencing solution with voice, video, and web conferencing. Offering industry-leading video setup and control capabilities, Cisco Unified MeetingPlace conferencing helps branch managers remain in constant contact with executives at headquarters. Its conferencing capabilities support a range of applications, from highly collaborative meetings to training sessions and presentations.

- Cisco Unified MeetingPlace conferencing is deployed “on network” behind the firewall to protect company security, and it integrates directly with the voice and data network and enterprise applications on the Cisco Integrated Services Router. It takes advantage of existing voice networks (IP and circuit-switched) to reduce or eliminate transport toll charges and recurring conferencing charges.
- The Cisco IP/TV® solution, a comprehensive streaming solution that delivers TV-quality video programming to desktop PCs or display screens, can be used to provide video content or video on demand. Branch personnel may can access live or recorded events by using a program listing updated whenever events are scheduled or content is added. This capability also allows customer content to be streamed to branch retail stores for promotional or educational purposes, for background music to be played, or for training sessions offered to personnel.
- The Cisco Application and Content Networking System (ACNS) on Cisco Integrated Services Routers delivers standard- to high-definition video quality for live streaming events and video on demand (VoD) over

IP networks. With Cisco ACNS, organizations can deliver effective, high-quality, large-scale corporate communications; on-demand training; and digital signage to remote and dispersed branch offices, schools, and stores. It eliminates the need for redundant digital media storage and streaming traffic traversing a WAN by taking advantage of unicast- and multicast-enabled LANs and WANs and preventing deployment of local storage and video streaming servers at remote sites. It efficiently scales video offerings to more users.

Newer video-related capabilities on the Cisco Integrated Services Router, complement the voice integration features and promote higher availability:

- **Video SRST:** This feature preserves video calling during network outages.
- **Cisco Unified CME autoregistration:** This feature allows no-touch deployments with few configuration errors.
- **High-density video distribution:** This feature uses the architectural improvements for voice processing in the integrated services router with the DSP on motherboard, allowing high-density conferencing for Cisco Unified CME (with at least 8 party ad-hoc and 32 party meet-me calls). Additional capabilities offered through streaming licenses include unicast/multicast stream splitting, live broadcasts, prepositioned digital media content for better end-user experience.

5.7 Bandwidth and Application Optimization

As part of its efforts to optimize WAN performance and bring more parity between LAN and WAN access speeds and experiences, Cisco has introduced innovative bandwidth- and application-optimization solutions. These solutions are supported via dedicated network modules on the Cisco Integrated Services Router, and they enhance the overall quality of application experience. Cisco offers a comprehensive solution framework for WAN optimization and application acceleration. This includes the Cisco Wide Area Application Services (WAAS) solution that enables organizations to improve application performance over their WAN links.

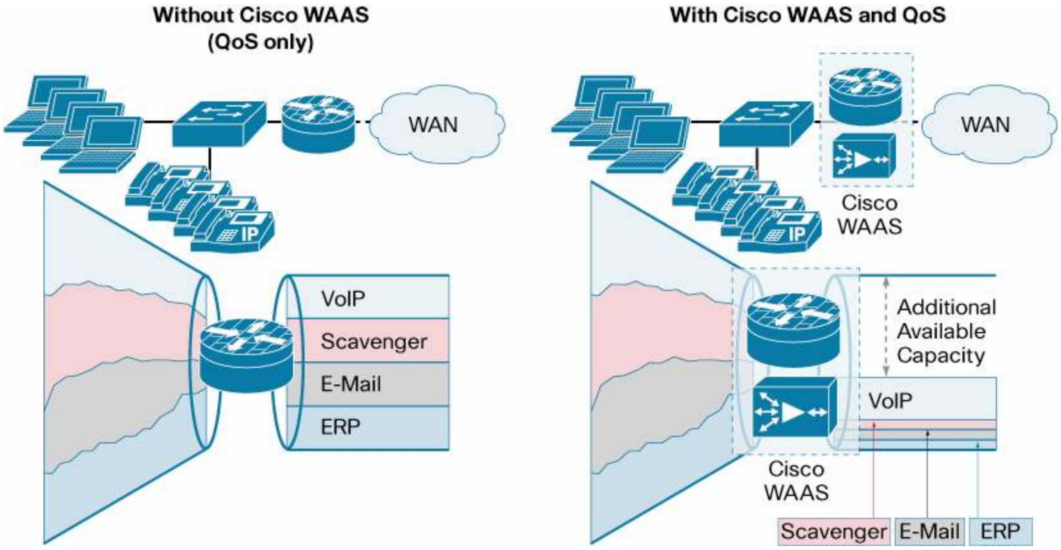
5.7.1 Cisco Wide Area Application Services (WAAS)

Cisco Integrated Services Routers offer a dedicated network module with Cisco WAAS Software that optimizes TCP-based applications across the WAN by using technologies such as compression, data redundancy elimination, transport optimization, application optimization and caching. The Cisco WAAS network module for Cisco Integrated Services Routers (NME-WAE-302-k9, NME-WAE-502-k9, NME-WAE-522-k9) delivers appliance-equivalent performance for Cisco Integrated Services Routers.

Cisco WAAS transparent architecture enables integration into the network and preservation of existing network services, thereby making WAN acceleration easy to deploy and operate. Network transparency and preservation of IP and TCP header information allows ease of operation and interoperability with network services such as quality of service (QoS), NetFlow, access control lists (ACLs), firewalls, Cisco Optimized Edge Routing, and IP service-level agreements (SLAs). Cisco WAAS is easy to deploy and manage, and it integrates with Cisco IOS Software (Figure 19).

Available on the Cisco 2800 and 3800 Series Integrated Services Routers , Cisco WAAS Software overcomes WAN latency, bandwidth, and packet-loss limitations with advanced protocol optimization technologies, thereby offering remote-office users LAN-like performance when accessing centralized files and applications over the WAN. Cisco WAAS utilizes protocol-specific optimizations such as latency mitigation, object caching, metadata caching, and specific application optimizations such as MAPI for Microsoft Exchange and HTTP/S for web applications

Figure 19. Cisco WAAS



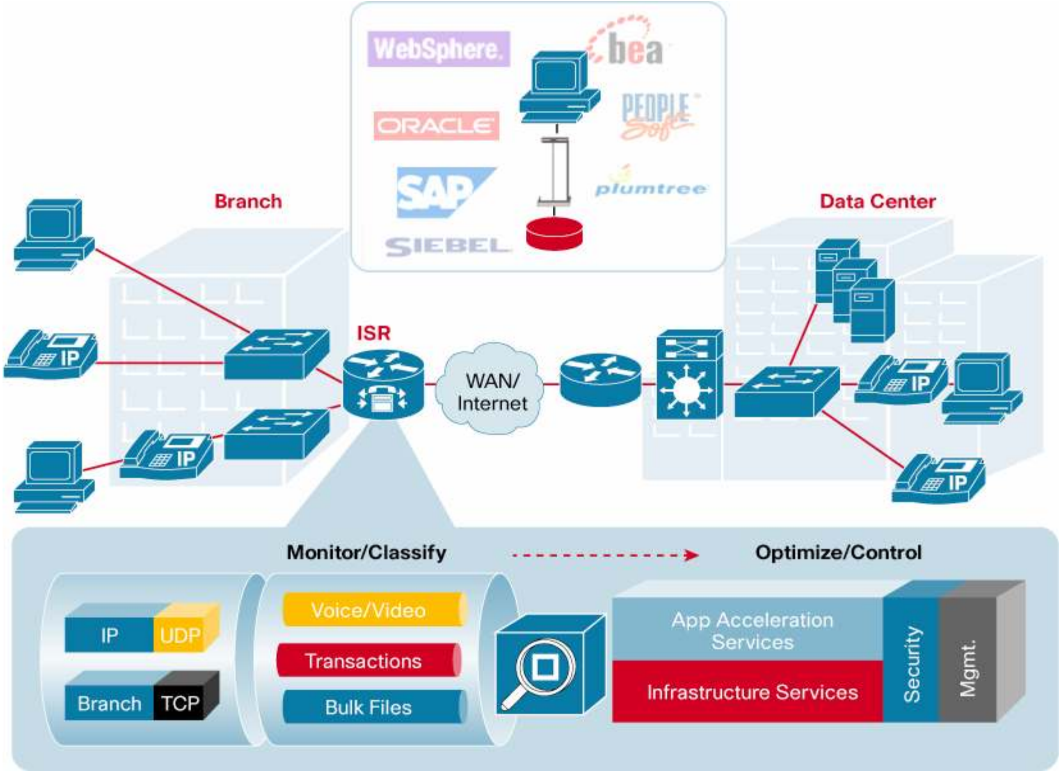
5.7.1.1 Accelerating Video using Cisco Wide Area Application Services

Cisco® Wide Area Application Services (WAAS) provides a simple and efficient solution for delivering high-quality live video and VoD throughout the enterprise while also providing state-of-the-art WAN acceleration for other TCP-based applications

Cisco WAAS 4.1 offers special protocol-level optimizations for Windows Media Technologies (WMT) over Real-Time Streaming Protocol (RTSP) according to specifications licensed from Microsoft. This special optimization is offered in addition to the generic Layer 4 optimization (transport flow optimization [TFO], data redundancy elimination [DRE], and Lempel-Ziv [LZ] compression) currently offered for other video formats and protocols, including VoD applications. This generic optimization covers video over HTTP, Adobe Flash, QuickTime, RealVideo, and any other video protocol delivered over TCP.

