



CISCO 7600 INTERNET ROUTER SOLUTIONS OVER SECURE DOD INFRASTRUCTURES

CISCO NETWORK SOLUTIONS OVER GENERAL DYNAMICS DOD/NSA CERTIFIED TYPE I ENCRYPTION TECHNOLOGIES

EXECUTIVE SUMMARY

The move by service provider, enterprise, and federal customers to migrate from existing ATM and time-division multiplexing (TDM) infrastructures to an IP-based backbone has been under way for some time now. In the Department of Defense (DoD), where backbone transports require Type I encryption levels of security, these “legacy” transport mechanisms (that is, ATM) continue to thrive because of their speed and familiarity within the DoD. In fact, ATM Type I encryption continues to be the fastest and most robust of the current Type I encryption technologies for high-speed backbone transports, and is still the most popular “service” that is offered by organizations responsible for providing transport services within the DoD.

INTRODUCTION

To meet the NSA Type I security demands by DoD customers, Cisco Systems® provides solutions that allow high-speed IP applications and services to be transported over various National Security Agency (NSA) Certified Type I encryption solutions, allowing secure DoD customers the same advantages of robust IP applications and services over secure DoD infrastructures. Secure IP backbone infrastructures within the DoD can now be built in line with the Type I encryption technology using OC-48 ATM router interfaces along with line-rate feature and service capabilities such as quality of service (QoS), Multiprotocol Label Switching (MPLS), and policing and shaping that allow high-speed service offerings without performance impact. For solutions requiring IP Type I encryption at Gigabit Ethernet rates and above, Cisco® offers high-speed solutions over generic routing encapsulation (GRE) tunnels, including unicast, multicast, Layer 3 VPNs (RFC 2547), Multicast VPN (MVPN), and IPv6.

This document provides an overview of the following:

- Type I encryption overview, which details:
 - Type I encryption
 - Current Type I encryption technologies most used
 - Techniques and network features required for building service-capable IP backbones over Type I encryption technologies (link and network encryptors)
- Cisco solutions that provide the required functions in a DoD/NSA Certified high-speed Type I environment for ATM, IP, and SONET, including:
 - Details and Cisco IOS® Software configuration example on demonstrated interoperability and functions between the General Dynamics OC-48 ATM Type I encryptor (KG-75) and the Cisco 7604 using OC-48 ATM Internet Flexibility (I-Flex) technology
 - Details and Cisco IOS Software configuration example on demonstrated interoperability and functions between the General Dynamics Gigabit Ethernet IP Type I encryptor (KG-175A) and the Cisco 7604 using the 2-port Gigabit Ethernet I-Flex technology

TYPE I ENCRYPTION OVERVIEW

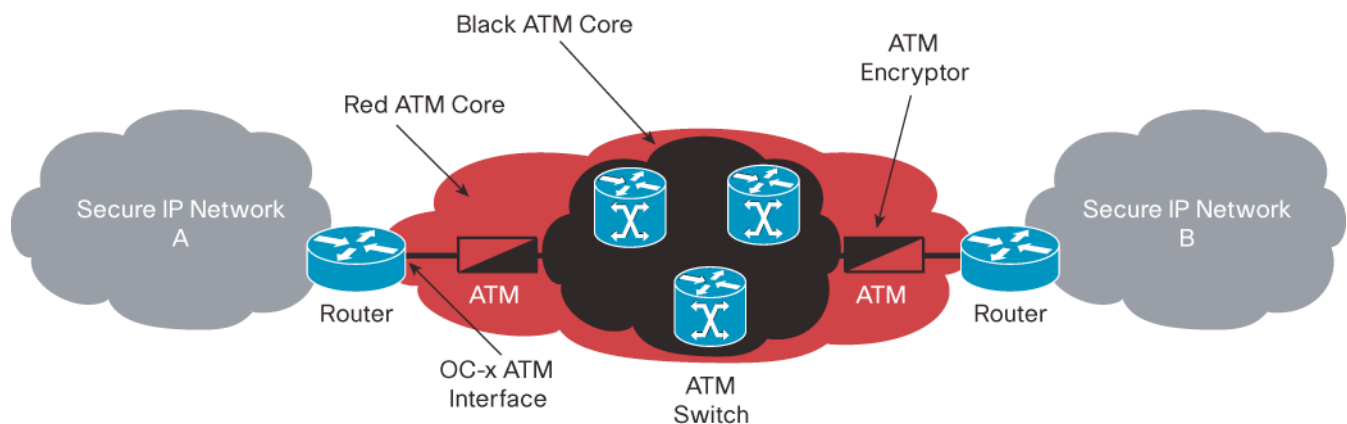
NSA is responsible for all U.S. Government encryption systems. Specifically, “One mission of the Agency is designing cipher systems that will protect the integrity of U.S. information systems.”^[1] Type I encryption/encryptors are specifically used for protecting classified information—and of course little information is known about the algorithms used. Various solutions support Type I encryption, including, IP, ATM, SONET, and Serial, to name a few. Type I encryption environments use a concept in referring to the encrypted or unencrypted networks as “red” and “black,” respectively. The “red” network indicates the network is in a secure facility and the data is not encrypted (commonly referred to as the “plaintext” interface), and the “black” network is the side of the network that carries the post-encrypted data (commonly referred to as the “cipher-text” interface). This is an important concept to understand when referring to the network topology and how it relates to the Type I encryption technologies being used. (Refer to Figure 1, 2, or 3 to view the red and black concept.)

