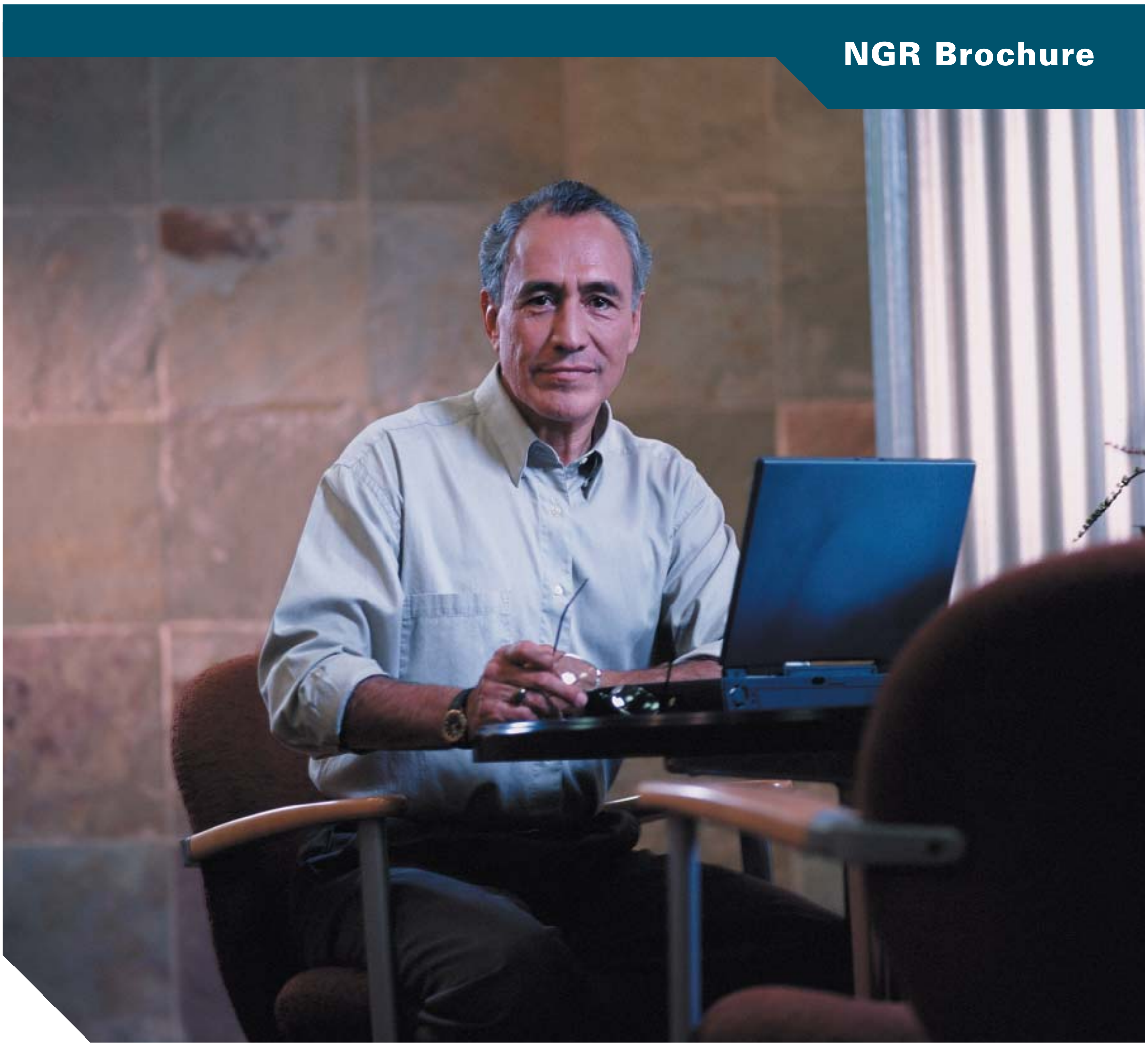
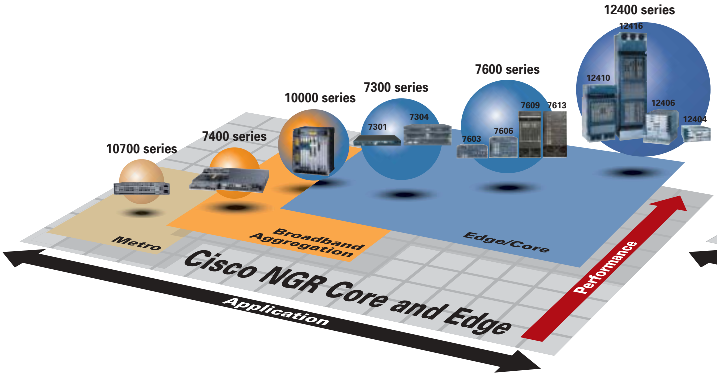
Cisco Systems

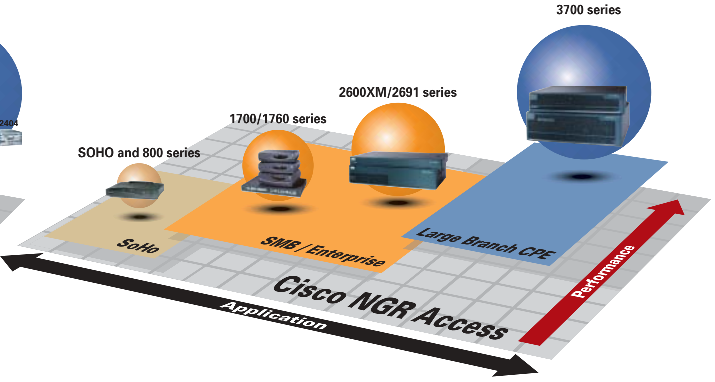
NGR Brochure



Cisco Next Generation **Routing**

Section 1	Issues for networking in the Broadband Era
Section 2	Next Generation WAN Services using MPLS
Section 3	Cisco's Next Generation IP Network Solution
Section 4	Cisco’s Next Generation Optical Ring Solution
Section 5	Service differentiation and Quality of Service
Section 6	Service with Security
Section 7	Cisco Next Generation Routers – Core and Edge
Section 8	Cisco Next Generation Routers – Access





Cisco Next Generation Routing (NGR) Solution Next Generation Internet in the **Broadband Era**

Broadband networking is rapidly expanding in usage; consequently, routers must support an ever growing range of features and service capabilities to meet the unique needs of this high growth area. As the world's leading router manufacturer, Cisco's routers are in widespread use, helping to support and expand the development and usage of the Internet and its rich service base. It is Cisco's charter to continue this focused development, building upon the success of Cisco deployments to date.

Scalability and performance for the Broadband Era

Communications companies around the world have deployed the Cisco 12400 series 10G model as their Next Generation backbone. All models feature interface and processor card compatibility, allowing for investment protection, convenient upgrading from the existing 12000 series, and expansion to 10G with a minimum of additional investment.

New service development infrastructure, bringing about new added value

In response to the popularity of broadband, Cisco has incorporated superior Quality of Service (QoS) technology to support new voice, and real-time video and data applications. NGR routers support a wide variety of MPLS technologies, enabling the network infrastructure to support new services. Examples include Traffic Engineering (including MPLS-VPN, extensively deployed throughout the industry); cutting-edge AToM (Any Transport over MPLS) technology, which enables layer 2 transport such as EoMPLS (Ethernet over MPLS); ATM and frame relay support.

Implementing NonStop IP service with GRIP (Globally Resilient IP)

The GRIP solution provides fault tolerance for an entire network. Even if network failures such as link and node failures occur, end-to-end IP service at the link and session levels is maintained without affecting end-user service. Quality assurance for end-to-end IP service from the backbone to the access point is enhanced dramatically, resulting in a highly stable, carrier-class up-time, IP-service environment.

Innovative Next Generation metro IP solution

RPR (Resilient Packet Ring), represents a key technology for the deployment of advanced IP ring technology. RPR is used by a large number of customers in the metro access arena, for providing an advanced, industry-first, IP-based metro Ethernet access solution. This ensures an optimum linkage between the router and the Ethernet base, a configuration that is rapidly growing in popularity due to the increase in broadband access. The router's high reliability and expandability provide an advanced, Next Generation metro infrastructure with the advantages of simplified network operation.

Service Differentiation and Quality of Service

A communications network forms the backbone of any successful organisation. Today's IP networks serve as the transport for a multitude of applications, including delay-sensitive voice and bandwidth-intensive video. Networks must therefore provide secure, predictable, measurable and sometimes guaranteed services to these applications. The secret to running an infrastructure that truly serves the business is to achieve the required Quality of Service (QoS) by managing the delay, delay variation (jitter), bandwidth and packet loss parameters on a network, while maintaining simplicity, scalability and manageability.

Service with security

The extensive, complex and open nature of the network environment increases the need for robust and comprehensive security, because any point the network touches must be protected, as well as protected against.

Embedded, integrated security must defend the network against external and internal threats, always striking a balance between the need for access and the need for protection.

This means security functionality must be embedded and integrated everywhere – from the core right to the network endpoints – it must also remain transparent to the user and the application.

Section 1

Issues for networking in the **Broadband Era**

In 2001, the first year of widespread broadband Internet access, there was a rapid shift from narrow-band, metered dial-up access to high-speed, always-on broadband access using ADSL and cable. From 2002 onwards, we entered a full-scale broadband era, in which broadband networks carry mission-critical, multi-service applications. This section describes issues relevant to the construction of the Next Generation networks for the new broadband era.

Faster access is not enough

The term "broadband" is widely used in the public arena and is recognised as a IT industry keyword.

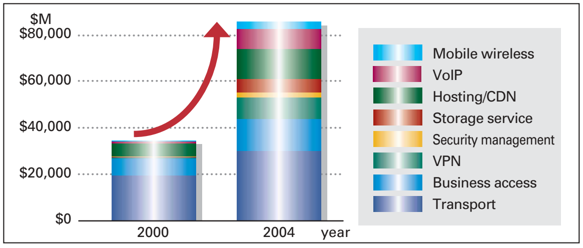
However, broadband is just a communications industry term that refers to data channel capacity – its importance lies in the services that can be based on a high-speed infrastructure. "Real broadband" will thus consist of a network featuring practical benefits, both for service users and service providers.

When real broadband is implemented, Internet usage, which is now mostly e-mail and file transfers – will change substantially. As in Korea, communication using video mail will become commonplace, and video on demand (VOD) may in time replace video rental to become the dominant form of home entertainment.

Broadband implementation will also have a great effect within companies. Faster corporate networks will enable the implementation of voice synthesis, unified messaging, VoIP teleconferencing, and networked, e-learning training applications. Work environments will become accessible from anywhere – on global business trips, at home, and in the office. As a result, work procedures will change significantly. Even information held by governments and other official bodies will become accessible anywhere, anytime.

In this manner, multi-service applications on the broadband network will enable end users to enjoy new lifestyles while providing carriers and service providers with new sources of income.

Figure 1-1 New IP value-added services expected to grow significantly in the future



Source: IDC, Dataquest, VSG, Yankee, Merrill Lynch

Next Generation network requirements

What type of network will be needed in the broadband era? Services using real-time voice and moving picture applications will require guaranteed bandwidth and the elimination of service variation, delay, and packet loss.

The reliability and operational efficiency of the network are also highly important. From a service provider's standpoint, the fundamental question is how to construct an efficient network that will generate sufficient return on investment.

We can summarise Next Generation network requirements as follows:

1 Scalability and performance
2 Infrastructure in which new, profitable, value-added services such as VPN and real-time content services are developed
3 High reliability, guaranteeing mission-critical services
4 Comprehensive cost reduction and operation efficiency
5 Offers a level of security appropriate to the user's needs

Cisco's Next Generation Routing development

Cisco's Next Generation Routers represent the results of the application of Cisco's advanced technology to these Next Generation network requirements.

Cisco NGRs employ an innovative adaptive network processor to achieve high performance, supporting mission-critical traffic while maintaining a rich set of functionality and flexibility. NGRs support the industry's most substantial MPLS specification, expanding service functionality and optimising Ethernet-based user access in the metro area. NGRs also enable high reliability and scalability in the construction of a broadband-era network infrastructure, providing an efficient network and simplified operations.

This document describes the NGR-based network solution and the supporting broadband-era technologies.

Section 2

Next Generation WAN Services using **MPLS (Multiprotocol Label Switching)**

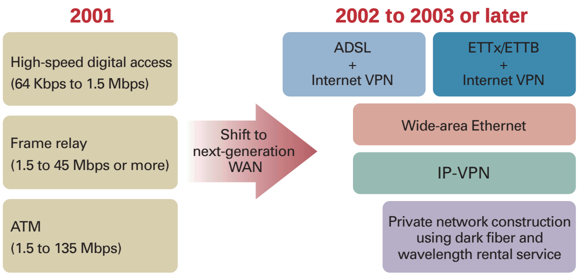
Section 2 introduces a wide variety of MPLS-applied technologies introduced by Cisco Systems to a large number of service providers around the world, and discusses the services that are based on these technologies. This section also summarises existing issues in corporate WAN services, describes solutions for these issues, and highlights the necessary characteristics of Next Generation WAN services.

Chapter 1 – Present WAN Market Trends

With the recent appearance of attractive new WAN services such as IP-VPN and wide-area Ethernet, corporate networks are significantly shifting from WANs based on the conventional leased circuit and frame relay type access to networks using these new WAN services. The corporate broadband WAN services currently attracting most attention are:

1. Internet VPN service over ADSL
2. Wide-area Gigabit Ethernet service
3. IP-VPN service

Figure 2-1 Domestic WAN service trends



- From 2000 onward, corporate networks using leased circuits and frame relays gradually begin to shift to networks using new WAN services.
- Seventy to eighty percent of contracts for corporate IP-VPN access-circuit subscribers involve high-speed digital leased circuits of 128 Kbps or less.

- The use of new WAN services is increasing at an accelerating pace.
- Use of services shifts toward inexpensive broadband services using ADSL and Ethernet. Contracts to provide the access circuits of companies using IP-VPN service increase, to meet the demand for inexpensive broadband access using ADSL.
- In metro areas and in regional companies, private network construction models using dark fiber begin to appear.
- From the second half of 2002 through 2003, Internet VPN using ETTX/ETTB is also expected to appear.

These new WAN services are outlined below.

Figure 2-2 Outline and comparison of new WAN services

	Internet VPN using ADSL	Wide-area Ethernet service	IP-VPN service
Outline of service	High-speed ADSL Internet connection and VPN technology are used to construct WANs	Ethernet services provided by carriers in corporate LANs are connected to construct WANs	MPLS-VPN provided by carriers is connected to construct WANs
Major security method	VPN special unit (IPSec firewall) is arranged in corporate APs	VLAN	MPLS label
Applicable user interface	ADSL	10/100/1000 copper/fibre Ethernet	13. Leased circuits (DA, HSD, FR, ATM), Ethernet, dial-up, and Internet
Topology	Flat type	Flat type/hierarchical type	Flat type
Communication protocol	IP only	No restriction	IP only
QoS	Not provided	Dependant on Implementation	Provided
User-connected equipment	ADSL modem	LAN switch or router	IIP equipment

The following summarises the characteristics of and issues relating to these new WAN services:

1. Internet VPN service over ADSL

Sales point

The greatest advantage of this service is that communication costs can be reduced significantly by connecting to the Internet over high-speed but inexpensive ADSL. The VPN product or in-built routing capability must be configured to ensure security, but this service can be simply and quickly introduced over the Internet.

Issues

The most critical issues when using the Internet for intra-company communications relate to security and line stability. ADSL cannot guarantee throughput and connectivity, so it is unsuitable for critical and urgent inter-company communications. Although ADSL has the advantage of being simple to install, the areas in which it can be used are restricted. If many access points exist across multiple areas, operational management and dual-homing design of lines must be taken into consideration. This service may be more suitable for remote users and remote branch connections, as opposed to full use with multiple connections.

2. Wide-area Ethernet service

Sales point

This service features a high cost-performance ratio when traffic demand is heavy, especially in metropolitan areas, because it employs inexpensive, high-speed Ethernet. Freedom to use any communication protocol, not just IP, provides the advantage of greater design freedom.

Issues

The use of LAN switches for wide-area Ethernet presents problems on both the user and carrier sides.

User issues

Wide-area Ethernet service provides greater design freedom, but also requires companies using the service to be meticulous over design and operational planning. When all connection points consist simply of LAN switches, broadcast and multicast communications are distributed to all points. In a wide-area network, this is an inefficient use of bandwidth, generating higher loads as a result of frame discard processing by network terminals, as well as troubleshooting difficulties.

Wide-area Ethernet also cannot guarantee bandwidth. VoIP applications require both guaranteed bandwidth and the ability to manage bandwidth from the enterprise. This involves additional costs as, generally, effective use of wide-area Ethernet service requires engineers with sophisticated routing knowledge in order to design, operate, and maintain the service; costs other than line charges must also be taken into consideration.

Carrier issues

If Ethernet, conventionally regarded as a LAN technology, is expanded to a WAN without modification, its failure management will be weak and expandability restricted. For example, only a maximum of 4,096 VLANs can be constructed per network – we describe this restriction later.

LAN switches transfer frames by learning the MAC addresses of incoming Ethernet frames. In terms of expandability, security, and fault recovery, this mechanism is inferior to IP routing where routing tables are based on the higher-layer routing protocol. Because Ethernet possesses no traffic engineering capability, it cannot support bandwidth guarantee services such as QoS.

3. IP-VPN service using MPLS

Sales point

The advantages of MPLS IP-VPNs consist of good connectivity and comprehensive value-added service capabilities. Access via different types of connection – ranging from low-speed, 64Kbps lines to Ethernet, dial-up and broadband Internet connections – can be freely combined. When deploying VoIP applications, enterprises can take advantage of bandwidth controls and latency guarantees under contracted service level agreements. Because the carrier provides a full-mesh, highly stable WAN network design, users no longer need to take network routing design into consideration. Compared with a wide-area Ethernet, this service can also simplify post-introduction operation management and design.

Issues

IP is the only supported communication protocol. If a protocol other than IP is currently used, the entire network must be tailored to IP; otherwise, this service must be partially used with an individual WAN service capable of layer 2 communication, incurring additional costs. Compared with a wide-area Ethernet service, this service may present more restrictions upon introduction.

Chapter 2 – Cisco Systems' Next Generation WAN Services

New WAN Services solutions

If a service were available to eliminate the disadvantages of wide-area Ethernet and IP-VPN services (see table in Figure 2.3), it would enhance the convenience of operating corporate networks and enable the seamless fusion of a wide-area Ethernet and IP-VPN, providing an ideal set of WAN services.

MPLS-applied technologies will prove extremely effective in implementing such services. One of the technologies currently attracting attention in the WAN market is Ethernet over MPLS (EoMPLS). This is gaining a reputation as a backbone core technology that addresses the weak points of wide area Ethernet with regard to fault tolerance and scalability. However, Cisco Systems does not view MPLS simply as a technology to strengthen specific WAN technologies such as wide-area Ethernet, but as a supporting solution for the future evolution of all WAN technologies.

The Ethernet foundation

Ethernet is capable of delivering broadband at significantly lower cost, and will therefore become the main interface for corporate WAN services, as well as the foundation on which Cisco Systems' next generation Next Generation WAN services will be built.

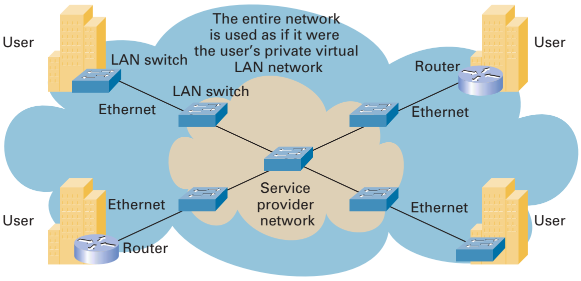
Current Ethernet services can be divided into three broad categories, ranging from a general LAN-switch-type model to a service using EoMPLS:

1. Layer 2 Ethernet (WAN)
2. Layer 3 Ethernet (MPLS IP-VPN)
3. Ethernet Virtual Leased Circuit Service (EVCS)

1. Layer 2 Ethernet (WAN)

Currently, most wide-area Ethernet services are provided in this manner. From a user standpoint, this service functions as if the carrier network's Ethernet switches are for their exclusive use, with all switching being based on the user's MAC address. The characteristics of and issues relating to this service are as explained in the previous chapter's discussion of Ethernet WANs.

