Accelerated Internet over Satellite Solution

Overview

This document provides deployment guidance for Cisco® Accelerated Internet over Satellite, a solution that combines the IP connectivity of Cisco Integrated Services Routers (ISRs) and the satellite wireless WAN (WWAN) link acceleration capabilities of the Cisco Network Capacity Expansion (NCE) service module. The document presents performance results achieved by combining the two products, outlines the required Cisco IOS® Software configuration, and describes deployment in a typical branch office. The goals of this guide are the following:

- To demonstrate that Cisco NCE, combined with a Cisco Integrated Services Router, achieves significantly higher HTTP transfer rates, webpage load times, and streaming video experience over a native satellite WWAN connection
- To make the deployment of this solution fast and predictable

Satellite Link Limitations

Whether used for primary access or as a backup link to a traditional wireline connection, satellite WWAN connectivity offers anywhere access to the Internet. For enterprises, the primary benefits of satellite WWAN include:

- Secure wireless connectivity to the enterprise network and the Internet
- Stationary or mobile network access from any location around the globe
- Greater network availability from divergent wireless and wireline network paths

Despite these benefits, sending data through a high-altitude satellite introduces a significant signal propagation delay that has a noticeable effect on the quality of user experience with satellite links. For geostationary orbit satellites (GEO), the round-trip delay is 500 to 600 milliseconds. This high latency and other technical factors, such as asymmetric data rates and high packet loss, affect the response time of content-rich and interactive Internet applications. The problem is further exacerbated by economic factors. Bandwidth can cost two to three times as much per month as other broadband alternatives, often forcing enterprises to settle for the minimum acceptable data rate. The Cisco NCE service module accelerates data transfer rates on WAN links that have limited bandwidth, high latency, and high error rates such as satellite, WiMAX, and third-generation (3G) wireless. This document shows that by combining Cisco Integrated Services Routers and Cisco NCE, you can increase the data rate on a satellite link by 400 to 2000 percent of its typical rate.

Cisco Integrated Services Routers

Cisco award-winning Integrated Services Routers combine data, voice, video, and wireless networking services into a single, secure platform that provides a one-stop solution for small offices, branch offices, and teleworkers. Designed to be a long-term, adaptable platform, Cisco Integrated Services Routers provide built-in capacity to support new applications and services that you can use today or activate in the future without incurring significant costs. These routers run the

industry-leading Cisco IOS Software, which offers the broadest range of network functions and supports all significant industry standards.

Main Features and Benefits

- Wireless networking enhances productivity and collaboration by enabling employees to access business applications from anywhere in the workspace.

- IP voice provides advanced communications such as call processing, voicemail, Automated Attendant, and conferencing functions to improve business communications and customer care while reducing the costs of maintaining a traditional voice system.

- IP video enables more cost-effective video surveillance and security systems, as well as supporting on-demand and live streaming media for consistent, high-quality learning, training, collaboration, and communications.

- Security components reduce the business risk associated with viruses and other security threats, such as network downtime, lost revenue, and harm to customer service.

- VPNs provide secure access to company assets for remote workers and teleworkers, and enable improved collaboration and responsiveness between employees, partners, and suppliers over a secure connection.

For more information about the Cisco Integrated Services Routers, visit http://www.cisco.com/en/US/products/hw/routers/index.html.

Cisco NCE Service Module

The Cisco NCE service module is a transparent proxy that increases the data transfer rate on a WAN link and improves response times of remotely hosted applications. The service module accelerates performance of any TCP application delivered over a wireless or wireline WAN. It is suitable for branch offices and remote sites with WAN connections that have limited bandwidth, high error rates, or high latency such as satellite, WiMAX, or 3G wireless. The Cisco NCE service module is available for Cisco 1841, 2800, and 3800 Series Integrated Services Routers, and is tightly integrated with the services provided on these award-winning products.

Main Features and Benefits

- Typical 4X WAN link throughput increase and remote application response time reduction

- TCP optimization through Stream Control Transmission Protocol (SCTP) encapsulation, TCP session multiplexing, advanced flow and congestion control, and other optimizations such as localized packet flow control

- Layer 4 multipacket compression, redundant header compression, ACK and packet bundling

- Integration into Cisco Express Forwarding, which helps ensure transparency to other Cisco IOS Software features such as firewall, intrusion prevention system (IPS), access control lists (ACLs), quality of service (QoS), and others

- Hub-to-spoke and meshed deployments with up to 10 concurrent remote peers

- No moving parts and automatic traffic bypass mechanism that reduces network disruption in case of failure

- Target applications include any TCP-based application delivered over a WAN

For more information about the Cisco NCE, visit
http://www.cisco.com/en/US/products/ps9702/index.html.

Cisco Accelerated Internet over Satellite Solution Performance

An outgoing TCP traffic flow routed through an interface connected to a satellite modem is intercepted by the Cisco NCE module. The module acts as a transparent performance-enhancing proxy (PEP) that terminates the sender's TCP session locally, compresses and bundles the sender's data, sends the data to a remote peer encapsulated with SCTP, unbundles and decompresses the data, and establishes a new TCP session remotely to deliver the data to its destination, while fully maintaining the end-to-end semantics of the original TCP session. Figure 1 shows the end-to-end deployment architecture of Cisco NCE.