Link-Layer Encryption Implementation

Although IP Type I encryption continues to evolve and becomes more accepted in the DoD, link-layer encryption (specifically ATM for high-speed requirements) still provides several advantages over IP Type I, and it remains a viable solution moving forward for building high-speed IP Core transports that require Type I encryption.

Although ATM and SONET are known more for transport technologies and operate at Layer 2 (versus Layer 3 for IP), each already has open standard methods for transporting IP over the specific technology. DoD customers looking to implement an IP-based core and offering any variation of IP Services have the capabilities to accomplish this today, without the need for an immediate overhaul of the existing transport network.

Figure 1. IP Transport over ATM Encryption



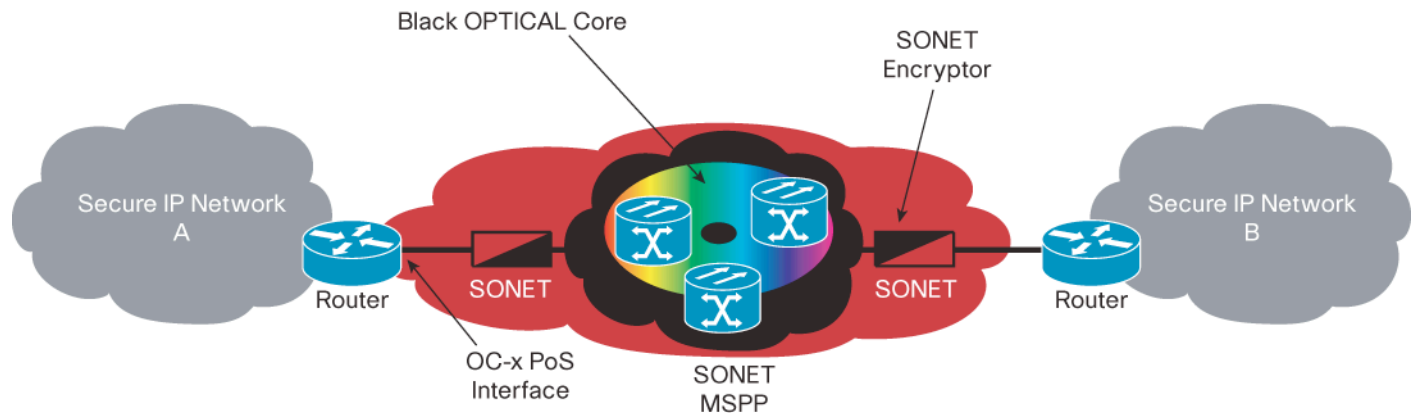
The red router in Figure 1 is directly attached to the ATM encryptor, and MPLS/IP can be enabled on the routers that are attached to the ATM core.^[2] IP over ATM (RFC 1483) permanent virtual circuits (PVCs), permits the transfer of IP packets transparently over the ATM network in an overlay type model. In this case, ATM is the transport mechanism and the ATM encryptor provides the necessary Type I encryption at Layer 2. This solution provides several advantages in IP backbones. First, because the encryption is performed on the ATM cell, certain IP mechanisms such as the IP QoS field (using IP Precedence or differentiated services code point [DSCP] bits) and MPLS labels (the label is sent in the ATM Adaption Layer 5 [AAL5] Subnetwork Access Protocol [SNAP] header) can be used, and they are transparent to the underlying ATM transport. Second, this solution eliminates the need for any complex tunneling techniques that are required over certain Layer 3 encryption devices.

^[1] <http://www.nsa.gov/about/index.cfm>

^[2] The router can also be front-ended with an ATM switch, which then connects to the ATM encryptor.

The same concept holds true for SONET (refer to Figure 2). SONET technology can also support an IP Core infrastructure offering IP Services, without the need for an immediate change in the transport layer and transport encryption solution.

Figure 2. IP Transport over SONET Encryption



Like IP over ATM, IP can use packet over SONET/SDH (POS) technology to support the transport of IP packets over SONET/SDH as well as support the IP QoS field (that is, type of service [ToS]/DSCP) and MPLS labels transparently over the SONET encryptors (the MPLS label for SONET is carried in the POS header as an Ether-type field, and is, therefore, transported transparently over the SONET KG).^[3] Although POS interfaces do not support subinterface capabilities, they do support channelization capabilities that allow the configuration of “logical” interfaces (and customers) over a single physical interface. This method can provide flexible configurations when connecting to SONET KGs. Current OC-12 SONET encryptors (the KG-189 is one example of a SONET encryptor) support STS grooming on increments of STS-1c, -3c, and -12c, so channelization can be accomplished on Channelized OC (that is, CHOC) POS interfaces at any of these STS increments, allowing multiple virtual interfaces out of a single physical POS interface. This simplifies implementation and reduces cost of router and Multiservice Provisioning Platform (MSPP) interfaces, and also reduces the number of encryptors required to manage, thus minimizing overall operation and management complexities.