Figure 2-3 Layer 2 Ethernet service

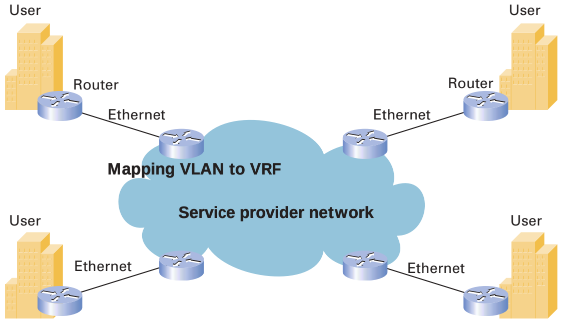


2. Layer 3 Ethernet (MPLS IP-VPN)

IP-VPNs accessed over Ethernet using MPLS have recently begun to be provided by some carriers as a new additional VPN-VPN service menu. This service is implemented by mapping user-set Ethernet VLAN (802.1q) information to the user's VPN information (MPLS VRF: VPN Routing and Forwarding instance) on the edge router at the carrier site. This service enables the user to use Ethernet for existing IP-VPN services.

The characteristics of and issues relating to this service are as explained in the previous chapter's discussion of IP-VPN service.

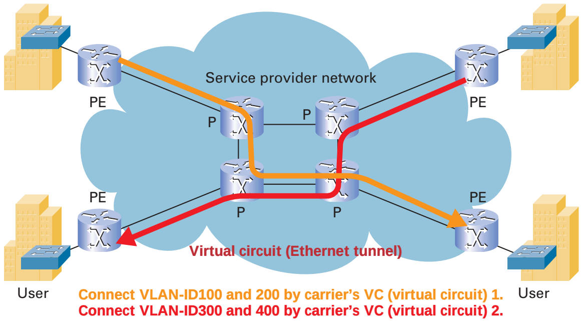
Figure 2-4 MPLS IP-VPN-type Ethernet service



3. Ethernet Virtual Leased Circuit Service (EVCS)

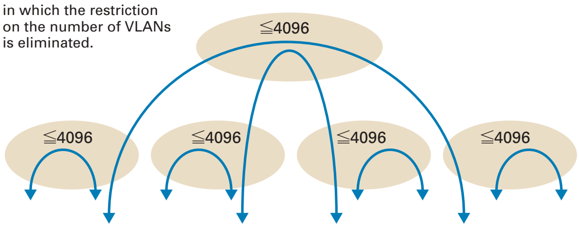
This is a new Ethernet service using EoMPLS as a network core. The service provider's virtual circuit (VC) can be freely used by mapping the user's Ethernet VLAN-ID to the virtual circuit ID. This may be easier to understand if the VLAN-ID is regarded as a Frame Relay DLCI in the example of a WAN service using Frame Relay and ATM. When EoMPLS is used as a network core, the user need not change the connection type so this service can be easily used in the same manner as existing LAN switch connections.

Figure 2-5 Ethernet virtual leased circuit service



Connect VLAN-ID100 and 200 by carrier's VC (virtual circuit) 1.
Connect VLAN-ID300 and 400 by carrier's VC (virtual circuit) 2.

Figure 2-6 Solution to Issue 1: Expandability is restricted



The VLAN-ID rewrite function enables construction of a hierarchical VLAN-ID domain in which the restriction on the number of VLANs is eliminated.

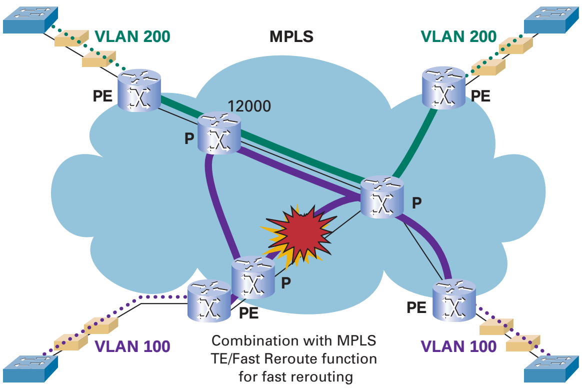
The greatest advantage of EoMPLS from a carrier's perspective is that it solves the problems faced by wide-area Ethernet. Based on examples of EoMPLS usage, let us review the issues relating to wide-area Ethernet constructed with LAN switches as listed in figure 2-3, and present some solutions.

Issue 1:	Restricted expandability (up to 4,096 VLANs per network)
Issue 2:	Weak backbone fault management
Issue 3:	No bandwidth guarantee

3.1 Issue 1: Expandability is restricted

As described in the previous chapter, wide-area Ethernet provides security for user traffic based on 802.1q VLAN, and the VLAN-ID is restricted to up to 4,096 types of 12-bit IDs. That is, a single layer 2 domain can accommodate up to 4,096 users. EoMPLS ensures that the VLAN-ID rewrite function is used in the carrier network and that multiple layer 2 domains are interconnected. As shown below, constructing a hierarchical layer 2 network theoretically enables the network to be infinitely expandable. If the VLAN-ID rewrite function is used, expansion of the network is likely to be required if MAC address learning is to be performed as with existing LAN switches; in this case over 4,096 learning tables must be processed in order to acquire the MAC address in the network core. When EoMPLS is used, MAC address learning is not performed in the core network but is instead transferred transparently. Problems such as learning-table expansion – scalability deterioration – due to network expansion and user MAC address interference in the carrier core do not arise.

Figure 2-7 Combination of EoMPLS and Traffic Engineering for robust core construction



Combination with MPLS TE/Fast Reroute function for fast rerouting

3.2 Issue 2: Weak backbone fault management

When node redundancy is secured in a network constructed with Ethernet switches, a forwarding loop is formed. This problem is attributable to the fact that Ethernet is designed to be bus-like; Ethernet is fundamentally the wrong solution. The traditional solution is for spanning tree protocol (STP) to block one or more interfaces resulting in a logically loop-free, tree-shaped topology. However, this method requires the logical topology to be recalculated at each configuration change due to interface or node failure. Because data flows must stop until all nodes have recalculated, a service interruption is experienced when the line is switched or a fault occurs. Normal operation of STP as expected requires that settings such as bridge priority and port cost are strictly managed throughout the entire network. This problem of design and operation is inherent in the expansion of a wide-area Ethernet.

The combination of EoMPLS and MPLS TE solves the problem

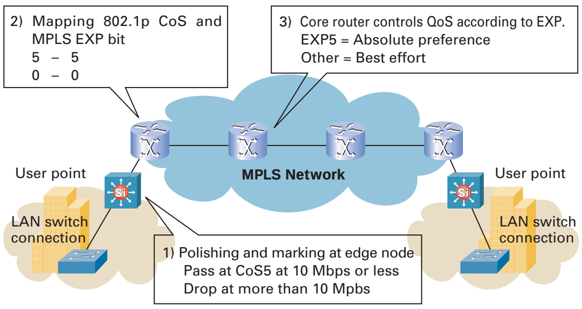
EoMPLS can be used together with the MPLS-provided traffic engineering feature. Network reliability is enhanced significantly because MPLS traffic engineering's “Fast Reroute” failure recovery mechanism is used to execute path switching within 50ms if a service provider’s line or node becomes faulty.

MPLS's traffic engineering feature also uses bandwidth efficiently – its Diffserv-aware TE function enables traffic prioritisation. EoMPLS can also be combined with efficient bandwidth utilisation and Diffserv-aware TE for enhanced serviceability and reliability.

3.3 Issue 3: No bandwidth guarantee

As described in the previous chapter, Ethernet does not provide a bandwidth guarantee mechanism. However, core adoption of MPLS enables use of the MPLS-QoS mechanism. This can be achieved by mapping 802.1q CoS information (802.1p) to the Experimental bit containing MPLS CoS information.

Figure 2-8 MPLS QoS mechanism


2) Mapping 802.1p CoS and MPLS EXP bit
5 – 5
0 – 0
3) Core router controls QoS according to EXP.
EXP5 = Absolute preference
Other = Best effort
User point
MPLS Network
User point
LAN switch connection
1) Polishing and marking at edge node
Pass at CoS5 at 10 Mbps or less
Drop at more than 10 Mpbs
LAN switch connection

QoS provided = Band guaranteed and delay distortion is small, at up to 10 Mbps.
QoS not provided = Band guarantee is not provided, and delay distortion is great.

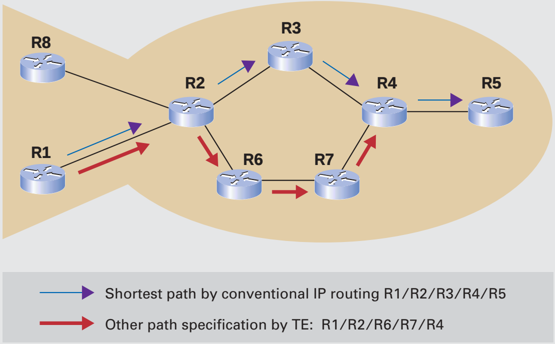
Technical Column

Functions that can be implemented by TE (Traffic Engineering)

With a conventional IP network backbone, traffic often centers on a specific path while other paths are hardly used. This is because the routing protocol, which always selects the shortest path, determines a path based only on the distance between two points and on the cost, regardless of congestion. This is one of the toughest issues in the optimization of a network infrastructure. Traffic Engineering technology effectively solves this issue, through implementation of the following major functions.

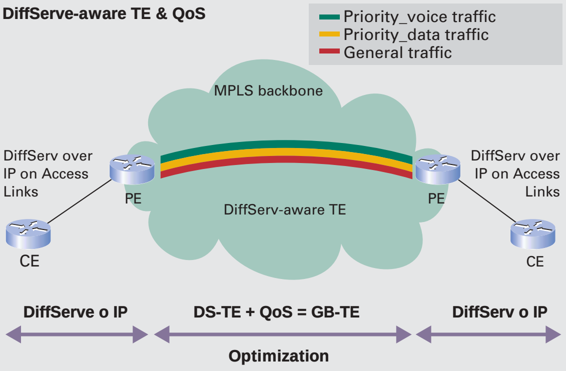
Explicit path setup

When setup of any LSP (Label Switched Path) is allowed, the network designer can perform more detailed path setup and management as required.


R8
R3
R2
R4
R5
R1
R6
R7
Shortest path by conventional IP routing R1/R2/R3/R4/R5
Other path specification by TE: R1/R2/R6/R7/R4

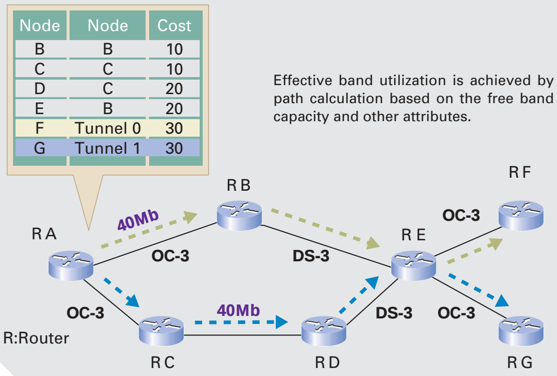
Diffserv-aware TE

The combination of Diffserv-aware TE and Queue service scheduler (MDRR LLQ) enables the implementation of a band-guarantee-type service.



Effective band utilization

The concept of "free band capacity" is introduced for path selection to enable identification of the use status of traffic and more effective band utilization.

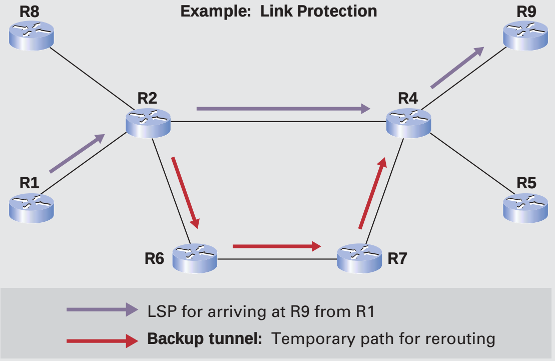


Node	Node	Cost
B	B	10
C	C	10
D	C	20
E	B	20
F	Tunnel 0	30
G	Tunnel 1	30

Effective band utilization is achieved by path calculation based on the free band capacity and other attributes.

Fast Reroute (Link Protection/Node Protection)

An alternate path is set up in anticipation of a fault to provide quick link and node recovery mechanisms.


R8
Example: Link Protection
R9
R2
R4
R1
R5
R6
R7
LSP for arriving at R9 from R1
Backup tunnel: Temporary path for rerouting

Summary – Hybrid-type WAN service using MPLS as a core

Multi-service hybrid Ethernet

Among corporate WAN services, Ethernets providing cost-effective broadband will be increasingly tailored to IP applications – research shows that most of today's corporate traffic runs over IP. In response, Cisco Systems offers multi-service Ethernet as a Next Generation WAN service, with MPLS as the network core, and Ethernet as the interface for corporate users.

Customers and their applications can use this service on a per-VLAN basis. It also supports QoS to differentiate specific VLANs. Although IP is the major communication protocol, this service also supports non-IP protocols. It may be easier to understand as a hybrid-type service implemented by combining the previously described Ethernet services.

As shown in the following diagram, layer 2 Ethernet and the MPLS IP-VPN provide different services for user A. This service enables the unrestricted combination of all menus of the three previously described WAN services.

For example, usable service modes include LAN switch connection for broadband connections in metropolitan areas, IP-VPN connection for local points, and inexpensive ADSL connection for branches and home workers. The combination of 6PE, capable of transporting IPv6 packets in the MPLS core, enables the provision of IPv4 and IPv6 services. A multi-service Ethernet that takes advantage of the convenience of IP-VPN effectively integrates the three new WAN services introduced in Chapter 1 and provides optimum services for all corporate users. This is Cisco's Next Generation WAN service.

Figure 2-9 Hybrid-type service

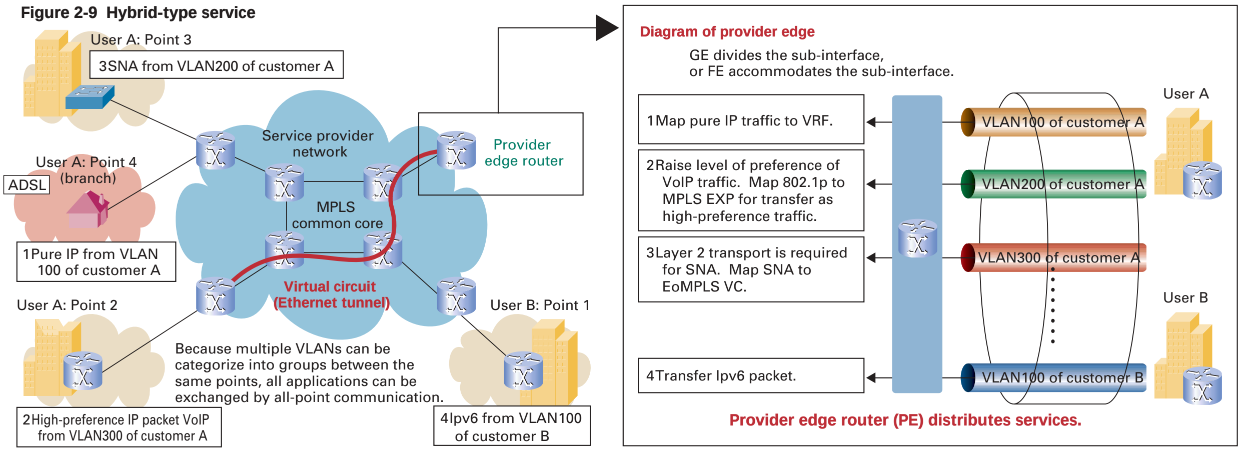

User A: Point 3
3SNA from VLAN200 of customer A
User A: Point 4 (branch)
ADSL
1Pure IP from VLAN 100 of customer A
User A: Point 2
2High-preference IP packet VoIP from VLAN300 of customer A
Service provider network
MPLS common core
Virtual circuit (Ethernet tunnel)
Provider edge router
User B: Point 1
4Ipv6 from VLAN100 of customer B
Because multiple VLANs can be categorize into groups between the same points, all applications can be exchanged by all-point communication.
Diagram of provider edge
GE divides the sub-interface, or FE accommodates the sub-interface.
1Map pure IP traffic to VRF.
2Raise level of preference of VoIP traffic. Map 802.1p to MPLS EXP for transfer as high-preference traffic.
3Layer 2 transport is required for SNA. Map SNA to EoMPLS VC.
4Transfer Ipv6 packet.
VLAN100 of customer A
VLAN200 of customer A
VLAN300 of customer A
VLAN100 of customer B
User A
User B
Provider edge router (PE) distributes services.

Figure 2-10

Figure 2-11 Summary: Next-generation multiservice Ethernet service proposed by Cisco Systems

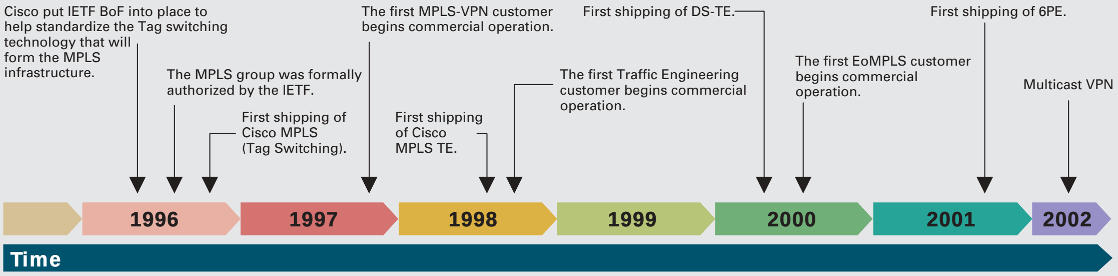
	Next-generation WAN service	Characteristics
Service cost	○	Optimal cost-performance is achieved through a combination of a low-speed leased circuit for small traffic volume at a small-scale point, an ADSL line for inexpensive and fast service, and an Ethernet for intercity communication, allowing for flexible future expansion and different connection combinations
Reliability	○	The Traffic Engineering feature secures reliability of the network backbone.
Multiprotocol	○	Communication protocol is not restricted. Layer 2 and layer 3 protocols are freely combined to support all applications.
High-quality service (QoS and SLA)	○	MPLS QoS enables the Ethernet service to employ QoS. QoS can be selected flexibly according to corporate needs.
Convenience (available area and interface)	○	All circuit types currently available in the WAN market can be freely combined for connection according to the traffic band for point connection, application, and location. In other words, all services can be used within the scope of IP-VPN and the wide-area Ethernet currently provided.
Operation, specialized design knowledge, and problems on user's side	○	Advanced routing design and operation techniques are not required. Services and applications can be freely selected from the provider service menu, connected, and employed based on the user's needs.

Technical Column

Figure 2-11 and 2-12

Part of the Cisco MPLS-related RFC/draft is shown below. Cisco has written or jointly written 50 or more MPLS-related drafts for the IETF (the following is part of a draft).

Figure 2-12 History of Cisco's MPLS technology



Cisco put IETF BoF into place to help standardize the Tag switching technology that will form the MPLS infrastructure.

The MPLS group was formally authorized by the IETF.

First shipping of Cisco MPLS (Tag Switching).

The first MPLS-VPN customer begins commercial operation.

First shipping of Cisco MPLS TE.

The first Traffic Engineering customer begins commercial operation.