Figure 1. Cisco NCE Deployment Architecture
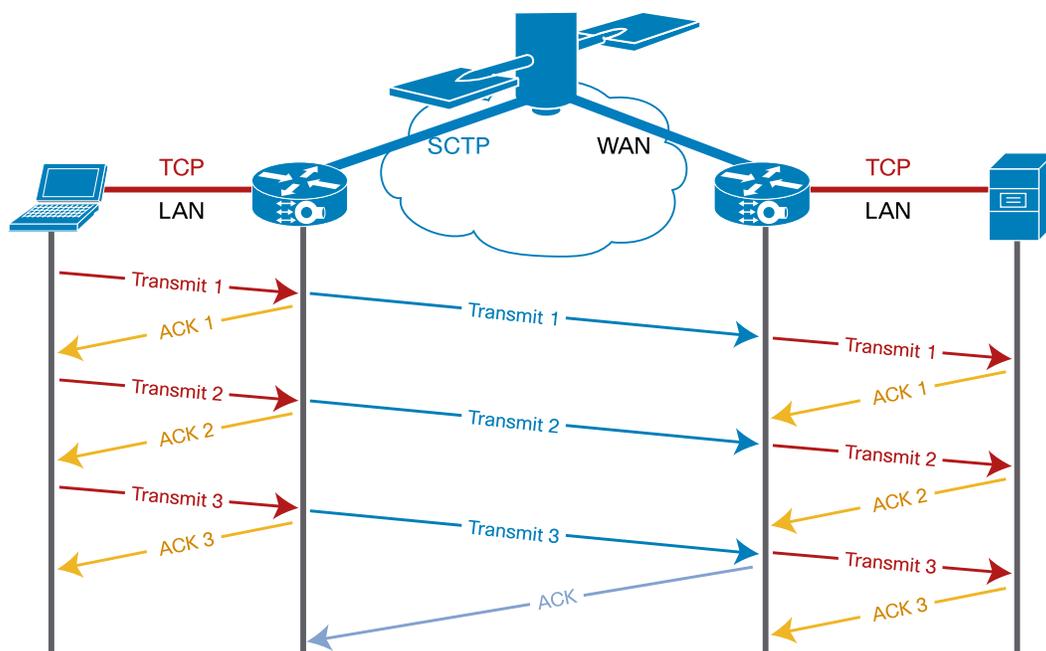
Repeated testing shows that data throughput and remote application response time on a satellite link improves 4 to 20 times when the Cisco Integrated Services Router and Cisco NCE service module are combined in a single solution. Table 1 shows downlink and uplink performance data of the HTTP protocol for various bandwidths and user counts on a native satellite link compared to the Cisco Accelerated Internet over Satellite solution. Figure 2 provides a graphical depiction of the total time necessary to download a 10-MB data set using HTTP with the Cisco Accelerated Internet over Satellite solution compared to the total time on a native satellite link. Figure 3 shows the total upload time for the 10-MB data set.

Table 1. HTTP Downlink and Uplink Data Rates for Various Satellite Links with the Cisco Accelerated Internet over Satellite Solution for 1 and 20 Users (In the 20-user scenarios, each user generates three concurrent TCP connections.)

Scenario	Actual Data Rate on 512/128kbps Link (kbps)	Cisco Accelerated Internet over Satellite on 512/128 kbps Link (kbps)	Gain Factor	Actual Data Rate on 1/0.256 Mbps Link (kbps)	Cisco Accelerated Internet over Satellite on 1/0.256 Mbps Link (kbps)	Gain Factor	Actual Data Rate on 2/0.512 Mbps Link (kbps)	Accelerated Internet over Satellite on 2/0.512 Mbps Link (kbps)	Gain Factor
1-user HTTP download	42	887	21.0	42	859	20.3	42	860	20.3
20-user HTTP download	508	2021	4.0	1010	4096	4.1	2021	8192	4.1
1-user HTTP upload	42	437	10.3	42	792	18.7	42	847	20.0
20-user HTTP upload	126	532	4.2	248	1010	4.1	507	2348	4.4

Figure 2. Total HTTP Download Time for a 10-MB File on a Native Satellite Link Compared to the Cisco Accelerated Internet over Satellite Solution for a Single User
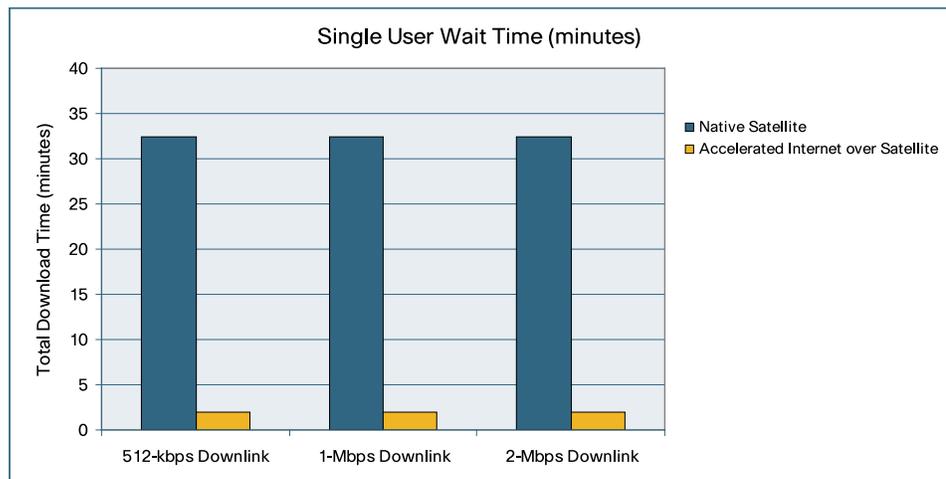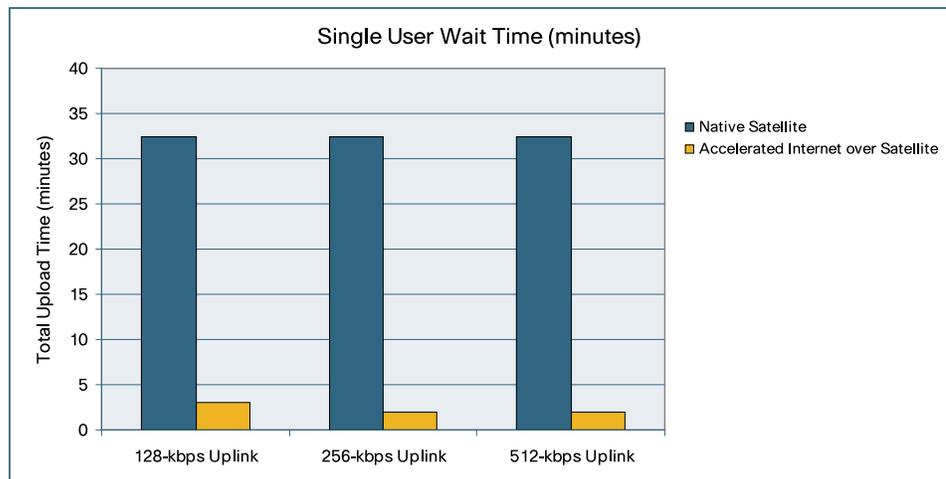