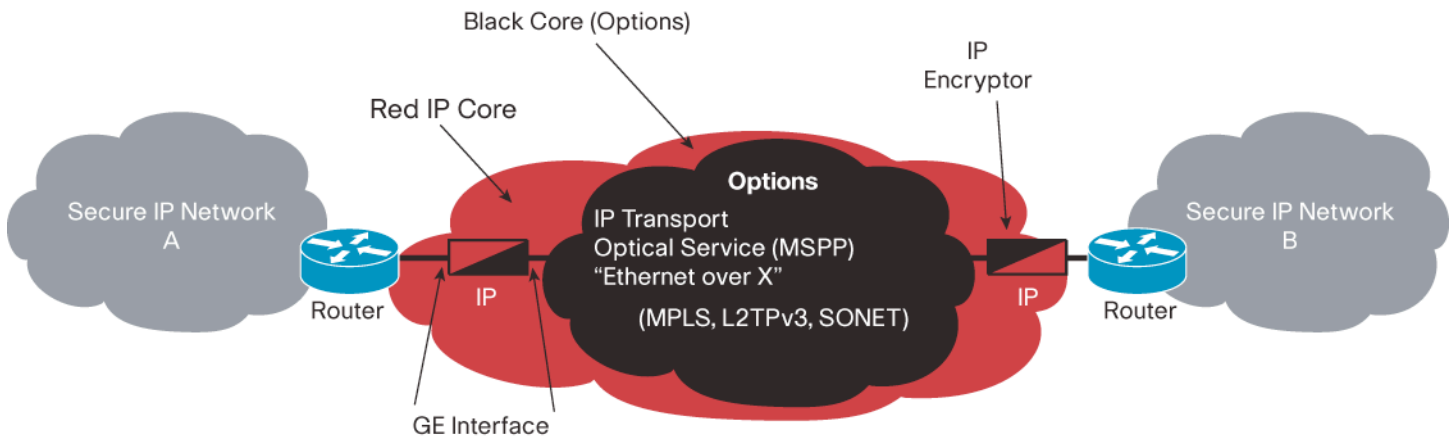
SONET/POS is most impressive in that it supports interface speeds up to OC-768 if encryption speeds move toward those levels of performance. (OC-768 was demonstrated by Cisco at the Cisco CRS-1 Carrier Routing System launch, which used OC-768 from San Francisco to San Jose.)

Network Layer Encryption

Network layer or IP encryption has seen a significant increase in overall interest within DoD, and because most organizations are in the process of moving all their applications over to IP, the move seems very logical. As seen in Figure 3, there are many options for “black” network transport when using IP encryptors, some of which are IP routers, MSPPs that support Ethernet over SONET/RPR, variations of Metro Ethernet services, or any technology that support Gigabit Ethernet transport (because the IP encryptors support Gigabit Ethernet on both the red and black side interfaces).

^[3] RFC 1619/2615, Point-to-Point Protocol (PPP) over SONET/SDH; RFC 1662, PPP in High-Level Data Link Control (HDLC)-like framing; and RFC 2615, PPP over SONET/SDH

Figure 3. IP Transport over IP Encryption (For Example, KG-175A)



With all these advantages, the transition toward IP encryption seems obvious; however, building networks with IP Type I technology does not come without its own set of challenges and limitations as it relates to transporting new IP applications and backbone services.

The current IP Type I technology is limited in its support of several network features that are critical in building an IP Services-capable core that can offer multiservice transport service (such as MPLS, QoS, and IP Multicast) over an IP backbone and reroute around network failures dynamically (such as support for standard routing protocol functions). Currently, the only way to avoid these limitations and enable IP core and edge functions that can support one or all listed features is to deploy some form of tunneling technique, most notably GRE tunnels on the red edge routers between provider edge routers.^[4]

GRE tunnels allow the transport of IP Services features through IP network encryptors. In its most generic form (and as stated in RFC 2784), GRE allows the transport of a “payload” packet (the packet needing to be encapsulated and delivered) that is then encapsulated in some other “outer” protocol (IP in this case), which is the delivery protocol, and that can then be routed between each end of the tunnel (two routers). The use of GRE allows the “IP Service” packets to be encapsulated inside the GRE packets (which are IP) and forwarded to the destination router, allowing the protocols to be “transparent” to the IP KG. Thus the GRE tunnel overcomes the IP encryptors limitation in understanding the various IP services, but also adds additional complexity that does not exist when using IP over ATM and SONET transports, such as:

- GRE reintroduces the “overlay” model that is normally overcome by Layer 3 when routing over a Layer 3 transport.
- It creates maximum transmission unit (MTU) concerns, because the GRE tunnel encapsulation adds overhead to the already header-heavy IP headers.
- Complexity increases greatly for network operators, both in configurations and troubleshooting.