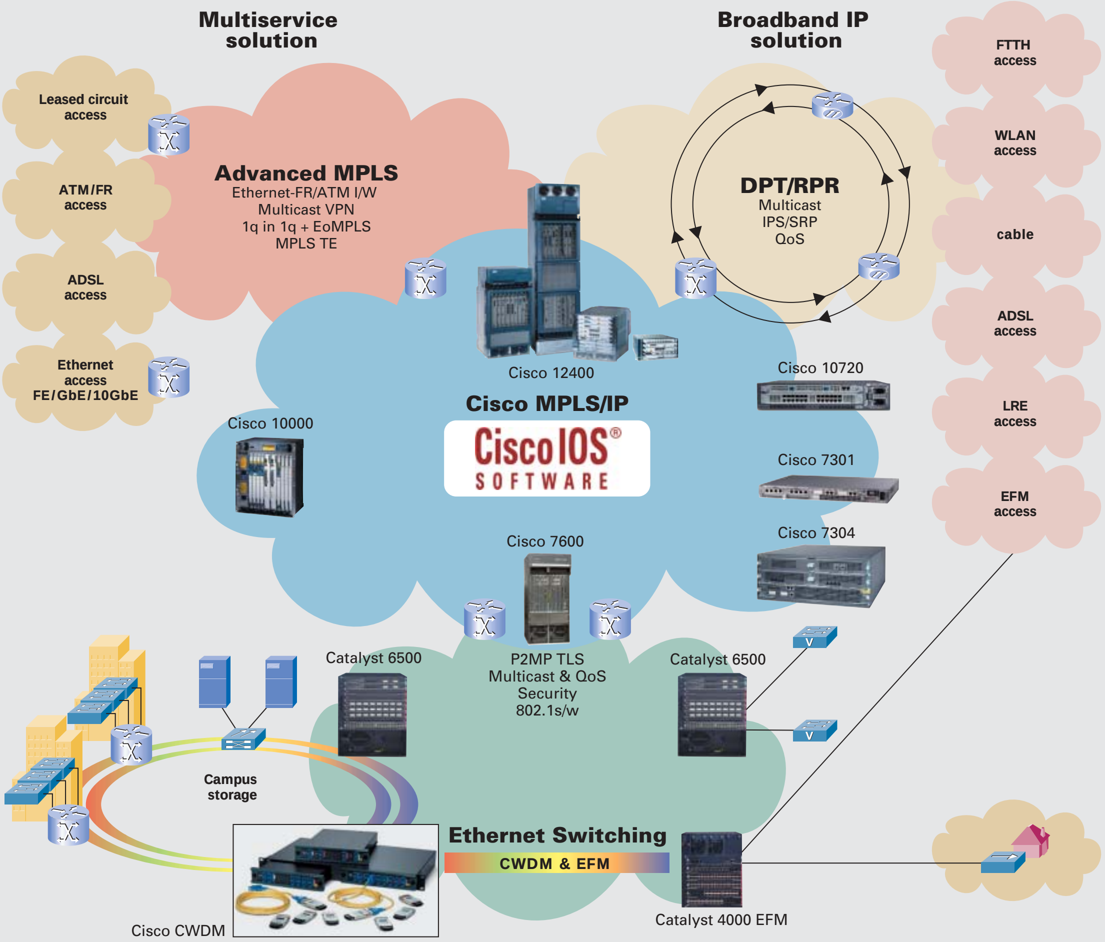
First shipping of DS-TE.

The first EoMPLS customer begins commercial operation.

First shipping of 6PE.

Multicast VPN

Figure 2-13 Cisco's next-generation multiservice Ethernet total solution



Section 3

Cisco’s Next Generation IP Network Solution: Implementing Nonstop IP Service

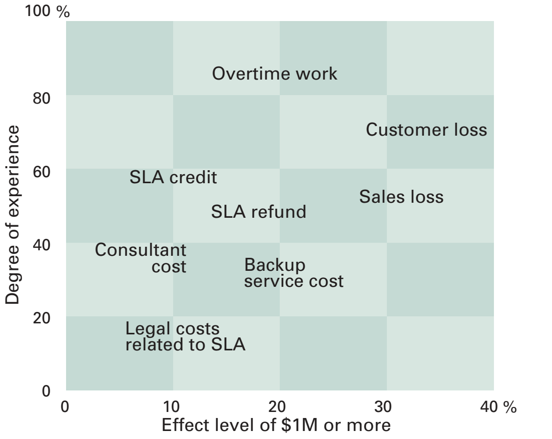
One of the most important issues determining network construction is reliability. It can be seen in terms of the equipment being used, circuits, and network design but key is the ability to quickly recover from a fault without affecting users or applications. Part III introduces Cisco’s latest solution to enhance the fault tolerance function of the entire network and to implement non-stop IP service.

Importance of IP service level reliability

As consumers and businesses grow more dependent on IP networks, reliability becomes critical. In particular, as broadband implementation progresses, mission-critical applications such as data storage, IP telephony, and video streaming are growing and becoming more important.

If network failure stops or interrupts mission-critical applications, corporate users may suffer significant damage to business operations. If network failure prevents service providers from providing services, sales decrease and providers will be penalised for breaking customer service level agreements. Both confidence in the service providers and customer satisfaction will fall. A network failure will also have a significant impact on a company’s human resources, due both to increased workloads for network operators and to the necessity of responding to complaints at call centres (see Figure 3-1). So any enhancement of network reliability is extremely critical: stable services increase customer satisfaction, maintain competitiveness with other companies, and minimise operational costs.

Figure 3-1 Impact of network failure



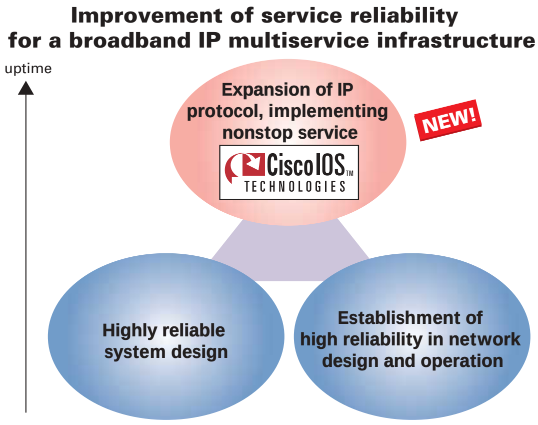
Research report on 50 US service providers (September 2001)

Cisco’s Globally Resilient IP (GRIP)

How is network reliability enhanced? The conventional approach to enhancing network reliability involves highly reliable system design with redundancy of major components such as power supplies, route processors, and switch fabrics, coupled with highly reliable network design and operation. In addition to these approaches, Cisco is the first to expand fault tolerance to the IP protocol level, providing a unique integrated solution to enhance the reliability of the entire network. This is Cisco’s Next Generation IP network solution, Globally Resilient IP (GRIP), designed for the implementation of non-stop IP service.

Cisco’s GRIP solution maintains end-to-end IP service at the link and session levels without affecting end users, even if a network failure such as a link or routing failure occurs. Consequently, failure recovery cost is reduced and network failure time and application interruptions decrease, resulting both in greater employee productivity and a reduction in network operational costs.

Figure 3-2 Cisco’s new approach


Improvement of service reliability for a broadband IP multiservice infrastructure
uptime
Expansion of IP protocol, implementing nonstop service
Cisco IOS TECHNOLOGIES
NEW!
Highly reliable system design
Establishment of high reliability in network design and operation

These functions are provided by the existing Cisco IOS software and hardware platforms, so return on the investment in Cisco products is increased, especially since functions incorporated in Cisco IOS software can be implemented through upgrades.

Latest GRIP technologies

GRIP as delivered by Cisco IOS consists of the following four newly developed, network resilient technologies which provide failure recovery and high reliability:

- Resilient link layer
- Resilient routing
- Resilient MPLS
- Resilient IP service

The following gives an overview of the individual technologies that make up GRIP:

Figure 3-3 Technological innovations enhancing the reliability of Cisco Globally Resilient IP

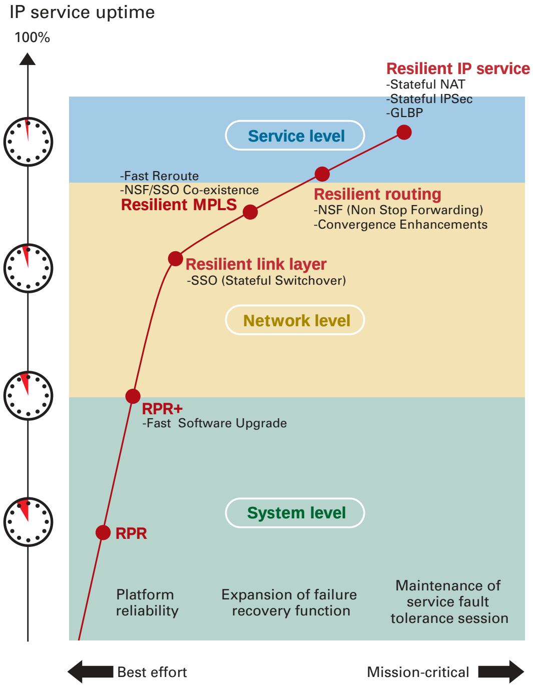
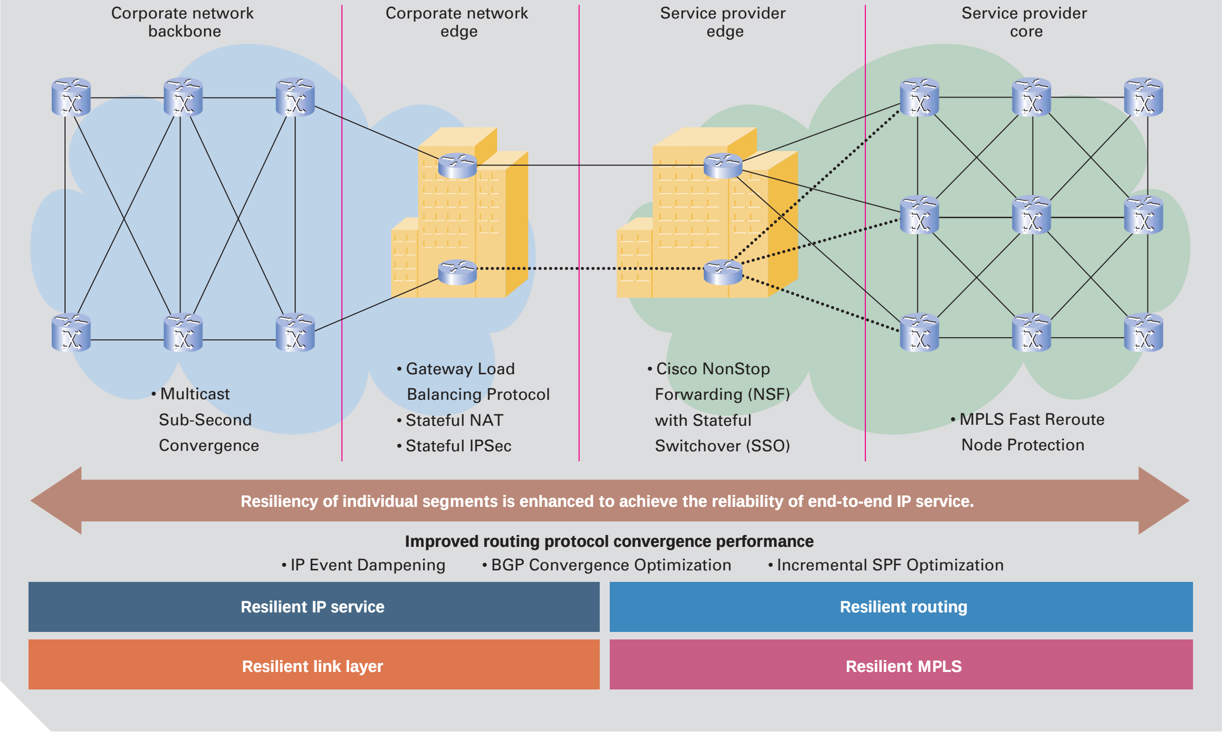


Figure 3-4

Figure 3-4 Cisco Globally Resilient IP (GRIP) solution for nonstop IP service


Corporate network backbone
Corporate network edge
Service provider edge
Service provider core
• Multicast Sub-Second Convergence
• Gateway Load Balancing Protocol
• Stateful NAT
• Stateful IPSec
• Cisco NonStop Forwarding (NSF) with Stateful Switchover (SSO)
• MPLS Fast Reroute Node Protection
Resiliency of individual segments is enhanced to achieve the reliability of end-to-end IP service.
Improved routing protocol convergence performance
• IP Event Dampening
• BGP Convergence Optimization
• Incremental SPF Optimization
Resilient IP service
Resilient routing
Resilient link layer
Resilient MPLS

Resilient link layer and Resilient routing

Stateful Switchover (SSO)

The Stateful Switchover (SSO) function switches from the active route processor to the standby route processor, while link (L2) state information is guaranteed to run concurrently and in synchronisation with failure recovery processing. As a result, reset from the link layer (L2) due to a failure is avoided and restart from the conventional link level is prevented, significantly reducing recovery time.

NonStop Forwarding (NSF)

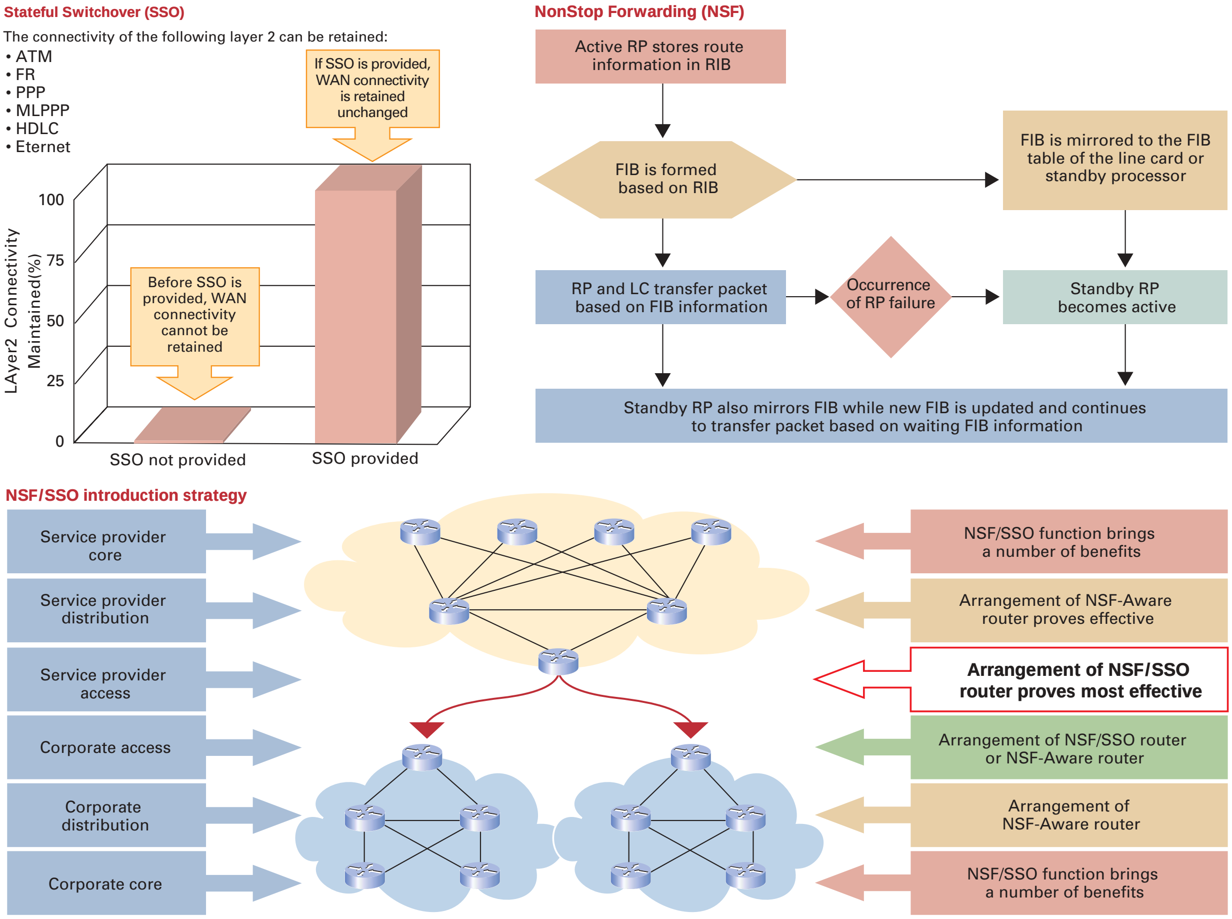
The NonStop Forwarding (NSF) function continues IP packet transfer to guarantee traffic flows if a routing (control plane) failure occurs.

NonStop Forwarding (NSF) and Stateful Switchover (SSO) are elements of the Resilient link layer and Resilient routing, provided concurrently by Cisco IOS. Combining these two functions maintains end-to-end IP service at the link and session levels, even if the route processor causes a failure, and prevents a network failure from affecting end-user service use. Mission-critical multi-services such as video and voice applications are unaffected and can continue to be used (see Figure 3-5).

In addition, the following Resilient routing functions are supported:

- **BGP (Border Gateway Protocol) Convergence Optimisation**
  The BGP Convergence Optimisation function significantly shortens the time required for reconstruction of the network route of a router using BGP. The time required for verification of the routing table of about 200,000 entries is reduced by as much as 40 per cent from the conventional scenario.
- **Multicast Sub-Second Convergence**
  The Multicast Sub-Second Convergence function enables construction of a route within one second if a failure occurs when multicasting is being used, for example, to distribute audio/video streams to clients within a company.
- **IP Event Dampening**
  The IP Event Dampening function selectively deletes from the network routing table any router causing an unstable data link (link flap) until the data link becomes stable again. This can shorten the network convergence time and stabilise the network.
- **Incremental SPF Optimisation**
  The Incremental SPF Optimisation function reconstructs only the affected part of the routing table (instead of the whole routing table) when a routine failure occurs. As a result, because only part of each routing table need be changed in the router (which is distant from the failure), quick convergence is achieved and an optimum IP traffic path can be quickly determined.

Figure 3-5 Resilient link layer and Resilient routing


Stateful Switchover (SSO)
The connectivity of the following layer 2 can be retained:
• ATM
• FR
• PPP
• MLPPP
• HDLC
• Eternet
If SSO is provided, WAN connectivity is retained unchanged
Before SSO is provided, WAN connectivity cannot be retained
LAyer2 Connectivity Maintained(%)
100
75
50
25
0
SSO not provided
SSO provided
NonStop Forwarding (NSF)
Active RP stores route information in RIB
FIB is formed based on RIB
FIB is mirrored to the FIB table of the line card or standby processor
RP and LC transfer packet based on FIB information
Occurrence of RP failure
Standby RP becomes active
Standby RP also mirrors FIB while new FIB is updated and continues to transfer packet based on waiting FIB information
NSF/SSO introduction strategy
Service provider core
Service provider distribution
Service provider access
Corporate access
Corporate distribution
Corporate core
NSF/SSO function brings a number of benefits
Arrangement of NSF-Aware router proves effective
Arrangement of NSF/SSO router proves most effective
Arrangement of NSF/SSO router or NSF-Aware router
Arrangement of NSF-Aware router
NSF/SSO function brings a number of benefits

*The adjacent router in the network must be NSF Aware to enable NSF/SSO.

Resilient MPLS

The Fast Reroute function dramatically improves fault tolerance in the network core where MPLS is employed. When network failures (such as link and node failures) occur, a very fast (several milliseconds) reroute function is provided to protect user traffic. This function can remarkably enhance network availability; the user need not even detect that a network failure has occurred (see Figure 3-6).