Figure 3. Total HTTP Upload Time for a 10-MB File on Native Satellite Link Compared to the Cisco Accelerated Satellite over Internet Solution for a Single User

Cisco NCE supports all TCP-based applications. Table 2 shows results of an integrated HTTP file download, FTP file download, and Simple Mail Transfer Protocol (SMTP) email send scenario for various bandwidths and user counts on a native satellite link compared to the Cisco Accelerated Internet over Satellite solution. The traffic profile was 70-percent HTTP, 20-percent FTP, and 10-percent SMTP. Figure 4 provides a graphical depiction of the total amount of data transferred in both directions in a 10-minute interval with the Cisco Accelerated Internet over Satellite solution compared to the total amount of data transferred on a native satellite link.

Table 2. Mixed-Traffic Aggregate Data Volume for Various Satellite Links with the Cisco Accelerated Satellite over Internet Solution for 1 and 20 Users in 10 minutes (In the 20-user scenarios, each user generates three concurrent TCP connections.)

Scenario	Data Transferred on 512/128 kbps Link (MB)	Cisco Accelerated Internet over Satellite on 512/128 kbps Link (MB)	Gain Factor	Data Transferred on 1/0.256 Mbps Link (MB)	Cisco Accelerated Internet over Satellite on 1/0.256 Mbps Link (MB)	Gain Factor	Data Transferred on 2/0.512 Mbps Link (MB)	Accelerated Internet over Satellite on 2/0.512 Mbps Link (MB)	Gain Factor
1-user HTTP and FTP download, or SMTP upload	3.1	63.3	20.4	3.1	62.8	20.3	3.1	63.0	20.3
20-user HTTP and FTP download, or SMTP upload	40.0	170.2	4.3	67.1	290.0	4.3	154.9	614.7	4.0

Figure 4. Total Amount of Data Transferred in 10 Minutes on a Native Satellite Link Compared to the Cisco Accelerated Satellite over Internet Solution Using Mix of 70-Percent HTTP (Down), 20-Percent FTP (Down), and 10-Percent SMTP (Up)
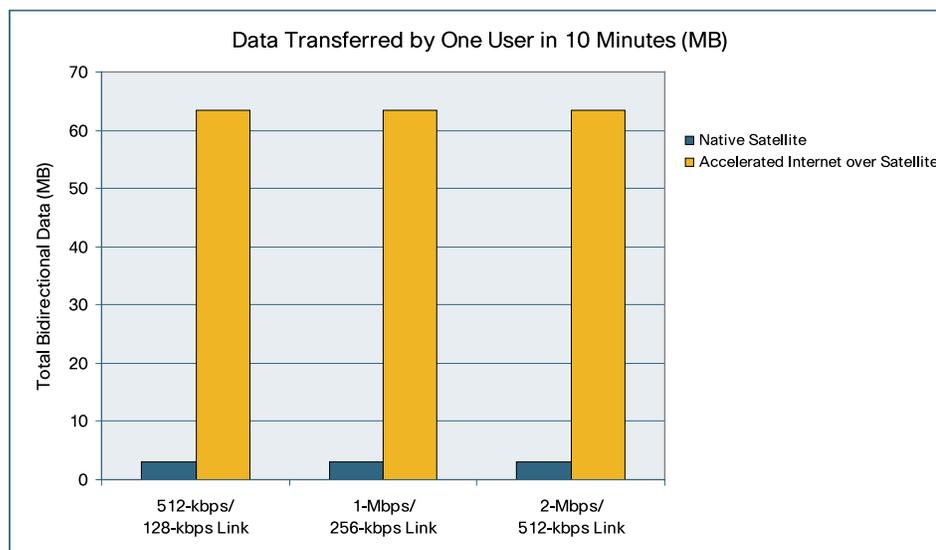
Cisco Accelerated Internet over Satellite Solution Performance Test Details

Cisco NCE accelerates WAN-bound traffic by using compression techniques and a variety of TCP protocol optimizations. The primary determinants of performance improvement are available bandwidth, link latency, packet-loss rate, compressibility of the data stream, and bandwidth usage. In the case of satellite, the first factor is economic and determined by business requirements. Therefore, several typical bandwidth configurations were used in testing. The second and third factors are determined by the choice of the satellite technology. Some variability exists depending on the altitude, weather, and other environmental factors. These factors for the most part cannot be controlled.