For live video events, the new Cisco WAAS 4.1 video application optimizer provides a simple solution with automatic and transparent video stream splitting at the edge of the network. The video optimizations provided by the Cisco WAAS 4.1 video application optimizer uses automatic stream classification at Layer 7 and does not require any management or coordination prior to or during the video event. This behavior enables reduced management overhead, simplifies the production of live video events, and allows each IT and video production group in the organization to concentrate on the task at hand.

Figure 20. Generic Framework for WAN and Application Optimization



5.7.2 Benefits of the Cisco WAAS Solution

Useful both for branches that want to optimize their network WAN bandwidth and consolidate their file servers and storage in centralized datacenters, as well as for service providers who want to add value to their bandwidth leasing, the Cisco WAAS solution provides significant overall benefits including:

- **Lower TCO:** Helps consolidate network, storage and file servers centrally, and eliminate or postpone the need to upgrade network bandwidth on existing WAN links of multisite and global organizations
- **Enhanced data protection:** Easier backup, restore, disaster recovery helps ensure business continuity
- **Reduced administration:** Easier overall management
- **Employee productivity:** Protocol-specific optimizations enable faster access to centralized back office applications and content, enhancing user productivity.
- **Latency, bandwidth and throughput improvements:** Cisco Network Capacity Expansion (NCE) module on Cisco Integrated Services Routers cost-effectively enables expansion of available bandwidth, reduction in bandwidth utilization, and increased data transfer rates on WAN links. Transparent network integration, allows Cisco WAAS to take advantage of traffic classification, QoS, policy-based routing, high availability, load balancing, and other network policies.

In turn, this permits network administrators to use freed bandwidth to roll out new applications such as voice and other advanced capabilities. They can additionally centralize remote resources to meet regulatory guidelines by consolidating branch servers, storage, and backup systems without impacting users. Cisco WAAS also improves the end-user experience by reducing latency, helping make workers more productive.

Since Cisco WAAS is an integrated services solution, it is deployed with zero additional footprint and adds no new appliances or recurring WAN costs. Service behavior is preserved through network transparency. With Cisco WAAS integrated with Cisco IOS Software, IT administrators achieve faster applications, reduced WAN expenses, and a consolidated branch through WAN optimization, application acceleration, and wide area fileservices.

Administrators benefit from a more easily managed WAN through better monitoring and provisioning, via NetFlow v9, better performance, visibility monitoring, and IP SLAs. They are also able to better preserve network services and protect their investment with dynamic autodiscovery and network transparency. Based on additional bandwidth, applications meet their goals through better QoS and call control using advanced queuing, shaping, and policing.

5.8 Wireless Applications

Providing a framework for a unified wireless architecture, Cisco Integrated Services Routers offer compelling wireless capabilities on the router platform.

5.8.1 Wireless LAN

Cisco Integrated Services Routers with wireless services provide a complete, secure, wireless infrastructure solution for enterprise branch offices, SMBs, public wireless LAN (WLAN) and Wi-Fi hotspots, and small remote offices and teleworkers. The Cisco Integrated Services Router portfolio supports integrated WLAN connectivity, Wi-Fi hotspot services, and centralized management.

Cisco is redefining best-in-class routing for the secure delivery of concurrent data, voice, video, and wireless services. The modular Cisco 1800, 2800, and 3800 Series as well as the fixed-configuration Cisco 800 and 1800 Series routers offer the industry's most comprehensive suite of wireless services to enable productivity enhancements for wireless enterprise branch offices, SMBs, public WLAN and Wi-Fi hotspots, small remote offices, and teleworker environments.

The Cisco Integrated Services Routers supporting the Cisco Unified Wireless Network enable deployment of secure, manageable WLANs optimized for remote sites and branch offices, including fast secure mobility, survivable authentication, and simplified management. The Cisco Unified Wireless Network addresses critical points of potential failure and helps enable resiliency and survivability for WLANs at remote locations and branch offices. This solution protects the WLAN by providing fast recovery from a variety of faults that may occur. With Cisco's high availability for remote WLANs, hardware and software work together to enable rapid recovery from disruptions and help ensure fault transparency to users and network applications.

The new Cisco 860, 880 and 890 fixed routers with IEEE 802.11n support both unified and autonomous deployments and are ideal for small branch offices and teleworkers who need to be connected to larger enterprise networks as well for as small businesses. This integrated Wi-Fi access point offers IEEE 802.11n draft 2.0 standard support for mobile access to high-bandwidth data, voice, and video applications through the use of multiple-input, multiple-output (MIMO) technology that provides increased throughput, reliability, and predictability. IEEE 802.11n wireless networks create a cohesive working environment by combining the mobility of wireless with the performance of wired networks. Cisco has innovative, next-generation wireless solutions that offer greater performance and extended reach for pervasive wireless connectivity. IEEE 802.11n technology delivers outstanding reliability and up to nine times the throughput of current IEEE 802.11 a/b/g networks. It makes wireless networks an integral part of every type of organization by offering the following benefits:

- Data rates of up to 600 Mbps support more users, devices, and mission-critical, bandwidth-intensive applications.
- New MIMO technology provides predictable WLAN coverage and reliable connectivity.
- Next-generation wireless technology provides the greatest investment protection to support emerging mobile applications.

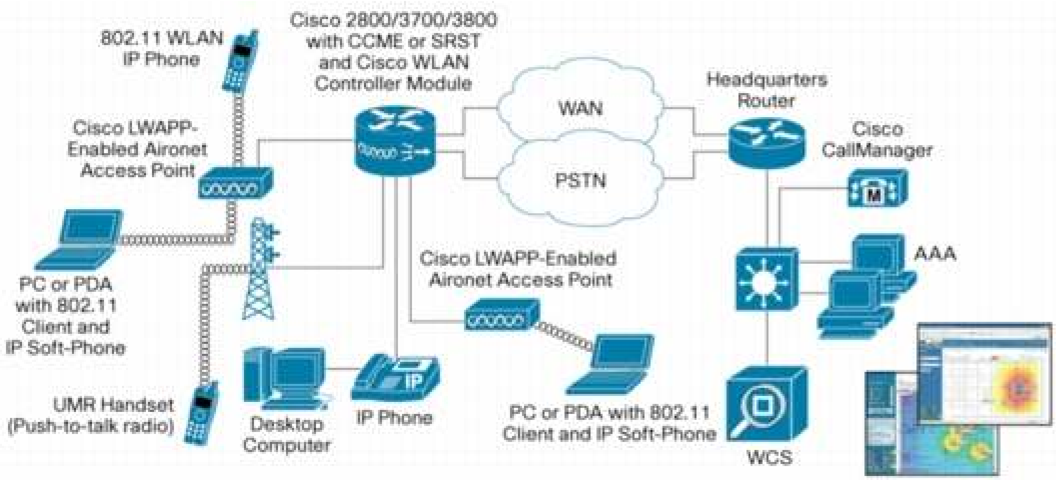
These routers help extend corporate networks to secure remote sites while giving users access to the same applications found in corporate offices for both data and voice applications. When users require WLAN access, visibility and control of network security are even more critical at the remote site. The new fixed Cisco Integrated Services Routers meet this need with a single device that combines integrated IEEE 802.11g/n capabilities with security features such as Wi-Fi Protected Access (WPA), including authentication with IEEE 802.1X with the Cisco Light Extensible Authentication Protocol (LEAP) and Protected EAP (PEAP) and encryption with the WPA Temporal Key Integrity Protocol (TKIP).

Cisco Wireless LAN Controllers

Cisco Wireless LAN Controllers work in conjunction with Cisco Lightweight Access Points and the Cisco Wireless Control System (WCS) to provide systemwide WLAN functions. As components of the Cisco Unified Wireless Architecture, Cisco Wireless LAN Controllers present network administrators with the visibility and control necessary to effectively and securely manage business-class WLANs and mobility services, such as enhanced security, voice, guest access, and location services. Cisco Wireless LAN Controllers help reduce overall operating expenses by simplifying network deployment, operations, and management. The flexibility allows network managers to design networks to meet their specific needs, whether implementing standalone or highly integrated network designs.

The Cisco Wireless LAN Controller Module allows SMBs and enterprise branch offices to cost-effectively deploy and manage secure WLANs. The module provides outstanding security, mobility, and ease of use for business-critical WLANs, delivering the most secure enterprise-class wireless system available today. As a Cisco Integrated Services Router module, it delivers centralized security policies, wireless IPS capabilities, award-winning radio frequency management, QoS, and Layer 3 fast secure roaming for WLANs. The Cisco Wireless LAN Controller Module manages 6, 8, 12, and 25 Cisco Aironet Lightweight Access Points and is supported on Cisco 2800 3800 Series Integrated Services Routers (Figure 21).

Figure 21. Cisco Wireless LAN Controller Module with Cisco Integrated Services Routers


802.11 WLAN IP Phone
Cisco 2800/3700/3800 with CCME or SRST and Cisco WLAN Controller Module
WAN
PSTN
Headquarters Router
Cisco CallManager
Cisco LWAPP-Enabled Aironet Access Point
PC or PDA with 802.11 Client and IP Soft-Phone
Cisco LWAPP-Enabled Aironet Access Point
AAA
UMR Handset (Push-to-talk radio)
Desktop Computer
IP Phone
PC or PDA with 802.11 Client and IP Soft-Phone
WCS

The Cisco Wireless LAN Controller Module enables enterprises to create and enforce policies that support business-critical applications. From voice and data services to location tracking, the Cisco Wireless LAN Controller Module provides the control, scalability, and reliability that IT managers need to build secure enterprise-class IEEE 802.11 wireless networks.