Figure 3-6 Resilient MPLS: Traffic Engineering FRR

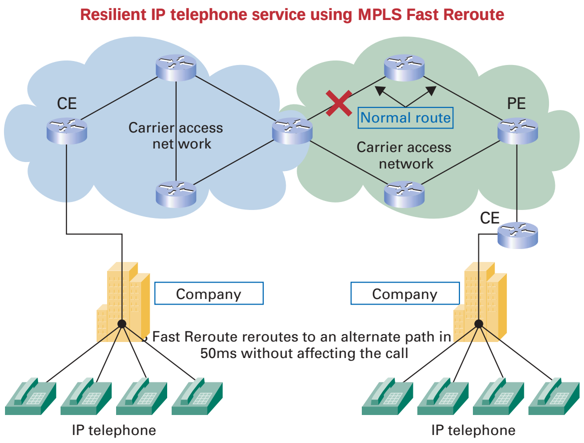
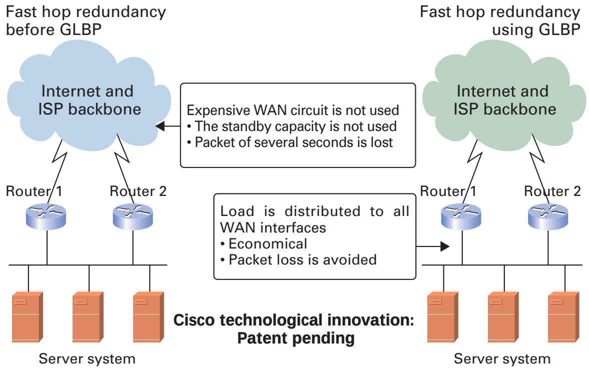

Resilient IP telephone service using MPLS Fast Reroute
CE
Carrier access network
Normal route
Carrier access network
PE
CE
Company
Company
Fast Reroute reroutes to an alternate path in 50ms without affecting the call
IP telephone
IP telephone

Figure 3-7 Resilient IP service: Gateway Load Balancing Protocol


Fast hop redundancy before GLBP
Fast hop redundancy using GLBP
Internet and ISP backbone
Expensive WAN circuit is not used
• The standby capacity is not used
• Packet of several seconds is lost
Internet and ISP backbone
Router 1
Router 2
Load is distributed to all WAN interfaces
• Economical
• Packet loss is avoided
Router 1
Router 2
Cisco technological innovation: Patent pending
Server system
Server system

Resilient IP service

Stateful IPSec and Stateful NAT

With the Stateful IPSec and Stateful NAT functions, the session state of IPSec and NAT (Network Address Translation) protocols is retained throughout the entire redundant router configuration. Even if a specific router causes a failure, real-time applications using these protocols can continue to be used.

Gateway Load Balancing Protocol

The Gateway Load Balancing Protocol function distributes IP traffic load into multiple routers in the corporate network backbone, greatly improving throughput. This function also establishes fault tolerance so that network resources are used efficiently and high reliability is achieved (see Figure 3-7).

Figure 3-8

Applicable platforms and implementation period

The major functions of Cisco's Globally Resilient IP (GRIP) can be obtained by upgrading the Cisco IOS software that comes standard with the Cisco 12000, 10000, and 7500 series Internet routers.

Nonstop IP service develops into a broadband IP multiservice infrastructure

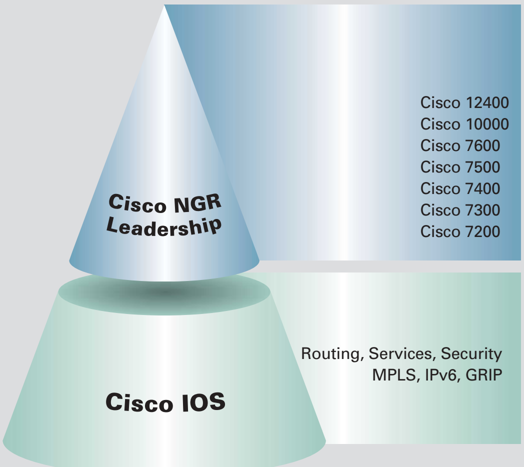


Figure 3-8 Cisco's Globally Resilient IP road map

Resilient category	Function	Applicable platform	Release period
Resilient link layer	Stateful Switchover (SSO)	12000, 10000, 7500	12.0 (22) S
Resilient routing	Cisco NonStop Forwarding (NSF)	12000, 10000, 7500	12.0 (22) S
	The adjacent router must be NSF Aware to enable Cisco NonStop Forwarding (NSF) and Aware NSF/SSO	7200, 7500, 10000, 12000	12.0 (22) S 12.2S
	BGP Convergence Optimization	12000, 10000, 7500	12.0 (22) S
	Multicast Sub-Second Convergence	12000, 10000, 7500 7200, 7600, 6500	12.0 (22) S / 12.1 (11b) E
	Incremental SPF Optimization	12000, 10000, 7500	12.0 (24) S
Resilient MPLS	MPLS Fast Reroute – Node Protection	12000, 7500, 7200	12.0 (22) S
	MPLS SSO coexistence	12000, 7500, 7200	12.0 (22) S
Resilient IP service	Gateway Load Balancing Protocol	12000, 10000, 7500, 7200	12.2 (Rel 1) S
	Network Address Translation Stateful NAT	7600, 7500, 7200	CQ1 2003
	Stateful IPsec	7200	CQ1 2003

Technical Column
Summary Report on Miercom Laboratory Test (Report 240402 for April 2002) Cisco 12000 guarantees **zero packet loss** for a route processor failure

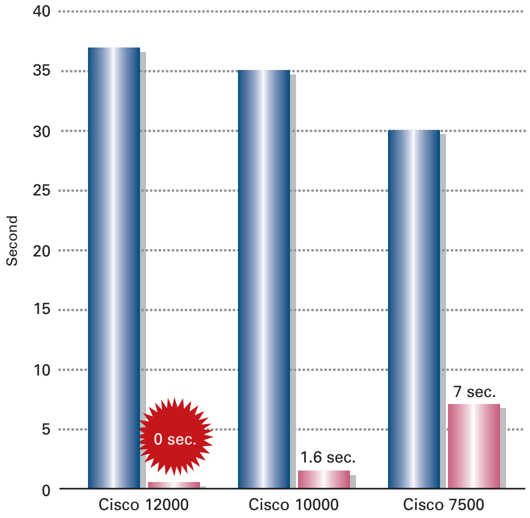
- Cisco NonStop Forwarding (NSF) combined with the Stateful Switchover (SSO) function significantly reduced the mean time to repair (MTTR).
- Route flap was zero during recovery on BGP, OSPF, IS-IS, and static route.
- During recovery (using multiple protocols such as Frame Relay, ATM, HDLC, PPP, and Ethernet) the state was retained and link flap was zero
- Cisco 12000 lost zero packets and recovered instantaneously without affecting transport of voice/video data during switchover of the route processor.

Overview

Cisco Systems asked Miercom to perform an analysis and performance evaluation test regarding Cisco NonStop Forwarding (NSF) combined with the Stateful Switchover (SSO) function, which forms one element of Cisco's Globally Resilient IP technology. The test aimed at verifying the time required for switchover when a route processor failure occurs for three types of edge routers (each with specific edge performance): the Cisco 12000 series Internet router, the Cisco 10000 series Internet router, and the Cisco 7500 series router. The test used 600 interfaces, 2,000 OSPF or IS-IS routes, and 65,000 BGP routes for each router.

Hardware and software failures were simulated for all three routers to measure the mean time to repair (MTTR) in seconds. In tests, the Cisco 12000 series Internet router lost zero packets and recovered spontaneously. The Cisco 10000 series Internet router recovered in 1.63 seconds on average. The Cisco 7500 series router recovered in six seconds on average (for a comparison between Cisco NSF/SSO and Cisco's most effective conventional recovery mechanism, Route Processor Redundancy+, see the following chart).

■Comparison of recovery time between Cisco Route Processor Redundancy+ and Cisco NSF/SSO



Validated by Miercom

INDEPENDENT LAB TESTED NETWORKS AS ADVERTISED™ MIER COMMUNICATIONS INC.

The MTTR for NSF/SSO and Cisco Route Processor Redundancy+ is compared (from occurrence of system failure through restarting of traffic). Cisco Route Processor Redundancy+ will prove to be the most effective redundancy function supported by the Cisco 12000/10000 series Internet router and Cisco 7500 series router before Cisco NSF/SSO is released.

Cisco routers with dual route processors

🟥 Cisco Nonstop Forwarding (NSF) with Stateful Switchover (SSO)
*Link flap is zero. *Route flap is zero.

🟦 Before Cisco NSF with SSO function is used

Test method

In order to demonstrate that Cisco NSF/SSO can be operated concurrently under the control of a wide range of interfaces and various protocols, the test bed was constructed in a network with sufficient port density. A series of three tests were performed – for the Cisco 12000 series Internet router, the Cisco 10000 series Internet router, and the Cisco 7500 series router, respectively.

Cisco NSF/SSO was set up on the routers to be tested and on all adjacent routers. Cisco NSF/SSO was disabled only when the reference test (using Route Processor Redundancy+) was performed. IXIA1600 was set so that two-way traffic was transported to all links and ports of the UUT (unit under test) in all tests. Cisco NSF/SSO was always set up in the UUT. At the start of each test, IXIA route advertisement, traffic flow, and ping were initiated. After normal traffic flow was confirmed, a failure was generated in the primary route processor and the effects of the failure on the traffic flow, link, and route were observed. When the primary processor automatically rebooted and was set up as the secondary processor, the test was terminated.

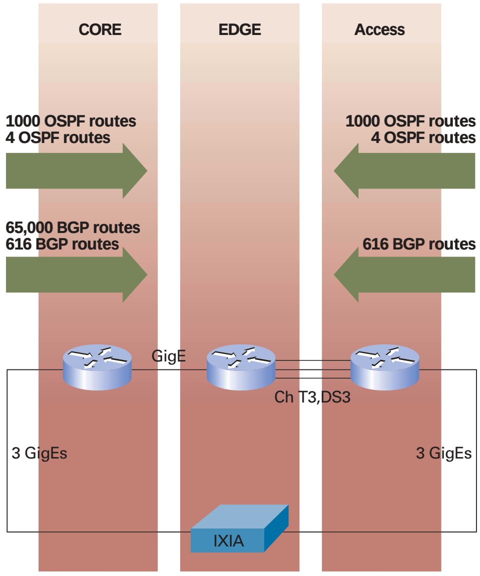
At first, all tests were performed with the IS-IS set. After these tests were terminated, the routers were set up once again and OSPF was used to perform the tests. For the second verification, a ping was transmitted from EnterpriseAccess1 (ENT1) to Core1 via the UUT. During switchover, the ping was monitored and the packet loss was measured. A ping was transmitted once every second. On the ENT and Core router console screens, the link flap and route flap were monitored. In the final test, Cisco NSF/SSO in the UUT was disabled in order to set the Route Processor Redundancy+ mode. The same test was performed to measure the recovery time for a ping from ENT1 to Core1 via the UUT, and the recovery time was compared with the recovery time when Cisco NSF/SSO was executed.

Conclusion

The results of the performance test performed by Miercom proved that Cisco IOS Software Release 12.0(22)S and the Cisco NSS/SSO function, which is one element of Cisco GRIP technology, reduced the MTTR for router processor failure and improved the availability of Cisco routers significantly.

The units under test were the Cisco 12000 series Internet router, the Cisco 10000 series Internet router, and the Cisco 7500 series router. The test results for all three routers showed that Cisco NSF/SSO improved the failover time significantly relative to the failover time for the Route Processor Redundancy+ mode.

■ Product configuration and test method



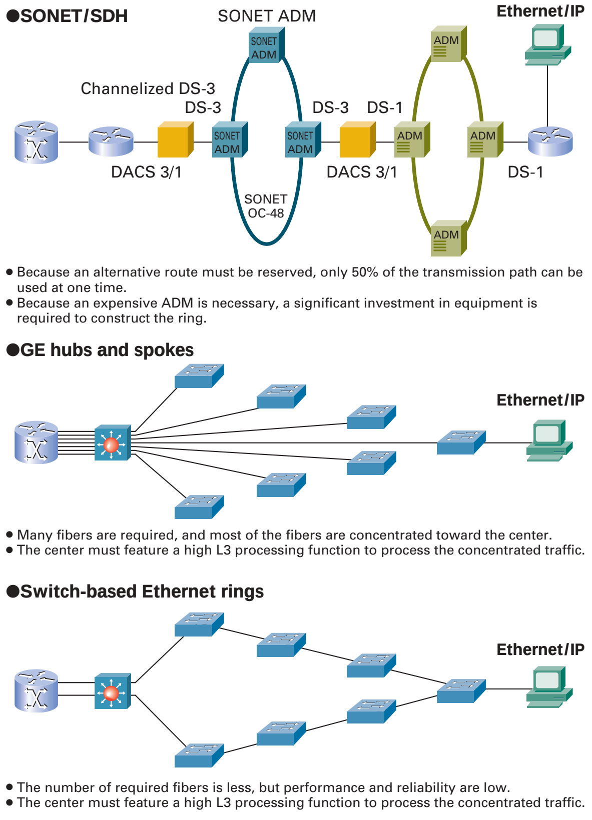
This article is an excerpt from Miercom's "Summary Report on Laboratory Test" Report 240402 (April 2002).

http://www.mier.com

DPT/RPR
Highly Reliable, Next Generation Optical Ring Solution

Part 3 described Cisco’s Next Generation IP network solution, the “Globally Resilient IP” (GRIP), which improves the network's failure recovery capability through the use of extended IOS functionality. Part 4 describes Dynamic Packet Transport/Resilient Packet Ring (DPT/RPR), which is gaining a reputation as an effective technology in the construction of reliable IP based networks, especially in metro areas.

Figure 4-1 Problems with network topology of a metro network



●SONET/SDH

- Because an alternative route must be reserved, only 50% of the transmission path can be used at one time.
- Because an expensive ADM is necessary, a significant investment in equipment is required to construct the ring.

●GE hubs and spokes

- Many fibers are required, and most of the fibers are concentrated toward the center.
- The center must feature a high L3 processing function to process the concentrated traffic.

●Switch-based Ethernet rings

- The number of required fibers is less, but performance and reliability are low.
- The center must feature a high L3 processing function to process the concentrated traffic.

Problems with Conventional Networks

When two or more locations in a particular area, such as in a metro network, are to be connected by fibre, a physical ring must be used to add resilience and make efficient use of fibre. In practice, SONET/SDH, which has been primarily used in the backbone networks of major carriers in North America, Europe and Japan, is comprised of two rings, and features superior reliability and expandability. However, SONET/SDH requires add-drop multiplexers (ADM) in the network, and consequently infrastructure build-out is costly.

This means service providers other than major carriers cannot afford to adopt this system. Moreover, one of the two rings of SONET/SDH is a backup ring and is not normally used, which is an inefficient use of connectivity infrastructure.

On the other hand, switch-based Ethernet with its hub-and-spoke networks prove very attractive in terms of cost. However, as also described in Part 3, they feature some operational challenges.

Birth of Highly Reliable, Next Generation Ring Network Technology: DPT/RPR

DPT/RPR was developed to resolve the problems of conventional network technology. DPT/RPR is a transport technology that directly sends IP packets in the same physical configuration as that of the SONET/SDH. DPT was released worldwide by Cisco Systems at the end of February 1999 and was used as the basis for the resilient packet ring (RPR) technology, to be standardised under IEEE 802.17 in March 2003.

DPT/RPR has been used by 200 or more customers, including the US company Sprint, E-Bone, Versatel, SUNet, as well as other major carriers, ISPs, and academic organisations around the world. DPT/RPR represents a new option in the construction of highly reliable networks. The following describes the features of DPT/RPR in more detail.

Figure 4-2 DPT/RPR standardization, led by Cisco Systems

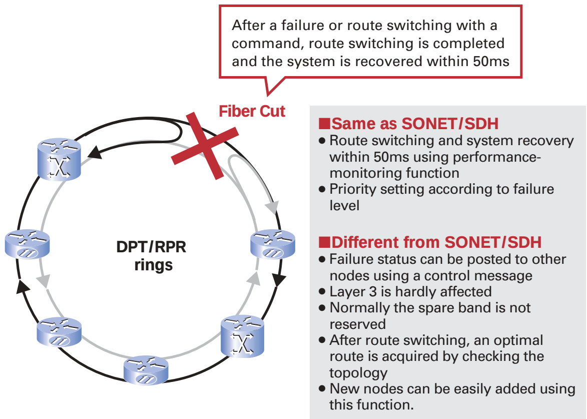
February 1999	Cisco releases DPT products
November1999	Shipping of the Cisco 12000 OC12DPF line cards begins Shipping of the Cisco 7200/7500 OC12DPF line cards begins
March 2000	**Shipping of the Cisco 12000 OC48DPF line cards begins**
June 2000	Shipping of the DPT Concentrator Cisco ONS15190 begins
August 2000	**Cisco submits IETF RFC 2892 (SRPv2)** **The IP over Packet Transport Rings (IPoPTR) BOF is held**
December 2000	**Cisco RPR Alliance is established**
March 2001	**First conference of the IEEE802.17 Working Group**
October 2001	**Shipping of the Cisco 10720 for metro networks begins**
November 2001	**A draft of the IEEE802.17 Working Group is proposed**
January 2002	**The first edition of the draft of the IEEE802.17 Working Group is approved**
April 2002	**Polling is performed by the IEEE802.17 Working Group**
June 2002	**Cisco 12000 OC-192DPT line cards released**
March 2003	**IEEE802.17 to be standardized**

Carrier-class reliability and failure resistance

The reliability and failure resistance of DPT/RPR match those of SONET/SDH. DPT/RPR circulates monitoring intelligent protection switching (IPS) control packets on the rings in order to transmit protection status and to maintain topology status. If a failure such as a line disconnection occurs, the system recovers within 50ms, with the faulty route immediately switched to the alternative route via a loopback at the failure point or pass-through, as with SONET/SDH.

In addition, DPT/RPR features special functions not supported by SONET/SDH. For example, the failure status can be posted to other nodes using a control message, failure does not influence layer 3 services, and the spare ring is usually unnecessary. Using these special functions, new nodes can be easily added without interrupting the current services.

Figure 4-3 Key technology of DPT/RPR:
High reliability through intelligent protection switching (IPS)


After a failure or route switching with a command, route switching is completed and the system is recovered within 50ms
Fiber Cut
DPT/RPR rings

■Same as SONET/SDH
- Route switching and system recovery within 50ms using performance-monitoring function
- Priority setting according to failure level

■Different from SONET/SDH
- Failure status can be posted to other nodes using a control message
- Layer 3 is hardly affected
- Normally the spare band is not reserved
- After route switching, an optimal route is acquired by checking the topology
- New nodes can be easily added using this function.

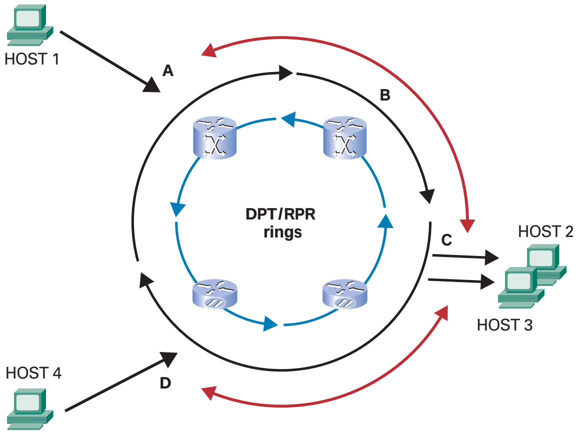
Full bandwidth use by DPT/RPR

DPT/RPR is also superior in terms of effective use of bandwidth. The DPT/RPR network is made of two symmetric optical rings passing traffic in opposite directions, as with SONET/SDH. DPT/RPR uses the spatial reuse protocol (SRP), which strips data at the destination instead of at the sender. Therefore, bandwidth occupation, which usually occurs in the FDDI/Token Ring system until the data returns to the source, does not occur, and the ring bandwidth of each node can be used equally. The bandwidth of both rings can be used if it is not being used by other nodes. On the OC-48 ring, data can be transmitted at up to 5Gbps.

Access line construction using optical rings

One of the most significant benefits of DPT/RPR is that users can connect directly to it. For example, multi-tenant buildings can be interconnected via a DPT/RPR ring, providing the building's occupants with high-speed, highly reliable services. The DPT/RPR ring solution thus enables the addition of new value-added services, providing new possibilities for broadband markets in metro areas.

Figure 4-4 Key technology of DPT/RPR:
Effective and equal band use via the spatial reuse protocol (SRP)



■Effective band use
- Destination stripping —— Data is stripped at the destination
- Simultaneous communication between two or more nodes —— The NxOC-48 band can be used

■Equal band use
- Equal band use —— Respective nodes can use the ring band equally
- Effective band use —— While other nodes are not using the band, all of the band can be used
- Expandability —— A large-scale ring may be constructed to accommodate many nodes (One ring can accommodate up to 128 nodes)

Glossary

DPT/RPR

DPT (Dynamic Packet Transport) is a packet transfer technology developed by Cisco Systems. The DPT system is underpinned by SRP and uses a two-way ring topology. DPT has already been adopted by 190 or more customers worldwide and is expected to form the core technology of Next Generation optical networks.

The RPR (Resilient Packet Ring) represents the latest packet ring technology and is being standardised as IEEE 802.17. Cisco's SRP forms the key technology of RPR, and Cisco is both actively involved in this standardisation work and chairs the IEEE 802.17 working group.