Compressibility of the data stream crossing the WAN link is determined by the application that is sending or receiving the data. To provide generally applicable and consistently reproducible results, the Cisco Accelerated Internet over Satellite solution was tested with the Standard Canterbury Corpus (http://www.data-compression.info/Corpora/CanterburyCorpus/), which is an industry benchmark for measuring performance of compression. The corpus consists of 11 file types representing typical data that users can directly process. These files were sent and received by HTTP and FTP applications. It is important to note that the Canterbury Corpus contains typical user data and only a small amount of data encoded for computer processing with markup languages such as XML or HTML. Data generated for computer processing represents a large percentage of typical network traffic and is highly compressible, and therefore the performance gain in a typical scenario would be even greater than presented in Tables 1 and 2.

All testing was performed on a Cisco 2811 Integrated Services Router with a satellite modem in the branch office, and a Cisco 3845 Integrated Services Router at the satellite hub. Refer to Figure 6 later in the document for additional details.

Cisco Accelerated Internet over Satellite Solution Configuration

The selection of the Cisco NCE model, in general, depends on the Cisco Integrated Services Router platform that will host the module. The Cisco NCE AIM-TPO-1 model is appropriate for WAN links with bandwidth less than 2 Mbps, and a Cisco NCE AIM-TPO-2 model is appropriate for all other WAN links. The Cisco NCE AIM-TPO-2 model also optimizes twice as many concurrent TCP connections as a Cisco NCE AIM-TPO-1 model, and therefore should be used when the number of users is large (more than 50) even though the bandwidth may be less than 2 Mbps. Table 3 summarizes the recommended configurations. The Cisco NCE TPO-AGGR-1 model is a central-site aggregator that connects with up to 50 sites, up to 12,500 concurrent TCP connections, up to 100-Mbps WAN bandwidth, and up to 300-Mbps total throughput on a Cisco 3845 Integrated Services Router.

Table 3. Recommended Configuration for Cisco Internet over Satellite Solution

Router	Hardware Configuration	Cisco NCE Model	Cisco IOS Software Release	Cisco IOS Software Image	Cisco NCE Software Release
Cisco 1841	Default	AIM-TPO-1	12.4(20)T or later	IP Base or Advanced Security (recommended)	2.0.1 or later
Cisco 2800 Series	Default	AIM-TPO-2	12.4(20)T or later	IP Base or Advanced Security (recommended)	2.0.1 or later
Cisco 3800 Series	Default	AIM-TPO-2	12.4(20)T or later	IP Base or Advanced Security (recommended)	2.0.1 or later
Headend aggregation	Default	TPO-AGGR-1	12.4(20)T or later	IP Base or Advanced Security (recommended)	2.0.1 or later

A satellite link typically has two uses in enterprise networks. In one use, the satellite provides the primary link connectivity at remote locations where no other connectivity option is available because of geographic remoteness or lack of a wired infrastructure. In the other, the satellite is used as a backup link, providing a truly divergent path to the Internet or enterprise network, thereby minimizing the possibility of lost connectivity. The configuration instructions that follow address both of these uses.

Configuring the Cisco NCE Service Module in Cisco IOS Software

The Cisco NCE Advanced Integration Module (AIM) is an internal service module. For TCP traffic to be forwarded to the module, the internal backplane link between the service module and the router must be configured, just as with any other routable link. Figure 5 shows a high-level view of the internal connection between Cisco IOS Software and the Cisco NCE service module.

Figure 5. Configuration of the Cisco NCE Advanced Integration Module
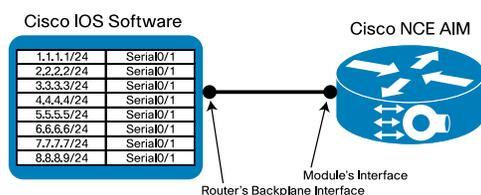

```
Router(config)# interface Transport-Opt-Service-Engine0/0 ! Enters NCE
module configuration mode

Router(config-if)# ip address 10.0.0.1 255.255.255.252 ! Assigns IP
address to the router's backplane interface

Router(config-if)# service-module ip address 10.0.0.2 255.255.255.252
! Assigns IP address to NCE interface

Router(config-if)# service-module ip default-gateway 10.0.0.1 !
Assigns default gateway for the service module

Router(config-if)# exit

Router(config)# ip route 10.0.0.2 255.255.255.255 Transport-Opt-
Service-Engine0/0 ! Sets routing table entry for NCE module
```

Configuring the Cisco NCE Service Module for Primary Access

Apply the following commands on the interface connected to the satellite modem. This example assumes that the interface connected to the satellite modem is the onboard Gigabit Ethernet port:

```
Router(config)# interface GigabitEthernet0/0 ! Enters router's onboard
Ethernet interface configuration mode
```

```
Router(config-if)# transport-opt 2 interface Transport-Opt-Service-
Engine0/0 ! Enables NCE traffic interception on the Ethernet interface
and assigns id 2 to the binding
```

```
Router(config-if)# exit
```

Configuring the Cisco NCE Service Module for Backup Access

When the satellite connection is used for backup and the Cisco NCE is used to provide acceleration on both the primary link and the backup link, then Cisco NCE interception must be configured on the primary WAN interface with a different ID. The following example assumes that the primary interface is serial:

```
Router(config)# interface Serial0/1/0 ! Enters serial interface
configuration mode
```

```
Router(config-if)# transport-opt 1 interface Transport-Opt-Service-
Engine0/0 ! Enables NCE traffic interception on the primary interface
and assigns id 1 to the binding
```

```
Router(config-if)# exit
```

In addition, the interface connecting the router to the satellite modem must be configured as a backup interface. There are several ways to configure an interface for backup. The following examples show the use of floating static routes with object tracking:

```
Router(config)# track 1 interface Serial0/1/0 ip routing ! Enables
tracking on the primary WAN interface
```

```
Router(config)# ip route 0.0.0.0 0.0.0.0 Serial0/1/0 track 1 ! Creates
a static default route for the primary WAN interface with object
tracking
```

```
Router(config-if)# ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0 200 !
Creates a static floating default route for the backup WAN interface
with metric higher than the primary interface default route
```