Although a multisite IP Core can be built with IP Type I encryptors, it is vitally important to exercise best practices. Caution needs to be taken to ensure the network scales properly; the routers must be able to handle the tunnel overhead and increased control plane layers; and all required applications must be able to exist in a tunnel environment (for example, IP fragmentation can exist and the hosts can react). Each of these problems can be overcome if the proper attention is given to the details, overall planning, and architecture.

^[4] Layer 2 Tunneling Protocol Version 3 (L2TPv3) is another tunneling option that can function over the IP encryption units (see: http://www.cisco.com/warp/public/cc/so/neso/vpn/unvpnst/l2tpv_wp.pdf)

CISCO SOLUTIONS OVER HIGH-SPEED TYPE I ENCRYPTION (OC-12 RATES AND ABOVE)

Cisco offers multiple high-speed routing solutions for customers that require Type I encryption in their core networks. This provides the capabilities for customers to deploy IP service-based solutions that include a wide range of IP transport mechanisms and applications, in areas where the Type I encryption is mandated without denying these customers the advantages of building high-speed IP network infrastructures that are capable of supporting IP Services such as MPLS, QoS, and IPv6, as well as support IP applications such as voice over IP (VoIP), video and multicast applications, e-learning, and others.

High-Speed IP Solutions over ATM Type I

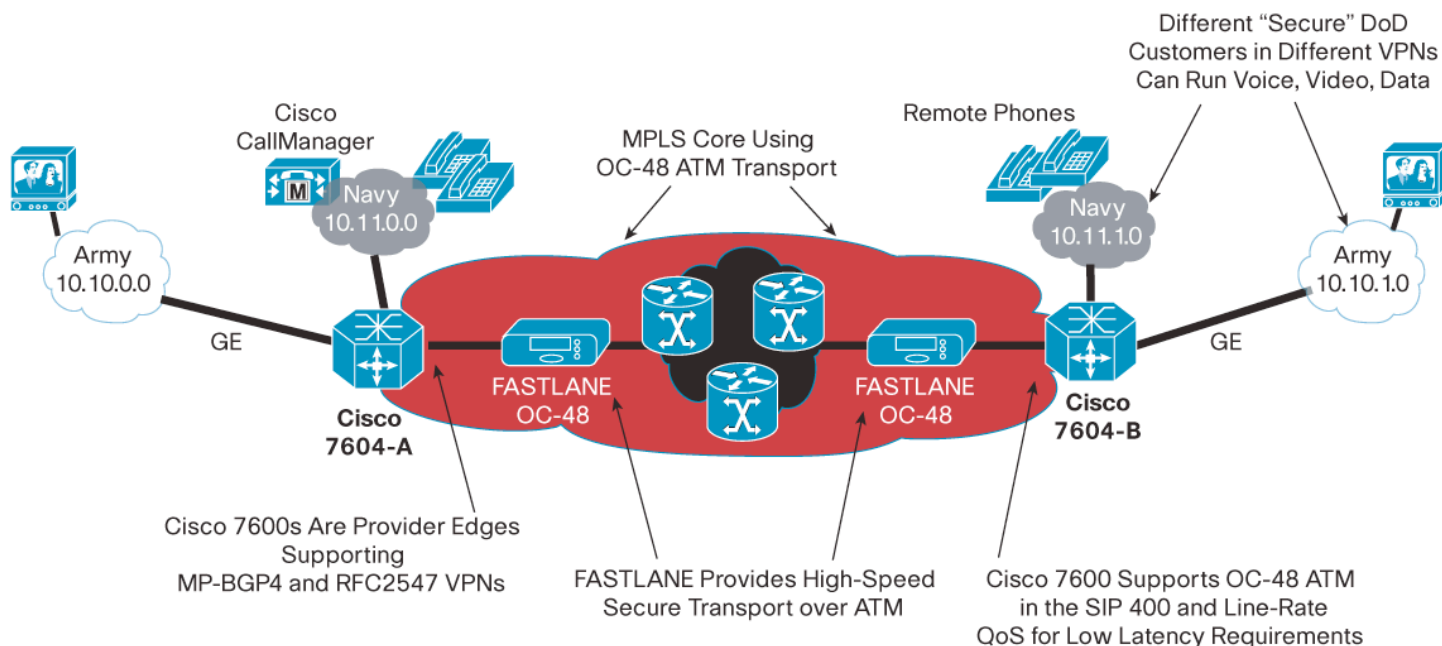
Although IP Type I encryption continues to evolve and is becoming more accepted in the DoD, link-layer encryption (specifically ATM and SONET for high-speed requirements) still provides several advantages over IP Type I, and it remains a viable solution moving forward for building high-speed IP Core transports that require Type I encryption.

Although ATM and SONET are known more for transport technologies and operate at Layer 2 (versus Layer 3 for IP), each already has open standard methods for transporting IP (and IP Services such as IP Multicast, MPLS, and QoS) over each specific technology. Secure DoD customers looking to implement an IP-based core and offering any variation of IP Services have the capabilities to accomplish this today, without the need for an immediate overhaul of the existing transport network.