SRP

SRP (Spatial Reuse Protocol) is a medium-independent protocol for media access control (MAC). SRP provides DTP/RPR as an element of the ring topology. In IETF, SRP is defined in RFC 2892. SRP was so-named because the spatial width of the band is used effectively in packet processing. SRP MAC supplies the basic functions of addressing, packet removal, bandwidth control, and control message transfer on packet rings.

Conclusion

As described above, DPT/RPR improves backbone reliability, critical in the current broadband age and likely to become even more so while providing the optimal solution for effective bandwidth use. DPT/RPR has the added benefit of allowing the construction of inexpensive, robust networks in metro areas through the use of DPT-enabled routers without the need for expensive facilities. In addition, DPT/RPR in combination with the MPLS technology can construct a highly intelligent network. Only Cisco with its wide range of products can provide such a complex backbone solution.

IP Multicast Solution using DPT/RPR

Because DPT/RPR supports IP multicast, a streaming image distributed from one office can be accessed by other offices simultaneously. When the sender of the streaming image sends packets by setting the multicast bit, an appropriate node on the ring receives the packets and sends them to the specified destination. This results in more effective use of bandwidth.

Figure 4.5 Cisco's Metro IP Solution

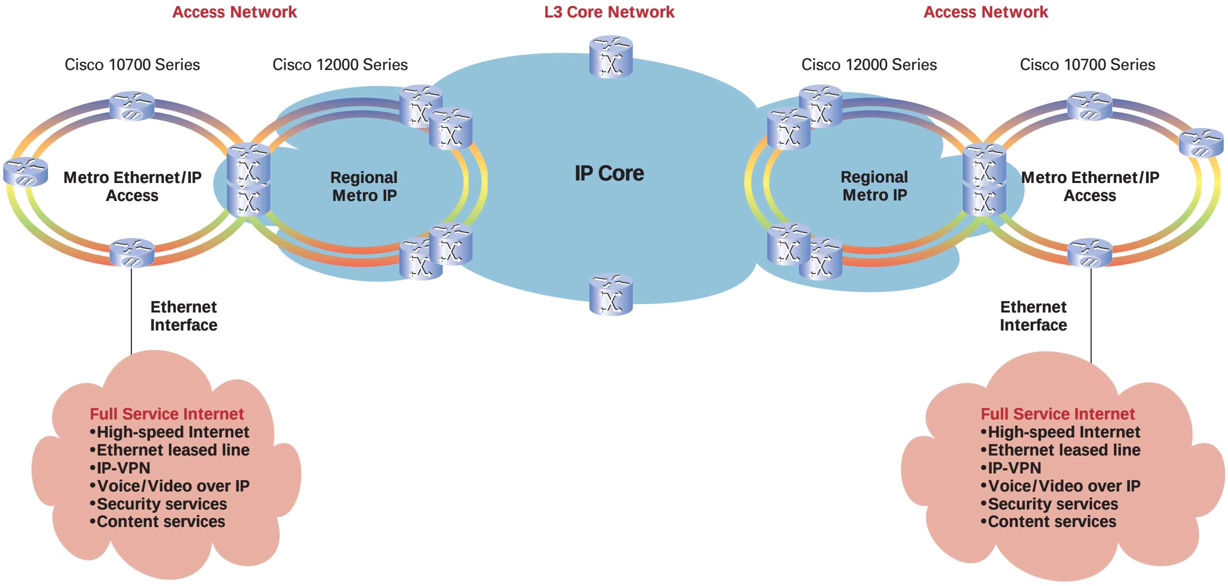
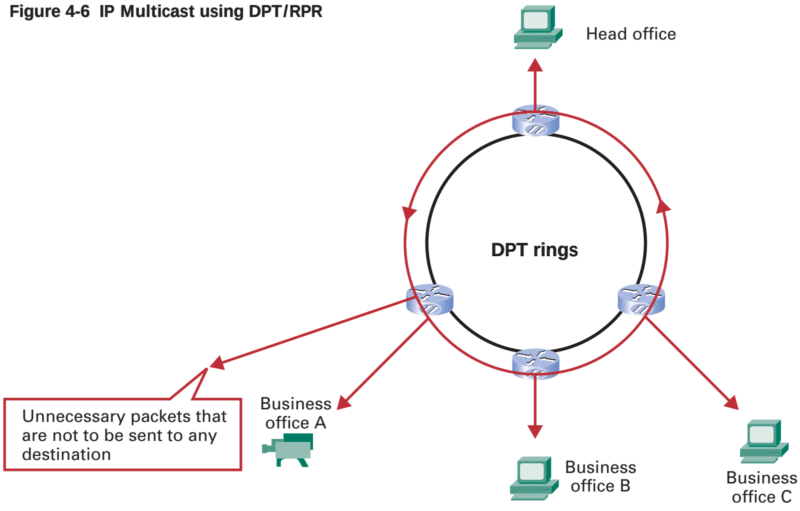


Figure 4-6 IP Multicast using DPT/RPR



■ **IP Multicast support on DPT**

- A camera image in business office A can be distributed to other offices through the supply of a single stream to DPT.

■ **Packet flow**

- The sending node can set the Multicast bit. The layer 3 services are less affected.
- An appropriate node on the ring receives the sent packets, and the sending node discards unnecessary packets.

Technical Column
Next Generation IP surveillance camera solution using DPT/RPR and IP Multicast

Surveillance camera solution to meet rapidly increasing needs

Effective surveillance camera solutions are now needed in a number of fields. Terrorist attacks in the US have greatly increased the demand for surveillance cameras worldwide; such systems are now in demand to enhance safety, assist in efforts to fight crime, and promote infrastructural development. In many countries, the demand for surveillance cameras in the health-care and welfare fields has also increased.

Thus there are a number of urgent reasons to develop a more reliable, high-performance surveillance system based on the latest information technology. Conventional surveillance camera solutions present numerous problems and are inadequate for the demands being placed upon them.

Issues with conventional surveillance camera systems

Based on analogue TV technology, conventional surveillance camera systems suffer from various problems such as image quality, real-time monitoring operation, and expandability – that is, the addition of equipment and consequent re-configuration. Moreover, most of the signal distribution systems, dedicated monitors, and other equipment required by such systems are both expensive and difficult to use.

Scalability

Both workload and costs are high when adding new bases and changing routes. A switching unit is necessary when images from two or more cameras must be surveyed on one monitor screen. Bandwidth-use efficiency is low, as both bandwidth and transmission path are fixed.

Image quality

Analogue TV signals are attenuated due to coaxial cable relaying. Image deterioration and transmission delay occur during digital-to-analogue conversion and vice versa, while image quality is further reduced due to signal routing via distributors and switching units.

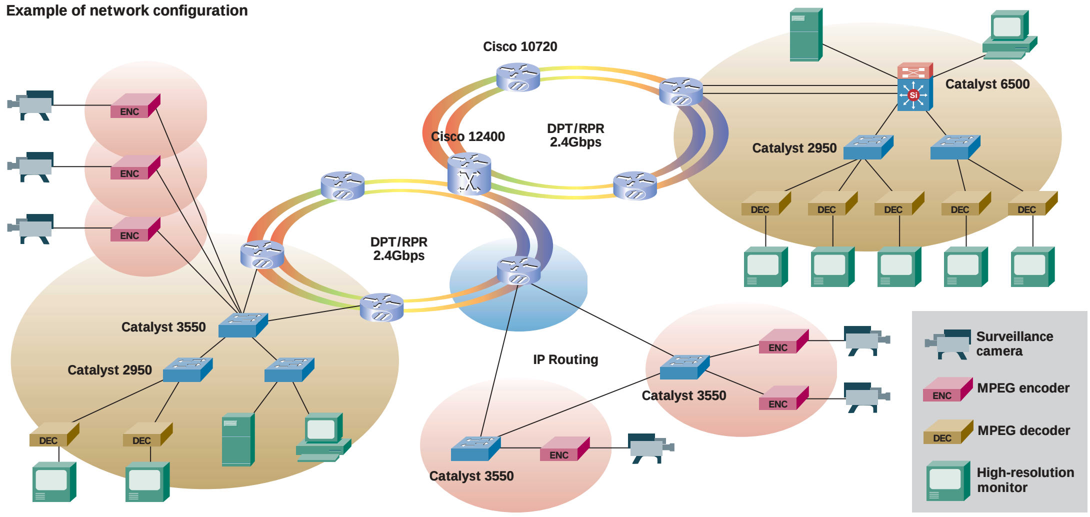
Cost of equipment

Generally, carrier equipment is very expensive. Expensive modules are required to accommodate carrier equipment in an IP network. Expensive distributors are required to survey two or more bases or two or more screens at a time.

Solution

The above problems can all be solved by installing a surveillance camera system based on an IP network using the latest DPT/RPR and IP Multicast (PIM-SM) technology. The Next Generation, IP surveillance camera solution provides high scalability, high reliability, and low cost, effectively meeting the needs of our rapidly changing times.

Example of Network Configuration featuring a Next-Generation IP Surveillance Camera System

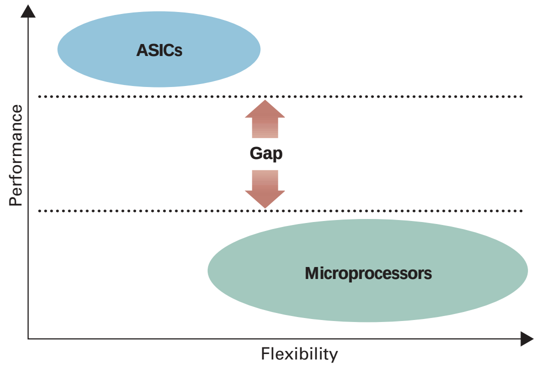


Technical Column
Adaptive network processing

CPU-based platforms feature excellent flexibility; they can deliver multiple functions that can be added to and changed through software upgrades. However, these platforms require certain improvements – for example, higher performance is needed to provide high-speed services, and greater capacity is required to accommodate high-density lines. On the other hand, ASIC-based platforms enable high speed forwarding optimised for core backbone applications. However, ASIC-based platform hardware must be replaced when a function is added or changed, and development requires a great deal of time. Rapid responses to customer needs are difficult to achieve.

Cisco System's adaptive network processing eliminates the gap between the two technologies, providing innovative solutions that reconcile high-speed throughput and superior flexibility using advanced, reprogrammable ASIC technology (Figure 1).

Figure 1



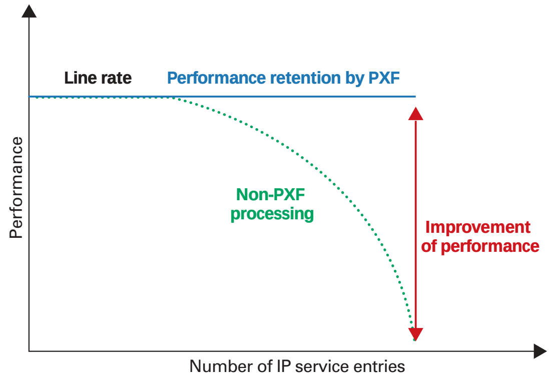
About Parallel Express Forwarding (PXF)

PXF is a revolutionary microprocessor technology developed by Cisco Systems, designed to provide advanced IP services while maintaining high performance. This technology represents an important component in the development of new services such as MPLS, VPN, and service differentiation, applied in combination with various function sets and a high-speed, large-capacity switching function. A patent for the PXF technology was obtained in the U.S. in 1999 (U.S. Patent No. 6101599).

Advanced IP services and high performance

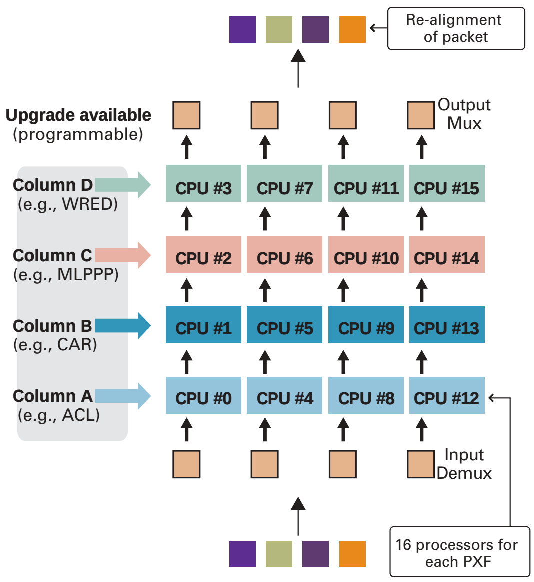
The main feature of PXF is that it can maintain high performance even with the addition of advanced IP services such as QoS and ACL. As shown in Figure 1, with conventional processing performed only by CPUs, maximum performance declines as services are added. However, with PXF, IP service can be provided while maintaining performance (Figure 2).

Figure 2 PXF Performance



This feature is enabled by a four by four, parallel processor array. In the PXF engine, different functions are undertaken for each column (Figure 3). Due to a combination of parallel processing and pipeline technologies, 16 packets can be processed simultaneously on a PXF engine, resulting in a sustainable, high packet transfer rate.

Figure 3 PXF processor

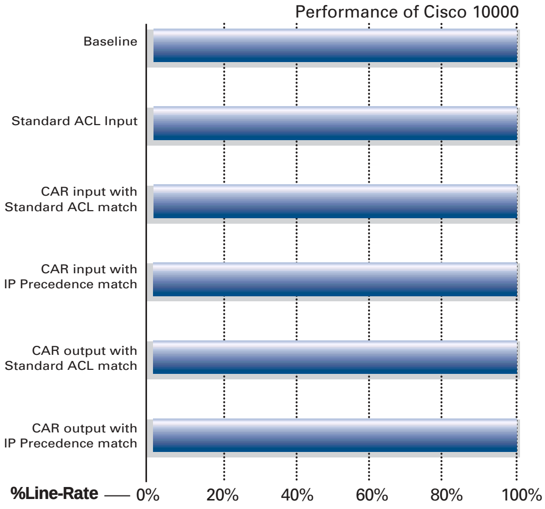


Note: The functions to be mounted in the respective columns depend greatly on the platform and IOS version.

Software upgrade available

One of the most important features of PXF is its on-demand, changeable network processing. The PXF engine can upgrade the software based on reprogrammable ASIC technology. Consequently, new functions and bug fixes can be implemented more quickly than with conventional ASIC-based solutions. While performance in practical use greatly depends on the individual network configuration, it is guaranteed, for example, that a Cisco 10000 with PXF installed will obtain high throughput – close to the line rate – when ACL and CAR service entries are added (Figure 4).

Figure 4 PXF IP service performance



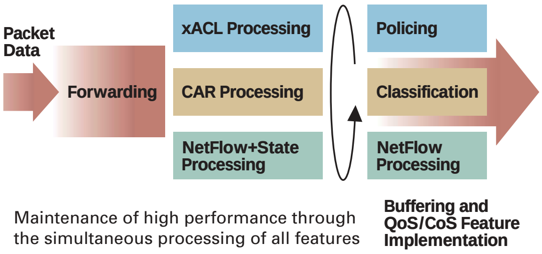
Currently, PXF is installed in the Cisco 10000 series, the Cisco 7600 series, the Cisco 7300 series and the Cisco 7400 series.

The IP Service Engine (ISE)

The ISE enables the Cisco 12000 series Internet router, the industry-standard high-end IP backbone router, to be used as a high-speed edge router. Combined with distributed packet transfer and innovative adaptive, wire-speed network processing, it enables high speed, high cost-performance IP services (Figure 5). The ISE provides the Cisco 12000 series with the highest flexibility ever achieved and can provide the world's fastest backbone and edge performance.

Accordingly, Internet service providers can supply new, value-added services using voice and video, expanding their business scales and improving profitability.

Figure 5 ISE fast edge function


Packet Data
Forwarding
xACL Processing
CAR Processing
NetFlow+State Processing
Policing
Classification
NetFlow Processing
Maintenance of high performance through the simultaneous processing of all features
Buffering and QoS/CoS Feature Implementation

Section 5

Service differentiation and **Quality of Service**

The Challenge

A communications network forms the backbone of any successful organisation. The network serves as a transport for a multitude of applications, including delay-sensitive voice, and bandwidth-intensive video. These business applications stretch network capabilities and resources, but also complement, add value, and enhance every business process. Networks must therefore provide secure, predictable, measurable, and sometimes guaranteed services to these applications. The secret to running an infrastructure that truly serves the business, end-to-end is to achieve the required Quality of Service (QoS) by managing the delay, delay variation (jitter), bandwidth, and packet loss parameters on a network, while maintaining simplicity, scalability, and manageability.

The Solution

Cisco IOS® software provides a complete tool chest of QoS features and solutions for addressing the diverse needs of voice, video, and data applications. Cisco IOS QoS technology lets complex networks control and predictably service a variety of networked applications and traffic types. Small to medium businesses, enterprises, and service providers all benefit from deploying Cisco QoS on their networks. Bandwidth, delay, jitter, and packet loss can be effectively controlled. By ensuring the desired results, the QoS features lead to efficient, predictable services for business-critical applications.

Using the rich QoS feature set in Cisco IOS software, businesses can build networks that conform to either the Internet Engineering Task Force (IETF) Integrated Services (IntServ) model or the Differentiated Services (DiffServ) model. Cisco IOS QoS features also provide value-added functionality such as network-based application recognition (NBAR) for classifying traffic on an application basis, a service assurance agent (SAA) for end-to-end QoS measurements, and Resource Reservation Protocol (RSVP) signalling for admission control and reservation of resources.

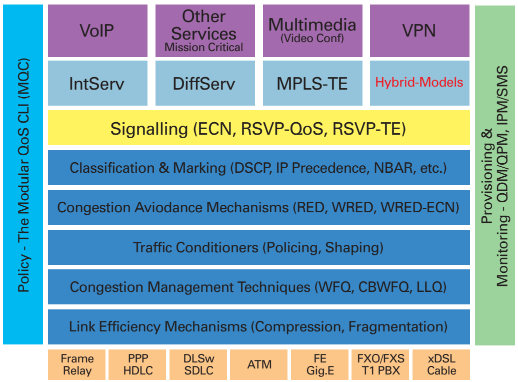
Applications

Small to medium businesses often cannot justify continual upgrade of the link-speeds in their networks. Cisco IOS software QoS features provide an alternative solution for taking charge of the available bandwidth and managing them efficiently to meet the application demands. Mechanisms such as link fragmentation and interleaving (LFI), Compressed Real-Time Protocol (CRTP), Weighted Fair Queuing (WFQ), and Low-Latency Queuing (LLQ) allow the most efficient distribution of the available bandwidth among the applications.

Enterprises can deploy Cisco IOS IntServ and DiffServ QoS features quickly and easily across an entire network. With end-to-end QoS solutions, business-critical and multimedia applications can be prioritised and assured the required network bandwidth and delay bounds. Expensive WAN connections can also be utilised as efficiently as possible, while ensuring low delay, jitter, and assured bandwidth for voice over IP (VoIP). RSVP, Class-Based Weighted Fair Queuing (CBWFQ), committed access rate (CAR), generic traffic shaping (GTS), and Weighted Random Early Detection (WRED) are just some of the core Cisco QoS tools for enterprises.

A service provider can offer QoS-enabled virtual private networks (VPNs) and non-VPN services to gain the competitive edge. The tightly integrated Cisco DiffServ and Multiprotocol Label Switching (MPLS) features enable further differentiation with end-to-end IP services. Service providers catering to traditional ATM and Frame Relay customers can also benefit from Cisco's IP QoS-to-ATM Class of Service (CoS) features, Frame Relay traffic shaping (FRTS), Frame Relay fragmentation (FRF.12), and other solutions. Finally, mapping RSVP reservations to ATM permanent virtual circuit (PVC) and switched virtual circuit (SVC) QoS is also a differentiating tool for service providers providing end-to-end QoS services.