Significant other benefits include the following:

- **Intelligent RF management**: The Cisco Wireless LAN Controller Module comes equipped with embedded software for adaptive real-time RF management. The Cisco Centralized Wireless Solution uses Cisco's patent-pending Radio Resource Management (RRM) algorithms, which detect and adapt to changes in the air space in real time. These adjustments create the optimal topology for wireless networking in much the same way that routing protocols compute the best possible topology for IP networks. Cisco RMM creates an intelligent RF control plane for self-configuration, self-healing, and self-optimization of the wireless network.

- **Enterprise-class security**: The Cisco Wireless LAN Controller Module adheres to the strictest level of security standards, including:

  ◦ IEEE 802.11i Wi-Fi Protected Access 2 (WPA2), WPA, and Wired Equivalent Privacy (WEP)

  ◦ IEEE 802.1X with multiple Extensible Authentication Protocol (EAP) types: PEAP, EAP with Transport Layer Security (EAP-TLS), EAP with Tunneled TLS (EAP-TTLS), and Cisco LEAP

  The result is the industry's most comprehensive WLAN security solution.

  In the Cisco Centralized Wireless LAN Solution, access points act as air monitors, communicating real-time information about the wireless domain to Cisco Wireless LAN Controllers. All security threats are rapidly identified and presented to network administrators through Cisco WCS, where accurate analysis can take place and corrective action can be taken.

  Cisco provides the only WLAN system that offers simultaneous wireless protection and WLAN service delivery, helping ensure complete WLAN protection, with no unnecessary overlay equipment costs or additional monitoring devices. The Cisco Centralized Wireless LAN Solution can be deployed initially as a standalone wireless IPS, and reconfigured later to add WLAN data service. This approach allows network managers to create a defense shield around their RF domains, containing unauthorized wireless activity until they are ready to deploy WLAN services.
- **Real-time application support:** The Cisco Centralized Wireless LAN Solution provides best-in-class performance to support real-time applications such as voice. The Cisco Wireless LAN Controller Module enables rapid handoff between access points, providing smooth mobility with no interruption in service to the client. Intelligent queuing and contention management schemes provide effective resource management of the air space. The Cisco Wireless LAN Controller Module also supports QoS capabilities that are Wi-Fi multimedia (WMM)-compliant and closely mirror the emerging IEEE 802.11e standard. Full compliance with the finished standard will be achieved through a software upgrade when the final standard is ratified.
- **Mobility**: The Cisco Wireless LAN Controller Module allows users to roam between access points and across bridged and routed subnets without requiring changes to underlying infrastructure. Security and QoS context information follows users wherever they roam, helping ensure that mobility does not compromise performance, reliability, or privacy. The Cisco Wireless LAN Controller Module does not require any modifications to existing infrastructures or client devices to enable mobility (mobile IP, for example).
- **Simplified deployment and management**: The Cisco Wireless LAN Controller Module is easy to deploy and cost effective to own and operate. It provides high flexibility for deployment in SMBs and enterprise branch offices. It supports zero-touch deployments that do not require manual configuration or preconfiguration of the access points. It also supports template-based configuration management. These intuitive templates enable the quick application of systemwide security configurations, QoS policies, mobility groups, back-end services, and other critical configurations through the easy-to-use, award-winning Cisco Centralized Wireless LAN Solution user interface. When deployed with the Cisco WCS, it supports enhanced monitoring and troubleshooting features, including intuitive heat map displays, alarm filtering, event correlation, and granular reporting tools.

5.8.2 3G Wireless WAN

With new high-speed 3G wireless technologies taking shape in the marketplace, businesses now have new drivers to engrain mobility into business processes. Many firms use 3G for remote access connectivity for mobile workers. New advancements in downlink and uplink speed and lower network latency now enable 3G to be used for basic connectivity in the office to enable business-critical applications. 3G is no longer reserved for the mobile and field worker.

Cisco is offering 3G Wireless WAN on the Integrated Services Router (ISR) platform to provide customers with true multipath WAN backup and rapidly deployable primary WAN connectivity. Cisco 3G solutions support the latest 3G standards HSPA (uplink data rate of 2.0 Mbps and upgradable to 5.7 Mbps and downlink 7.2 Mbps) and EVDO Rev A (uplink data rate of 1.8 Mbps and downlink of 3.2 Mbps) which are backward compatible with widely deployed networks namely HSDPA/UMTS/EDGE/GPRS and EVDO Rev 0/ 1xRTT respectively.

Cisco 3G WWAN supported on 880 series (fixed ISRs) and 1841/2800/3800 series (modular ISRs) combine traditional enterprise router functionality, such as remote management, advanced IP services such as VoIP and security, with mobility capabilities of 3G wide-area network (WAN) access. Utilizing high-speed 3G wireless networks, routers can replace or complement existing landline infrastructure, such as dialup, frame relay and ISDN.

Examples of use case scenarios for 3G enabled ISRs such as:

- **3G as primary access:** 3G provide typical uplink speeds of 600 -1400 Kbps, downlink of 800 – 3200 Kbps and round trip latency under 120ms, offer a secure, high speed and cost-effective alternative to traditional landline access methods such as frame relay and ISDN. Many environments that rely on ports providing uplink access in the 56-Kbps to 256-Kbps range could benefit from added flexibility and mobility from 3G.
- **3G as backup access:** Companies seeking network redundancy and business continuity for critical applications and communications can leverage emerging high-speed wireless networks as an optimal alternative to terrestrial wired connections.
- **Cost savings and usability:** Retail environments that rely on low-speed port connections for point-of-sale transactions or new store site locations where wireline access may not be available
- **Solution flexibility and rapid implementation:** Making use of temporary locations such as automated teller machine (ATM) connections at sporting events or data connectivity to support promotional retail kiosks

Additional benefits of Cisco 3G enabled ISR include rapid deployment, remote management, portability, operational efficiency and scalability.

5.9 Cisco Application Extension Platform

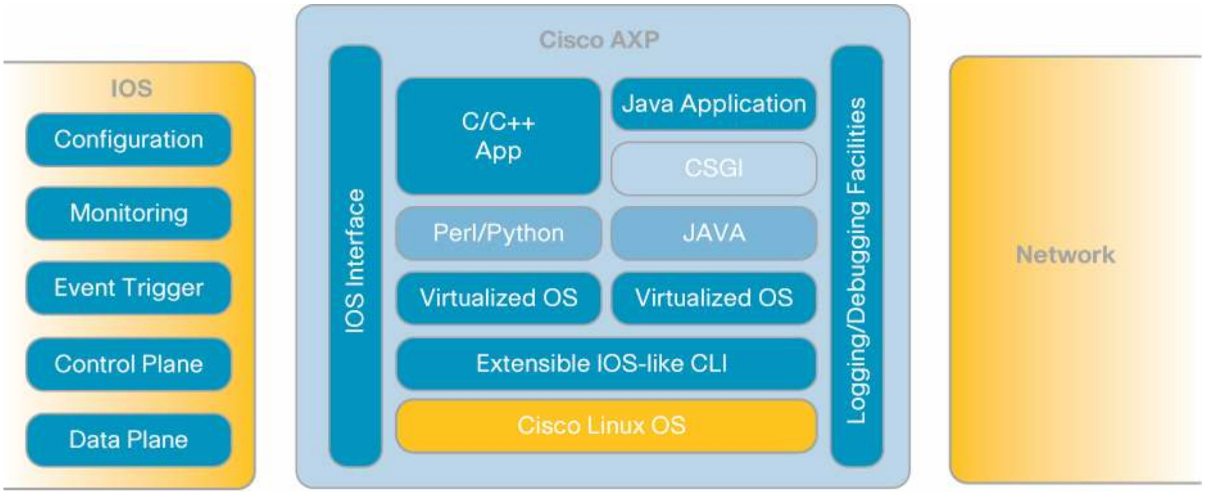
The Cisco AXP on Cisco Integrated Services Routers establishes an open network platform to facilitate the extension of flexible hosting functions to application services. Cisco AXP physically resides inside the Cisco Integrated Services Router (as a network module or advanced integration module) and provides a service platform for applications to run all or portions of their code.

The Cisco AXP service modules can enhance the function, intelligence, and flexibility of the router by running applications that interface with the Cisco Integrated Services Router. The applications also can use router services through the APIs, resulting in unique capabilities and function.

- Cisco AXP allows third parties such as system integrators, managed service providers, and large enterprise customers to extend the functions of Cisco Integrated Services Routers by providing their own value-added integrated services.
- On the application service module, Cisco AXP hosts applications in a separate runtime environment with dedicated resources.
- Cisco AXP provides APIs so that functions such as packet analysis, event notification, and network management can be used by hosted applications.

With Cisco AXP, customers can develop their own applications to run on the router. Various languages such as Java, C, Perl, Bash, and Python are supported, and additional language support can be added (Figure 22).