OC-48 ATM Demonstration Using Cisco 7604 SIP 400 and General Dynamics KG-75 ATM Encryptors

The Cisco 7600 OC-48 ATM solution was demonstrated at the General Dynamics Users Conference in Las Vegas, Nevada, in June 2005, using the Cisco 7604 SPA Interface Processor-400 (7604 SIP 400). The demonstration, shown in Figure 4, displayed the support for Layer 3 VPNs (RFC 2547) over the OC-48 ATM interface, all over the KG-75 Type-I ATM encryptor. Voice and video applications were configured within their unique virtual routing and forwarding (VRF) instance, each performing voice calls and video sessions over the OC-48 ATM link. (Note: Additional “best-effort” data traffic was generated to simulate low-priority user data.) Although the applications did not generate high volumes of traffic, Low-Latency Queuing (LLQ) was applied to the interface to properly prioritize the voice and video streams ahead of the best-effort data traffic to assure that the proper delay and jitter requirements of the codecs were met.

Figure 4. MPLS VPNs over OC-48 FASTLANE (KG-75)—Demonstrated at Encryption Show, Las Vegas, Nevada—June 1–2, 2005



Following is a configuration example for the OC-48 ATM interface with MPLS enabled in a point-to-point example.

7604-B

```
!
7604-B#
!
!
mpls label protocol ldp
!
!
interface ATM3/1/0
  no ip address
!
interface ATM3/1/0.50 point-to-point
  ip address 172.16.10.2 255.255.255.0
  tag-switching ip
  pvc 50/50
!
```

Cisco Solutions over ATM Type I Networks

Cisco offers multiple platforms that are capable of supporting ATM speeds from DS-3 up to OC-12. In late 2005, the Cisco 7600 Series platform will introduce support of the OC-48 ATM Shared Port Adaptor (SPA) interface on the Cisco 7600 Series SPA Interface Processor-400 (7600 SIP 400). The OC-48 ATM SPA will augment the currently available OC-3 and OC-12 ATM SPAs.^[5] This will give DoD customers requiring ATM Type I encryption the capabilities of line-rate OC-48 ATM throughput and services (for example, QoS and access control lists [ACLs] with no performance impact) through their OC-48 ATM infrastructure. Because ATM Type I encryptors encrypt data at the ATM-cell level, customers can build high-speed MPLS/IP core infrastructures, fully capable of supporting most MPLS service capabilities and all IP applications available—even those that require low-latency transport such as voice and video over IP. The Cisco 7600 is currently the only platform that will initially support OC-48 ATM, with future router platforms to follow (refer to Table 1).

Table 1. Cisco 7604 System—Supporting OC-48 ATM

Product Description	Product Number
Cisco 7604 Chassis, 4 Slots, 2 Cisco Catalyst 6500 Series/7600 Series Supervisor Engine 720-3BXLs (Part Number 2SUP720-3BXL), and 2 Power Supplies	7604-2SUP720XL-2PS
1-port OC-48/STM-16 ATM SPAs	SPA-1XOC48-ATM
Cisco 7600 Series SPA Interface Processor-400	7600-SIP-400