Figure 5-1 The Cisco QoS Framework



Policy - The Modular QoS CLI (MQC)
VoIP
Other Services
Mission Critical
Multimedia
(Video Conf)
VPN
IntServ
DiffServ
MPLS-TE
Hybrid-Models
Signalling (ECN, RSVP-QoS, RSVP-TE)
Classification & Marking (DSCP, IP Precedence, NBAR, etc.)
Congestion Aviodance Mechanisms (RED, WRED, WRED-ECN)
Traffic Conditioners (Policing, Shaping)
Congestion Management Techniques (WFQ, CBWFQ, LLQ)
Link Efficiency Mechanisms (Compression, Fragmentation)
Frame Relay
PPP HDLC
DLSw SDLC
ATM
FE Gig.E
FXO/FXS T1 PBX
xDSL Cable
Provisioning &
Monitoring - QDM/QPM, IPM/SMS

Cisco IOS QoS Technology

Cisco IOS QoS Tools are divided into six main categories:

Classification & Marking

Packet classification features allow traffic to be partitioned into multiple priority levels, or classes of service. Packets can be classified in a variety of different ways—ranging from input interface, to NBAR (Network Based Application Recognition) for difficult to classify applications, to arbitrary access-control lists. Classification is the first component of the Modular QoS CLI (MQC), the simple, scalable, and powerful QoS framework in IOS. The MQC allows for the clear separation of classification, from the policy applied on the classes, to the application of a QoS policy on an interface or sub-interface. You can also mark packets in a variety of ways (Layer 2: 802.1p/Q / ISL, ATM CLP bit, Frame-Relay DE-bit, MPLS EXP bits, etc., and Layer 3: IP Precedence, Differentiated Services Code Point (DSCP), etc.) using the policy-framework component of the MQC.

Congestion Avoidance

The Weighted Random Early Detection (WRED) algorithm provides for congestion-avoidance on network interfaces by providing buffer management, and allowing TCP traffic to throttle back before buffers are exhausted. This helps avoid tail-drops, and global synchronisation issues, thereby maximising network utilisation and TCP-based application performance. The policy-framework component of the MQC accommodates WRED.

Congestion Management

Often a network interface is congested (even at high speeds, transient congestion is observed), and queuing techniques are necessary to ensure that the critical applications get the forwarding treatment necessary. For example, real-time applications such as VoIP, stock-trading, etc. may need to be forwarded with the least latency and jitter (up to a provisioned limit). Cisco's Low-Latency Queuing (LLQ) provides for such a solution. For other non-delay sensitive traffic (such as FTP, HTTP, etc.), other queuing techniques such as CBWFQ, and MDRR (Modified Deficit Round-Robin) may be used. The queuing techniques can be instantiated using the policy-framework of the MQC as well.

Traffic Conditioning

Traffic entering a network can be conditioned by using a policer or shaper. A policer simply enforces a rate-limit, while a shaper smoothes the traffic flow to a specified rate by the use of buffers. Once again, mechanisms such as CAR (Committed Access Rate), GTS (Generic Traffic Shaping), and FRTS (Frame-Relay Traffic Shaping) can be configured without/within the MQC framework.

Signalling

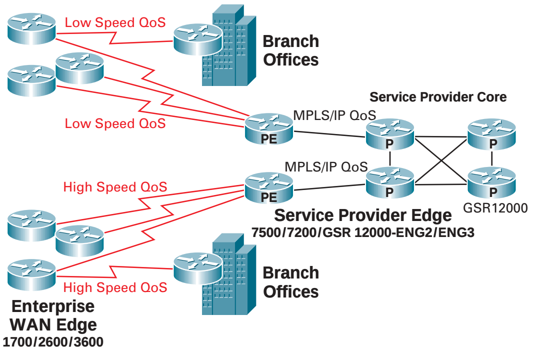
Cisco IOS, in addition to supporting provisioned QoS (including the IETF DiffServ [Differentiated Services] Model with techniques such as CAR, GTS, L3 packet marking, etc.) also provides for the Integrated Services (IETF-IntServ) model. Resource Reservation Protocol (RSVP) is the primary mechanism to perform Admission Control for flows in a network.

A perfect example is the case of VoIP (Voice over IP). A call is completed only if the resources are available for it, ensuring that a call coming into a network does not bump or affect the quality of existing calls. Another technique called QPPB (QoS Policy Propagation via BGP) allows for indirectly signalling (using the community-list attribute in BGP) the forwarding priority for packets destined toward an autonomous system, AS-path, or IP-prefix. This is a highly useful feature for service providers and large enterprises.

Link Efficiency Mechanisms

Streaming video and voice traffic uses the Real-Time Protocol (RTP). IP, UDP, and RTP packet headers can be compressed from approximately 40 bytes down to 5-8 bytes. This saves tremendous amount of bandwidth in the case of low speed links, and when supporting a large number of media streams. In addition, FRF.12 (Frame-Relay Forum specification for frame-fragmentation) and Cisco LFI (Link Fragmentation & Interleaving) allow for fragmenting large data packets, interleaving them with RTP packets, and maintaining low delay and jitter for media streams.

Figure 5-2 Implementing QoS across Enterprise and SP networks



Section 6

Service with Security

Today's networks are more extensive in terms of geographic reach and the internal and external communities they interconnect. They are more complex, support a wide variety of applications and services, and handle converged data, voice, and video traffic across wired and wireless connections. They are also increasingly open—they use untrusted public networks, connect partners, and are a business tool that touches both customers and suppliers. In fact, the division between private and public networks has blurred.

The extensive, complex, and open nature of the network environment increases the need for robust and comprehensive security, because any point the network touches must be protected, as well as protected against.

Drivers for Integration

This section considers factors that drive the need for integrated, embedded network security.

Increased Threat

The network is increasingly both a target and a source of attack:

- A recent study by Riptech, a real-time information protection company, reveals that network security breaches are up 28 per cent from the last half of 2001 to the first half of 2002.
- A 2002 FBI report reveals that 85 per cent of the businesses surveyed have detected computer security breaches within the last 12 months.
- The threat may come from untrusted outsiders or trusted employees. In their 2001 survey, the FBI found 91 per cent of respondents reported insider network abuse.

Threats may originate from deep within the organisation, or from the very edges of the network. The implication is that protection must exist at all points in the network, not just the perimeter or the ingress/egress to untrusted domains. Only security that is embedded and fully integrated can provide this pervasive defence.

Organisational Impetus

The responsibility for security policy, deployment, and purchase is changing. The network operations (NetOps) and security operations (SecOps) teams no longer operate in an isolated manner. The traditional deployment model has been for NetOps to purchase and roll out the networking infrastructure, while SecOps, with a significantly smaller budget and resource base, acted as a discrete and highly specialised team. The two teams had different, divergent roles—the function of NetOps was to provide access, while SecOps had the mission to limit access. This led to intra-organisational tension. However, the increased threat level and need to secure new technologies such as wireless and IP telephony has since forced SecOps and NetOps to work more closely together. In addition, the CxO level is now increasingly involved in security strategy and deployment, and this executive level of involvement has more closely drawn NetOps and SecOps together. Organisational integration drives the requirement for integrated and embedded security. If SecOps and NetOps are jointly deploying security, the task is greatly simplified when the security solution is an integrated one.

Total Cost of Ownership

Security deployment is a priority for all organisations but budgets are tight in today's economy. Integrated security offers the lowest total cost of ownership:

- Adding security services to an already deployed networking device means the existing chassis, power supply, LAN/WAN cards, and other components can be reused. If the networking device is itself modular and offers scalable performance, cost of ownership is further reduced.
- Existing management and monitoring systems can manage the new security services.
- Current support contracts may either cover or be cost-effectively extended to cover new security capabilities.
- The requirement for staff training may be reduced when existing systems are "reused" as security platforms.
- Where load balancing is deployed as part of an integrated security solution, the organisation can reduce the number of, and hence investment in, servers and security systems such as firewalls.

Exploding Scale

This paper has discussed the increasingly extensive nature of the network, which is one aspect of the scale issue. The network must now cope with an expanded population of users, sites, and services. It must handle ever-increasing amounts of traffic, whether data, voice, or video. The network now includes wired and wireless connectivity. Effectively managing this environment is very challenging, if not impossible, unless an organisation takes an integrated approach. The scale problem is significantly reduced, for example, if an integrated management system is available to manage a network of integrated devices, supported by a unified identity framework.

Product Availability

Between 2000 and 2002, there has been a significant move from single-function networking and security devices to multi-function systems. Networking devices such as routers and switches now provide enhanced connectivity and networking services with the addition of sophisticated security services. In parallel, single-function security appliances such as firewalls and VPN concentrators have benefited from additional security services such as intrusion detection. In summary, the availability of products offering integrated features helps propel or at least satisfy the market requirement for integration.

Solution Integration

Finally, all components of the network must interoperate and function as a cohesive whole.

Consider the data centre. It contains multiple servers connected to the external environment via switches and routers. The servers must be protected. The routers and switches must have their own countermeasures to defend themselves. In addition, the entire architecture must be available and scalable, as well as maintain an integrated management subsystem that controls it.

The Cisco Integration Strategy

The integration of security throughout the network is a fundamental aspect of Cisco's development and marketing strategy. Cisco's integration plans include the following components:

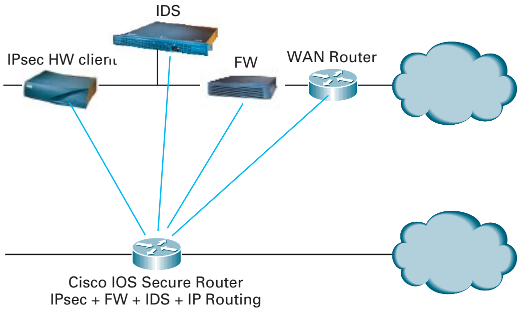
- To provide an increasing amount of security functionality integrated within Cisco IOS® Software. This software cuts across all Cisco platforms, from the teleworker and remote office solution extending to the head end.
- To provide security functionality within discrete security appliances and within integrated networking devices that also provide LAN and WAN connectivity.
- To provide a management and monitoring infrastructure that supports the easy deployment of integrated, embedded security.
- To provide a scalable and high-availability security framework. The network is now an essential business tool that can never be out of service.
- Finally, to provide a deployment model for customers and organisations wanting to deploy integrated, embedded security. This is the function of the Cisco SAFE Blueprint.

The Cisco SAFE Blueprint

The Cisco SAFE Blueprint provides a series of guidelines for security deployment. The blueprint provides tangible steps for organisations actively seeking to deploy integrated, embedded security. Cisco SAFE Blueprint white papers are written from a product-agnostic perspective, which means they do not specifically recommend Cisco products as the basis for security deployment. They also assume a heterogeneous environment may exist.

As one example, Cisco has provided a blueprint specifically for the enterprise, where the network is split into modules, since a modular approach helps deployment and budgeting. Within modules, the Cisco SAFE Blueprint recommends an optimum design for reliable network security. The corporate Internet module provides access from the campus core to the untrusted Internet domain. To provide comprehensive network security, the network has overlapping layers of secure routers providing access control, network and host-based intrusion detection systems scanning for attack signatures, and VPN tunnel initiation and termination devices.

Figure 6-1 The Integration of Security and Routing



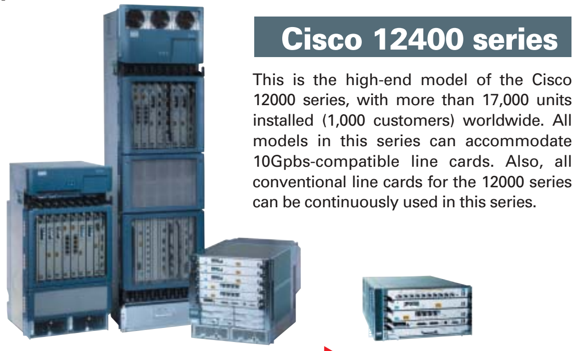
Section 7

Cisco Next Generation Routers - Core and Edge

Cisco Next Generation Routers (NGRs) enable the construction of IP networks that satisfy the requirements of the next-generation, broadband-based Internet. Cisco's NGRs are the industry's most advanced product and feature cutting-edge technologies, including the MPLS, GRIP and DRT/RPR technologies introduced in this document.

Major applications of Cisco NGR

Cisco offers the Cisco 7300, Cisco 7400, Cisco 7600, Cisco 10000, Cisco 10700, and Cisco 12400 series as NGR platforms, responding to the requirements of diverse applications, including broadband access, metro IP, Internet data centres, edges, backbones, and various next-generation networks.

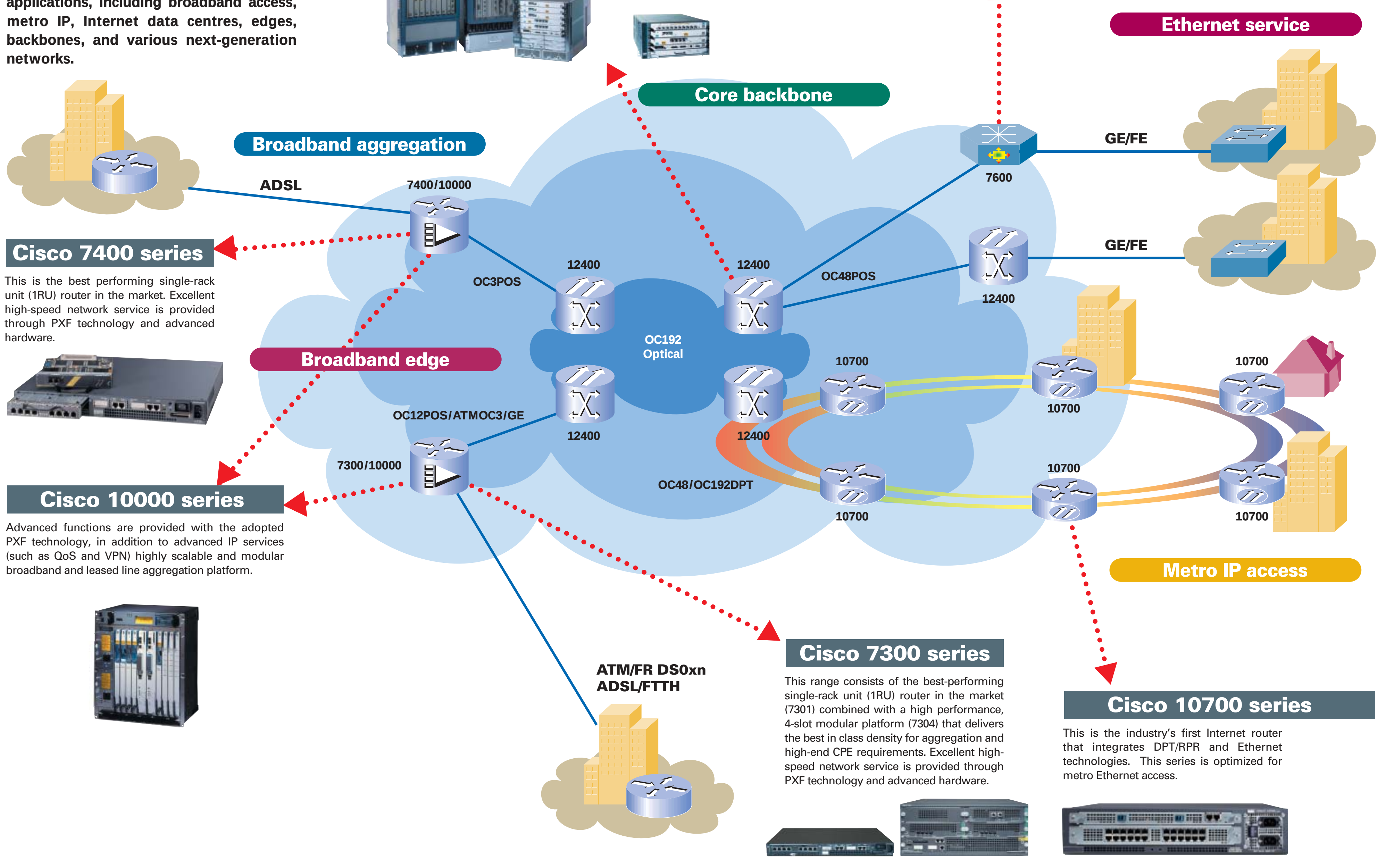


Cisco 12400 series

This is the high-end model of the Cisco 12000 series, with more than 17,000 units installed (1,000 customers) worldwide. All models in this series can accommodate 10Gpbs-compatible line cards. Also, all conventional line cards for the 12000 series can be continuously used in this series.

Cisco 7600 series

This is a next-generation, mid-range router provided with an optical edge. Accommodates lines ranging from low-speed connections to 10Gbps Ethernet. High performance and high-quality services can also be provided through a 256Gbps crossbar switch fabric and PXF.



Cisco 7400 series

This is the best performing single-rack unit (1RU) router in the market. Excellent high-speed network service is provided through PXF technology and advanced hardware.

Cisco 10000 series

Advanced functions are provided with the adopted PXF technology, in addition to advanced IP services (such as QoS and VPN) highly scalable and modular broadband and leased line aggregation platform.

Cisco 7300 series

This range consists of the best-performing single-rack unit (1RU) router in the market (7301) combined with a high performance, 4-slot modular platform (7304) that delivers the best in class density for aggregation and high-end CPE requirements. Excellent high-speed network service is provided through PXF technology and advanced hardware.

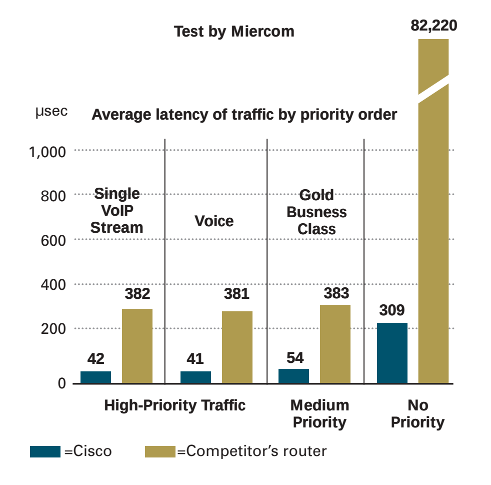
Cisco 10700 series

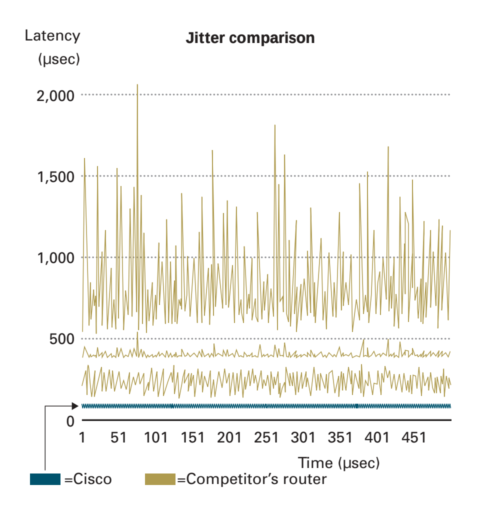
This is the industry's first Internet router that integrates DPT/RPR and Ethernet technologies. This series is optimized for metro Ethernet access.

Cisco NGR - ideally suited for multi-service networks

When delay-sensitive data such as sound and video are placed on the IP network, they must be sent without packet loss or delay, even in the event of traffic congestion. In the performance test conducted by Miercom, Cisco's next-generation backbone router Cisco 12400 series was proven to perform priority control of traffic without packet loss or sequence error, and to maintain strict jitter control even during congestion.

* For details, refer to www.mier.com.





Section 8

Access Routers

The core and edge segments of the network provide the high-speed bandwidth pipes and resilient topology for handling large volumes of data within national, international and worldwide boundaries. These large capacity networks may utilise the facilities of multiple Service Providers (SPs) in order to provide a physical and/or virtual Enterprise network linking several different locations.

So the core/edge constitute the “information highways”, but where does the actual traffic come from and what generates it? This will be discussed in the following paragraphs as we introduce the Cisco Access Router product portfolio.

The access segment is primarily responsible for traffic generation and is synonymous with the branch office location in the network. A typical branch office may house up to 250 employees, supported across multiple IP subnets, with low-end LAN switching equipment and a single WAN connection into the nearest edge/core router with perhaps an ISDN link for back-up. Conversely, the branch office may house only five employees in a small business or it might even be a single Teleworker’s home office. Either way, an access router needs to understand similar routing protocols to those used in the rest of the network, albeit at somewhat lower data rates than its edge/core counterparts.

E1 data rate (i.e. 2.048 Mbps) or a fraction thereof (n x 64 kbps) is generally taken as the average bandwidth pipe for an access router in Europe today. Some organisations may utilise multiple E1s or even an E3 (34 Mbps), but the relatively high cost of leased line bandwidth compared to, say, North American T1 rates (1.544 Mbps) imposes a cost threshold for most access applications.