The following example uses the interface tracking capabilities of Cisco IOS Software:

```
Router(config)# interface Serial0/1/0 ! Enters serial interface
configuration mode
```

```
Router(config-if)# backup interface GigabitEthernet0/0 ! Sets the
interface going to Satellite modem as a backup interface for this
primary interface
```

```
Router(config-if)# backup delay 10 0 ! (Optional) Sets delay before
forcing switchover to backup link (10 seconds) and then back to the
primary (immediate). This reduces effects of flapping links
```

```
Router(config-if)# exit
```

Configuring the Cisco NCE Service Module

```
NCE(config)> tpo id 2 ! Enters interface to Satellite modem binding
configuration mode
NCE(config-tpo-id)> sctp-peer 172.16.0.1 ! Configures remote peer
address and specifies that all optimized traffic will be marked with
IP Type of Service value of 0
NCE(config-tpo-id)> exit
```

If the satellite link is used for backup, Cisco NCE binding must be configured for the primary interface:

```
NCE(config)> tpo id 1 ! Enters primary WAN interface binding
configuration mode
NCE(config-tpo-id)> sctp-peer 172.16.0.2 ! Configures remote peer
address and specifies that all optimized traffic will be marked with
IP Type of Service value of 0
NCE(config-tpo-id)> exit
```

For more information about the Cisco NCE module, visit
http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/cnce/1.0/installation/guide/NCEUserDoc.html.

By default, the Cisco NCE uses a high-speed congestion and flow-control mechanism to adjust the rate at which traffic is sent over the WAN link. This mechanism provides superior performance over the standard TCP congestion and flow-control mechanism. Two additional flow-control mechanisms are provided. One is the default SCTP congestion and flow control (`bandwidth-profile default-sctp` command) that is SCTP-standard compliant but offers less performance. The other is explicit rate control (`bandwidth-profile rate-control` command) that enables the configuration of peak and guaranteed bandwidth. The latter option can provide additional performance improvement on a dedicated link with well-known bandwidth parameters. You should set peak bandwidth to the maximum bandwidth available on the satellite link, and guaranteed bandwidth to the lowest bandwidth available on the link. You should configure the uplink values at the central-site Cisco NCE module, and the downlink values on the branch-office module. In a typical scenario, where bandwidth is guaranteed with a Service-Level Agreement (SLA), set the guaranteed bandwidth to the SLA value. Set the peak bandwidth to the maximum rate the service provider allows. If bandwidth bursting is not allowed, you should generally set peak bandwidth to your agreed-upon rate, guaranteed to 90 percent of that value. However, the improvement using this static bandwidth configuration over the default high-speed mechanism is marginal, and may not justify the additional configuration complexity.

You can configure the Cisco NCE module rate control at the branch-office site with the following commands:

```
NCE(config)> tpo id 2 ! Enters binding configuration mode for the
interface to modem
NCE(config-tpo-id)> bandwidth-profile rate-control ! Specifies static
bandwidth configuration
NCE(config-tpo-id)> bandwidth 256 230 ! Sets peak and guaranteed
bandwidth for uplink
```

You can configure Cisco NCE module rate control at the central site with the following commands:

```
NCE(config)> tpo id 2 ! Enters binding configuration mode for the
interface to modem
NCE(config-tpo-id)> bandwidth-profile rate-control ! Specifies static
bandwidth configuration
NCE(config-tpo-id)> bandwidth 1024 922 ! Sets peak and guaranteed
bandwidth for downlink
```

To reset congestion and flow control back to the default high-speed option, use the following command:

```
NCE(config)> tpo id 2 ! Enters binding configuration mode for the
interface to modem
NCE(config-tpo-id)> bandwidth-profile hs-sctp ! Specifies high-speed
SCTP flow/congestion control
```

Cisco NCE is a symmetric solution that requires termination of optimized traffic flows at a central site that is hosting the remote applications or serving as a gateway to the Internet. The termination is provided by a Cisco NCE aggregation device, which is typically one of the Cisco 3800 Series routers equipped with the Cisco NCE Network Module (NME-TPO). A single Cisco NCE Network Module supports aggregation of traffic from up to 50 sites, and the Cisco 3845 Integrated Services Router can be equipped with up to four Cisco NCE Network Modules, providing aggregation for up to 200 remote sites and branch offices. You can deploy the Cisco NCE aggregation device either in-path or out-of-path. Out-of-path deployment requires a redirection mechanism to be enabled on the device aggregating the WAN traffic. Refer to the Cisco NCE documentation for additional deployment instructions.

Typical Branch-Office Deployment of Cisco Accelerated Internet over Satellite Solution

A typical branch-office deployment uses satellite either for primary access or as a backup link. The following section provides a test case and a configuration example for a typical remote location where the satellite link is used for primary connectivity. A test case and a configuration example for the backup link scenario are provided later in the document.

For the primary link test case scenario, Cisco NCE intercepted all non-enterprise TCP traffic. The remote site ran Cisco 2800 Series Integrated Service Routers with a Cisco NCE AIM service module. The satellite hub ran the Cisco 3800 router with a Cisco NCE enhanced network module (NME) deployed out-of-path. Services such as firewall, VPN, and multicast were configured to demonstrate the capabilities of the Cisco Accelerated Internet over Satellite solution. Figure 6 provides the topology of the test scenario, and Table 4 lists features that were configured on the router.