HIGH-SPEED IP SOLUTIONS OVER IP TYPE I

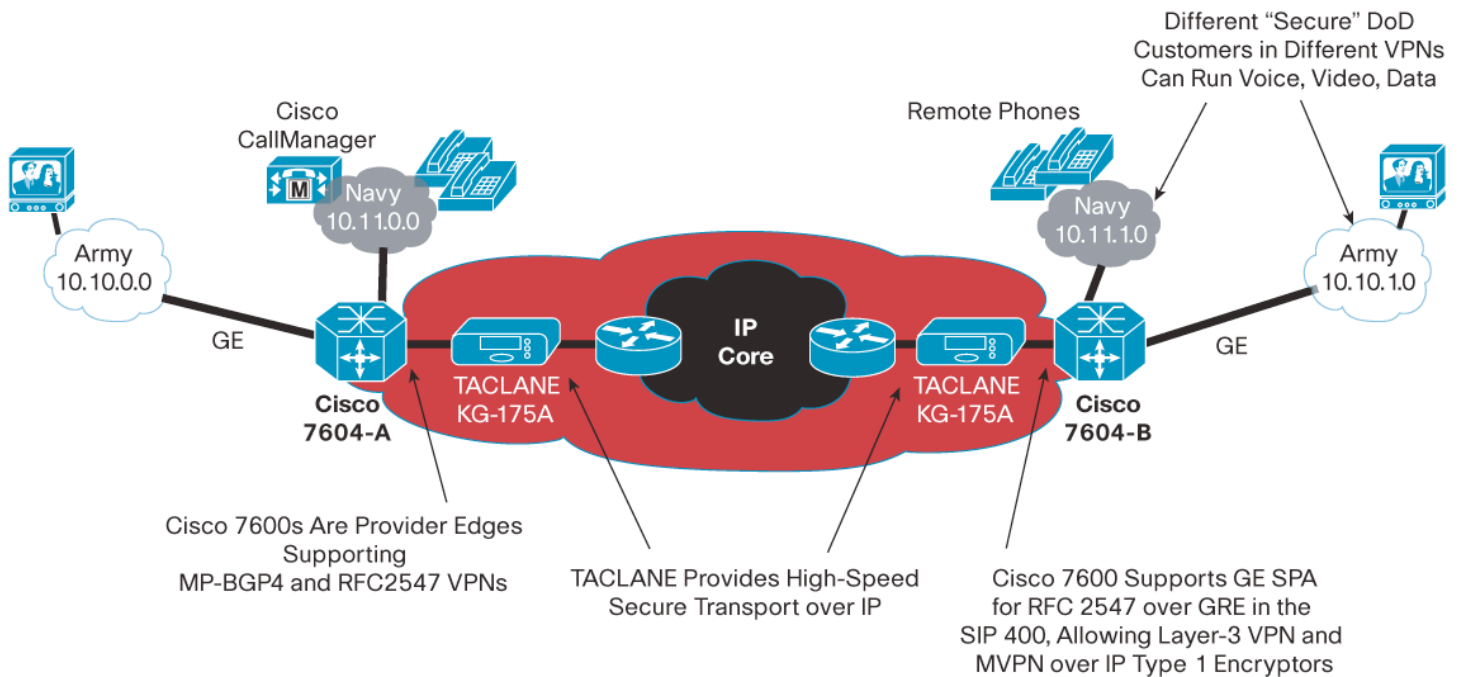
Network layer or IP encryption has seen a drastic increase in overall interest within DoD, and because most organizations are in the process of moving all their applications over to IP, the move seems logical. There are many options for black (that is, the network transport after the data leaves the encryptor), some of which are IP routers, MSPPs that support Ethernet over SONET/Resilient Packet Ring (RPR), variations of Metro Ethernet services, or any technology that supports Gigabit Ethernet transport (because the IP encryptors support Gigabit Ethernet on both the red and black side interfaces).

Layer 3 MPLS VPN Demonstration Using Cisco 7604 SIP 400 and General Dynamics KG-175A Gigabit Ethernet IP Encryptors

The Cisco 7604 Layer 3 MPLS VPN solution over IP Type I encryptors was also demonstrated at the General Dynamics Users Conference. This demonstration, shown in Figure 5, displayed the same support as with the OC-48 ATM demonstration; however, this solution required high-speed GRE tunnel support for Layer 3 VPNs (RFC 2547) so it could function over the KG-175A Gigabit Ethernet IP Type I encryptor. Voice and video applications were configured within their unique VRF instance, each performing voice calls and video sessions over the Gigabit Ethernet encrypted network with the same QoS applied as in the OC-48 ATM demonstration (refer to details in the section “OC-48 ATM Demonstration Using Cisco 7604 SIP 400 and General Dynamics KG-75 ATM Encryptors”).

^[5] Cisco offers many different types of SPA interfaces. Refer to the following URL for more information about the various SPA solutions:
http://www.cisco.com/en/US/products/ps6267/prod_module_series_home.html

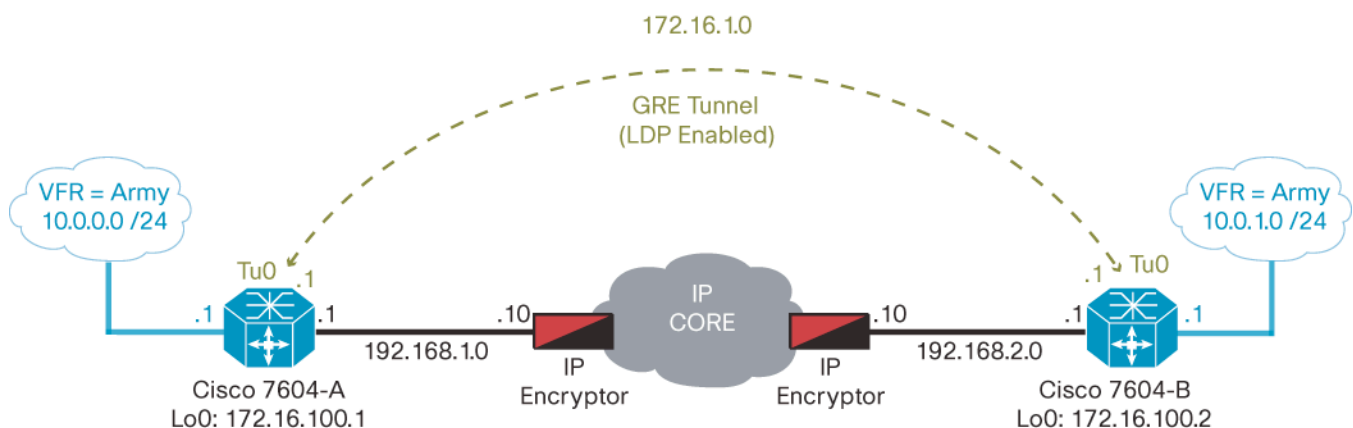
Figure 5. MPLS VPNs over GD TACLANE (KG-175A)—Demonstrated at Encryption Show, Las Vegas, Nevada—June 1–2, 2005



Layer 3 MPLS VPN over GRE Demonstration—Configuration Example

This section provides a sample configuration for configuring MPLS VPNs over GRE tunnels (Figure 6). As can be viewed in the example diagram, this configuration was done over KG-175A encryptors and the configuration examples display the functions to make this work. This feature can be used in multiple environments that require tunneling over an IP core. This example uses a single VRF (VRF = Army), and the provider edge-customer edge routing protocol within each VRF (the customer edge router is not shown in the diagram) is Routing Information Protocol Version 2 (RIPv2).

Figure 6. Network Topology



Cisco IOS Software Configuration Examples

Cisco 7604-A	Cisco 7604-B
<pre> 7604-A# version 12.2 ! hostname 7600-A ! ! ip vrf army rd 10:1 route-target export 10:1 !(Both Import/Export route-targets of 10:1 must match 7600-B's) route-target import 10:1 ! ! --- Army VRF configuration ! mpls label protocol ldp ! ! interface Loopback0 ip address 172.16.100.1 255.255.255.255 ! interface Tunnel0 ip address 172.16.1.1 255.255.255.0 tag-switching ip (MPLS [LDP] is enabled on the GRE tunnel interface) tunnel source 192.168.1.1 (tunnel source is Gig interface 2/0/0) tunnel destination 192.168.2.1 (tunnel destination is the Gig interface on the adjacent router B) ! interface GigabitEthernet1/2 ip vrf forwarding army (enable VRF "army" on the customer facing interface) ip address 10.0.0.1 255.255.255.0 media-type rj45 ! </pre>	<pre> 7604-B#sh run version 12.2 ! hostname Router-B ! ! ip vrf army rd 10:1 route-target export 10:1 route-target import 10:1 ! mpls label protocol ldp ! interface Loopback0 ip address 172.16.100.2 255.255.255.255 ! interface Tunnel0 ip address 172.16.1.2 255.255.255.0 tag-switching ip tunnel source 192.168.2.1 tunnel destination 192.168.1.1 ! interface GigabitEthernet1/2 ip vrf forwarding army ip address 10.0.1.1 255.255.255.0 ip helper-address 10.1.20.1 media-type rj45 ! interface GigabitEthernet3/0/0 ip address 192.168.2.1 255.255.255.0 negotiation auto ! ! router ospf 1 log-adjacency-changes network 172.16.0.0 0.0.255.255 area 0 ! </pre>

```

interface GigabitEthernet2/0/0
 ip address 192.168.1.1 255.255.255.0
 negotiation auto
 ! --- (Note there is NO MPLS enabled on this
 interface... only on the GRE tunnel interface)
 !
 !
router ospf 1
 log-adjacency-changes
 network 172.16.0.0 0.0.255.255 area 0
 !
 ! --- Note that the "network" statement under
 OSPF includes only the 172.16.0.0 address space,
 which is also associated with the GRE tunnel.
 This simplifies the amount of routing
 configurations required as the 192.168.0.0 space
 is only used between the router and the
 Encryption Unit (directly Connected), therefore
 OSPF is not aware of that address space and it
 reduces the amount of configuration required.
 !
router rip
 version 2
 !
 address-family ipv4 vrf army (RIPv2 is used to
 exchange CE-PE routes within the ARMY VRF)
 redistribute connected
 redistribute bgp 1 metric 1
 network 10.0.0.0
 no auto-summary
 exit-address-family
 !
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 172.16.100.2 remote-as 1 (points to
 Loopback 0 on 7600-B)
 neighbor 172.16.100.2 update-source Loopback0
 no auto-summary
 !

```

```

router rip
 version 2
 !
 address-family ipv4 vrf army
 redistribute connected
 redistribute bgp 1 metric 1
 network 10.0.0.0
 no auto-summary
 exit-address-family
 !
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 172.16.100.1 remote-as 1
 neighbor 172.16.100.1 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 172.16.100.1 activate
 neighbor 172.16.100.1 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf army
 redistribute rip
 no auto-summary
 no synchronization
 exit-address-family
 !
ip classless
ip route 192.168.1.0 255.255.255.0
192.168.2.10
 !
 !
line con 0
line vty 0 4
 password cisco
 no login
 !
end

```

```

address-family vpnv4 (Basic MPLS VPN V4
information via MP-BGP)
neighbor 172.16.100.2 activate
neighbor 172.16.100.2 send-community extended
exit-address-family
!
address-family ipv4 vrf army
redistribute rip
no auto-summary
no synchronization
exit-address-family
!
ip classless
ip route 192.168.2.0 255.255.255.0 192.168.1.10
!
! --- This static route points to the encryption
units IP address (192.168.1.10) as the next-hop
to get to the Ethernet interface (192.168.2.0) on
the far-end 7600-B. The encryption unit will
handle routing packets destined for it and to the
far-end router.
!
!
line con 0
line vty 0 4
password cisco
no login
!
end

```

Cisco Solutions over IP Type I Encrypted Networks

As discussed in earlier sections, for those customers that require IP Service capabilities at line-rate Gigabit Ethernet performance over IP Type I encryptors, the need to support each of these over GRE tunnels is mandated. Features required at line rate over GRE include:

- Unicast
- Multicast
- Layer 3 VPN (RFC 2547)
- Multicast VPN (support for IP Multicast VPNs)
- IP Version 6

Several platforms in the Cisco router portfolio can support these features in software that is sufficient for certain customer requirements.^[6] These platforms include:

- Cisco 7200
- Cisco 7300
- Cisco 7500
- Cisco 1800, 2800, and 3800 integrated services routers

For customers who require support for each of the features for line-rate Gigabit Ethernet speeds and above, the Cisco 7600 supports each of these features at rates up to 10 million packets per second (pps). The current Gigabit Ethernet Type I encryptors available can support line-rate Gigabit Ethernet rates at 9000 Byte frame sizes, so for customers requiring this type of throughput, the Cisco 7600 should be considered as the platform of choice where hardware performance “over GRE” is required in the forwarding plane. In support of this solution, Cisco Systems will deliver a 2-port Gigabit Ethernet SPA^[7] that will enable support for Layer 3 MPLS VPNs (L3VPNs) over GRE tunnels in late 2005 (Table 2).^[8]

Table 2. Cisco 7604 System—Supporting L3VPN over GRE Feature

Product Description	Product Number
Cisco 7604 Chassis, 4 slots, 2 Cisco Catalyst 6500 Series/7600 Series Supervisor Engine 720-3BXLs (Part Number 2SUP720-3BXL), and 2 Power Supplies	7604-2SUP720XL-2PS
2-port Gigabit Ethernet SPAs	SPA-2XGE
Cisco 7600 Series SPA Interface Processor-400	7600-SIP-400

HIGH-SPEED IP SOLUTIONS OVER SONET TYPE I

Although this was not demonstrated, the fastest available Type I SONET encryption solution currently available in the market is the KG-189 SONET encryptor (currently up to OC-12 rates with capabilities to OC-48), and there is current development for solutions that extend to OC-48, OC-192, and beyond. Like ATM, SONET encryption is a link-layer technology (and the IP layer is transparent to the encryption process); therefore, the entire feature set of IP Services (MPLS, QoS, etc.) and applications can be run over a SONET transport Type I core without the requirement of tunneling techniques.

Cisco Solutions over IP Type I Encrypted Networks

Because the current SONET Type I encryption solutions are transparent to the IP layer, building an IP backbone over an encrypted Type I SONET transport is no different for the DoD than it is for public service providers and enterprises in that the broad range of Cisco router platform choices for customers requiring speeds up to OC-192 is the same for each.


The options of platforms that are currently capable of supporting OC-192 POS include:

- Cisco 7600 Series
- Cisco XR 12000 and 12000 series
- Cisco CRS-1 Carrier Router System

^[6] Performance will vary based on multiple factors, including processor, enabled features, etc.

^[7] Cisco offers many different types of SPAs. Refer to the following URL for more information about Cisco SPAs:
http://www.cisco.com/en/US/products/ps6267/prod_module_series_home.html

^[8] The L3VPN over GRE solution requires the 2-port Gigabit Ethernet SPA + Cisco 7600 SIP 400 combination to allow the MPLS over GRE function.



Each platform has unique advantages that, based on the customer requirements, make it the ideal solution both short- and long-term as it relates to features and functions, high availability, performance, and price. The key is that for customers requiring SONET Type I encryption plus a high-end router solution, the Cisco high-speed POS router portfolio can offer a variation of choices and flexibility for the features and functions required.

SUMMARY

Network backbones continue to evolve toward an IP application transport infrastructure. Therefore, it is vital that customers such as the DoD, faced with unique network requirements, including the mandate of Type I encryption devices, be able to take advantage of next-generation network features and have the ability to offer high-quality IP transport for these new applications.

IP Service transport and application offerings continue to evolve as well. A broad set of multiservice transport capabilities needs to be offered to customers, such as Layer 2 and Layer 3 VPNs, QoS offerings, IP Multicast support, LAN extension transport, as well as IPv6 transport, among others. A broad set of application offerings should include voice, video, and data—all IP-based. The move to an IP-based VPN service also simplifies the mechanisms to offer centralized services to external and internal customers, such as access to network storage, intrusion detection resources, surveillance, disaster recover, and others, while maintaining the required transport over a Type I encrypted backbone.

Cisco solutions will continue to play a vital role for the DoD as it continues to evolve its networks to allow support for all the available network services, integrating the required transport mechanisms regardless of the encryption technology used. This provides Cisco DoD customers the many advantages of MPLS/IP, QoS, IP Multicast, and IPv6 transport, without limiting their functions within the core or edge of the network where Type I encryption is required.

**Corporate Headquarters**

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

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

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

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

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

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • 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

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

205258.L_ETMG_SP_9.05