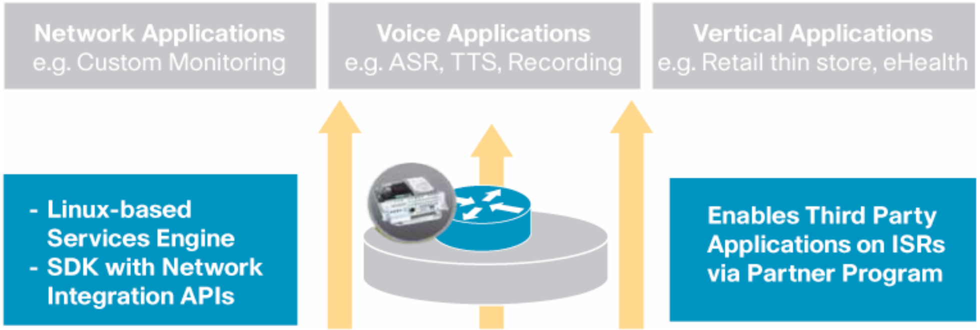
Figure 22. Cisco Application Extension Platform Framework



Cisco AXP's standards-based hosting infrastructure includes a hardened Cisco Linux OS, a virtualized application OS through Linux V-Server technology, and a logging and debugging infrastructure. Cisco AXP also allows installation of additional language and library support during the installation process so that customers are not limited to the out-of-the-box support shipped with each Cisco AXP service module.

Through Cisco AXP virtualization services to applications, customers can extend the existing network utilities footprint to include even more specific applications, each running its own separate virtual container on the same Cisco AXP service module (Figure 23).

Figure 23. Third-Party Application Hosting on Cisco Integrated Services Routers Through Cisco AXP


Network Applications
e.g. Custom Monitoring
Voice Applications
e.g. ASR, TTS, Recording
Vertical Applications
e.g. Retail thin store, eHealth
- Linux-based Services Engine
- SDK with Network Integration APIs
Enables Third Party Applications on ISRs via Partner Program

Cisco AXP also offers a software development kit (SDK) that enables critical packaging functions and a management interface that facilitates centralized management schemes. Cisco AXP management services provides centralized and proactive monitoring by forwarding Cisco AXP application and Cisco Integrated Services Routers alerts to central management tools.

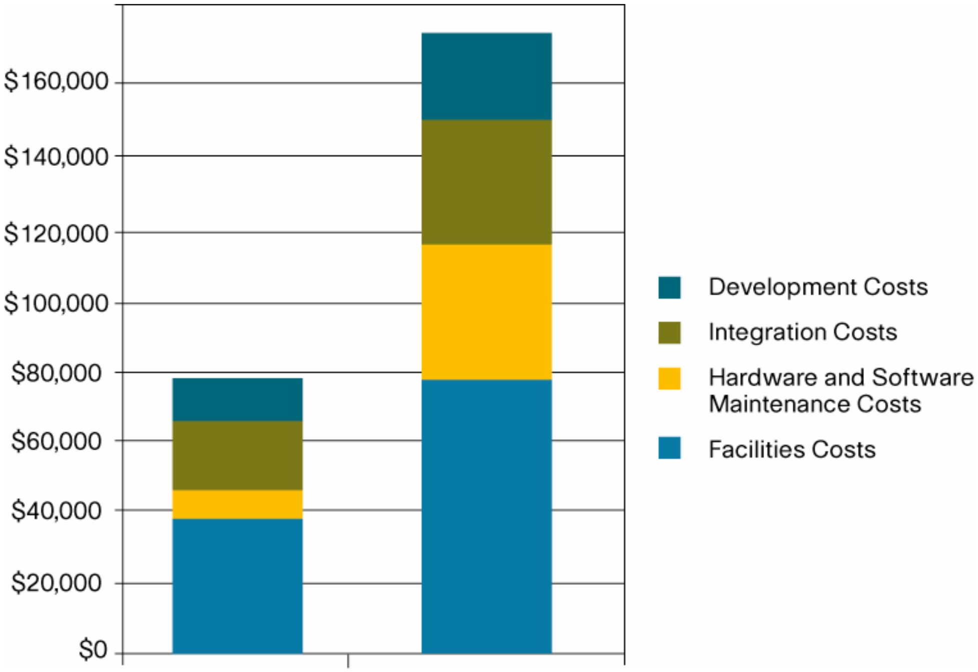
5.9.1 Cisco AXP: Doing More with Less

Cisco AXP truly uses the network as a platform and enhances the performance of the application by interacting with common network services such as authentication, security, and routing to applications. Cisco AXP can be separated into two fundamental areas:

- Facilities and frameworks to host third-party applications
- Service APIs to integrate the application into the network

Ownership and operation of a Cisco AXP environment can yield cost savings in several primary areas. A TCO model based on rigorous research and empirical data from use cases can be used to detail the possible cost savings. This model looks at operating expenses in a scenario with 10 branch-office sites. Each branch office is estimated to have an average of 50 employees. The model accounts for expenditures over a 3-year lifecycle. It factors in development, integration, maintenance, and facilities costs. Figure 24 illustrates the consolidated cost savings from the TCO model.

Figure 24. Consolidated Cost Savings from a Cisco AXP Deployment



As shown in the figure, there is a clear savings of US$87,000 in a 10-branch scenario over 3 years. These savings indicate that Cisco AXP basically pays for itself during the 3-year lifecycle in contrast to the assumed TCO of a system of independent appliances.

The second-order benefits of employing the Cisco AXP technology include the capability to run multiple applications on a virtualized OS. Instead of running several servers with low utilization, you can run one Cisco AXP blade at optimum capacity, reducing costs as well as requiring less administrative staff.

5.10 Network Management and Instrumentation

One of the most important features in a product is its manageability. This Cisco Integrated Services Router provides a comprehensive management framework to suit all aspects of the management lifecycle both for device-level management and network-level management. In addition an open framework for integration with 3rd-party management tools is also provided.

Cisco management solutions address a broad range of needs and capabilities. These include:

- Integrated tools with streamlined user interfaces to simplify management tasks
- Automation with extended visibility to ease network deployment and hardware migration
- Zero-touch deployment options to further minimize deployment and operational costs
- Provisioning templates, configuration management, and monitoring tools to reduce risks from planed and unplanned network changes
- Robust “network view” of configuration, connection, and security policy compliance

- Active performance monitoring, alerting and isolation of trouble to predict and mitigate outages, while providing the right information for quick trouble identification and resolution
- Advanced analytics providing “what-if” analysis, configuration verification, and failure analysis for network resiliency planning
- Easy-to-use security monitoring and provisioning tools to help ensure security compliance
- Additional, comprehensive, end-to-end security tools to enable a self-defending network
- Enable new services through an integrated management framework that combines foundation management and advanced technology management services with the ability to integrate and cross uses tools for advanced and more detailed data, analysis and control
- Allow customers to add additional management solutions to address prioritized needs without causing disruptions in service or accessibility

5.10.1 Cisco Router and Security Device Manager

The Cisco Router and SDM is an easy-to-use web-based GUI and is meant for single-device management. It implements NSA guidelines and ICSA and Cisco TAC recommendations and provides one-touch router lockdown. It is factory-loaded and free of cost and is the industry-leading router and comprehensive security device management tool for VPN, firewall, routing, wireless, LAN and WAN interfaces, and QoS. It can significantly reduce the technical expertise required to configure the Cisco Integrated Services Router and reduce configuration errors.

5.10.2 Cisco Configuration Professional

Cisco Configuration Professional is a GUI-based device management tool for Cisco Integrated Services Routers. The application simplifies router, security, unified communications, WAN, and basic LAN configuration through easy-to-use wizards.

Cisco Configuration Professional is a valuable productivity-enhancing tool for network administrators and channel partners deploying routers in medium-sized businesses and enterprise branch offices. The application allows you to implement router, unified communications, and security configurations quickly and easily, thereby reducing costs. Cisco Configuration Professional configurations are approved by the Cisco Technical Assistance Center (TAC), meaning that configuration checks built into the application reduce errors