In addition to its normal routing, LAN and WAN functionality, the physical location of the access router on the periphery of the network means that it must provide a high degree of security capability, both in terms of protection against external attack and also in restricting access between different user groups in the same facility. Other requirements of the access router include the ability to handle a diverse range of traffic types and end-user applications, notably voice, facsimile and perhaps video, in parallel with the normal data flows typical of file transfer, e-mail and Web browsing applications. Quality of Service (QoS) parameters and their enforcement across the network are therefore a key factor in ensuring that the different quality metrics inherent within such traffic mixes are maintained.

From a connectivity standpoint, the access router needs to be extremely versatile in terms of the different WAN interfaces that it supports. These range from E3, E1 and T1 leased lines through ISDN (PRI and BRI rates), ADSL, G.SHDSL and various types of modem dial-up connection over the PSTN. LAN interfaces are nominally 100 Mbps Ethernet with 10 Mbps auto-sensing capability, although some Token Ring environments still exist. Modularity is key in providing flexible routing platforms, which are capable of meeting the diverse physical access requirements of different organisations, large and small alike.

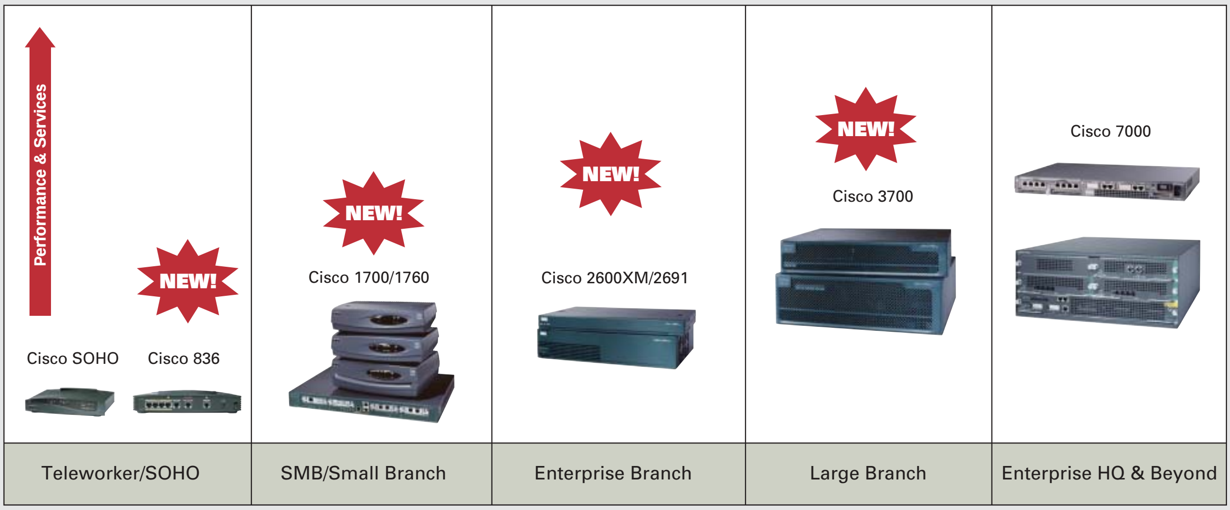
Cisco Systems offers the industry’s broadest and most versatile portfolio of secure, high-performance access routers available today. Used in combination with our edge and core segment routers, these access routers enable the deployment of a wide array of services to the farthest reaches of an organisation, from the home office to the small office to the large Enterprise branch office.

Cisco Access Router Portfolio

Most Industry analysts agree that the access routing marketplace can be segmented into three broad classifications, namely Small Office/ Home Office or SOHO, the Small to Medium Business (SMB) or Low-End and the Enterprise Mid-Range.

The precise definitions of each of these segments in terms of platform performance and number of concurrent users/applications supported is debatable, but within Cisco the terminology is applied across our access router portfolio as follows:

Figure 8-1



SOHO Segment	-	Cisco SOHO 7x/9x and 800 Series routers
Low-End Segment	-	Cisco 1721/1751 and 1760 Series routers
Mid-Range Segment	-	Cisco 2600XM and 3700 Series routers

The relative positioning of these access routers in terms of performance and typical deployment is shown in the above graphic.

What's Important?

In a nutshell – Security, Availability, Quality of Service (QoS) and Management

High Availability

These days, it's hard to distinguish the network from the company. If one stops working, so does the other. That's why networks based on equipment from Cisco Systems offer unsurpassed availability, and, just as importantly, unsurpassed resilience in the face of interruptions.

To maintain productivity – and by extension, profitability – networks must be available all the time, providing employees with global, around-the-clock access to business applications and information, while ensuring appropriate internet access.

And since a network is only as reliable as its weakest link, all segments must be resilient enough to immediately bounce back from unexpected connection, component, or power failures.

To some extent, availability depends on the overall design of the network. In many cases, companies will deploy dual routers with the Hot Standby Routing Protocol that Cisco pioneered, enabling one device to seamlessly take over if the other one fails.

But availability also hinges on the design of the individual routers themselves. That's why Cisco builds layers of redundancy and resiliency into the hardware, from backup processors and power supplies to hot-swappable line cards.

Such safeguards work in tandem with Cisco IOS® Software features, including several recent enhancements collectively known as Globally Resilient IP, or GRIP. Cisco Nonstop Forwarding with Stateful Switchover, for example, enables a router's primary and backup processors to synchronize state information. That way, if a hardware or software problem knocks out the primary processor, the backup processor will pick up where it left off, without needing to reboot the system or line cards, and without losing a single data packet.

And because Cisco IOS® Software runs from the enterprise backbone to the outermost reaches of the WAN, these capabilities can increase the availability of every segment of your network, and increase the productivity of every branch of your company.

Advanced Quality of Service

Imagine a city with wide roads and plenty of lanes, but no traffic lights. Things might flow smoothly enough at 3 a.m., but come rush hour, the resulting free-for-all would inevitably leave some motorists stranded in gridlock.

On the highways and byways of corporate networks, quality of service, or QoS, brings order and control to the bare asphalt of bandwidth. By prioritizing traffic, QoS ensures your most important applications and users get the bandwidth they need. For example, even slight delays in IP voice traffic will impact sound quality. But if an e-mail gets held up for a few seconds, no one will know the difference. So instead of just letting these applications compete for bandwidth, QoS mechanisms step in to direct traffic, waving voice and video packets through while the e-mail momentarily waits behind traffic lights.

By establishing priorities and policies that recognize such distinctions, companies can better meet the needs of all users and applications. The alternative is to blindly throw more bandwidth at every performance problem that comes along, an unrealistic expectation in these tough economic times. QoS tools provided by Cisco Systems allow our customers to meet the business requirement to do more with less.

An intelligent infrastructure based on Cisco switches and routers provides a level of QoS sophistication that is simply unmatched in the industry. To provide true end-to-end QoS, Cisco routers classify and mark both inbound and outbound data packets, inserting tags that tell other network devices how traffic should be handled. As packets move across the network, policing and shaping mechanisms regulate the flow of traffic to ensure policies and priorities are enforced.

At the first sign of bottlenecks, congestion avoidance features take active steps to clear the way for the most vital data. Weighted Random Early Detection, for example, selectively drops packets based on IP precedence to keep high-priority traffic flowing.

At the same time, advanced QoS features lend networks greater flexibility, making it easy to adjust to changing requirements and priorities. So easy, in fact, that policies can shift according to time of day, accommodating different business needs and patterns of network usage.

Integrated Security

These days, it takes a lot more than a firewall to protect corporate networks.

After all, access is rapidly being extended beyond traditional corporate boundaries to branch offices, mobile workers, partners, suppliers, and customers. And that's a good thing, since it allows companies to do business more quickly and efficiently than ever. But it also opens up new risks, both internally and externally.

Cisco integrated security solutions provide the industry's most comprehensive and scalable safeguards, enabling you to protect productivity gains and reduce network operating costs from the head office to the branch office and beyond. It starts with the Cisco SAFE Blueprint, which simplifies all aspects of security design and rollout. Whether you're reinforcing the entire network at once or taking incremental steps, SAFE serves as a guide to best practices in corporate networks, focusing on expected threats and methods of mitigation, rather than specific topologies. It's a flexible, dynamic strategy for implementing multiple layers of defense, so the failure of one system will not be likely to compromise network security overall.

By the same token, the array of security features integrated into Cisco routers gives you the choice of implementing whatever levels of protection measures they need, wherever they need them. Integrated AAA services (Authentication, Authorization, and Accounting), virtual private network services, intrusion detection systems, content filtering, and stateful firewalls are all available to keep data safe as it moves through and between networks – without impacting performance.

In a study released last year, the FBI and the Computer Security Institute surveyed 503 U.S. computer security practitioners in the public and private sectors, and found that 90 percent had detected security breaches within the previous 12 months.

The most commonly reported problems included employee abuses of network resources, system penetration by hackers, and denial-of-service attacks. Any of these issues would be alarming, but together they demonstrate the range of threats companies face today, and show why no single point of defense is enough.

Integrated security is a hallmark of all Cisco products, from the switches and routers that form an intelligent network infrastructure, to Cisco PIX® Firewalls, VPN Concentrators, Intrusion Detection appliances, IP phones, and wireless access points. That level of protection should be reassuring to employees, partners, and customers alike.

Cisco SOHO and 800 Series

The Cisco SOHO and 800 Series broadband access routers make it easy and affordable to extend the power and applications support inherent in Cisco IOS® technology to small businesses, small remote offices and Teleworkers, providing superior security, reliability and flexibility at low cost. These products deliver secure, multi-user access to the Internet or corporate Enterprise LAN through either a single ISDN (BRI), ADSL, G.SHDSL, ADSL-over-ISDN or synchronous serial connection (up to 512 kbps), or via an Ethernet WAN port connected to an external broadband modem. All products employ a lightweight desktop form factor for ease of installation and quiet operation.

The Internet has improved the business performance of all enterprises regardless of their physical size. From awareness to lead generation and from simple Web site browsing through to e-Commerce, the Internet has clearly demonstrated its value worldwide. However, accessing the Internet also opens the LAN to the threat of unauthorized access and the "always-on" DSL/Cable technology increases the risk of attacks from the external world. Today network security has become a real concern to all businesses.

The Cisco SOHO and 800 Series broadband access routers provide easy Internet access while protecting the network against any external threat. The routers offer an all-in-one solution delivering Internet access and fully-fledged integrated security.

- Stateful Inspection Firewall to defend the network against and protect router resources against denial-of-service (DoS) attacks
- High-speed 3DES IPSec encryption for VPN connections
- Immediate security policy change and update throughout the entire VPN network with Cisco's unique Easy VPN solution
- Intrusion detection and prevention of network viruses such as Code Red and Nimda with over 100 different signatures
- URL filtering to prevent illegal access to referenced/classified sites on the Internet

Figure 8-3

Model	WAN	Ethernet	Features	Phone Ports
Traditional WAN Access				
Cisco 801	One ISDN BRI S/T	1-port 10Base-T	Firewall, IPSec VPN, remote management	None
Cisco 803	One ISDN BRI S/T	10Base-T (RJ-45) 4-ports Hub	Firewall, IPSec VPN, remote management	2 RJ-11 Analog phone ports
Cisco 805	One Smart SeriaL port for Synch or Asynch dial	1-port 10Base-T	Firewall, IPSec VPN, remote management	None
SOHO Series				
Cisco SOHO71	Ethernet	4-port 10Mbps Hub	Firewall, remote management	None
Cisco SOHO91	Ethernet	4-port 10/100Mbps Switch	Firewall, IPSec 3DES VPN, remote management	None
Cisco SOHO76	ADSL AnnexB	1-port 10Mbps	Firewall, remote management	None
Cisco SOHO96	ADSL AnnexB	4-port 10/100Mbps Switch	Firewall, IPSec 3DES VPN, remote management	None
Cisco SOHO77	ADSL	4-port 10Mbps Hub	Firewall, remote management	None
Cisco SOHO97	ADSL	4-port 10/100Mbps Switch	Firewall, IPSec 3DES VPN, remote management	None
Cisco SOHO78	G.SHDSL	1-port 10Mbps	Firewall, remote management	None
800 Broadband				
Cisco 806/831	Ethernet	4-port 10Mbps Hub / 4-port 10/100Mbps Switch	Firewall, IPSec VPN, IDS, URL Filtering, IP QoS, remote management	IP Phone
Cisco 826/836	One ADSL AnnexB / + ISDN Backup	1-port 10Base-T / 4-port 10/100Mbps Switch	Firewall, IPSec VPN, IP QoS + IDS, URL Filtering, remote management	None / IP Phone
Cisco 837	One ADSL	4-port 10/100Mbps Switch	Firewall, IPSec VPN, IDS, URL Filtering, ATM QoS, IP QoS, remote management	IP Phone
Cisco 827-4V	One ADSL	1-port 10Base-T	Firewall, IPSec, VPN, ATM QoS, IP QoS, remote management	4 RJ-11 Analog FXS ports
Cisco 828	One G.SHDSL	10Base-T (RJ-45)	Firewall, IPSec VPN, ATM QoS, IP QoS, remote management	None

Cisco SOHO and 800 Series

When to Deploy

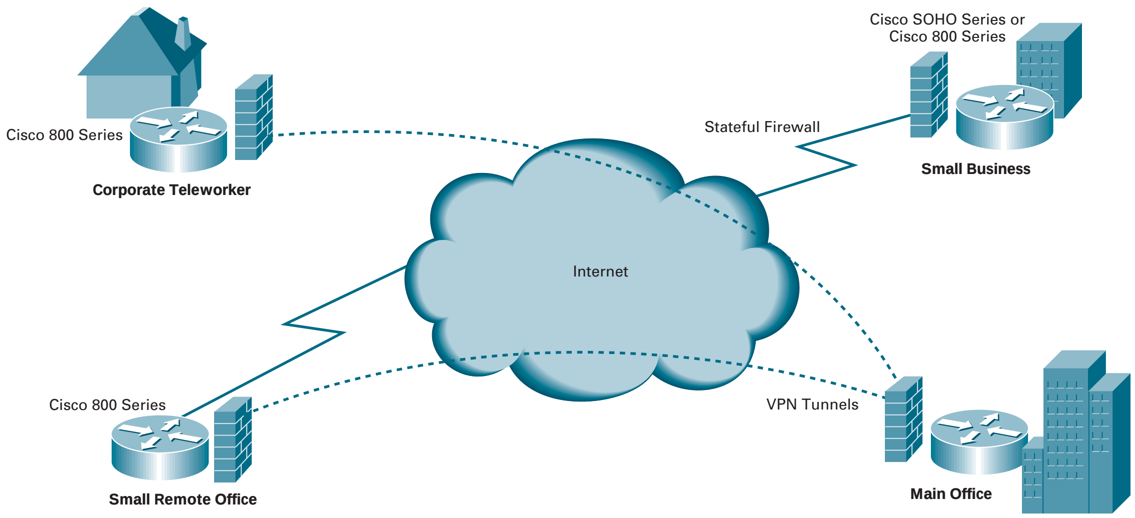
The Cisco SOHO Series is recommended when you need to deploy:

- Small office/home office multi-user access
- Integrated LAN Protection with stateful firewall
- Intranet VPN applications with few users remotely located

The Cisco 800 Series is recommended when you need to deploy:

- Small office/teleworker with multi-user access
- Corporate Intranet application with integrated Firewall and VPN services
- Advanced QoS for bandwidth management and IP voice support
- Remote sites fast deployment
- Comprehensive security and protection

Application Example



Cisco 1700 Series

The Cisco 1700 Series of modular access routers is designed to provide a cost-effective, integrated routing platform for small and medium-sized businesses and Enterprise small offices, ensuring that new services can be deployed efficiently as application needs evolve. These products provide flexibility and manageability through modular design to meet demanding requirements such as comprehensive security (including hardware-based encryption), multiservice data/voice, video/facsimile integration and business class xDSL support.

All products in the 1700 Series utilise a desktop form factor similar to the SOHO/800 Series products, with the exception of the 1760 which has a standard rack-mount enclosure. Interface flexibility is provided through combinations of WAN Interface Card (WIC), Voice Interface Card (VIC) and/or Versatile WIC (VWIC) plug-in modules.

Cisco 1700 Series

Platform Overview

	WICs	VICs	VICs/ WICs	Fixed LAN Ports	DRAM (default MB)	DRAM (max MB)	FLASH (default MB)	FLASH (max MB)	Power Supply
Cisco 1710	-	-	-	1	32	64	16	16	AC
Cisco 1721	2	-	-	1	32	96	16	16	AC
Cisco 1751	-	1	2	1	32	96	16	16	AC
Cisco 1751-V	-	1	2	1	64	96	32	32	AC
Cisco 1760	-	2	2	1	32	96	16	64	AC
Cisco 1760-V	-	2	2	1	64	96	32	64	AC

Many customers who already use the Cisco 1600 Series access routers are now migrating to the 1700 Series for increased modularity and support of concurrent data/voice applications. The graphic on the following page provides a summary of the available migration options.

Figure 8-6

Cisco 1600

Cisco Prod No.	Description
CISCO1601-R	**Cisco 1601-R Router** (One serial sync/async WAN)
CISCO1602-R	**Cisco 1602-R Router** (One serial WAN with 56K DSU/CSU)
CISCO1603-R	**Cisco 1603-R ISDN Router** (One ISDN BRI WAN)
CISCO1604-R	**Cisco 1604-R ISDN Router (NT1)** (One ISDN BRI WAN with NT1)
CISCO1605-R	**Cisco 1605-R Router** (Two port 10-BASE-T Ethernet LAN and one modular WAN slot)

No comparable Cisco 1600

Cisco 1721 (data)

Cisco Prod No.	Description
CISCO1721 WIC-1T=	**Cisco 1721 Access Router Base Model** Serial sync/async WAN interface card
CISCO1721 WIC-1DSU-56K4=	**Cisco 1721 Access Router Base Model** 1-port 4-wire 56/64K DSU/CSU WAN interface
CISCO1721 WIC-1B-S/T=	**Cisco 1721 Access Router Base Model** 1-port ISDN BRI WAN interface card
CISCO1721 WIC-1B-U=	**Cisco 1721 Access Router Base Model** 1-port ISDN BRI WAN interface card with NT1
CISCO1721 WIC-1B-U=	**Cisco 1721 Access Router Base Model** 1-port Ethernet interface card
CISCO1721-VPN/K9	Cisco 1721 with VPN encryption module. 48MB DRAM, Cisco IOS IP Plus/3DES/FW
CISCO1721-ADSL	Cisco 1721 with ADSL WIC (WIC-1ADSL)
CISCO1721-SHDSL	Cisco 1721 with G.SHDSL WIC (WIC-1SHDSL)
CISCO1721-VPN/K9-A	Cisco 1721 with VPN encryption module with ADSL WIC, 48MB DRAM, IP Plus/FW/3DES

Cisco 1760 (data + voice)

Cisco Prod No.	Description
CISCO1760 WIC-1T=	**Cisco 1760 Access Router Base Model** Serial sync/async WAN interface card
CISCO1760 WIC-1DSU-56K4=	**Cisco 1760 Access Router Base Model** 1-port 4-wire 56/64K DSU/CSU WAN interface
CISCO1760 WIC-1B-S/T=	**Cisco 1760 Access Router Base Model** 1-port ISDN BRI WAN interface card
CISCO1760 WIC-1B-U=	**Cisco 1760 Access Router Base Model** 1-port ISDN BRI WAN interface card with NT1
CISCO1760 WIC-1B-U=	**Cisco 1760 Access Router Base Model** 1-port Ethernet interface card
CISCO1760-VPN/K9	Cisco 1760 with VPN encryption module. 48MB DRAM, Cisco IOS IP Plus/3DES/FW
CISCO1760-ADSL	Cisco 1760 with ADSL WIC (WIC-1ADSL)
CISCO1760-SHDSL	Cisco 1760 with G.SHDSL WIC (WIC-1SHDSL)
CISCO1760-VPN/K9-A	Cisco 1760 with VPN encryption module with ADSL WIC, 48MB DRAM, IP Plus/FW/3DES

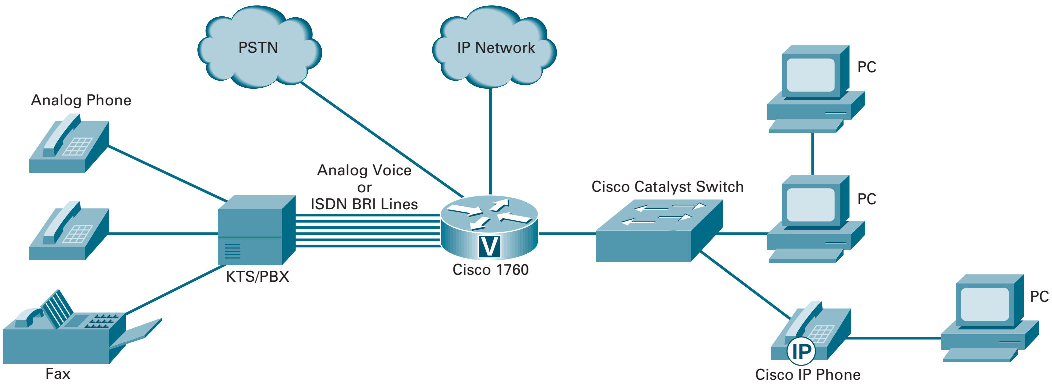
Cisco 1700 Series

When to Deploy

The Cisco 1700 Series is ideal for customers who need:

- The flexibility to add or change WAN services to support changing needs and applications, including VPNs, integrated voice/fax/data over the WAN, broadband DSL and cable access services
- An integrated access solution that combines a best-in-class router with firewall, high-speed encryption, VPN tunnel server, DSU/CSU, and ISDN NT-1 functions in one platform
- VPN remote aggregation to terminate VPN software clients at the branch office
- High-speed business-class DSL connectivity on a secure, high-performance modular platform
- A secure access solution with VPN (T1/E1 speeds) and firewall for enterprise small branch offices and small to medium-sized businesses
- Multiservice voice/video/fax/data integration
- Up to five serial interfaces (including the AUX port);
  for example: retail/point-of-sale or small bank branch office applications

Application Example



Cisco 2600XM Series Modular Access Routers

Cisco extends Enterprise-class versatility, integration and power to branch offices with the Cisco 2600XM Series of modular access routers. With >1.5 million 2600 Series units installed worldwide to date, this popular series of products offers network managers and service providers considerable flexibility and investment protection in a compact, single-box solution. The Cisco 2600XM models and high-end Cisco 2691 platform are the latest additions to the 2600 Series family, providing even more flexibility, performance and memory, as well as higher service densities to support present and future branch office requirements.