There are several options for directing traffic to the Internet:

- Split tunneling with an IPsec GRE tunnel for enterprise traffic and a WAN interface for Internet traffic: The traffic is routed to the Internet from the satellite service provider's hub.
- A single IP Security (IPsec) generic routing encapsulation (GRE) tunnel for both enterprise and Internet traffic: The traffic is routed to the Internet from the enterprise central site.
- Mixed traffic over unsecured link

- Split tunneling with GRE tunnel for enterprise traffic and WAN interface for Internet traffic: The traffic is routed to the Internet from the satellite service provider's hub.

The primary link test case scenario provides configuration for the first option. The backup link test case scenario later in the document provides configuration for the second option. The last two options are less secure forms of the first two.

In the primary link test case scenario, an IPsec GRE tunnel was created for enterprise traffic. Internet traffic was routed directly through the WAN interface connected to the satellite modem. Cisco NCE was configured to optimize only the Internet traffic. The configuration shown in Table 6 provides an example of split tunneling with an IPSec GRE tunnel and shows a full configuration for a typical remote site router. Table 5 provides explanation of IP address assignment for this test case. Table 7 provides Cisco NCE configuration at the remote site and Table 8 Cisco NCE configuration at the satellite hub.

Figure 6.   Deployment Scenario for Internet over Primary Satellite Link with Split Tunneling
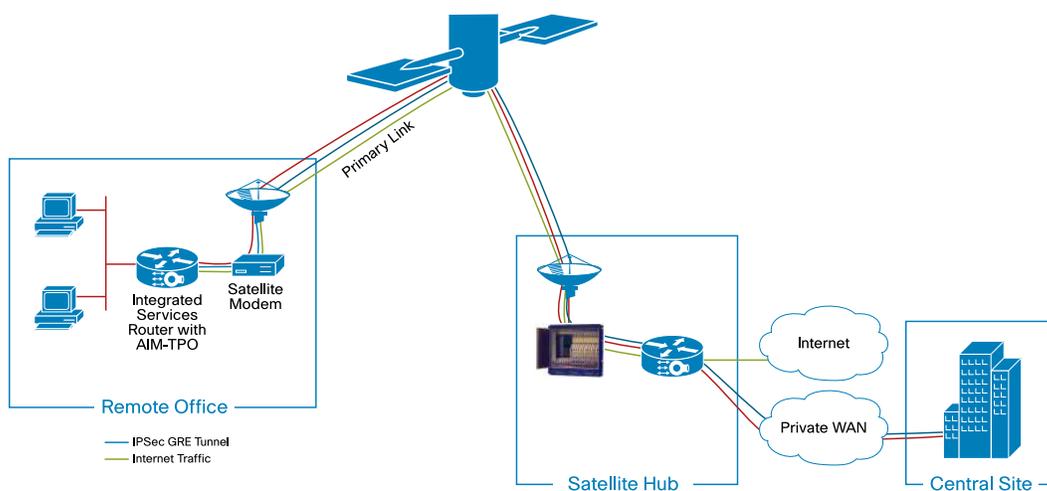

Table 4.   Features Enabled for Internet over Primary Satellite Link with Split Tunneling Test

Category	Feature or Detail
Cisco NCE software image	Release 2.0.0
Cisco IOS software image	Release 12.4(20)T
Primary WAN	Satellite
Internet access	Split tunneling
Routing	EIGRP
Addressing	Network Address Translation (NAT) and Port Address Translation (PAT); IP Multicast; and Dynamic Host Configuration Protocol (DHCP)
Data privacy	IPsec GRE with 3DES encryption
Perimeter protection	Classic firewall (CBAC)

Internet over Primary Satellite Link with Split Tunneling Test

Description	Split tunneling for Internet and enterprise traffic with TCP optimization
Test setup	• The branch-office router used the Ethernet interface connected to the satellite modem as its primary WAN interface. • The branch-office router was configured with features listed in Table 4. • The branch-office router had one Cisco NCE module. • The satellite hub router had one Cisco NCE module. • Enterprise traffic was carried in an IPsec GRE tunnel. • Internet traffic was carried directly over the Ethernet interface. • Cisco NCE was configured on the Ethernet interface.
Procedure	• The IXIA traffic generator sends HTTP traffic from the hub site through the branch-site router. • Cisco NCE show commands are used to verify that the traffic is optimized on the link.
Pass or fail criteria	The WAN interface shows optimization.
Result	Pass

Table 5.   Addressing Used in Primary Satellite Link with Split Tunneling Scenario

Device	Address/Subnet
LAN interface	10.0.0.1/24
Primary WAN interface	209.165.201.1/30
Tunnel interface	209.165.201.5/30
Router backplane interface	10.0.1.1/30
Cisco NCE interface	10.0.1.2/30
Cisco NCE peer 1	172.16.1.2/30

Table 6.   Branch-Office Router Configuration for Primary Access over Satellite with Split Tunneling

```
version 12.4
!
hostname Branch
!
ip dhcp excluded-address 10.0.0.1
10.0.0.30
ip dhcp excluded-address 10.0.0.245
10.0.0.254
!
ip dhcp pool PCS
   network 10.0.0.0 255.255.255.0
   default-router 10.0.0.1
!
ip inspect name FW-BRANCH dns
ip inspect name FW-BRANCH cuseeme
ip inspect name FW-BRANCH ftp
ip inspect name FW-BRANCH h323
ip inspect name FW-BRANCH https
ip inspect name FW-BRANCH icmp
ip inspect name FW-BRANCH imap
ip inspect name FW-BRANCH pop3
ip inspect name FW-BRANCH netshow
ip inspect name FW-BRANCH rcmd
ip inspect name FW-BRANCH realaudio
ip inspect name FW-BRANCH rtsp
ip inspect name FW-BRANCH esmtp
ip inspect name FW-BRANCH sqlnet
ip inspect name FW-BRANCH
```

```
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key VPN-KEY address
0.0.0.0 0.0.0.0
!
crypto ipsec transform-set XFORM esp-
3des esp-md5-hmac
!
crypto ipsec profile VPN-SEC
 set transform-set XFORM
!
interface Tunnel0
 ip address 209.165.201.5
255.255.255.252
 ip inspect FW-BRANCH out
 ip pim sparse-dense-mode
 tunnel source FastEthernet0/0
 tunnel destination 209.165.201.2
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VPN-SEC
!
```

```
interface FastEthernet0/0
 ip address 209.165.201.1
255.255.255.252
 ip inspect FW-BRANCH out
 ip nat outside
 transport-opt 1 interface Transport-Opt-
Service-Engine0/0
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.255.255.0
 ip nat inside
!
interface Transport-Opt-Service-
Engine0/0
 ip address 10.0.1.1 255.255.255.252
 ip nat outside
 service-module ip address 10.0.1.2
255.255.255.252
 service-module ip default-gateway
10.0.1.1
!
router eigrp 100
 network 10.0.0.0 0.0.0.255
 network 209.165.201.4 0.0.0.3
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
ip nat pool NCE-POOL 209.165.201.1
```

streamworks		209.165.201.1 prefix-length 24
ip inspect name FW-BRANCH tftp		ip nat inside source list 100 pool NCE-POOL overload
ip inspect name FW-BRANCH tcp		
ip inspect name FW-BRANCH udp		ip nat inside source static 10.0.1.2 209.165.201.1
ip inspect name FW-BRANCH vdolive		!
no ip domain lookup		access-list 100 permit 132 host 10.0.1.2 host 172.16.1.2
ip multicast-routing		access-list 100 permit ip 209.165.201.0 0.0.0.3 any

Table 7.   Branch-Site Cisco NCE Module Configuration

```
hostname NCE

tpo id 1
sctp-peer 172.16.1.2
exit

tpo ip nat inside source 209.165.201.1 172.16.0.1 255.255.255.0
```

Table 8.   Satellite Hub Cisco NCE Module Configuration

```
hostname NCE

tpo id 1
sctp-peer 209.165.201.1
exit
```

You can use Cisco NCE to simultaneously accelerate throughput and remote application response time on both a primary link and a backup link. If the primary link fails and the router switches over to the satellite backup link, Cisco NCE switches over and continues to accelerate traffic on the satellite link, as shown in Figure 7. In this use case, aggregation of Cisco NCE connections can be performed at two possible locations. Either the enterprise hosts an aggregator with two Cisco NCE Network Modules or the satellite hub has one aggregator for the backup link and the enterprise has a second aggregator for the primary link. Table 9 lists features that were enabled on the router to test the former use case.

Note: When Cisco NCE is configured for interception on both the primary and backup interfaces, each link must have a dedicated peer device that cannot be shared with the other link. Therefore, when there is only one headend aggregation device, it must have at least two Cisco NCE Network Modules to support a dual primary and backup configuration. However, multiple remote sites with both primary and backup interface interception can share the two aggregation modules, up to the 50-remote-sites limit. This constraint will be removed in future releases of the product.

In the following test scenario, a serial wireline link was configured for primary access and a satellite WWAN link for backup. Cisco NCE was configured to optimize traffic on both the primary and backup links. Initially the traffic was directed over the primary access link. When the primary link was disrupted, the traffic switched to the backup link. After some time, the primary link became active again, and traffic switched away from the backup link. In all cases, Cisco NCE continued to optimize traffic on whichever link was active. In this test scenario the traffic is directed to the Internet from the enterprise central site. Group Encrypted Transport VPN is used for the primary link connection and IPsec GRE tunnel for the backup link.

The configuration shown in Table 11 shows an IPsec GRE tunnel used for both enterprise and Internet traffic, and shows full configuration for a typical remote-site router. Table 10 provides explanation of IP address assignment for this test case. Table 12 provides Cisco NCE configuration at the remote site and Tables 13 and 14 provide Cisco NCE configuration at the enterprise central site.

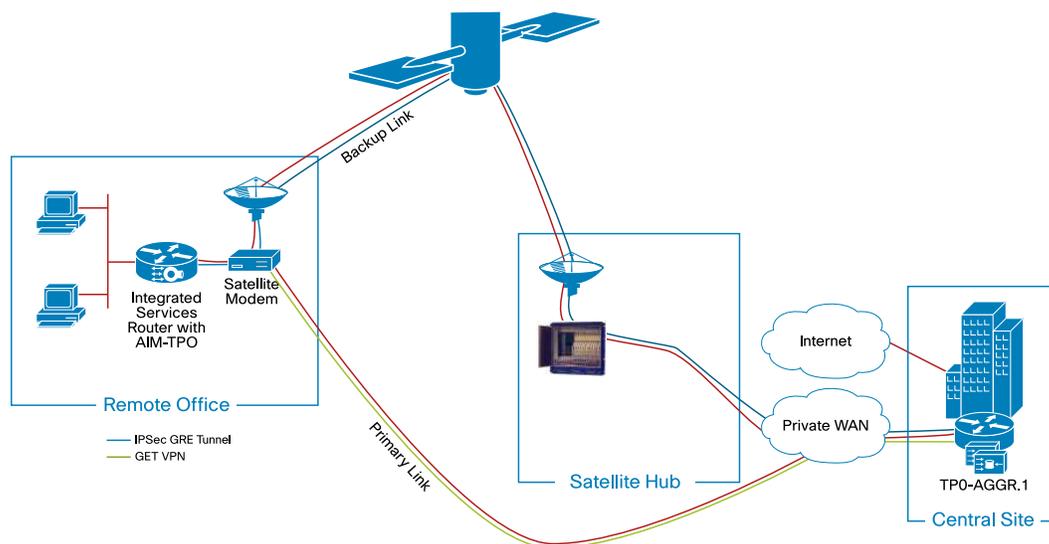**Figure 7.** Deployment Scenario for Primary-to-Backup Switchover Test

Table 9. Features Enabled in the Primary-to-Backup Switchover Test

Category	Feature or Detail
Cisco NCE software image	Release 2.0.0
Cisco IOS software image	Release 12.4(20)T
Primary WAN	Serial
Backup WAN	Satellite connected to Ethernet interface
Internet access	From central site
Routing	EIGRP
Addressing	IP Multicast
Data privacy	Group Encrypted Transport VPN with 3DES encryption on primary link; IPsec GRE with 3DES encryption on backup link
Perimeter protection	Classic firewall (CBAC)

Primary-to-Backup Switchover Test

Description	Primary-to-backup link switchover with continued optimization of TCP traffic
Test setup	• The branch-office router used the serial interface for primary access and the Ethernet interface connected to the satellite modem for backup. • The branch-office router was configured with features listed in Table 9. • The branch-office router had one Cisco NCE module. • The central-site router had two Cisco NCE modules. • There were two SCTP associations between the branch-office router and the central site for each interface. • Each SCTP association was carried in a GRE tunnel over both Ethernet and cellular interfaces.

Procedure	• The IXIA traffic generator sends HTTP traffic from the central site through the branch-site router. • Cisco NCE show commands are used to verify that the traffic is optimized on the primary link. • While the traffic is being transmitted, the primary link is pulled out to simulate a link failure. • Immediately after the link is pulled out, traffic should start to fail. • After a short time, HTTP flows are reestablished on the backup link. • Cisco NCE show commands are used to verify that the traffic is optimized on the backup link.
Pass or fail criteria	The primary link shows optimization, traffic continues to flow after switchover, and the backup link shows optimization.
Result	Pass

Cisco IOS Software and Cisco NCE Configuration

Table 10. Addressing Used in Primary-to-Backup Switchover Scenario

Device	Address/Subnet
LAN interface	10.0.0.1/24
Primary WAN interface	209.165.201.1/30
Tunnel destination	209.165.201.5/30
Backup WAN interface	209.165.201.9/30
Router backplane interface	10.0.1.2/24
Cisco NCE interface	10.0.1.2/24
Cisco NCE peer 1	172.16.1.2/16
Cisco NCE peer 2	172.16.2.2/16

Table 11. Branch-Office Router Configuration

```
version 12.4
!
hostname Branch
!
no ip domain lookup
ip multicast-routing
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key VPN-KEY address
0.0.0.0 0.0.0.0
!
crypto ipsec transform-set XFORM esp-
3des esp-md5-hmac
!
crypto ipsec profile VPN-SEC
 set transform-set XFORM
!
crypto gdoi group GET-GROUP
 identity number 1357924680
 server address ipv4 209.165.201.2
 crypto map VPN-MAP local-address
FastEthernet0/0
!
crypto map VPN-MAP 1 gdoi
 set group GET-GROUP
!
```

```
interface Tunnel0
 ip address 209.165.201.5
255.255.255.252
 ip pim sparse-dense-mode
 tunnel source FastEthernet0/0
 tunnel destination 209.165.201.10
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VPN-SEC
!
interface Serial0/0/0
 backup interface FastEthernet0/0
 backup delay 10 0
 crypto map VPN-MAP
 ip address 209.165.201.1
255.255.255.252
 transport-opt 1 interface Transport-Opt-
Service-Engine0/0
!
interface FastEthernet0/0
 ip address 209.165.201.9
255.255.255.252
 transport-opt 2 interface Transport-Opt-
Service-Engine0/0
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.255.255.0
!
```

```
interface Transport-Opt-Service-
Engine0/0
 ip address 10.0.1.1 255.255.255.252
 service-module ip address 10.0.1.2
255.255.255.252
 service-module ip default-gateway
10.0.1.1
!
router eigrp 100
 network 10.0.0.0 0.0.0.255
 network 209.165.201.0 0.0.0.3
 no auto-summary
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 network 209.165.201.4 mask
255.255.255.252
 network 209.165.201.8 mask
255.255.255.252
 neighbor 209.165.201.10 remote-as
65016
 distribute-list 20 in
 no auto-summary
!
access-list 20 permit 209.165.201.8
0.0.0.3
!
lp route 0.0.0.0 0.0.0.0 209.165.201.2
lp route 0.0.0.0 0.0.0.0 209.165.201.10
```

Table 12. Branch-Site Cisco NCE Module Configuration

```
hostname NCE

tpo id 1
sctp-peer 172.16.1.2
exit

tpo id 2
sctp-peer 172.16.2.2
exit
```

Table 13. Central-Site Cisco NCE Module 1 Configuration

```
hostname NCE1

tpo id 1
sctp-peer 10.0.1.2
exit
```

Table 14. Central-Site Cisco NCE Module 2 Configuration

```
hostname NCE2

tpo id 1
sctp-peer 10.0.1.2
exit
```

Conclusion

- Repeated testing shows that data throughput and remote application response time on a satellite link improves 4 to 20 times when the Cisco NCE service module and Cisco Integrated Services Router are combined in a single solution.

- Cisco NCE works transparently with Cisco IOS Software features and services.

- In cases where the satellite link is used for backup, the Cisco Accelerated Internet over Satellite solution can be configured to provide traffic acceleration for both the satellite backup link and the primary WAN link.

CISCO

Americas Headquarters	Asia Pacific Headquarters	Europe Headquarters
Cisco Systems, Inc.	Cisco Systems (USA) Pte. Ltd.	Cisco Systems International BV
San Jose, CA	Singapore	Amsterdam, The Netherlands

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