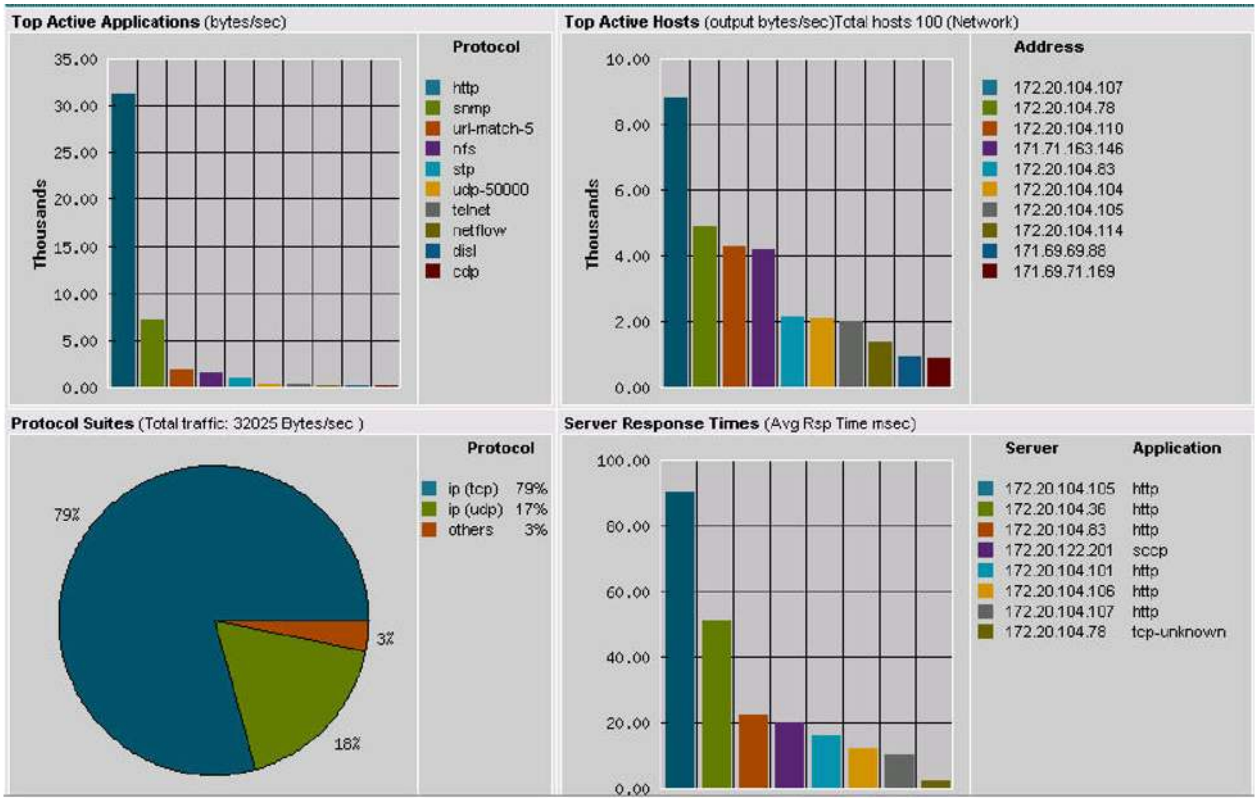
5.10.3 Cisco Network Analysis Module

The Cisco Branch Routers Series Network Analysis Module (NME-NAM) is an integrated service module that offers performance monitoring, traffic analysis, and advanced troubleshooting to meet the performance assurance needs of today's dynamic and evolving enterprises. It can be activated in the Cisco Integrated Services Router without negatively affecting performance, users, or other services.

The unique design of Cisco Branch Routers Series NAM combines a rich set of embedded data collection capabilities and performance analytics with a remotely accessible, web-based Traffic Analyzer GUI, all of which reside on a single network module that is easily installed into the Cisco 2800 and 3800 Series Integrated Services Routers.

The web-based GUI provides quick access to the configuration menus and application performance views for voice, video, and TCP-based applications. It also offers comprehensive traffic analysis with detailed information about VLANs, differentiated services (DiffServ), hosts, conversation pairs, and application use that is essential for managing effective and reliable delivery of applications (Figure 25).

Figure 25. Monitoring with Cisco Branch Routers Series NME-NAM Traffic Analyzer



The Cisco Branch Router Series NME-NAM offers a broad set of application performance measurements to accurately characterize the end-user experience for the services delivered in the branch office. It offers standards-based voice-quality measuments using mean opinion score and key performance indicators such as jitter and packet loss. It also monitors performance for TCP-based application using transaction and session-based statistics such as response time, retransmission time, transaction time, and data transfer time.

The Cisco Branch Router Series NME-NAM complements the Cisco WAAS solution on the Cisco Integrated Services Router, providing important predeployment and postdeployment visibility into traffic patterns and trends. Cisco WAAS accelerates traffic without modifying IP headers, helping ensure that data collection and analysis are uncompromised. The Cisco Branch Router Series NME-NAM uses the built-in instrumentation on Cisco Wide Area Application Engine (WAE) devices to provide end-to-end visibility in a Cisco WAAS environment. It delivers baseline metrics that can be used to measure business impact and monitor ongoing operations, and it offers critical insight into the behavior of new hosts and applications that appear on the WAN.

5.10.4 OAM Enhancements to Support Metro Ethernet Access

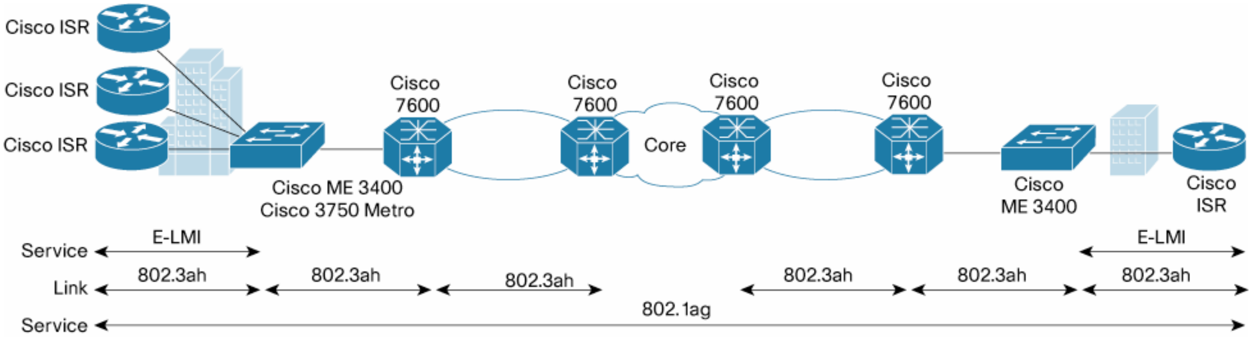
To enhance the manageability of Ethernet access on the Cisco Integrated Services Routers, standards-based features are implemented for operations, administration, and maintenance (OAM). Carrier Ethernet OAM and connectivity fault management on the Cisco Integrated Services Routers provide the following capabilities (Figure 26):

- **Metro Ethernet Forum (MEF) 16**: Ethernet local management interface (E-LMI) customer-edge function
- **IEEE 802.1ag**: Connectivity fault management (CFM) OAM
- **IEEE 802.3ah** - Link protection and monitoring

Benefits of these services include:

- End-to-end service manageability
- First-mile physical connectivity verification
- Proactive service status and availability

Figure 26. Carrier Ethernet OAM with End-to-End Manageability

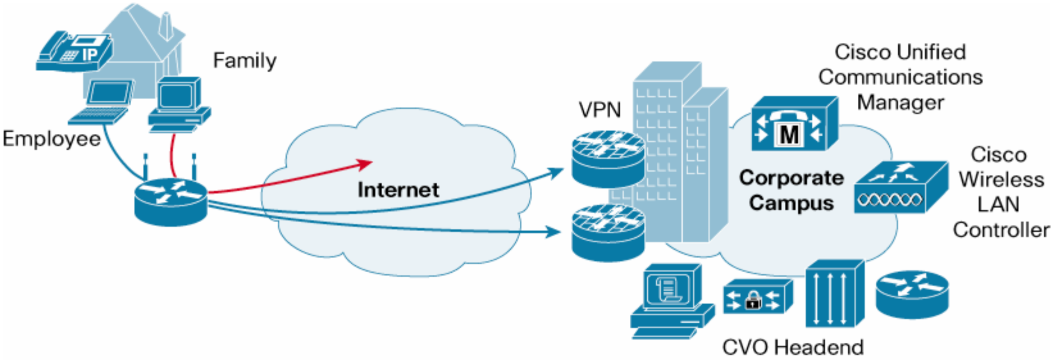


5.11 Cisco Virtual Office

The Cisco Virtual Office solution provides secure, rich network services to workers at locations outside the traditional corporate office, including teleworkers, full- and part-time home-office workers, mobile contractors, and executives. By providing extensible network services that include data, voice, video, and applications, the Cisco Virtual Office effectively creates a comprehensive office environment for employees, regardless of their locations (Figure 27).

The Cisco 870, 880, and 1800 Series Integrated Services Routers support Cisco Virtual Office for a teleworker scenario; Cisco 1800 and 2800 Series Integrated Services Routers for small office and home office (SOHO) access; and Cisco 1800, 2800, and 3800 Series Integrated Services Routers for a site-to-site or branch-office deployment.

Figure 27. Cisco Virtual Office Components


IP
Family
Employee
Internet
VPN
Cisco Unified Communications Manager
M
Corporate Campus
Cisco Wireless LAN Controller
CVO Headend

A typical Cisco Virtual Office include the following components:

- **Remote-site presence:** This equipment, which resides on the end user's premises, includes a Cisco 800 Series Integrated Services Router and a Cisco Unified IP Phone 7965G.
- **Headend presence:** This portion of the solution is responsible for remote-site aggregation; it includes a VPN router to aggregate and terminate the secure, encrypted tunnels from each remote-site location. This infrastructure also supports other VPN technologies such as SSL and L2TP over IPsec VPNs, effectively serving as a single point of convergence for multiple secure-access technologies. The headend also includes centralized management software for policy, configuration, and identity controls.

- **Deployment and ongoing services:** Service offerings from Cisco and approved partners support successful headend solution component deployment and integration, provide consultative guidance for automating the deployment and management of remote sites, and deliver ongoing operational support and optimization.

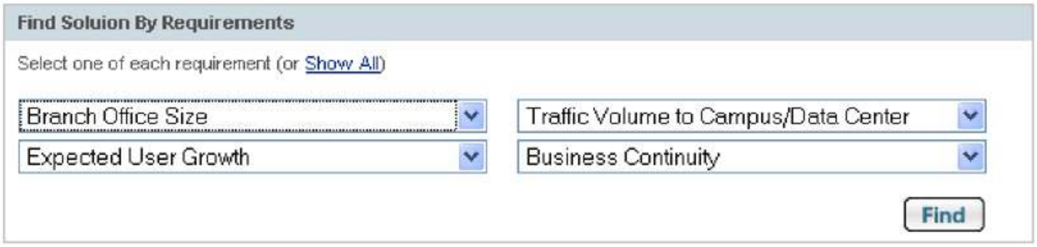
From an IT perspective, the Cisco Virtual Office solution provides a headend architecture for simplified management and operations. This architecture drastically improves IT scalability, offers robust and flexible security, and reduces costs while improving the manageability of remote sites.

5.12 Cisco Validated Designs

To help enterprises plan and deploy a branch office network, the Cisco Integrated Services Branch Networks offer Cisco Validated Design solutions on those network services that integrate directly into Cisco Integrated Services Routers.

The Cisco Validated Design solutions address requirements of six typical branch-office networks that provide business-relevant functions, such as network security, unified communication, and application optimization. Figure 29 shows the set of inputs that can be specified to identify an appropriate design for the branch office. Figure 30 shows sample output.

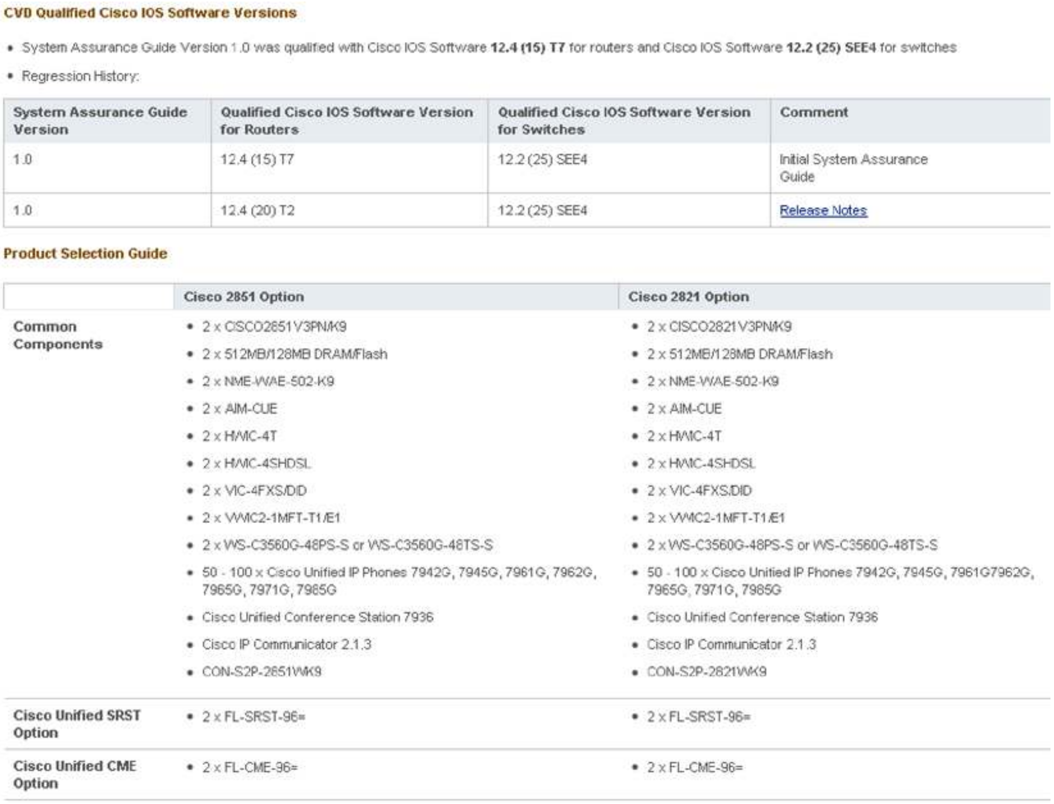
Figure 28. Specifying Branch-Office Solution Requirements



Find Soluion By Requirements

Select one of each requirement (or Show All)

Figure 29. Sample Output of the Cisco Validated Designs for Cisco Integrated Services Routers



CVD Qualified Cisco IOS Software Versions

- System Assurance Guide Version 1.0 was qualified with Cisco IOS Software **12.4 (15) T7** for routers and Cisco IOS Software **12.2 (25) SEE4** for switches
- Regression History:

System Assurance Guide Version	Qualified Cisco IOS Software Version for Routers	Qualified Cisco IOS Software Version for Switches	Comment
1.0	12.4 (15) T7	12.2 (25) SEE4	Initial System Assurance Guide
1.0	12.4 (20) T2	12.2 (25) SEE4	Release Notes

Product Selection Guide

	Cisco 2851 Option	Cisco 2821 Option
Common Components	• 2 x CISCO2851V3PN/K9 • 2 x 512MB/128MB DRAM/Flash • 2 x NME-WAE-502-K9 • 2 x AIM-CUE • 2 x HWIC-4T • 2 x HWIC-4SHDSL • 2 x VIC-4FXS/DID • 2 x VWIC2-1MFT-T1/E1 • 2 x WS-C3560G-48PS-S or WS-C3560G-48TS-S • 50 - 100 x Cisco Unified IP Phones 7942G, 7945G, 7961G, 7962G, 7965G, 7971G, 7985G • Cisco Unified Conference Station 7936 • Cisco IP Communicator 2.1.3 • CON-S2P-2851WK9	• 2 x CISCO2821V3PN/K9 • 2 x 512MB/128MB DRAM/Flash • 2 x NME-WAE-502-K9 • 2 x AIM-CUE • 2 x HWIC-4T • 2 x HWIC-4SHDSL • 2 x VIC-4FXS/DID • 2 x VWIC2-1MFT-T1/E1 • 2 x WS-C3560G-48PS-S or WS-C3560G-48TS-S • 50 - 100 x Cisco Unified IP Phones 7942G, 7945G, 7961G7962G, 7965G, 7971G, 7985G • Cisco Unified Conference Station 7936 • Cisco IP Communicator 2.1.3 • CON-S2P-2821WK9
Cisco Unified SRST Option	• 2 x FL-SRST-96=	• 2 x FL-SRST-96=
Cisco Unified CME Option	• 2 x FL-CME-96=	• 2 x FL-CME-96=

Each Cisco Validated Design solution has undergone an extensive design review, an intensive system assurance test program, and a comprehensive documentation effort. An ongoing, sustained development plan helps ensure that Cisco Validated Design solutions are periodically updated to reflect the evolution of networking technologies and ongoing business requirements.

Cisco Integrated Services Branch Networks provide technical decision makers with a solution that enables them to design and deploy a secure, reliable, high-performance, yet functionally rich, remote-office network infrastructure. The solution includes the following elements:

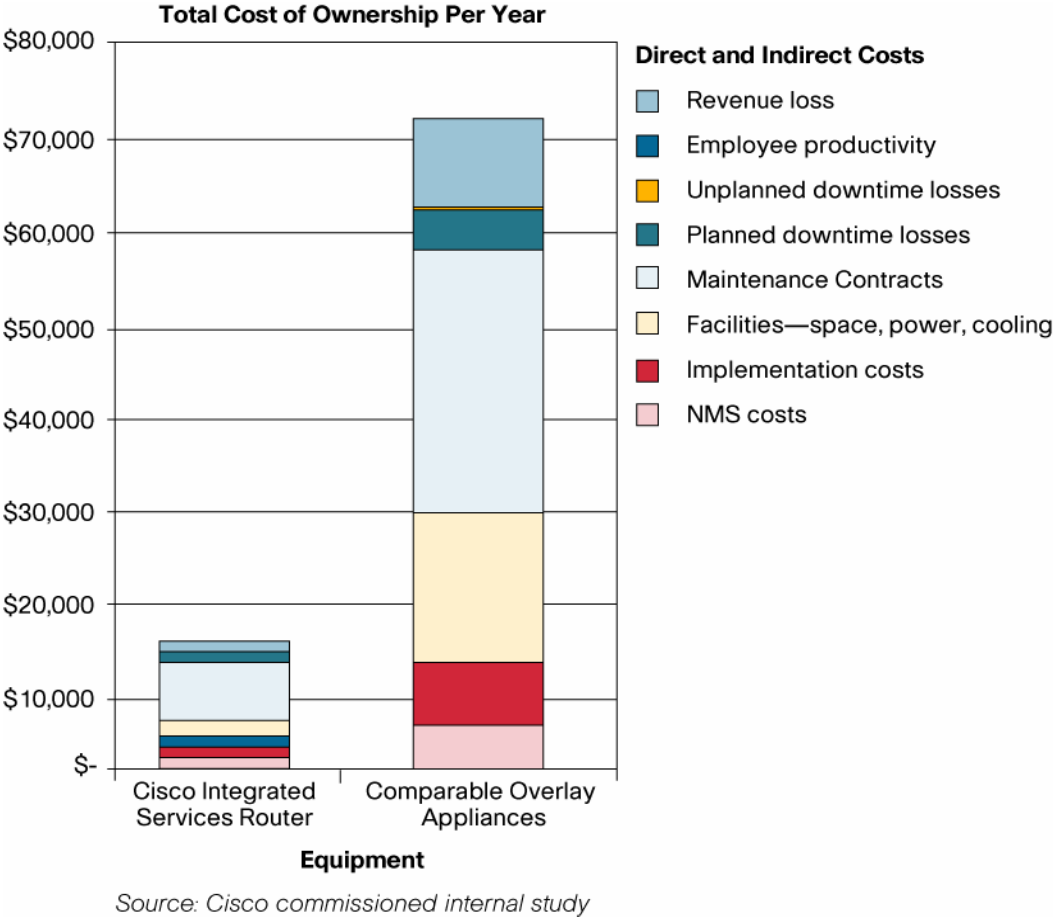
- **Design validation:** Increases integrity and quality of branch network infrastructure
- **Documentation:** Provides detailed design, implementation, and testing information
- **Product recommendations:** Offers product selection and software release guidance
- **Configuration toolkit:** Simplifies, accelerates, and automates network deployment
- **Sustained development plan:** Extends value and protects infrastructure investment
- **Hardened Cisco IOS Software recommendation: Reduces** time to market and support costs

6.0 Benefits of a Cisco Integrated Services Router

The benefits of using integrated services on the branch router are manifold both for the device owner who owns and manages the device as well as the end user who experiences services off the integrated services router.

- **Lower operational costs and TCO:** Typically the costs for initial purchase are minimal compared to the ongoing operational costs. The industry generally assigns 20% of the total lifetime costs for a system toward CapEx and the remaining 80% toward OpEx and unscheduled blackouts (Figure 31).

Figure 30. Comparing TCO of a Cisco Integrated Services Router with Overlay Appliances



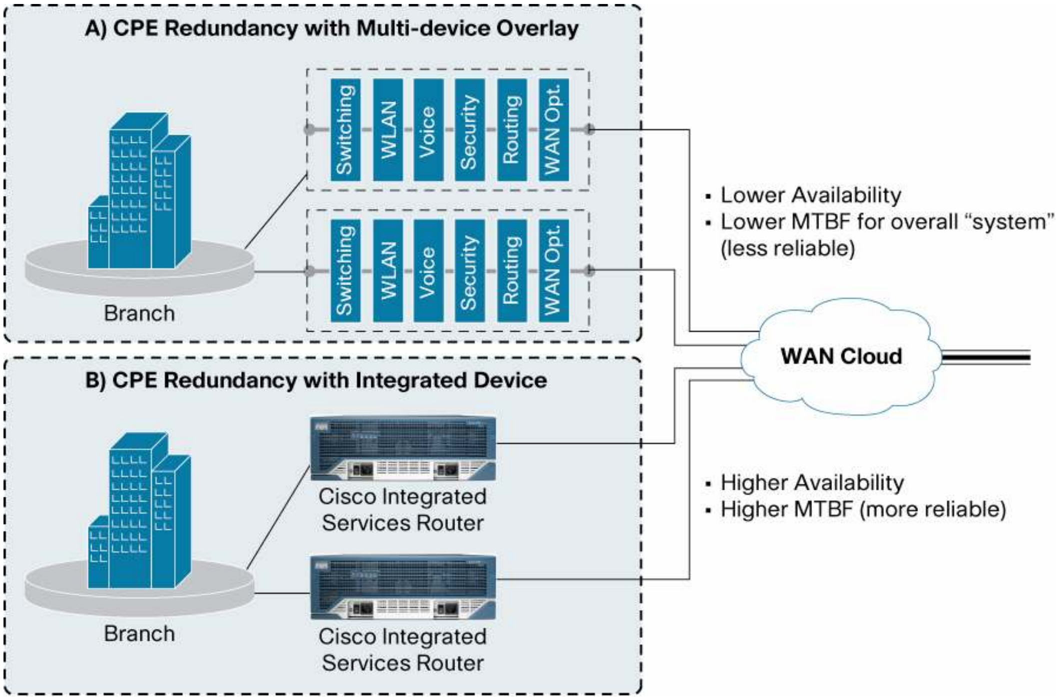
Source: Cisco commissioned internal study

An internal Cisco commissioned study to find out the TCO savings for the Cisco Integrated Services Router as opposed to a set of comparable overlay appliances (for a similar functional solution deliverable) estimated direct and indirect cost savings in the range of 40-70% per year considering operational costs alone.

- **Enhanced productivity:** From an administrative standpoint, with lower maintenance, lesser troubleshooting, minimal training etc., the productivity and efficiency of the IT department is enhanced.
- **Higher availability:** Today’s multi-service networks demand high availability to deliver on “anytime” services. The ability to have multi-level redundancy and quick failover either at a system or network level is essential for business continuity.
- From a network engineering standpoint, it is common practice to make the critical components of the CPE network redundant to provide for failover in case the primary device fails. This can cause problems in an overlay scenario with:
  - The cost factor of duplicating multiple devices
  - The overall system availability which, in fact, goes down because the number of “weak links” in the chain potentially increases

Statistical modeling for reliability engineering states that the more the components in an overall system, the lower is the Mean Time between Failures (MTBF), and lower is availability (Figure 32).

Figure 31. Comparison of CPE Redundancy Deployment Scenarios


A) CPE Redundancy with Multi-device Overlay
Switching
WLAN
Voice
Security
Routing
WAN Opt.
Switching
WLAN
Voice
Security
Routing
WAN Opt.
Branch
▪ Lower Availability
▪ Lower MTBF for overall "system" (less reliable)
WAN Cloud
B) CPE Redundancy with Integrated Device
Cisco Integrated Services Router
Cisco Integrated Services Router
Branch
▪ Higher Availability
▪ Higher MTBF (more reliable)

A redundant solution with a single Cisco Integrated Services Router is far superior from a cost, availability, and manageability perspective.

To further minimize downtime, the higher-end Cisco Integrated Services Routers such as the Cisco 3800 Series implement a host of availability features at the system level. These include optional redundant power supplies, Error Checking and Correction (ECC) memory for improved fault isolation and correction, USB Flash memory for ease of image recovery, advanced temperature monitoring and variable-speed cooling fans, Cisco IOS Software Warm Reboot for improved bootup times, network-module online insertion and removal, and field-replaceable components such as fan tray, motherboard, and power supplies (Cisco 3845 only).

Additionally, Cisco IOS Software provides for resiliency at the control and data planes and allows for a variety of network engineering solutions to enhance availability.

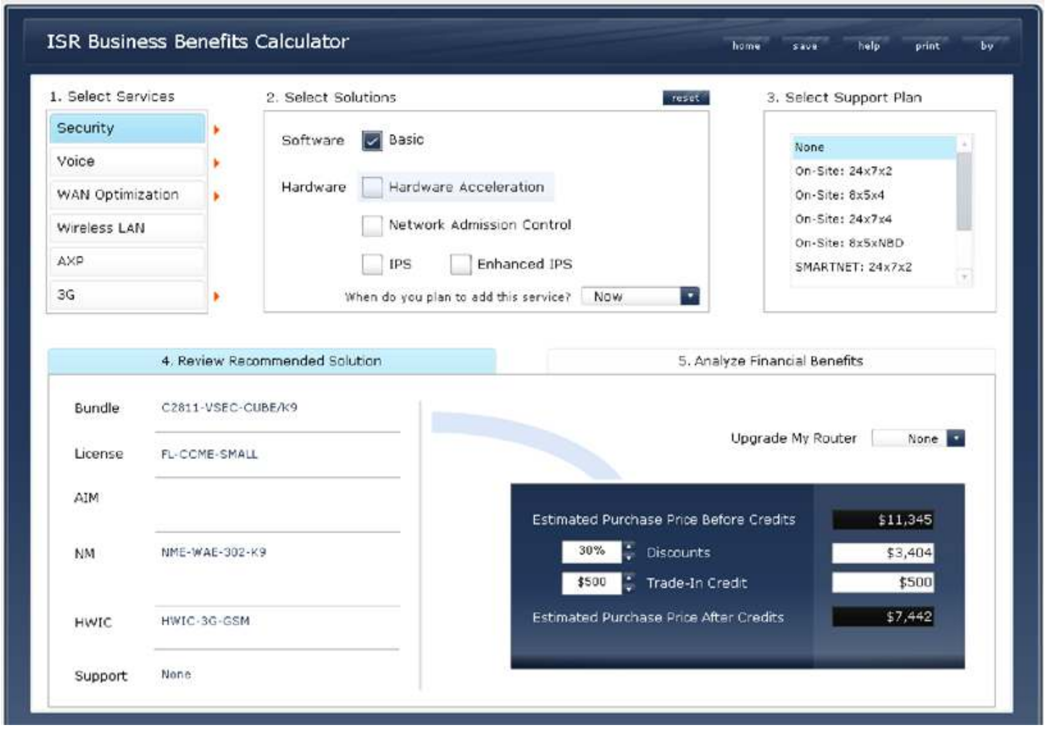
Other significant benefits of adopting a Cisco Integrated Services Router follow:

- **Smaller form factor**: Smaller rack-space consumption and less power requirements are significant advantages for space-constrained IT departments, data centers, and service providers offering managed service solutions.
- Effective monitoring and diagnostics**: It is far easier to integrate OAM capabilities and** to troubleshoot.
- **Easier systems integration:** It is easier to configure, deploy and maintain.
- **Simpler end-to-end solution design:** Simpler topologies, lesser interoperability issues lead to a superior solution.
- **Cisco brand:** Buying and deploying a Cisco Integrated Services Router also means building on the staying power of a market leader with a track record for meeting customer and channel commitments.
- **Enhanced productivity:** From an administrative standpoint, with lower maintenance,

6.1 Cisco Integrated Services Routers Business Benefits Calculator

The Cisco Integrated Services Routers Business Benefits Calculator helps model various requirements of a typical branch-office network that provides business-relevant functions such as network security, unified communications, WAN optimization, WLAN, 3G, and Cisco AXP. Figure 32 shows a snapshot of the modeling tool.

Figure 32. Snapshot of Cisco Integrated Services Routers Business Benefits Calculator: Model Service Requirements for Branch Offices



Software ☑ Basic

Hardware □ Hardware Acceleration

□ Network Admission Control

□ IPS □ Enhanced IPS

When do you plan to add this service? Now

Bundle	C2811-VSEC-CUBE/K9
License	FL-CCME-SMALL
AIM	
NM	NME-WAE-302-K9
HWIC	HWIC-3G-GSM
Support	None

Upgrade My Router None

	Estimated Purchase Price Before Credits	$11,345
30%	Discounts	$3,404
$500	Trade-In Credit	$500
	Estimated Purchase Price After Credits	$7,442

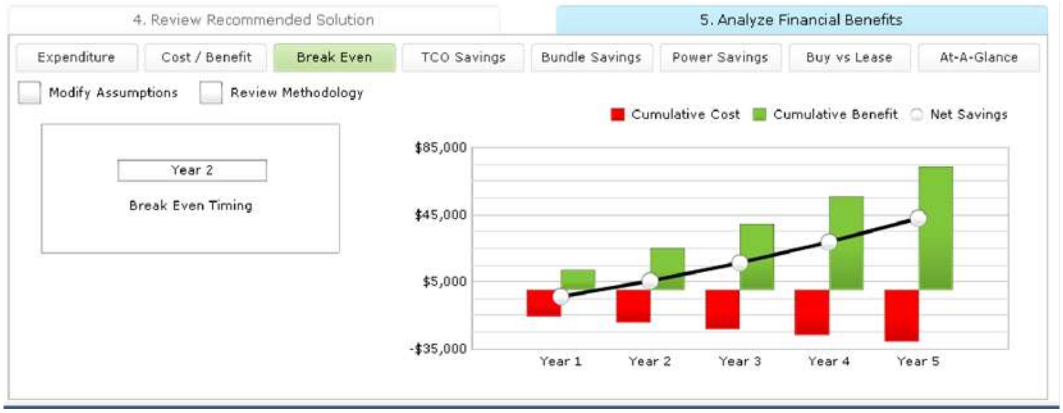
Figure 33 shows the various input and output parameters that can be modeled by the tool.

Figure 33. Cisco Integrated Services Routers Business Benefits Calculator: I/O Specifications

Inputs	Output
ISR services	Base platform / bundle recommendation
Branch business profile	TCO analysis : ISR vs overlay solution
Branch network operations	Break-even analysis
Financial deal Terms	Bundle vs. A la Carte comparision
Support contracts	Power Savings

In a typical deployment, the estimated break-even point to recover the cost of equipment is by year 2 for a fully loaded Cisco Integrated Services Router (Figure 34).

Figure 34. Cisco Integrated Services Routers Business Benefits Calculator: Break-Even Analysis



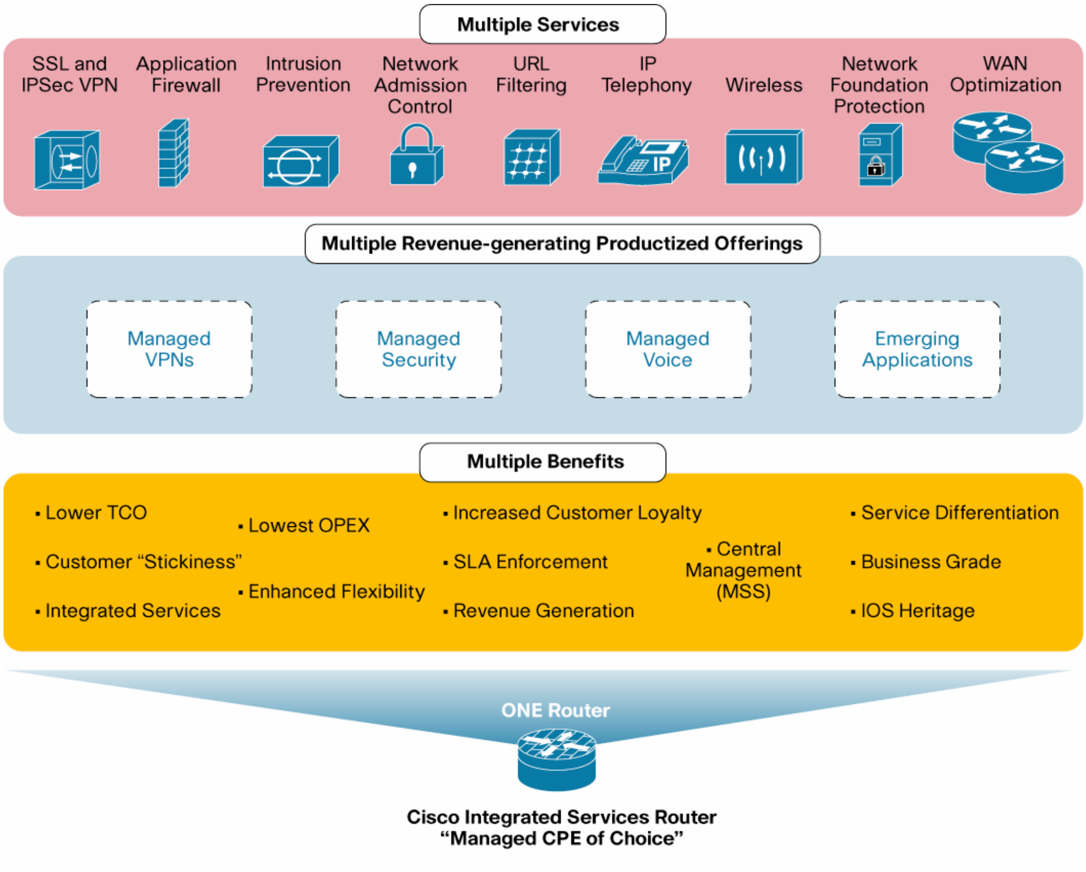
Year 2

Break Even Timing

7.0 Relevance to Managed Service Providers

Service providers offering managed services stand to gain significantly by deploying the Cisco Integrated Services Router as a managed CPE offering. Today service providers all over the world are helping their customers turn on managed VPNs, Firewall, NAT, Hi-touch security services and voice solutions with the Cisco Integrated Services Router.

Figure 35. The Cisco Integrated Services Router as a Complete Solution Platform for Managed Services



7.1 Benefits to Service Providers

- **Move up the services chain:** The Cisco Integrated Services Router helps service providers enhance the value of their offerings, moving beyond offering simple connectivity and managed WAN and thereby generating additional recurring revenue. It is easier to "turn on" new services such as Cisco WAAS or Tunnel-less VPNs by simply adding a new module or by a planned software upgrade.
- **Increases customer loyalty and "stickiness":** Additional services can be rolled out of the same platform and with minimal network downtime.
- **Eliminates constant equipment upgrades: Multiple** services can be offered through one integrated platform.
- **Easier security policy enforcement:** With the Cisco Integrated Services Router, administering security policies is considerably easier. Applying security patches as well as granular control of inbound and inbound traffic are simplified.
- **Comprehensive tools and reports:** Having one integrated device to manage vastly simplifies data gathering and report generation that can easily be customized per the Service-Level Agreement (SLA) with the customer. A variety of Cisco tools are available for this purpose.
- **Simplified management:** This is a huge advantage for service providers. The "zero-touch" provisioning of the Cisco Integrated Services Router through the Cisco Configuration Express tool is very popular, along with other Cisco Network Management System (NMS) and Managed Services Solution (MSS) offerings.
- **Lower operational costs:** While the CapEx savings are also significant, ongoing operational costs for managed service providers (MSPs) can be considerably lower with the Cisco Integrated Services Router, as opposed to managing multiple point-play overlay CPE products.

> "Cisco integrated services routers give us an opportunity to provide customers with a solution that includes high performance, a wide range of connectivity options, and new services. In addition to delivering high performance, the Cisco integrated services routers allow us to take full advantage of our advanced network and service platforms to deliver more benefits to customers than ever before."
> **—Claudio Contini, marketing director, Telecom Italia**

7.2 Benefits to Managed Enterprise and SMB Customers

Managed CPE customers using the Cisco Integrated Services Router tend to experience lower downtime, higher network availability, and simplicity from a network administration perspective.

- **Better investment protection:** Newer services can be turned on quickly either via software upgrades or by inserting new modules without the need for costly equipment swap.
- **Enhanced business efficiency:** With a central point of contact for one integrated device, businesses can be more productive and efficient, focusing on their core strengths instead of constantly having to liaison with their service provider to modify or upgrade services.
- **Increased security and performance:** Customers who use Cisco Integrated Services Routers for managed solutions constantly experience better network performance and security.
- **Lower pricing:** Managed services customers also experience pricing gains because their MSPs are able to bundle relevant productized services on one integrated platform, as opposed to a fragmented pricing approach.

8.0 Conclusion

Today's SMBs, enterprises, and service providers place an increasingly high value on network infrastructure, recognizing that the network is key to effective use of business and consumer applications. Clearly, the branch router plays a critical role in enabling these applications and delivering on scalable, high-performance voice, video, data, and mobility services.

The award-winning Cisco Integrated Services Router portfolio empowers branch networks by offering a modular framework of services on a single integrated device. By doing so, it effectively transforms traditional branch networks from expensive, layered, multi-box environments to a single, powerful, cost-effective platform for integrated business services. With this powerful concept, enterprise branch offices and SMBs are empowered to support localized decision making, enhance collaboration and increase productivity while service providers are enabled to offer a wide range of revenue-generating managed services.

9.0 References

- http://www.cisco.com/go/isr
- http://www.cisco.com/go/routersecurity
- http://www.cisco.com/application/pdf/en/us/guest/products/ps5853/c1031/cdccont_0900aecd801aa204.pdf
- http://www.cisco.com/go/ios
- http://www.cisco.com/en/US/netsol/ns663/networking_solutions_sub_solution.html
- http://www.miercom.com
- http://www.cisco.com/en/US/netsol/ns676/networking_solutions_solution.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-530872-01 6/09