All 2600 Series access routers employ a standard rack mount construction and standard 1RU height, with the exception of the Cisco 2691 which has 2RU height. The modularity concept of the 2600 series is identical to that of the 1700 series in that all WICs, VICs and VWICs are readily interchangeable cross platforms, meaning increased investment protection for evolving WAN and service needs, reduced sparing costs, and the ability to standardise a network on one platform regardless of access medium.

In addition, the 2600XM series utilises a larger form factor Network Module (NM) to achieve higher density services. There is provision for internal daughter cards or AIMs (Advanced Integration Modules) to support CPU offload functions such as encryption, data compression, voice coding and ATM SAR, thus maintaining routing performance despite the activation of value added services.

This level of modularity and flexibility allows Enterprises and Service Providers such additional options as integrated 10/100 LAN switching, dual Fast Ethernet (FE) ports on the chassis for the separation of public and private LAN domains, integrated content delivery, high density digital and analog voice options, and high density serial port density for terminal services.

Figure 8-8

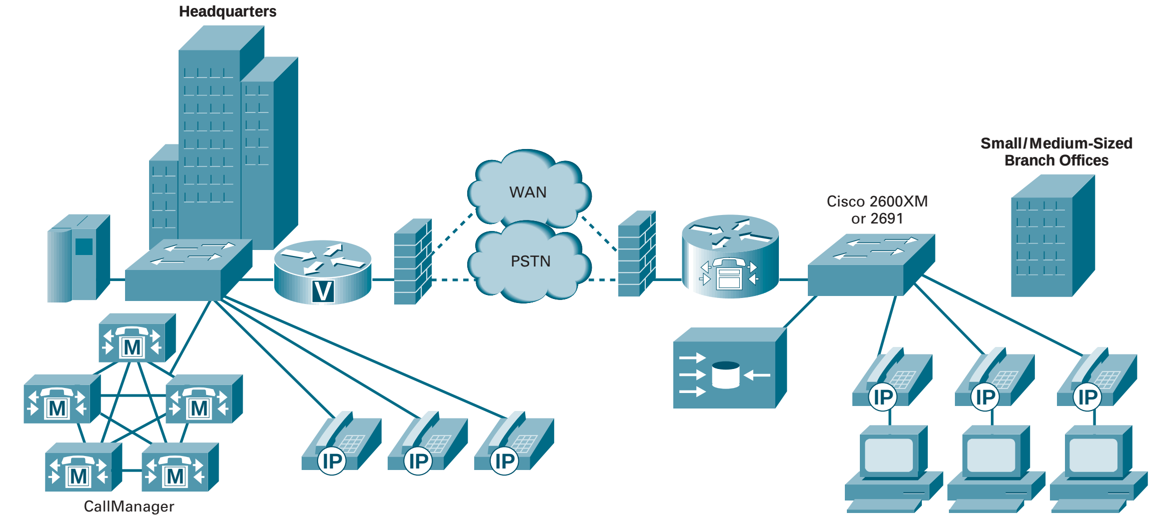
Platform Overview

	NMs	AIM	WICs	Fixed LAN Ports	Performance (Kpps)	DRAM (MB)		Flash (MB)		Power Supply
						default	max	default	max	
Cisco 2610XM / 2611XM	1	1	2	1 / 2 FE	20	32	128	16	48	AC, DC, RPS
Cisco 2612	1	1	2	1TR, 1E	15	32	64	8	16	AC, DC, RPS
Cisco 2620XM / 2621XM	1	1	2	1 / 2 FE	30	32	128	16	48	AC, DC, RPS
Cisco 2650XM / 2651XM	1	1	2	1 / 2 FE	40	64	128	16	48	AC, DC, RPS
Cisco 2691	1	2	3	2 FE	70	64	256	*32	*128	AC

* Compact Flash

Cisco 2600XM Series

Application Example



Options

- Voice-enabled routers
- VPN-enabled routers
- Integrated stateful firewall
- WCCP for content networking
- Dial access
- Integrated low-density switches

Sometimes the customer application may be implemented using products from either the 1700 Series or the 2600XM Series. This is particularly true for low-end rack-mount requirements where the Cisco 1760 and 2610XM routers offer comparable functionality and modularity at the WIC/VIC level. Use the following graphic as a guide in deciding which option to use.

Cisco 2600XM Series

When to Deploy

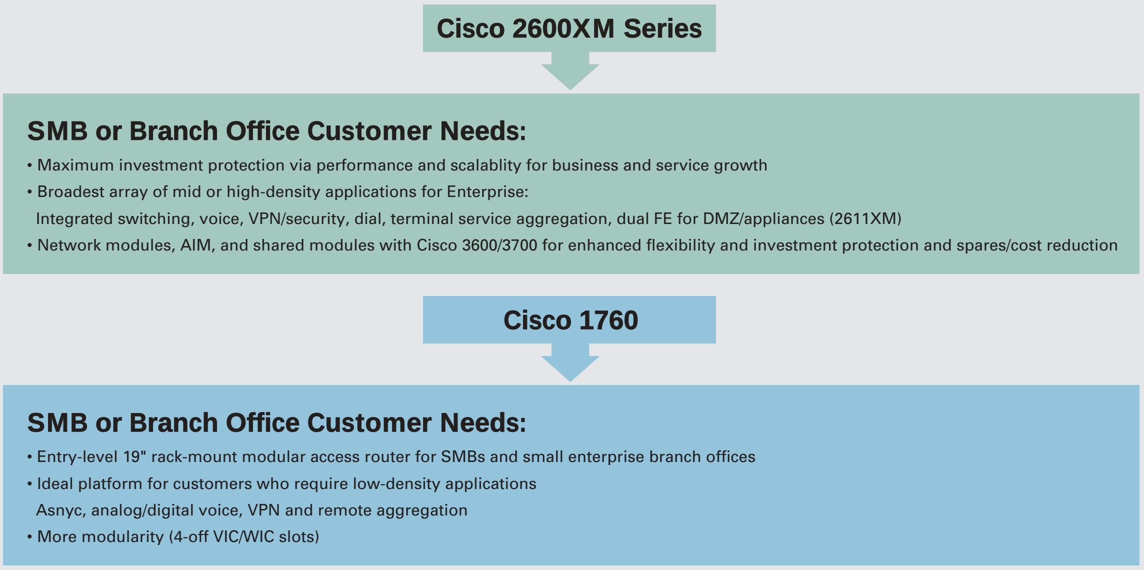
Deploy the Cisco 2600XM Series when you need:

- A cost-effective solution for the long term that adapts to evolving network requirements
- Virtual private network (VPN) extranet access with firewall protection to reduce costs and increase security for partners and employeees
- Dial concentration with async, ISDN, or analog modems
- Integrated routing and switching functionality
- Voice/fax/data multiservice integration
- Serial device concentration of point-of-sale devices, ATMs, alarm systems, SDLC controllers with legacy terminals and LAN devices sharing a single WAN connection
- High-speed business-class DSL connectivity on a secure, high-performance modular platform
- Support for advanced QoS features such as the Resource Reservation Protocol (RSVP), Weighted Fair Queuing (WFQ), and IP Precedence to reduce recurring WAN costs

Transition Information

The new Cisco 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, and 2651XM routers should be deployed in scenarios that previously called for Cisco 2610, 2611, 2620, 2621, 2650, and 2651 routers, respectively. The new XM models offer improved performance and increased default memory and maximum memory at no additional cost.

Figure 8-11



Cisco 2600XM Series

SMB or Branch Office Customer Needs:

- Maximum investment protection via performance and scalablity for business and service growth
- Broadest array of mid or high-density applications for Enterprise:
  Integrated switching, voice, VPN/security, dial, terminal service aggregation, dual FE for DMZ/appliances (2611XM)
- Network modules, AIM, and shared modules with Cisco 3600/3700 for enhanced flexibility and investment protection and spares/cost reduction

Cisco 1760

SMB or Branch Office Customer Needs:

- Entry-level 19" rack-mount modular access router for SMBs and small enterprise branch offices
- Ideal platform for customers who require low-density applications
  Asnyc, analog/digital voice, VPN and remote aggregation
- More modularity (4-off VIC/WIC slots)

Cisco 3700 Series Modular Access Routers

The Cisco 3700 Series Multiservice Access Routers are a new family of modular routers that enable flexible and scalable deployment of e-Business applications in an integrated branch office access platform. These routers are also ideally positioned to satisfy the needs of those customers who already use the widely-deployed and successful Cisco 3600 Series router product family. For customers planning to migrate services from legacy infrastructure and to distribute new applications from the core to the edge of the enterprise, the Cisco 3700 Series accelerates customers' cost reduction benefits of e-Business applications, reduces total cost of ownership of branch office infrastructure and improves competitive leverage of the network.

The Cisco 3700 Series routers are equipped with two on-board Fast Ethernet (FE) interfaces, three WAN Interface Card (WIC slots) and two Advanced Integration Module (AIM) slots, in conjunction with two or four network module (NM) slots. The Cisco 3725 features dual NM slots, one of which can accommodate a double-width High Density Service Module (HDSM) slots. There are four NM slots on the Cisco 3745 and these can be configured to take two HDSMs according to the particular customer's modularity requirements.

The Cisco 3700 Series platforms also include optional -48V DC integrated inline power, internal redundant AC or DC Power options and hot-swap Online Insertion and Removal (OIR) capabilities for like network modules (Cisco 3745).

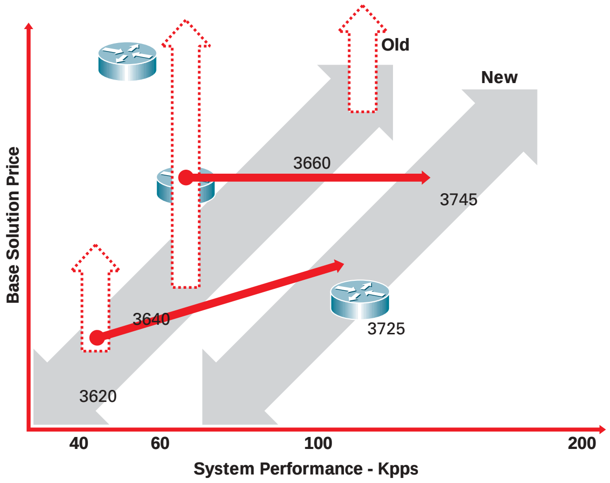
Cisco 3700 Series

Platform Overview

Platform	NMs	AIM	WICs	Fixed LAN Ports	Performance (Kpps)	DRAM (MB)		Flash (MB)		Power Supply
						default	max	default	max	
Cisco 3725	2	2	3	2 FE	100	128	256	32	128	AC, RPS
Cisco 3745	4	2	3	2 FE	225	128	256	32	128	AC, DC, RPS

The Cisco 3700 Series routers can represent the natural evolution of the Cisco 3600 Series by providing nearly full feature parity but most of all providing the performances and densities to take advantage of new cost saving and productivity enhancing applications.

Figure 8-13 Cisco 3600 to 3700 Transition Value



When to Deploy

Deploy the Cisco 3700 Series when you need:

- New levels of branch office service density in a compact form factor
- Integrated flexible routing and low-density switching (16- or 36-ports)
- Flexible, incremental, and scalable migration to a converged branch office network
- Compatibility with more than 90% of the world's legacy analog and digital TDM PBXs
- Survivable Remote Site Telephony (SRST) features that enable branch offices to leverage centralized call processing while providing local branch IP Telephony redundancy
- Support for advanced quality of service (QoS), bandwidth optimization, and data fragmentation, as well as voice call admission control, call control, and queuing mechanisms, without sacrificing the expected data performance needed for future growth
- Available features such as redundant power, online insertion and removal components, and field replaceable components

Cisco 3640 to 3725

The Cisco 3725 represents a compelling solution pricing for integrated services configurations.

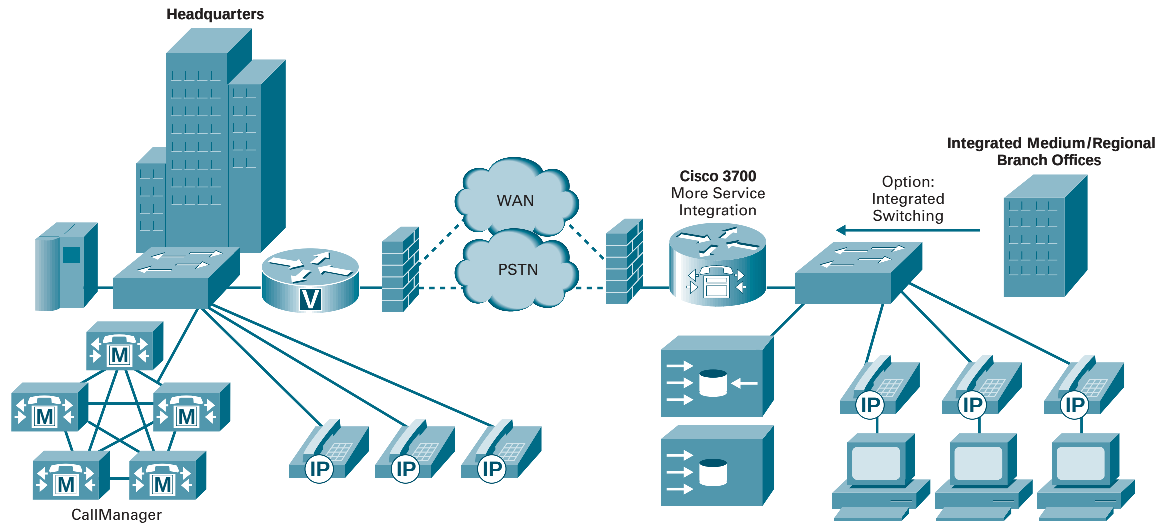
It offers 2 – 3 times the performance and interface density and at the same time 2 – 4 times default and maximum memory configurations.

Cisco 3640 to 3745

Migrating from Cisco 3640 to Cisco 3745 allows customers to enjoy the benefits of higher services integration. Multiple applications can run concurrently on the same router (Firewall/VPN, Routing, Voice etc.) thus limiting the need for external individual appliances, hence driving down the overall system maintenance and management costs. The Cisco 3745 offers 4-fold performance increase over the Cisco 3640, in addition to the higher memory capability cited for the Cisco 3725.

Cisco 3700 Series

Application Example



Options

- Voice-enabled routers
- VPN-enabled routers
- Integrated stateful firewall
- WCCP for content networking
- Dial access
- Integrated low-density switches

So Why Deploy Access Routers from Cisco?

Five main reasons to guarantee solution flexibility and rapid return on investment (ROI):

Modularity

Many routers offer only a fixed configuration platform with no expansion capability to support enhanced software feature sets or new technologies such as voice, xDSL, Security, IP telephony, Content, etc.

Cisco 1700, 2600XM and 3700 Series Access Routers offer fully modular chasses, significantly better performance and security, and a diverse range of hardware expansion capabilities to support additional LAN/WAN interfaces, integrated 10/100 Mbps LAN switching, voice gateway and IP telephony applications.

The Cisco 3725 and 3745 routers provide high-performance mid-range platforms which utilise the same common expansion capabilities as the 2600XM range but with the added benefit of OIR (Online Insertion/Removal) to minimise router downtime.

The default memory capacities of these Access Routers allow support for the latest Cisco IOS® software feature sets and the ability to hold multiple images in system Flash memory.

Advanced Quality of Service (QoS)

Allows a customer to allocate levels of “priority” to their network traffic so that business critical applications receive the best performance. These “QoS” features are enabled through Cisco IOS® and they allow bandwidth to be assigned across applications to avoid bottlenecks, minimise latency (crucial for multiservice data/voice) and improve end-to-end system response.

All of the Cisco 800, Cisco 1760, Cisco 2600XM, Cisco 2691 and Cisco 3700 Series routers support an extensive range of QoS features through Cisco IOS®.

Enhanced Security

Protects data across the network and from all unauthorised devices by including optional Firewall, Intrusion detection, and VPN (Virtual Private Network) Services.

Mitigates concerns with advanced authentication and filtering features, which forward or drop packets based on source/destination or application.

Support for IPSec is a key requirement when implementing any VPN (Virtual Private Network) security solution and this is a key feature of the advanced Cisco IOS® images available for all Cisco Access Router platforms.

All Cisco 800, 1700, 2600XM and 3700 series platforms offer encryption service options in hardware, which enables wire-speed encryption across the WAN. SOHO routers utilise software-based encryption for cost-effective deployment where throughput requirements are less than 384 kbps.

Flexibility

A modular access router provides the flexibility to add applications and new functions when required. For example, customers are able to:

- Upgrade WAN Access Services (e.g. ISDN to DSL, etc) to take advantage of changing WAN pricing and services offered by their local service provider(s)
- Add security and firewall protection,
- Add multiservice voice and a host of other services

All using the same base platform and avoiding the need for a forklift upgrade.

The inherent flexibility of the Cisco 1700, 2600XM and 3700 series Access Routers ensures that any network expansion or new technology can be implemented in a phased approach ... on your customer’s timescales and project budget!

IOS Telephony Services (ITS)

ITS is embedded into Cisco IOS® and integrates traditional Key System and Hybrid PBX-like features onto Cisco’s Access Routers. With ITS features we can cost-effectively address the under-48-station voice and data market on a single router platform. Turn your router’s latent power into an IP-based telephony solution ... today!

ITS is available as a simple Cisco IOS® software upgrade for all access routers in the range Cisco 1751 to 3745.

CISCO SYSTEMS

EMPOWERING THE
INTERNET GENERATION

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Tel: +1 408 526 4000
+1 800 553 NETS (6387)
Fax: +1 408 526 4100

European Headquarters
Cisco Systems Europe s.a.r.l.
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France

Tel: +33 1 58 04 60 00
Fax: +33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Tel: +1 408 526 7660
Fax: +1 408 527 0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 9, 80 Pacific Highway
P.O. Box 469
North Sydney
NSW 2060 Australia

Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia
Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe