

MACH5 Acceleration Guide

Version 6.5.x and later

Guide Revision: 9/21/2018



Legal Notice

Copyright © 2018 Symantec Corp. All rights reserved. Symantec, the Symantec Logo, the Checkmark Logo, Blue Coat, and the Blue Coat logo are trademarks or registered trademarks of Symantec Corp. or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE. SYMANTEC CORPORATION PRODUCTS, TECHNICAL SERVICES, AND ANY OTHER TECHNICAL DATA REFERENCED IN THIS DOCUMENT ARE SUBJECT TO U.S. EXPORT CONTROL AND SANCTIONS LAWS, REGULATIONS AND REQUIREMENTS, AND MAY BE SUBJECT TO EXPORT OR IMPORT REGULATIONS IN OTHER COUNTRIES. YOU AGREE TO COMPLY STRICTLY WITH THESE LAWS, REGULATIONS AND REQUIREMENTS, AND ACKNOWLEDGE THAT YOU HAVE THE RESPONSIBILITY TO OBTAIN ANY LICENSES, PERMITS OR OTHER APPROVALS THAT MAY BE REQUIRED IN ORDER TO EXPORT, RE-EXPORT, TRANSFER IN COUNTRY OR IMPORT AFTER DELIVERY TO YOU.

Symantec Corporation

350 Ellis Street
Mountain View, CA 94043

www.symantec.com

9/21/2018

Contents

Acceleration Concepts	10
What is the Blue Coat Acceleration Solution?	10
What is WAN Optimization?	11
What are the MACH5 Deployment Types?	12
What are Acceleration Tunnels?	14
What is Traffic Acceleration on the MACH5?	15
<i>Intercepting a Service</i>	15
<i>Traffic Modes</i>	15
<i>Levels of Acceleration</i>	15
<i>Acceleration Techniques</i>	16
What is Service Interception?	17
What is Client IP Address Reflection?	17
What is Connection Forwarding?	19
What is Caching?	20
What are Proxies?	20
Getting Started	21
What is the Blue Coat Sky User Interface?	21
<i>Tabbed Interface</i>	21
<i>Panels</i>	22
<i>Saving and Undoing Changes</i>	22
<i>"Advanced" Buttons</i>	22
<i>Interaction Between Blue Coat Sky and the Management Console</i>	22
<i>Advanced Configuration and Reporting</i>	23
Get Started with Acceleration	24
<i>Prepare for an Acceleration Deployment</i>	24
<i>Integrate the Appliance into the Network</i>	27
<i>Configure Acceleration</i>	32
<i>Define the Applications to Accelerate</i>	34
<i>Verify the Acceleration Deployment</i>	35
<i>Configure Network Connectivity</i>	39
<i>Configure and Test the Bridge Mode on In-Path Appliances</i>	45
Manage the Appliance	47
Deploy the MACH5 Appliance	48
Select a Recommended Deployment	48
Deploy In-Path Acceleration Peers	49
<i>Deploy a Concentrator Peer In-Path</i>	50
<i>Deploy a Branch Peer In-Path</i>	56

Deploy Virtually In-Path Acceleration Peers	62
<i>What is WCCP?</i>	63
<i>Deploy a Concentrator Peer Virtually In-Path</i>	67
<i>Deploy a Branch Peer Virtually In-Path</i>	77
Redundant Acceleration Topology	83
<i>Deploy In-Path with Redundant Links</i>	84
<i>Deploy Virtually In-Path in a Redundant Layer 2 Network</i>	98
Acceleration Strategies	109
Reduce Bandwidth Usage	109
Accelerate Applications	110
Verify Application Acceleration	111
Define Exceptions for Traffic Management	113
What are Protocols?	114
Examples of Custom Services	116
<i>What is ADN Last Peer Detection?</i>	117
<i>What is the TCP Window Size?</i>	119
General Proxy Settings	120
HTTP Proxy	121
What is the HTTP Proxy?	121
Optimize Users' Web Experience	121
Streaming Media Proxies	123
What are the Streaming Media Proxies?	123
Fine Tune Streaming Proxy Settings	125
Improve Quality of Streaming Media	126
Control Streaming Media Traffic	126
Limit Bandwidth of Streaming Media	127
Accelerate Encrypted Flash Traffic	128
SSL Proxy	130
What is the SSL Proxy?	130
<i>Requirements</i>	130
Accelerate SSL Traffic	131
Encrypted MAPI Proxy	133
What is Encrypted MAPI?	133

Accelerate Encrypted MAPI Traffic	134
<i>Identify CAS Array to Optimize MAPI</i>	135
CIFS Proxy	136
What is the CIFS Proxy?	136
What is SMB Signing?	137
SMBv1	137
SMBv2	137
Accelerate CIFS	138
Accelerate CIFS by Pre-Populating the Cache	138
Thin Client Processing	139
What is Thin Client Processing?	139
Accelerate Citrix Traffic	140
<i>Enable Thin Client Processing</i>	141
<i>Disable Compression and Encryption on Citrix</i>	141
Accelerate Microsoft RDP Traffic	143
<i>Disable Compression and Lower Encryption on RDP</i>	143
Disable Compression and Encryption on RealVNC	145
Disable Compression and Encryption on NX	146
ISATAP Proxy	147
What is ISATAP?	147
What is the ISATAP Proxy?	150
Accelerate ISATAP Traffic	151
Configure the ISATAP Proxy	151
Verify ISATAP	152
<i>Verify ISATAP Processing</i>	153
<i>Verify ISATAP Optimization</i>	153
Secure the ADN	154
What is Secure ADN?	154
<i>Unmanaged ADN Security</i>	154
<i>Managed ADN Security</i>	155
What are the Acceleration Modes?	156
What are the Acceleration Roles?	157
Monitor WAN Optimization	159
Get Visibility into your Network Traffic	159

<i>Refresh Intervals for Sky Reports</i>	159
<i>Session Report Column Descriptions</i>	160
Monitor Bandwidth Utilization	164
Create Consolidated Traffic Reports using NetFlow	165
<i>Configure NetFlow</i>	165
<i>What is NetFlow?</i>	166
Maintain the MACH5 Appliance	168
What is Health Monitoring?	168
Alert Messages	169
<i>Device Health Alerts</i>	170
<i>Other Alerts</i>	172
Manage SGOS Images and Licenses	174
What is Software Version Management?	174
What is the Physical Appliance License?	175
<i>Trial Licenses</i>	175
<i>About License Expiration</i>	176
<i>Installing Permanent Licenses</i>	176
What is the Virtual Appliance License?	176
Solve a Problem	178
What tools are available to troubleshoot appliance issues?	178
How can I troubleshoot problems with TCP connections?	179
<i>Troubleshoot Bypassed Connections</i>	179
<i>Troubleshoot Intercepted Sessions</i>	181
Why is my network slow?	182
Why is all traffic being bypassed?	183
Why is ISATAP traffic being bypassed?	183
Why is all ISATAP traffic using the ISATAP Proxy?	184
Why are users seeing TCP connection errors in an ISATAP deployment?	184
Why is some traffic getting routed through the management port?	185
<i>About Preferred IP Selection</i>	185
<i>Configure a Preferred IP List</i>	186
Why is the device health reporting as Warning or Critical?	187
Why is the CPU usage so high?	187
<i>Configure Adaptive Compression</i>	188
Why is there a byte cache warning for a connection?	189
Why are old peers showing up in my byte-cache dictionary?	189

Why isn't the Flow Collector receiving NetFlow records?	190
Troubleshoot Duplicate Serial Numbers	191
<i>Resolving the Duplicate Serial Number Error Message</i>	<i>191</i>
Troubleshoot Stolen Time	192
<i>Recovering from Excessive Stolen Time Accumulation</i>	<i>192</i>

Acceleration Concepts

This chapter describes the concepts you need to understand before deploying a Blue Coat acceleration solution. It includes the following topics:

What is the Blue Coat Acceleration Solution?	10
What is WAN Optimization?	11
What are the MACH5 Deployment Types?	12
What are Acceleration Tunnels?	14
What is Traffic Acceleration on the MACH5?	15
Intercepting a Service	15
Traffic Modes	15
Levels of Acceleration	15
Acceleration Techniques	16
What is Service Interception?	17
What is Client IP Address Reflection?	17
What is Connection Forwarding?	19
What is Caching?	20
What are Proxies?	20

What is the Blue Coat Acceleration Solution?

Blue Coat's acceleration solution offers the following main benefits:

- Optimizes use of existing WAN bandwidth
- Improves application response times
- Improves the efficiency of application protocols
- Prioritizes the applications that matter most
- Reduces data transfer where possible
- Accelerates file sharing, email, and browser-based applications

An Application Delivery Network (ADN) is the core of Blue Coat's acceleration solution. An ADN defines the framework that enables application acceleration between various corporate sites separated by a WAN, with a MACH5 appliance located in each of the core and branch offices.

What is WAN Optimization?

WAN optimization is a set of technologies for accelerating, compressing, and securing application traffic across distributed network environments. As organizations and employees become more distributed, the productivity of users in branch and remote offices becomes increasingly important to the success of the business as a whole. WAN optimization enables fast, secure access to critical applications wherever users are working: at headquarters, in branch offices, or when traveling.

By deploying WAN optimization across the network, organizations can increase productivity and reduce costs. Server storage can be centralized into the data center—or outsourced entirely—to reduce management expenses without negatively impacting the end user experience. WAN costs can be contained and even reduced as repetitive data is removed from the WAN link. Branch users will no longer have to wait for applications and data delivered across the WAN, and data center backups will complete within their allotted window.

A WAN optimization solution should:

- Optimize use of existing WAN bandwidth
- Improve application response times
- Improve the efficiency of application protocols
- Prioritize the applications that matter most
- Reduce data transfer where possible
- Accelerate file sharing, email, and browser-based applications

An *Application Delivery Network* (ADN) is the core of Blue Coat's WAN optimization solution. An ADN defines the framework that enables application acceleration between various corporate offices separated by a WAN. In an ADN, MACH5 appliances are integrated into the network to provide visibility, acceleration, and control for all TCP (and UDP streaming) traffic sent over the WAN, including Web (HTTP), secure Web (SSL), file sharing (CIFS), Microsoft Outlook/Exchange (MAPI), DNS, live and on-demand streaming (RTSP, MMS, streaming over HTTP) traffic, and TCP-based applications.

Illustrated Acceleration Example

The following series of diagrams illustrate how acceleration works. Through byte caching, compression, protocol optimization, and object caching technologies, the acceleration solution reduces WAN traffic and improves the user experience.

(Dashed lines) The acceleration peers advertise their availability to the ADN manager.

User Jeff requests a PowerPoint presentation from a file share named ExampleCorpPresentations on a server located at the Data Center. The Branch peer intercepts the request and opens a connection to the Concentrator peer, which retrieves the content. The application is determined by policy to be mission-critical; the connection receives maximum allowed WAN bandwidth. The Concentrator peer optimizes the data and sends it back over the WAN and through the Branch peer, where the content is decompressed, cached, and sent to Jeff's system.

Jeff changes the content on two slides and saves the file. When Jeff saves the file, the data is transmitted from Jeff's system to the Branch peer, which caches the new file, compresses the data, and sends only the changed data (representing the two modified slides) over the WAN. The Concentrator peer decompresses the data and sends the updated file to the server.

An hour later, user Bob requests the same PowerPoint presentation. The Branch peer serves the updated file from the object cache after verifying with the server that its cached copy is current.

At the corporate campus, Maya retrieves the file from the ExampleCorpPresentations share and modifies some content.

Jeff requests the file again. This time, the Branch peer registers a partial cache hit, as most of the object data in the byte cache is unchanged. A check to the Concentrator peer indicates new object data (Maya's changes). Only the new content is retrieved over the WAN.

What are the MACH5 Deployment Types?

For acceleration to occur, all inbound and outbound TCP packets in the connection must pass through the MACH5 appliances at each end of the WAN (for example, at the branch office and at the data center). There are two recommended deployment types that allow the MACH5 appliance to receive packets for acceleration. Where you install your acceleration nodes and what deployment type you use at each site depends on your specific network topology and goals.

In-Path Deployment

In an in-path deployment, the MACH5 appliance is physically inserted into the path of the clients and servers—all traffic must pass through the appliance as shown in the drawing below. This is the recommended deployment type because it ensures that all traffic passes through the MACH5 appliance.

The in-path MACH5 appliance (ProxySG) intercepts the application traffic you want to optimize and bridges all other traffic. Generally, Blue Coat recommends using a hardware bridge and pass-through card for in-path deployments. This is because the hardware pass-through card has two interfaces that pass traffic when there is no power, enabling the MACH5 appliance to fail to a connected state without interrupting traffic.

If you plan to use multiple MACH5 appliances for redundancy at a given site, you can use a software bridge rather than installing a hardware bridge. Software bridges fail closed; that is, they do not pass traffic when there is no power. Because software bridges fail closed, you can use them in redundant deployments so that packets can be redirected to another MACH5 appliance for optimization.

In-path deployments work well at sites where:

- Network outages are acceptable during MACH5 appliance installation.
- Scalability at the site is not an issue.
- You want to be able to use [client IP reflection](#). (See "What is Client IP Address Reflection?" on page 17)
- You want to use [transparent tunnels](#). (See "What are Acceleration Tunnels?" on the facing page)

Virtually In-Path Deployment

In a virtually in-path deployment, the MACH5 appliance is not in the physical path of clients and servers, but relies on an external device (a switch or router) to redirect traffic to the MACH5 appliance. The illustration below shows an example of a virtually in-path deployment in which a router redirects packets to the MACH5 appliance.

There are several ways to deploy aMACH5 appliance virtually in-path including Web Cache Communication Protocol (WCCP), Layer 4 switches, or policy-based routing (PBR). Blue Coat recommends using WCCP to deploy a MACH5 appliance virtually in-path. Note, however, that this requires Cisco routers/switches that support WCCP.

Virtually in-path deployments work well at sites where:

- Network outages are not acceptable during MACH5 appliance installation.
- WCCP-capable routers and switches are in use.
- You don't want the MACH5 appliance in the physical data path.
- Ease of scalability is important.
- You want to be able to use [client IP reflection](#). (See "What is Client IP Address Reflection?" on page 17)
- You want to use [transparent tunnels](#). (See "What are Acceleration Tunnels?" on the facing page)
- The MACH5 appliance must not be a single point of failure.

What are Acceleration Tunnels?

When a Branch peer intercepts application traffic for optimization, it initiates a TCP connection with the Concentrator peer at the site hosting the application server. This TCP connection between acceleration peers is called an *acceleration tunnel*.

There are three types of acceleration tunnels as described in the table below. The tunnel type determines the extent to which the packet header information (source IP address, destination IP address, and destination port) from the original packet is retained as the packet travels from client to server across the network.

Tunnel Type	Description
Transparent	With a transparent tunnel connection, the original destination IP address and port are maintained. Depending on the desired level of transparency, the connection over the WAN can use the original client's IP address or the IP address of the Branch peer. Transparent tunnels are enabled by default; no additional configuration is required. To use transparent tunnels, both the Branch peer and the Concentrator peer must be deployed in-path or virtually in-path. Transparent tunnels are not reused, therefore the MACH5 appliance must use additional resources to create new tunnels.
Translucent	With a translucent tunnel connection, the Branch peer uses its own address as the source IP address and the Concentrator peer's IP address as the destination IP address while retaining the destination port of the server. When you use translucent acceleration tunnels, all client traffic is aggregated at the Concentrator peer and you cannot determine traffic use by a specific client, but you will be able to see overall traffic by server ports. Use translucent tunnels when the Branch peer is in-path or virtually in-path and the Concentrator peer is out-of-path and there is a need to preserve WAN statistics by service port.
Explicit	With an explicit tunnel connection, the Branch peer uses its own address as the source IP address and the Concentrator peer's IP address as the destination IP address. Additionally, it uses a destination port number of 3035 (plaintext) or 3037 (secure). Explicit tunnels do not provide granular metrics about which servers and clients use the most network resources. If you are connecting to a Concentrator peer that is deployed out-of-path, you must use explicit or translucent tunnels.

To establish the tunnel, the ADN Concentrator peer and the ADN Branch Peer must be able to communicate over the tunnel listening port, which is 3035 (plaintext) or 3037 (secure) by default. In an out-of-path deployment, the explicit tunnel and the control connection is established on this port. On an in-path or virtually-in path deployment, the control connection for the transparent or translucent tunnel is established on this port. If the ADN Concentrator peer and the ADN Branch peer cannot communicate over this control connection, byte-cache dictionary synchronization and other non-application-related activities will fail.



Acceleration devices identify transparent and translucent tunnels by placing a value inside the TCP headers. Network devices that remove or modify values found in the fields of the TCP header will cause these tunnels to fail. Intermediary network devices that perform deep packet inspection or NAT firewalls might remove required TCP option information.

What is Traffic Acceleration on the MACH5?

Using the MACH5 appliance's traffic management capabilities, you can define acceleration rules for handling the different types of traffic flowing through the device. These rules determine whether a specific type of traffic (a service) is accelerated and which types of acceleration techniques are applied. Blue Coat Sky delivers pre-configured rules, but you have the freedom to modify them if you like. By accelerating network services, you can reduce the amount of traffic that traverses the WAN, effectively making more bandwidth available without upgrading the link size.

Intercepting a Service

When the MACH5 appliance *intercepts* a service for acceleration, it applies any of several [techniques](#) to optimize/accelerate the traffic. When a service passes through the MACH5 appliance without being controlled in any way, the traffic is *bypassed*. The MACH5 appliance applies default intercept/bypass settings to the services that it recognizes: *Intercept* for those services that can benefit from optimization and *Bypass* for those that pass through the MACH5 appliance without processing. Some services are set to bypass by default, but could benefit from interception—you can decide whether you want/need to accelerate any of these services. Note that these services may require specific knowledge of the local network environment.

See [Modify a Service's Acceleration Setting](#).

Traffic Modes

In *acceleration mode*, the MACH5 appliance attempts to optimize all services that have interception enabled. If you answer yes to the question about activating acceleration in the configuration wizard, acceleration mode will be enabled. In *bypass mode*, intercept settings are ignored and all traffic passes through the MACH5 appliance without any attempt at optimization. If you answer no to the acceleration question, bypass mode will be selected.

- **Acceleration mode:** honors the service configuration and intercepts the specified services
- **Bypass mode:** Ignores intercept settings; disables acceleration

See [Select the Traffic Mode](#).

Levels of Acceleration

There are three levels of acceleration: Application, Data, and Network. The MACH5 appliance assigns a default acceleration level appropriate for each intercepted service.

- **Application:** Utilizes protocol-specific optimizations. Depending on the protocol type, one or more of the following techniques is used to accelerate the traffic in that service: network optimization, byte caching, compression, object caching, protocol optimization.
- **Data:** Reduces bandwidth usage for most types of TCP traffic in the service.

- **Network:** Improves handling of packet loss and congestion. Network level accelerates traffic that cannot be accelerated at higher levels.

Acceleration Techniques

The MACH5 appliance can perform the following types of acceleration.

Method	Description
Network optimization	On high-latency networks or networks experiencing packet loss, the appliance improves network efficiency and relieves congestion by adjusting TCP window sizes.
Byte caching	Replaces byte sequences in traffic flows with reference tokens. The byte sequences and the token are stored in a byte cache on a pair of MACH5 appliances (for example, one at the branch, the other at the data center). When a matching byte sequence is requested or saved, the MACH5 appliance transmits the token instead of the byte sequence. By eliminating repeated patterns of non-cacheable data (or data going over protocols for which a proxy isn't available) from being sent across the WAN, byte caching allows further reduction in WAN bandwidth. The byte cache can be populated by data sent in either direction, and matches can also occur on data flowing in either direction.
Compression	GZIP compression removes extraneous/predictable information from traffic before it is transmitted. The information is decompressed at the destination's MACH5 appliance.
Object caching	The MACH5 appliance caches HTML pages, images, streaming content, and CIFS file data so that it can serve this data directly to clients; object caching saves time and bandwidth since the content needn't be accessed repeatedly across the WAN.
Protocol optimization	Application-layer optimizations use techniques such as read-ahead, pipelining/prefetch, and meta-data caching to reduce "chattiness" in network protocols (such as HTTP and CIFS).
Bandwidth management	Prioritizes and/or limits bandwidth by user or application, allowing WAN usage to reflect business priorities. You can create bandwidth rules using over 500 attributes, such as application, website, URL category, user/group, and time/priority.



Override rules (such as static bypass and restricted intercept) can also be established. See [Add Static Bypass Rules](#) and [Add Restricted Intercept Rules](#).)

What is Service Interception?

A proxy service is a logical grouping of traffic flows that share the same characteristics, such as a specific application or protocol. FTP, HTTP, HTTPS, and RTSP are all services that the MACH5 appliance recognizes.

To manage a particular type of traffic, the appliance must intercept the service for that traffic. When a service is intercepted, the MACH5 appliance looks for that type of traffic and upon detection, intercepts the connection, initiates a new connection to the traffic destination and retrieves the content, and performs an action (such as compression or caching) before delivering the content to the user.

In an in-path deployment, the appliance intercepts specific protocols such as FTP, HTTP, HTTPS, and RTSP. In an explicit deployment, the appliance intercepts the Explicit HTTP service. If needed you can change the service intercept settings.

When a service passes through the appliance without being controlled in any way, the traffic is *bypassed*. In other words, services that aren't intercepted are bypassed. If you set any of the standard services to bypass, the appliance will not monitor or control that traffic. Network traffic that isn't associated with any of the standard services is automatically bypassed.

What is Client IP Address Reflection?

By default, the Branch peer uses its own IP address when creating a tunnel connection with a Concentrator peer. However, in some deployments you can configure the acceleration nodes so that the client IP address is retained. This process is called *client IP address reflection*.

Blue Coat recommends configuring client IP address reflection whenever possible because it provides maximum visibility for network usage statistics and enables user-based access control to network resources.

The deployment type and tunnel type determines whether you can use client IP address reflection. The table below summarizes the possible tunnel type-deployment type combinations and indicates whether client IP address reflection can be achieved in each.

Branch peer > Concentrator peer Deployment Types	Supported Tunnel Types	Client IP Reflection to Server?
in-path to in-path	Transparent	Yes
in-path to virtually in-path or virtually in-path to in-path	Explicit Translucent	
virtually in-path to in-path		
virtually in-path to virtually in-path		
in-path to out-of-path	Explicit Translucent	No
virtually in-path to out-of-path		

The following sections detail the client IP address reflection behavior across the various tunnel types:

Client IP Address Reflection Across Transparent Tunnels

When you configure client IP address reflection with transparent tunnels, there are three tunnel subtypes that determine the extent to which the client IP address is preserved along the route from the peer to the destination application server. Note that in all three subtypes, the destination port and destination IP address are always preserved throughout the transaction; the only difference is how, or if, the client IP address is preserved. Each transparent tunnel subtype is detailed in the table below.

Transparency Level	Description
Basic	Basic transparent tunnels do not reflect the client IP address. This is the default transparent tunnel type and it requires no configuration.
Partially Transparent	Partially transparent tunnels reflect (that is, preserve) the client IP address from the Branch peer to the Concentrator peer, but not to the origin content server (OCS) (see Figure 1-3). In this configuration, you only need to configure the client IP address reflection options on the Branch peer. Use partially transparent tunnels when you want to avoid asymmetric routing conditions on the Concentrator (data center) location.
Fully Transparent	<p>Fully transparent tunnels preserve the client IP address, destination IP address, and port information across the WAN to the application server (see Figure).</p> <p>Fully transparent tunnels provide the most accurate network monitoring metrics because the client's IP address, destination port, and destination IP address are preserved throughout the transaction. Therefore, you should use fully transparent tunnels when maximum network control and granularity are required, such as when using ACLs or other forms of authentication or when you want to capture accurate network monitoring statistics (such as NetFlow data).</p>

Client IP Address Reflection Across Translucent Tunnels

Translucent tunnels with client IP address reflection preserve the original destination port across the WAN. Across the WAN, the source IP address is the address of the Branch peer and the destination IP address is the address of the Concentrator peer as detailed in the table below. When the Concentrator peer connects to the OCS, it will spoof the original client's IP address.

Packet Header Field	Value
Source IP Address	Branch peer's IP address across WAN; client's IP address from Concentrator peer to OCS
Destination IP Address	Concentrator peer's IP address
Destination Port	Original port specified in client packet (for example, port 80 for HTTP)

Client IP Address Reflection Across Explicit Tunnels

Explicit tunnels with client IP address reflection do not preserve any attribute of the original client's request across

the WAN. Across the WAN, the source IP address is the Branch peer's address and the destination IP address is that of the Concentrator peer as shown in the following table. When the Concentrator peer connects to the OCS, it will spoof the original client's IP address.

Packet Header Field	Value
Source IP Address	Branch peer's IP address across WAN; client's IP address from Concentrator peer to OCS
Destination IP Address	Concentrator peer's IP address
Destination Port	3035 for plain text data 3037 for secure data (when security features are configured and enabled)

The figure below shows how client IP address reflection works across the different tunnel types.

What is Connection Forwarding?

TCP Connection Forwarding is a Blue Coat feature that enables MACH5 appliances to share TCP connection information and selectively forward TCP connections to other MACH5 appliances. Connection Forwarding is useful in transparent deployments where asymmetric routing conditions exist. An asymmetric route is one in which the path from client to server is different than the return path from server to client. Asymmetric routes are common in networks with external load balancing or redundant routes when client IP reflection is enabled.

In asymmetric routing conditions, Connection Forwarding is a simple solution that resolves a complex network routing problem. Using Connection Forwarding to track connections, administrators do not need to reconfigure switches and/or routers to ensure that connections are routed to the correct appliance.

The figure below illustrates the Connection Forwarding process.

Connection Forwarding requires two or more MACH5 appliances configured as peers. To create a Connection Forwarding group, each MACH5 must be configured with the IP addresses of all other MACH5 appliances in the group. This enables all of the group members to share TCP connection information, allowing them to identify which connections exist on which appliances. When a group member receives a connection it either processes it or forwards to another peer in the group using IP-in-IP encapsulation (similar to Generic Route Encapsulation).

What is Caching?

With object caching, an object is saved locally so that it can be served for future requests without requiring retrieval from the origin content server (OCS) on the Web. These objects can be PDFs, videos, or images on a Web page, to name just a few. When objects are cached, the only traffic that needs to go across the Internet are permission checks (when required) and verification checks that ensure that the copy of the object in cache is still fresh. By allowing objects to be shared across requests and users, object caching greatly reduces the bandwidth required to retrieve contents, minimizes the latency associated with user requests, and significantly increases performance.

To improve response times for frequently accessed content, the MACH5 appliance stores the objects in a cache on its hard drives. The appliance can serve requests without contacting the OCS by retrieving content saved from a previous request made by the same client or another client.

What are Proxies?

The MACH5 appliance is a *proxy server* that acts as an intermediary for requests from clients in a local network wanting to download or access information from origin content servers (OCS) on the Web. A client makes a request to an OCS, but the appliance, acting as a proxy server, processes the request. Content is placed in the cache to be provided to other users, and the proxy provides the file to the user who requested the content.

The MACH5 appliance contains a number of protocol-specific proxies for managing different types of traffic, such as HTTP, CIFS, SSL, and streaming.

Getting Started

This chapter explains how to get started with your Blue Coat acceleration solution. It includes the following topics:

What is the Blue Coat Sky User Interface?	21
Tabbed Interface	21
Panels	22
Saving and Undoing Changes	22
"Advanced" Buttons	22
Interaction Between Blue Coat Sky and the Management Console	22
Advanced Configuration and Reporting	23
Get Started with Acceleration	24
Prepare for an Acceleration Deployment	24
Integrate the Appliance into the Network	27
Configure Acceleration	32
Define the Applications to Accelerate	34
Verify the Acceleration Deployment	35
Configure Network Connectivity	39
Configure and Test the Bridge Mode on In-Path Appliances	45
Manage the Appliance	47

What is the Blue Coat Sky User Interface?

This topic describes the characteristics of the Blue Coat Sky user interface.

Tabbed Interface

Blue Coat Sky has a tabbed interface with features organized into three tabs.


- **Report tab**—offers reports that provide detailed information about traffic on the MACH5.
- **Configure tab**—includes settings for configuring acceleration and pre-population.
- **System Settings tab**— includes controls for configuring your system time, interfaces, gateways, DNS servers, and WCCP. There are also tools for loading new versions of software, installing licenses, and troubleshooting.

Panels

Some screens in the user interface have collapsible and expandable panels. Click the icon to the left of the panel name to expand the panel to view its contents; click the icon to collapse the panel when you are finished.

Saving and Undoing Changes

Each configuration/settings screen in the user interface has two buttons: **Commit all** and **Undo all**, located in the top right of the screen.

Blue Coat Sky does not require that you save configuration changes before proceeding to another screen in the user interface. In the left navigation pane, a  icon appears next to any items that you have changed, but not yet saved. The **Commit all** button saves any configuration changes you have made on all screens. When you log out, you will be prompted to save your changes if you have forgotten to use the **Commit all** button.

When you click the **Commit all** button, all field entries are automatically validated and saved. The system will not allow you to save entries that include errors.

Caution: Clicking the browser's refresh, back, or forward buttons will discard any uncommitted configuration settings.

You also have an option to undo your unsaved settings with the **Undo all** button. This button discards any changes you have made and not yet committed.

"Advanced" Buttons

In relevant locations throughout the Blue Coat Sky user interface, there are buttons for **Advanced configuration**, **Advanced settings**, and **Advanced statistics**. These buttons open a new window for the full-featured Advanced Management Console so that you can do additional configuration tasks or view advanced statistical reports not available in the streamlined Blue Coat Sky user interface. See "Advanced Configuration and Reporting" on the facing page.

Interaction Between Blue Coat Sky and the Management Console

Care must be taken when the Blue Coat Sky and the Advanced Management Console browser windows are open at the same time, and you are making configuration changes in both user interfaces. Configuration changes will *not* automatically synchronize between the two interfaces.

Blue Coat recommends that you make configuration changes to one user interface at a time, and save your configuration changes before leaving the interface. Here is a suggested workflow when you find it necessary to make configuration changes in both user interfaces:

1. In Blue Coat Sky, make your configuration changes and save them (**Commit all**).
2. Open the Advanced Management Console, make your configuration changes and save them (**Apply**).
3. Refresh your Blue Coat Sky browser window to incorporate the changes made in the Advanced Management Console.

By following the workflow above, you can avoid losing configuration changes.

It's important to understand how certain actions in Blue Coat Sky relate to configuration changes in the Advanced Management Console:

- **Commit all**—Clicking **Commit all** saves all the configuration changes you have made in Blue Coat Sky and incorporates any configuration changes that were saved in the Management Console. If there are any conflicting changes made in the two user interfaces, the Blue Coat Sky changes override those made in the Management Console.
- **Undo all**—Clicking **Undo all** backs out any uncommitted configuration changes made in Blue Coat Sky and incorporates the configuration changes that were saved in the Management Console. Note that the **Undo all** button in Blue Coat Sky does *not* undo configuration changes made in the Management Console.
- **Refresh**—Clicking the browser's refresh button incorporates any configuration changes that were saved in the Management Console. Note that the browser's refresh button will display the Monitor tab after updating the configuration. Do not use the refresh button if you have any unsaved changes in Blue Coat Sky.
- **Log out / Log in**—Each time you log in to Blue Coat Sky, the configuration will be refreshed with any changes made and saved in the Management Console.

Advanced Configuration and Reporting

Blue Coat Sky is a streamlined user interface that offers reports and configuration options specifically applicable to customers using the MACH5 appliance for WAN optimization. The full-featured Management Console (referred to here as the Advanced Management Console, or simply MC) is still available for more advanced configuration and reports and is typically just a button-click away. Just look for the **Advanced configuration**, **Advanced settings**, and **Advanced Statistics** buttons in Blue Coat Sky. For example, the bottom of the Configure tab's navigation pane has an **Advanced configuration** button that opens up a window for the Advanced Management Console, with the Configuration tab displayed; you will need to go here to configure VLANs, policies, failover, load balancing, and other advanced configuration settings. Similarly, the Blue Coat Sky Report tab offers an **Advanced statistics** button that displays the Statistics tab in the Advanced Management Console.

Because Blue Coat Sky contains a subset of the options available in the Advanced Management Console, some Sky users may find it necessary to go to the MC for advanced configuration. When related settings have been configured in the MC, a message or icon may appear indicating that a custom or advanced configuration exists. For example, on the Traffic Management configuration page, the Custom icon appears for the acceleration method of

some of the services. Clicking the link or icon opens a window to the applicable page in the Advanced Management Console.

See also "Interaction Between Blue Coat Sky and the Management Console" on page 22.



To go to the Advanced Management Console directly (without using the links and buttons in Blue Coat Sky), type the following:

`https://<ip-address>:8082/mgmt`

The default HTTPS console port is 8082. If you changed the port number, substitute the one you configured.

Get Started with Acceleration

To deploy your MACH5 appliances as acceleration nodes, you must complete the following basic tasks. The way you complete the tasks will depend on the [deployment type](#) you have selected. (See "What are the MACH5 Deployment Types?" on page 12)



For best results, use one of the deployments that has been tested and recommended by Blue Coat. For step-by-step examples that show how to set up the Blue Coat-recommended deployments, see "Select a Recommended Deployment" on page 48.

1. "Prepare for an Acceleration Deployment" below.
2. "Integrate the Appliance into the Network" on page 27.
3. "Configure Acceleration" on page 32.
4. (Branch peers only) "Define the Applications to Accelerate" on page 34.
5. "Verify the Acceleration Deployment" on page 35.

Prepare for an Acceleration Deployment

Before you can configure acceleration, you must plan your deployment. What applications do you want to optimize? How many MACH5 appliances do you need to install? Where are you going to install them? What deployment type will work best at each site? What do you need to do to make your appliances work with your other network equipment? Complete the following planning and preparation steps to ensure a successful acceleration deployment.

1. Make sure you have considered the number of users and amount of traffic generated by each site so that you can correctly determine which MACH5 platform you need and the number of appliances required at each site

When planning your ADN, you must determine where MACH5 appliances are required based on where your application servers are running, where the clients that use the applications are located, and whether the particular applications can benefit from ADN optimization.

As a general rule, you must deploy at least one MACH5 appliance at the sites where the remote clients are located and one MACH5 at the sites hosting your application servers. Depending on the number of concurrent users for a particular application, you may need additional MACH5 appliances at the sites to provide load balancing.

2. Choose your deployment type if you have not already done so. (See "What are the MACH5 Deployment Types?" on page 12)
3. Complete the configuration worksheets that pertain to your deployment:
 - "Plan the Configuration of the Concentrator Peers" on page 54
 - "Plan the Configuration of Branch Peers" on page 61
 - "Plan WCCP Configuration" on page 73 (for virtually in-path deployments)
 - "Plan Configuration of Acceleration Peers" on page 90 (for redundant deployments)
4. Make sure all appliances are running the same version of SGOS. Blue Coat recommends that you upgrade all appliances to SGOS 6.2 or higher and then restore them to the factory default state before starting the acceleration configuration. This ensures that all acceleration peers are compatible and that can all take advantage of the latest acceleration enhancements. See Upgrade/Downgrade an SGOS Image.
5. Decide what [acceleration mode](#) you want to use. By default, the appliances operate in an Open unmanaged mode. If you want to use an Open managed or Closed acceleration network, you must install and configure an ADN Manager before you configure your other acceleration nodes. See Configure the ADN Managers.
6. Test network connectivity between all sites where you plan to install acceleration nodes. From a client at each site, make sure you can ping the other sites.
7. Ensure compatibility with other network equipment:
 - If you have a firewall between sites, make sure the port required for acceleration nodes to communicate (the tunnel listening port) is open. By default this port is set to 3035 (plain) and 3037 (secure).
 - (virtually in-path deployments only) Verify that the Cisco model hardware and IOS version supports the WCCP features required for this deployment. See "WCCP Tested Platforms" on page 74 for a list of the Cisco hardware and software platforms and WCCP capabilities that have been tested with the MACH5 appliance.

- (redundant deployments only) Make sure all routers are configured with Hot Standby Routing Protocol (HSRP).
8. If you will be installing MACH5 appliances in-path, make sure you have scheduled a network downtime window so that you can install the appliance(s) into the physical data path.
 9. Define a plan for testing each of the applications that you will be intercepting so that you will be able to determine whether the application is being optimized as expected. You will need a separate test plan for each application, which includes identifying test clients and test servers for each application.

Plan the Configuration of the Concentrator Peers

Use the [Concentrator Peer Configuration Worksheet](#) to record the information you need to gather before installing a MACH5 appliance that will act as a Concentrator peer only (that is, it will not be intercepting client application traffic). Record the information you need to perform the initial installation and configuration of the MACH5, such as the required network addresses, the switch port and router interface to which to connect the MACH5, and the link settings you must configure on the MACH5 (they must match the settings defined on the switch/router to which you are connecting the appliance). In addition, if you use a non-native VLAN for management traffic, you should record the VLAN ID here.

Complete a separate worksheet for each Concentrator peer you plan to deploy.



The [worksheet](#) is an interactive PDF form that you can fill in on screen before printing. You may also want to save the completed worksheet file for future reference.

Plan the Configuration of Branch Peers

Use the [Branch Peer Configuration Worksheet](#) to record the information you need to gather before installing a MACH5 appliance as a Branch peer.



The [worksheet](#) is an interactive PDF form that you can fill in on screen before printing. You may also want to save the completed worksheet file for future reference.

This worksheet includes the following sections:

Network Configuration Information—Record the information you need to perform the initial installation and configuration of the MACH5, such as the required network addresses, the switch port and router interface to which to connect the MACH5 LAN and WAN ports, and the link settings you must configure on the MACH5 (they must match the settings defined on the switch/router to which you are connecting the appliance). In addition, if you use a non-native VLAN for management traffic, you should record the VLAN ID here.

Service Configuration Information—Identify the services (and the corresponding port numbers) that the appliance needs to intercept. In addition, you must identify a client and a server to use to test whether each service is being optimized properly. For example, if you will be optimizing CIFS traffic, you should identify a Microsoft Windows

client and server to use to test the file sharing operations, such as opening a file on a remote application server, modifying the file on the client, and saving the file back to the file share. You will need to identify similar types of tests for each application that you plan to intercept and you will need to identify a client and a server to use to conduct these tests.

Complete a separate worksheet for each Branch peer you plan to deploy.

Plan WCCP Configuration

If you are deploying the MACH5 appliance virtually in-path, you must plan your WCCP deployment. To configure WCCP, you must define settings on both the WCCP-capable Cisco router(s) and the MACH5 appliance(s) that make up the redirection service group. The WCCP service group on the router and on the MACH5 define what traffic the router should redirect, the method the router should use to forward packets to the MACH5 appliance, and the algorithm to use to choose a MACH5 to which to redirect traffic. For more detailed information about WCCP and the settings you can define, refer to the *WCCP Reference Guide*.

To simplify the WCCP configuration process, record the settings you plan to use for each service group on the [WCCP Configuration Worksheet](#).



The [worksheet](#) is an interactive PDF form that you can fill in on screen before printing. You may also want to save the completed worksheet file for future reference.

For each service group, this worksheet includes the following sections:

Router Configuration for Service Group—Define the routers that are part of the service group. For each router, record the interfaces on which you will enable redirection and the interface to which the ProxySG MACH5 appliance will connect.

ProxySG Configuration for Service Group—Define the WCCP settings for the service group, including what ProxySG interface to include in the service group, what forwarding/return method the router will use to forward redirected packets to the ProxySG, the assignment type the router will use to pick a ProxySG to receive the redirected packet, and the IP addresses of the router(s) in the service group. Note that the WCCP settings that are supported vary greatly from router to router. To determine what features are supported on your specific routing/switching platform, refer to the documentation for your specific hardware platform and IOS version.

This worksheet assumes that you have one router and one MACH5 in each service group. However, each service group may actually include multiple routers and/or MACH5 appliances (up to 32 of each). In addition, each router and each MACH5 can be configured with multiple service groups, each with a different set of redirection rules. Use as many worksheets as you need to document your planned WCCP service group settings.

Integrate the Appliance into the Network

You must complete the following tasks when integrating MACH5 appliances into the network as acceleration nodes. Note that the actual steps for each task may vary based on the deployment type and acceleration role of the appliance. (See "What are the MACH5 Deployment Types?" on page 12 and "What are the Acceleration Roles?" on page 157)

1. Set up network connectivity to the appliance. See "Configure Network Connectivity" on page 39 .
2. Rack mount the MACH5 appliance. Refer to the *ProxySG Quick Start Guide* for instructions.
3. Cable the MACH5 appliance in the network. See "Cable the Appliance" below.
4. (in-path deployments only) Ping a host at the remote site to ensure that traffic is passing through the MACH5 appliance.
5. Power on the appliance and then launch Blue Coat Sky. See Log in to the .
6. (virtually in-path deployments only) Configure WCCP on the router and on the MACH5. See Configure WCCP.
7. Verify the link settings. See "Verify Link Settings" on page 30.
8. Check the health state of the appliance. See "Check the Health State of the Appliance" on page 31.
9. Conduct network connectivity tests. See "Conduct Network Connectivity Tests" on page 31.

Configure Network Connectivity

The procedure for configuring the basic network information on the MACH5 appliance varies depending on whether you are configuring the appliance in-path or virtually in-path. Use one of the following procedures to configure the basic settings:

- Configure Basic Network Information for an In-Path Acceleration Peer
"Configure Basic Network Information for an In-Path Acceleration Peer (Serial Console)" on page 54 or "Configure Basic Network Information for an In-Path Acceleration Peer (Web Wizard)" on page 42
- "Configure Basic Network Info for a Virtually In-Path Acceleration Peer" on page 75



The procedures that follow assume that you are running SGOS version 6.4 or higher. If you are not running SGOS version 6.4 or higher on all MACH5 appliances that you plan to deploy as acceleration nodes, you should upgrade them before proceeding. See Upgrade/Downgrade an SGOS Image.

In addition, you must restore the appliance to the factory default settings before configuring it as an acceleration node. To do this, enter the **restore-defaults** **factory-defaults** command from the CLI (config) prompt.

Cable the Appliance

The way you cable the appliance depends on the deployment type:



With in-path deployments, there will be some network downtime when installing the MACH5 appliance.

In-path deployments:

1. Install the pass-through card before cabling the appliance. For more information, refer to the pass-through card installation instructions for your platform.
2. Connect the MACH5 LAN interface to the switch using a straight-through cable.
3. Connect the MACH5 WAN interface to the router using a crossover cable.

Virtually in-path deployments:

Connect the MACH5 LAN interface to the switch/router as follows:

- If you are connecting to a switch, use a straight-through cable.
- If you are connecting to a router, use a crossover cable.



You must attach the MACH5 LAN interface to a dedicated network reachable by the Cisco router; do not attach the MACH5 appliance to a network that will traverse a router interface on which you plan to configure WCCP redirection. In addition, to use L2 forwarding/return on a Cisco Layer-3 switch, you must install the MACH5 appliance on the same broadcast domain as a dedicated Layer-3 interface on the switch.

WCCP Service Group States

If the router and the MACH5 appliance were able to successfully negotiate capabilities and form the service group, the group's state will be *Ready*. If the State column in the WCCP Configuration Status screen displays a different state, look it up in the tables below.

Service Group Formation States

The following states are typical messages you may see while service groups are in the process of forming.

State	Description
Initializing	WCCP was just configured and the MACH5 is getting ready to send out its first HERE_I_AM message.
Negotiating assignment	The MACH5 received the I_SEE_YOU message from the router, but has not yet negotiated the service group capabilities.
Negotiating membership	The MACH5 sent the HERE_I_AM message and is waiting for an I_SEE_YOU message from the router.

Service Group Problem States

The following states indicate the reason that the service group was not able to form. If you see one of the states listed below, you should fix the problem by either reconfiguring WCCP on the MACH5 or on the router so that the

settings match.

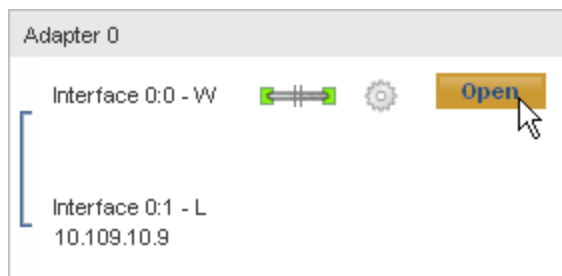
State	Description
Assignment mismatch	The router does not support the assignment type (hash or mask) that is configured for the service group.
Bad router ID	The home router specified in the service group configuration does not match the actual router IP address.
Bad router view	The list of MACH5 appliances in the service group does not match those in the router.
Capability mismatch	The WCCP configuration on the MACH5 includes capabilities that the router does not support.
Interface link is down	The MACH5 cannot send the HERE_I_AM message because the interface link is down.
Packet forwarding mismatch	The router does not support the forwarding method (GRE or L2) that is configured for the service group.
Packet return mismatch	The router does not support the return method (GRE or L2) that is configured for the service group.
Service group mismatch	The router and the MACH5 have a mismatch in port, protocol, priority, and/or other service flags.
Security mismatch	The service group passwords on the router and the MACH5 do not match.

Note: When a service group is in one of the above states, the following alert will display in the Alerts panel: *WCCP group state error found*. Because the MACH5 appliance won't be able to receive any redirected traffic from the router, this is considered to be a critical error.

Verify Link Settings

To verify that the configured link settings (speed/duplex) on the MACH5 interface match the configured settings on the connected switch/router interface:

1. Select **System Settings > Adapters & Interfaces**.
2. In the box that corresponds to the bridge that is connected to the switch or router in the **Adapter Overview** section of the tab, click **Open**.



3. Verify that the **Speed and duplex** settings match the settings that are defined on the router or switch interface.
4. Click **Close**.
5. If you made any changes, click **Commit all**.

Check the Health State of the Appliance

In the Blue Coat Sky banner, make sure the Device [health](#) is **OK**. If the device health is **Warning** or **Critical**, click the link to view details about the health issues. (See "What is Health Monitoring?" on page 168)



You can also view details about [alerts](#) by clicking a link in the **Alerts** panel in the right side of the Sky Management Console banner. (See "Alert Messages" on page 169.)



Conduct Network Connectivity Tests

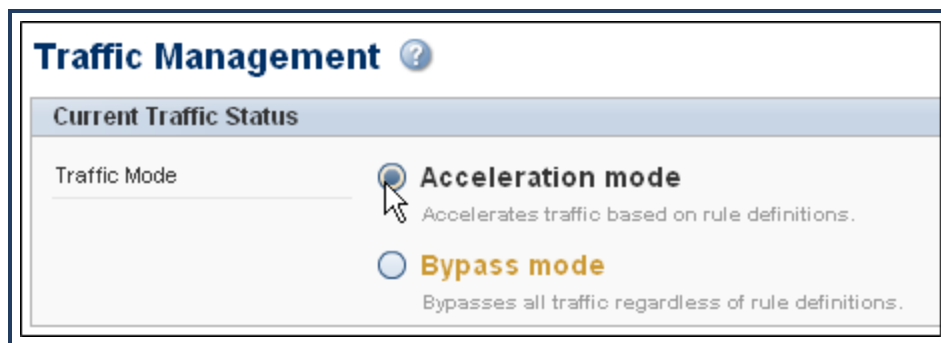
Before enabling acceleration, verify network connectivity by performing the following checkpoint tests:

1. On each MACH5 appliance, open a serial connection and launch the command-line interface (CLI).
 - a. Verify connectivity between sites by pinging a device at each remote acceleration site.
 - b. Test HTTP connectivity by entering the following command from the CLI: **test http get www.bluecoat.com**. If the test is successful, the request and response headers will display along with a message indicating that the test was successful.
2. From a client at each branch, verify HTTP connectivity from a browser. For example, verify that you can access the Blue Coat public Internet page by going to the following URL:
http://www.bluecoat.com.

3. From the Advanced Management Console on each acceleration node (https://<ProxySG_IP_address>:8082/mgmt), check for the following errors:
 - a. To check for cyclic redundancy check (CRC) errors, select **Statistics > Advanced > TCP > Show TCP/IP Statistics**.
 - b. To check for input/output errors select **Statistics > Network > Interface History**. Make sure there are not any errors on the **Input Errors** or **Output Errors** tabs.
4. Verify that the MACH5 appliance is bypassing traffic. by selecting **Statistics > Sessions > Active Sessions > Bypassed Connections**.

Configure Acceleration

1. If you did not enable acceleration during initial configuration, enable it now.
 - a. In Blue Coat Sky, select **Configure > Acceleration > Traffic Management**.
 - b. Select **Acceleration mode**.



- c. Click **Commit all**.



In Open configurations such as this one, you do not need to configure an ADN manager. If you want to change this deployment to an Open Managed or a Closed deployment, see "Switch Acceleration Modes" on the facing page.

2. **Enable client IP reflection.**

(Branch peers only) Verify that client IP reflection is enabled for outbound tunnel connections as follows:

- a. Select **Configure > Proxy Settings > General**.
- b. Verify that the **Reflect client's source IP when connecting to servers** checkbox is selected. This setting should be enabled by default if you specified that you would be using an acceleration deployment

during initial configuration. If it is not selected, select it now.

- c. If you made any changes, click **Commit all** to save the settings.

(Concentrator peers only) When a connection from a branch office has client IP reflection enabled, preserve the client IP when the MACH5 appliance is connecting to servers, as follows:

- a. Select **Configure > ADN > Concentrator**.



- b. Verify that **Preserve the client IP address when connecting to servers** is selected.
- c. Click **Commit all** to save the settings.

3. (Virtually in-path deployments only) Enable IP Forwarding.

- a. Click **Advanced configuration** to launch the Advanced Management Console.
- b. Select **Configuration > Network > Routing**.
- c. Select **Enable IP forwarding**.



- d. Click **Apply**.

Switch Acceleration Modes

The acceleration mode determines which peers an acceleration node can form tunnel connections with. When switching from one mode to another, you must consider the order in which you transition each node as described in the following sections.

Switching from a Closed ADN to an Open ADN

To switch the mode from Closed to Open, you simply uncheck the **Allow transparent tunnels only within this managed network** option on the ADN manager(s) as described in *Set ADN Mode to Open or Closed*.

Switching from an Open ADN to a Closed ADN

1. Configure an ADN manager, if one is not already enabled. See *Configure the ADN Managers*
2. Configure each ADN node that you want to be part of the Closed ADN to connect to the ADN manager(s). See *Select an ADN Manager for a Node*.
3. If any of the nodes need to advertise server subnets, set up the advertisements.
4. After you configure the ADN manager(s) and connect each node to them, change the ADN mode to Closed as described in *Set ADN Mode to Open or Closed*.

Define the Applications to Accelerate

The MACH5 appliance automatically intercepts a default set of services based on your deployment (explicit or transparent). However, you can customize the applications and services that get accelerated as follows:

1. From Blue Coat Sky, select **Configure > Acceleration > Traffic Management**.
2. Modify which services get intercepted and bypassed by selecting the radio button in the **Intercept** or **Bypass** column of the Services table as appropriate. You can only select services that can be accelerated.

Service name	Acceleration techniques	Intercept	Bypass	Edit	Del
BGP	Monitor only	<input type="radio"/>	<input type="radio"/>		
Blue Coat ADN	Monitor only	<input type="radio"/>	<input type="radio"/>		
Blue Coat Managem...	Monitor only	<input type="radio"/>	<input type="radio"/>		
OPFS	Application level	<input type="radio"/>	<input type="radio"/>		
Osco IPsec VPN	Monitor only	<input type="radio"/>	<input type="radio"/>		
OBric	Network level	<input type="radio"/>	<input type="radio"/>		
Default	Data level	<input type="radio"/>	<input type="radio"/>		
DNS	Application level	<input type="radio"/>	<input type="radio"/>		
Echo	Monitor only	<input type="radio"/>	<input type="radio"/>		
Endpoint Mapper	Application level	<input type="radio"/>	<input type="radio"/>		
Explicit HTTP	Application level	<input type="radio"/>	<input type="radio"/>		
External HTTP	Application level	<input type="radio"/>	<input type="radio"/>		
FTP	Application level	<input type="radio"/>	<input type="radio"/>		
FTPS	Monitor only	<input type="radio"/>	<input type="radio"/>		
H.323	Monitor only	<input type="radio"/>	<input type="radio"/>		

3. For tips on accelerating specific types of traffic, see the following topics:
 - "Optimize Users' Web Experience" on page 121
 - "Improve Quality of Streaming Media" on page 126

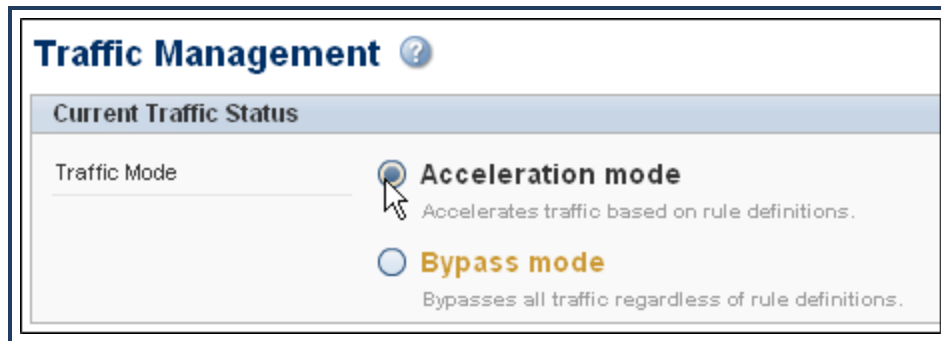
- "Accelerate CIFS " on page 138
- "Accelerate Encrypted MAPI Traffic" on page 134

Verify the Acceleration Deployment

The final step in an acceleration deployment is to verify that connectivity persists between the connected sites and that application traffic is optimized as expected. The following steps describe how to verify a successful acceleration deployment.

1. Verify that acceleration is enabled on each acceleration node.

- a. Launch Blue Coat Sky (https://<ProxySG_IP_address>:8082/sky).
- b. Select **Configure > Acceleration > Traffic Management**.
- c. If it's not already selected, select **Acceleration mode**.



- d. Click **Commit all** to save your changes.
- ### 2. Conduct network connectivity tests to ensure that the network is still functioning as expected.
- a. On each MACH5, open a serial connection and launch the command-line interface (CLI).

- Verify connectivity between sites by pinging a device at each remote acceleration site. For example, from the CLI enter **ping 10.110.10.102**.
- Test HTTP connectivity by entering the following command from the CLI: **test http get www.bluecoat.com**. If the test is successful, the request and response headers will display along with a message indicating that the test was successful.

```

Executing HTTP get test
* HTTP request header sent:
GET HTTP://www.bluecoat.com/ HTTP/1.0
Host: www.bluecoat.com
User-Agent: HTTP_TEST_CLIENT
* HTTP response header rcv'd:

```

```
HTTP/1.1 200 OK
Date: Mon, 04 Apr 2011 18:29:12 GMT
Server: Apache
X-Powered-By: PHP/5.2.8-pl1-gentoo
Last-Modified: Mon, 04 Apr 2011 18:20:15 GMT
ETag: "05b333772705b9a762259bdfc6bd73f2"
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: must-revalidate
Content-Type: text/html; charset=utf-8
Connection: close
Set-Cookie:
SESS1f24b8cf75f5ff2452d9394328af1ed2=b03e8d74d1ae546742f35bf7836364b
7; expires=Wed, 27 Apr 2011 22:02:32 GMT; path=/; domain=.bluecoat.com
Measured throughput rate is 511.99 Kbytes/sec
HTTP get test passed
```

- b. From a client at each branch, verify HTTP connectivity from a browser. For example, verify that you can access the Blue Coat public Internet page by going to the following URL:
<http://www.bluecoat.com>.
- c. From the Advanced Management Console on each acceleration node
(https://<ProxySG_IP_address>:8082/mgmt), check for the following errors:
 - To check for cyclic redundancy check (CRC) errors, select **Statistics > Advanced > TCP > Show TCP/IP Statistics**.

TCP/IP Interface Statistics ALL

Interface:	loopback
Maximum Transmission Unit (MTU) size	16384
Type of interface	AF_LINK
Ethernet address	N/A
Interface network address	Link#1
Device name	lo0
Link status	UP
Link duplex mode	HALF
Link speed	unknown
Link connector	unknown
Link type	unknown
Number of times interface was down	0
Packets received	2355598
Packets sent	2355598
Total number of bytes received	1565832480
Total number of bytes sent	1565832480
Input errors	0
Output errors	0
Packets received via multicast	0
Packets sent via multicast	0
Packets received via broadcast	0
Packets sent via broadcast	0
Dropped on input	0
Destined for unsupported protocol	0
Number of receive lockups	0
Receive CRC errors	0
Receive alignment errors	0
Receive resource errors	0
Receive overrun errors	0
Receive CDT errors	0
Receive short frames	0
Receive sequence errors	0

Bytes Sent Bytes Received Packets Sent Packets Received Input Errors Output Errors					
Interface	Bytes Sent	Bytes Received	Input Errors	Output Errors	
▶ 0:0	397.563 KB	14.817 MB	0	0	
▶ 0:1	0 B	0 B	0	0	

- d. (in-path deployments only) Verify that the MACH5 appliance is bridging bypassed traffic by going to the **Report > Acceleration Reports > Active Sessions** report and selecting **Bypassed Sessions** from the **Connection type** drop-down list). You should see connections for the services you are not accelerating.

3. Verify traffic acceleration.

- For each type of application that you have enabled for acceleration, run some test traffic from a client at each branch so that you can verify that the application is being accelerated successfully. For example, if you are accelerating CIFS traffic, open a shared folder on the application server and copy some files from the shared folder back to the client. Similarly, for HTTP traffic, request a Web page from the HTTP server at the remote site.
- After you run your test traffic for each application, launch Blue Coat Sky on each branch peer
- Select **Report > Acceleration Reports > Active Sessions**.
- Verify that all of the applications you tested show up as intercepted (select **Intercepted Sessions** from the **Connection type** drop-down list).
- (optional) Filter the list of active sessions by selecting a value from the **Filtered by** drop-down list.
- For each application or service, verify that acceleration is being applied. Look for colored icons in the **Comp**, **BC**, **OC**, **PO**, and **BWM** columns. Keep in mind, however, that not all acceleration techniques apply to all traffic types. Also some techniques, such as byte caching and object caching, require traffic to be flowing for some time before the benefits can be applied to individual sessions.

Compression (Comp)

Byte Caching (BC)

The Byte Caching Warning icon displays when a control connection with the peer is not established and the dictionaries are out of sync. This can happen, for example, in a transparent unmanaged ADN if the concentrator peer sends a control IP address that is not accessible from the branch peer. If you see this icon, you can fix the issue by specifying preferred IP addresses on the concentrator.

Object Caching (OC)

Protocol Optimization (PO)

Bandwidth Management (BWM)

4. After traffic has been running for some time, you can go back to the Report tab and verify WAN optimization on your network:

- The Bandwidth Savings report shows the percent of bandwidth saved due to various acceleration techniques on the MACH5 appliance. You can view reports that show bandwidth savings for all traffic or for a single service or proxy. See Analyze Bandwidth Savings.
- Use the Bandwidth Usage graph on the Traffic Summary report to verify reduction in WAN traffic. See View Traffic Summary.
- The Object Caching report shows the bandwidth savings gained from object caching. See View Benefits of Object Caching.
- The Active Sessions report lists the savings for each open session. See List Active Sessions.

Configure Network Connectivity

The procedure for configuring the basic network information on the MACH5 appliance varies depending on whether you are configuring the appliance in-path or virtually in-path. Use one of the following procedures to configure the basic settings:

- Configure Basic Network Information for an In-Path Acceleration Peer
"Configure Basic Network Information for an In-Path Acceleration Peer (Serial Console)" on page 54 or "Configure Basic Network Information for an In-Path Acceleration Peer (Web Wizard)" on page 42
- "Configure Basic Network Info for a Virtually In-Path Acceleration Peer" on page 75

The procedures that follow assume that you are running SGOS version 6.4 or higher. If you are not running SGOS version 6.4 or higher on all MACH5 appliances that you plan to deploy as acceleration nodes, you should upgrade them before proceeding. See Upgrade/Downgrade an SGOS Image.



In addition, you must restore the appliance to the factory default settings before configuring it as an acceleration node. To do this, enter the `restore-defaults factory-defaults` command from the CLI (config) prompt.

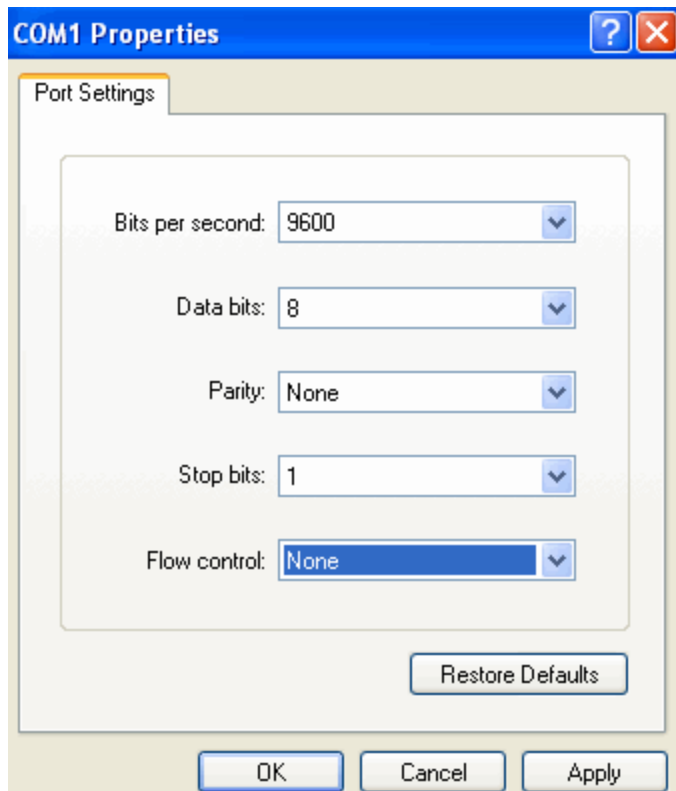
Configure Basic Network Information for an In-Path Acceleration Peer (Serial Console)

Use the following procedure to connect to the MACH5 appliance serial console and configure the basic network settings on an appliance that you plan to deploy in-path as an acceleration peer. You can use whatever terminal emulation software you want. This procedure shows how to perform initial configuration using Windows HyperTerminal.

Symantec Corp. MACH5 Acceleration Guide

1. To launch Windows HyperTerminal, select **Start > Programs > Accessories > Communications > HyperTerminal**.
2. (Optional) Name the connection for later use.
3. Select the communication port and set the communication parameters.

For example, select COM1 and set the communication parameters as shown below:



4. Click **OK** to save your settings.
5. Activate the serial console and launch the setup console for a manual setup.
 - a. Connect the serial cable from your laptop to the MACH5 and power on the appliance. The appliance will go through a bootup process. This may take a moment.
 - b. Press **Enter** three times to activate the MACH5 serial console.
 - c. When prompted, enter **2** to launch the setup console.
 - d. When prompted, enter **a** to initiate a manual setup.
6. Enter **a** to specify that you are configuring the appliance for acceleration.

Step 2: Which solution would you like to implement?

a) Acceleration
 b) Other solution
 Your choice: [] a

7. To specify an in-path deployment, enter **a**.

Step 3: How will you deploy this device?

a) Physically in-path
 b) Virtually in-path using WCCP
 c) Any other
 Your choice: []a

8. (optional) Enter the new name for the appliance when prompted or press **Enter** to accept the default name.

9. Configure the interface:

- a. When prompted, enter **y** to specify that you want to configure the inactive link.
- b. Enter the IP address.
- c. Enter the subnet mask.
- d. Press **Enter** to specify that you want the appliance to automatically detect speed/duplex settings.
- e. If you use a VLAN other than the native VLAN for your management traffic, enter **y** when prompted to configure a VLAN and then enter the VLAN ID when prompted.
- f. Press **Enter** to continue.

10. Configure other interfaces, if available. For example, if a four-port LAN option card is installed, you will need to configure the settings for each bridge pair. Each pair should be assigned a unique IP address.

11. Follow the prompts in the script to configure the default gateway address, DNS server address, and the administrator ID and password.

12. When prompted, press **Enter** to turn on acceleration immediately.

13. To save your settings, press **Enter**.



Be sure to configure IP addresses for physically-inline bridge interfaces, as well as for the management port if you are using it. If you configure an IP address for the management port only, some traffic may get inadvertently routed through this port instead of the expected interface.

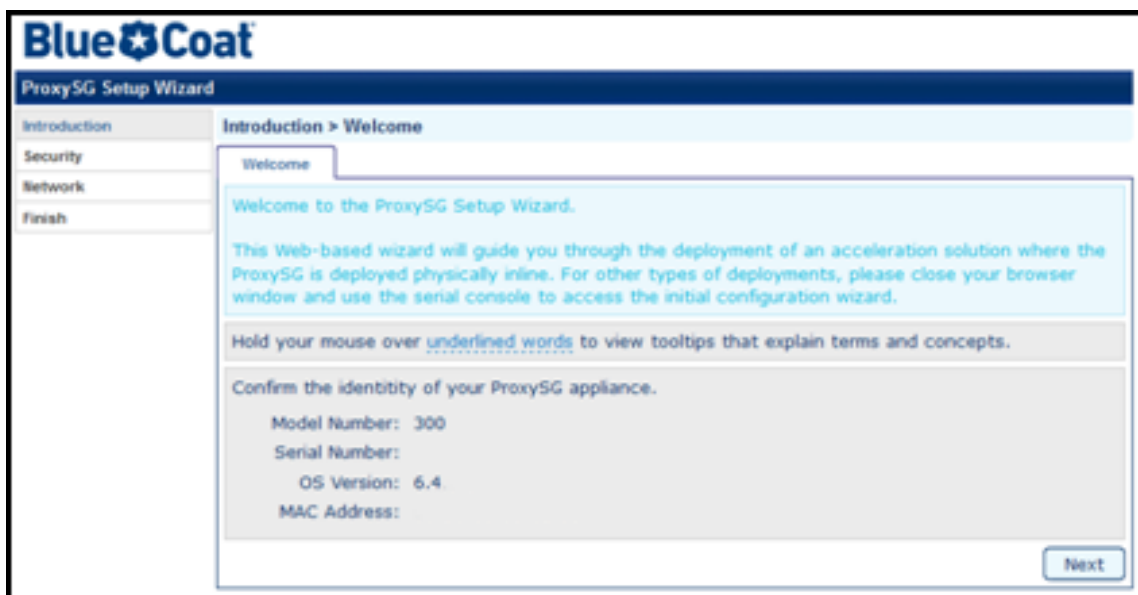
Configure Basic Network Information for an In-Path Acceleration Peer (Web Wizard)

The Web-based Setup Wizard allows you to configure the MACH5 appliance remotely with a Web browser, without having to connect to it via the serial console. The Web Wizard has the following requirements:

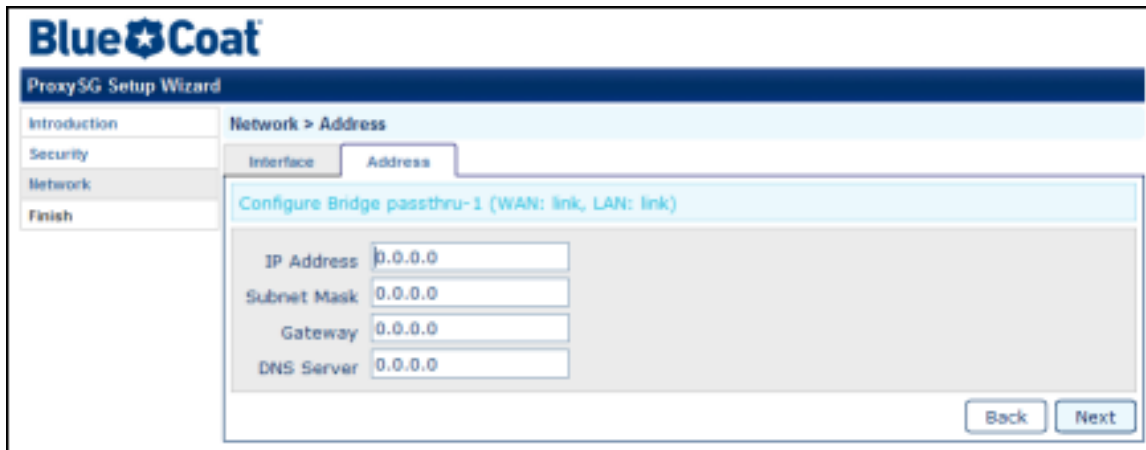
- The MACH5 appliance must be in-path (not virtually in-path or out-of-path).
- The computer system you are using to remotely configure the appliance must be on the same LAN as the appliance and have a direct network communication path to the MACH5 appliance.
- The computer system must also have a default route whose destination is a router on the other side of the MACH5. If the computer's connectivity to the Internet goes through the MACH5 appliance, this condition is satisfied.
- If you are not physically at the computer system on the LAN side of the MACH5 appliance, you should have Remote Desktop (or similar functionality) enabled on the computer system.

Use the following procedure to configure the basic network settings on an appliance that you plan to deploy in-path as an acceleration peer.

1. (If applicable) If you are not physically at the computer system on the LAN side of the MACH5 appliance, initiate a Remote Desktop session (or similar functionality) to the computer system that will be used for configuring the MACH5.
2. On a client PC that is on the same LAN as the MACH5 appliance, open a Web browser.
3. Enter <http://proxysg.bluecoat.com:8083>. The Welcome screen displays.



4. Click **Next**. The Security panel appears, with the Console tab selected.
5. Follow the screen prompts to configure the security options for the Console, CLI, and Serial Port.
6. Follow the screen prompts to configure the network settings. With the Web Wizard, you will be able to configure a single interface or a hardware bridge that operates as a network interface.



7. When prompted to confirm your settings, click **Configure**.
8. Click the displayed link (for example, <https://192.12.14.12:8082>) to log into the configured appliance.

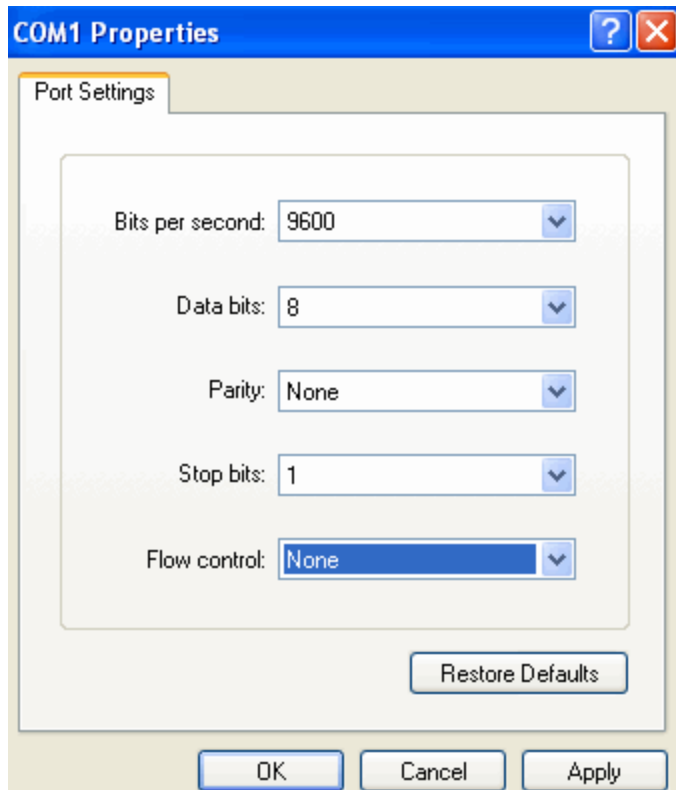
Note that the Web Wizard does not enable acceleration. You need to go to the Sky Management Console to enable acceleration, define the applications to accelerate, configure other network interfaces, and perform further configuration. See "Configure Acceleration" on page 32, "Define the Applications to Accelerate" on page 34, and Configure Interface Settings.

Configure Basic Network Info for a Virtually In-Path Acceleration Peer

Use the following procedure to connect to the MACH5 serial console and configure the basic network settings on an appliance that you plan to deploy virtually in-path as an acceleration peer. You can use whatever terminal emulation software you want. This procedure shows how to perform initial configuration using Windows HyperTerminal.

1. To launch Windows HyperTerminal, select **Start > Programs > Accessories > Communications > HyperTerminal**.
2. (Optional) Name the connection for later use.
3. Select the communication port and set the communication parameters.

For example, select COM1 and set the communication parameters as shown below:



4. Click **OK** to save your settings.
5. Activate the serial console and launch the setup console for a manual setup.
 - a. Connect the serial cable from your laptop to the MACH5 and power on the appliance. The appliance will go through a bootup process. This may take a moment.
 - b. Press **Enter** three times to activate the MACH5 serial console.
 - c. When prompted, enter **2** to launch the setup console.
 - d. When prompted, enter **a** to initiate a manual setup.
6. Enter **a** to specify that you are configuring the appliance for acceleration.

Step 2: Which solution would you like to implement?

 - a) Acceleration
 - b) Other solution

Your choice: [] **a**
7. To specify a virtually in-path deployment, enter **b**.

Step 3: How will you deploy this device?

 - a) Physically in-path
 - b) Virtually in-path using WCCP

c) Any other
Your choice: []b

8. (optional) Enter the new name for the appliance when prompted or press **Enter** to accept the default name.
9. Configure the interface(s).
 - a. When prompted, select the interface to configure or press **Enter** to select the default interface.
 - b. Enter the IP address.
 - c. Enter the subnet mask.
 - d. Press **Enter** to specify that you want the appliance to automatically detect speed/duplex settings.
 - e. If you use a VLAN other than the native VLAN for your management traffic, enter **y** when prompted to configure a VLAN and then enter the VLAN ID when prompted.
 - f. Press **Enter** to continue.
10. Follow the prompts in the script to configure the default gateway address, DNS server address, and the administrator ID and password.
11. When prompted, press **Enter** to turn on acceleration immediately after configuring WCCP.
12. To save your settings, press **Enter**.

Configure and Test the Bridge Mode on In-Path Appliances

The bridge mode determines whether traffic will continue to flow through an in-path appliance if the appliance loses power or is powered down for any reason. In Fail Open mode, the MACH5 appliance fails to a connected state (that is, traffic continues to flow uninterrupted). In Fail Closed mode, the MACH5 appliance fails to a disconnected state (that is, traffic is blocked instead of bridged). The bridge mode you should use depends on your deployment:

- If you have a single in-path MACH5, Blue Coat recommends that you configure the MACH5 appliance to fail to a connected state. If the appliance loses power or is powered down for any reason, traffic flows from one Ethernet port to the other. Therefore, traffic flows uninterrupted, although it is not intercepted by the MACH5 appliance.
- If you have redundant, in-path MACH5 appliances, you should configure the MACH5 to fail to a disconnected state so that the connection can be forwarded to the redundant appliance for

optimization. This ensures that traffic remains uninterrupted and that policy (as configured) continues to be applied for all traffic intercepted by the MACH5.

The following sections describe how to configure fail open/fail closed as well as how to test whether fail open is working properly:

- "Configure the Bridge Mode" below
- "Test the Fail Open Functionality" on the facing page

Configure the Bridge Mode

Some ProxySG models (such as the 300, 600, 810, 900 and 9000) have a programmable network adapter that can be used as a pass-through bridge or as a network interface card (NIC).

1. Launch the Advanced Management Console (https://<ProxySG_IP_address>:8082/mgmt).
2. Select **Configuration > Network > Adapters > Bridges**.
3. Select the bridge you want to configure and then click **Edit**. The Edit Bridge dialog displays.
4. Select the bridge Mode that is appropriate for your deployment from the drop-down list:
 - **Fail Open**—If the ProxySG fails, all traffic passes through the bridge so clients can still receive data. If you are deploying a single in-path ProxySG, select this option.
 - **Fail Closed**—If the ProxySG fails, traffic is blocked, not bridged. You should configure fail closed only if you have redundant in-path ProxySG appliances and you plan to configure Connection Forwarding so that connections to one ProxySG can be automatically optimized by the other ProxySG appliance(s) in the Connection Forwarding group in the event of a failure. For information on Connection Forwarding, see "What is Connection Forwarding?" on page 106.

The screenshot shows the 'Edit Bridge' dialog box. The 'Bridge Name' field contains 'passthru-2'. The 'Failover Group' dropdown is set to '<none>'. The 'Mode' dropdown is open, showing 'Disabled' as the selected option, with 'Fail Open' and 'Fail Closed' as other visible options. The 'Propagate Failure' checkbox is unchecked. A 'Clear Bridge Statistics' button is at the bottom.



If the bridge adapters are not programmable, the mode commands are not visible.

5. To save your changes, click **OK** and then click **Apply**.

Test the Fail Open Functionality

If you have configured the MACH5 appliance to Fail Open, you should test that traffic continues to flow through the appliance while it is powered off as described in the following procedure.

1. Power off the MACH5 appliance.
2. Initiate a client request for content from the remote site. For example, go to a client system at the branch and request a file from a file server at the data center.
3. If you receive the requested content, the MACH5 appliance is failing to a connected state as expected. If you cannot access the requested content, check to make sure that you have connected the hardware bridge ports on the ProxySG appliance (these are labeled LAN and WAN) to the proper interfaces on the router and the switch.

Manage the Appliance

Refer to the following topics to learn how to log in to and out of the UI and how to shut down the ProxySG Virtual Appliance.

Deploy the MACH5 Appliance

For instructions on configuring the MACH5 appliance to operate in one of the supported deployments, select your deployment type:

Select a Recommended Deployment	48
Deploy In-Path Acceleration Peers	49
Deploy a Concentrator Peer In-Path	50
Deploy a Branch Peer In-Path	56
Deploy Virtually In-Path Acceleration Peers	62
What is WCCP?	63
Deploy a Concentrator Peer Virtually In-Path	67
Deploy a Branch Peer Virtually In-Path	77
Redundant Acceleration Topology	83
Deploy In-Path with Redundant Links	84
Deploy Virtually In-Path in a Redundant Layer 2 Network	98

Select a Recommended Deployment

In an acceleration deployment, MACH5 appliances are configured as *acceleration nodes*, meaning that acceleration has been enabled on them. When an acceleration node intercepts application traffic that has been configured for acceleration, it forms a TCP connection, called a tunnel, with the upstream acceleration node. The two nodes, called *acceleration peers*, send application requests and responses across the tunnel and employ the acceleration techniques that are appropriate for the specific application. The acceleration node that intercepts client traffic is referred to as a Branch peer; the acceleration node that accepts the tunnel connection on the other end of the WAN is called a Concentrator peer. An individual MACH5 appliance can act as both a Concentrator peer and a Branch peer; the only difference is its role in a specific tunnel. (See "What are the Acceleration Roles?" on page 157.)

The steps for installing and configuring your acceleration peers depend on the deployment type you have selected and whether you require redundancy. (See "What are the MACH5 Deployment Types?" on page 12) The following examples show step-by-step procedures for configuring acceleration nodes in each of the recommended deployment scenarios. For best results, use the following deployment examples to guide you in configuring your acceleration network:

- "Deploy In-Path Acceleration Peers" on the next page
- "Deploy Virtually In-Path Acceleration Peers" on page 62

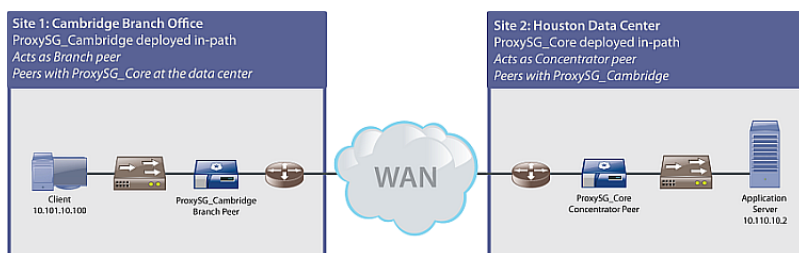
- "Redundant Acceleration Topology" on page 83

Deploy In-Path Acceleration Peers

In the following example, acceleration is deployed in a network that includes a branch office with clients accessing applications located on application servers at the corporate data center. A single MACH5 appliance is deployed in-path at each location as follows:

- **Site 1: Cambridge Branch Office**—The in-path MACH5 appliance at this location acts as a Branch peer, intercepting client application traffic and establishing outbound transparent tunnel connections with the Concentrator peer at the data center to optimize the traffic.
- **Site 2: Houston Data Center**—The in-path MACH5 appliance at this site acts as a Concentrator peer, accepting inbound tunnel connections from the remote Branch peer at the Cambridge site. It then recreates the application request data and forwards the request to the application server. When the Concentrator peer receives the application response data from the application server it returns it to the Branch peer over the same tunnel.

Notice that the deployments at each site are identical except that the Cambridge MACH5 acts as a Branch peer only and the Houston MACH5 acts as a Concentrator peer only.



When configuring acceleration, you should configure the Concentrator peer first and then configure your Branch peers. In this deployment, application acceleration starts automatically with a set of default applications as soon as both the Concentrator peers and Branch peers are configured. You can use the Sky Management Console to verify application acceleration and monitor connectivity between acceleration peers.

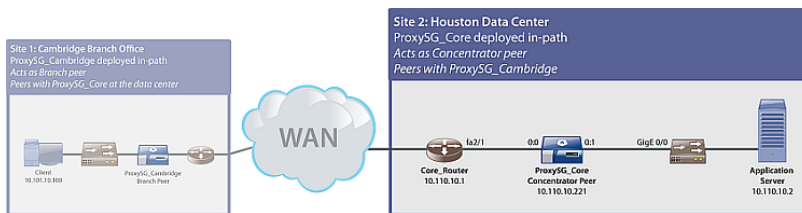
The following sections describe how to configure each of the MACH5 appliances in this example topology and show how to verify that traffic is being accelerated as expected:

1. "Deploy a Concentrator Peer In-Path" on the facing page
2. "Deploy a Branch Peer In-Path" on page 56
3. "Verify the Acceleration Deployment" on page 35

Deploy a Concentrator Peer In-Path

This example shows how to deploy the Concentrator peer in a basic in-path configuration. This section shows the deployment of the Concentrator peer only; for an example of how to configure a Branch peer, see "Deploy a Branch Peer In-Path" on page 56.

At this site, the Concentrator peer, ProxySG_Core, is configured as an acceleration node. It will accept inbound tunnel connections from the Branch peer at the Cambridge site.



A MACH5 can act as both a Concentrator peer and a Branch peer depending on its role in a given tunnel. In this example, ProxySG_Core does not intercept client traffic and therefore it acts as a Concentrator peer only.

Step 1: Prepare for an Acceleration Deployment

1. Plan the configuration of the concentrator peers. A worksheet is available to record your configuration settings. See "Plan the Configuration of the Concentrator Peers" on page 54.
2. Make sure all MACH5 appliances are running SGOS version 6.5 with the factory default settings.
 - a. Upgrade all appliances as described in Upgrade/Downgrade an SGOS Image.
 - b. After upgrading, restore the appliance to its factory default state using the `restore-defaults factory-defaults` CLI command. Note that you must be connected to the MACH5 console to issue this command.
3. Before you install the MACH5 appliance, test network connectivity to the remote sites. You will repeat this step after the appliance has been installed to reverify network connectivity.

For example, to ping a host at a remote site as shown in the [topology diagram](#), type the following commands at the command prompt on a local client:

```
ping 10.101.10.100
```

4. If you have a firewall between the ADN Concentrator peer and the ADN Branch peer, make sure the tunnel listening port is open. This port allows the creation of the control connection for the tunnel, which enables byte-cache dictionary synchronization. By default, the tunnel listening port is set to 3035 (plain) and 3037 (secure).

Step 2: Integrate the Appliance into the Network

1. Connect to the MACH5 serial console (9600, 8, N, 1) and launch the Blue Coat ProxySG configuration wizard. For detailed instructions, see "Configure Basic Network Information for an In-Path Acceleration Peer (Serial Console)" on page 54.

```

----- CONFIGURATION START -----
Welcome to the Blue Coat ProxySG 210 configuration wizard.
This appliance's serial number: 0408063522

-----
You can get field help by entering a question mark ? in the fields.
You can move backwards through the steps by pressing the UP arrow.
You can exit the wizard without saving your changes
-----

Step 1: How do you plan to configure this appliance?
a) Through a manual setup
b) Through a Director-managed setup
Your choice: ☐ a

Step 2: Which solution would you like to implement?
a) Acceleration
b) Other solution
Your choice: ☐ a

Step 3: How will you deploy this appliance?
a) Physically in-path
b) Virtually in-path using WCCP
c) Any other
Your choice: ☐ a

Step 4: Appliance name [ProxySG 210 0408063522] ProxySG_core

Step 5: You have the following hardware bridge interface:
Configure interface 0:0-0:1? Inactive link [No] y
IP address ☐ ..... 10.110.10.221
Subnet mask ☐ ..... 255.255.255.0

Speed and duplex undetected
Automatically detect when link exists [Yes] .
Does this interface require a VLAN? [NO] ....

Step 6: Default gateway ☐ 10.101.10.1
>> Pinging 10.101.10.1...FAILED

Step 7: Primary DNS server ☐ 10.101.10.100
>> Testing DNS server
>> Attempting to resolve www.bluecoat.com in the background

Step 8: Administrator ID [admin]

Step 9: Administrator password ☐ *****
Retype administrator password ☐ *****
>> Password is easily guessed. Choose another? Y/N [Yes] n

Step 10: Activate acceleration immediately? [Yes]

```

2. Power off the MACH5 appliance.
3. Rack mount the MACH5 appliance, but do not power it on. Refer to the *ProxySG Quick Start Guide* for rack-mounting instructions. Note that the appliance must have a hardware bridge card with pass-through support.



With in-path deployments, there will be some network downtime when installing the MACH5 appliance.

4. Cable the appliance as follows:
 - Connect the MACH5 LAN interface to the switch using a straight-through cable.
 - Connect the MACH5 WAN interface to the router using a crossover cable.
5. Before you power on the MACH5 appliance, test the fail open functionality, which allows traffic to pass

through the appliance in the event of an outage. To do this, ping a host at the remote site (going through the MACH5appliance).

6. Power on the MACH5 appliance.
7. Verify network connectivity to remote sites by repeating the ping test. Check adapter LEDs and cables if you cannot reach the remote sites.
8. Go to the following URL to launch the Sky Management Console: `https://<ProxySG_IP_address>:8082`.

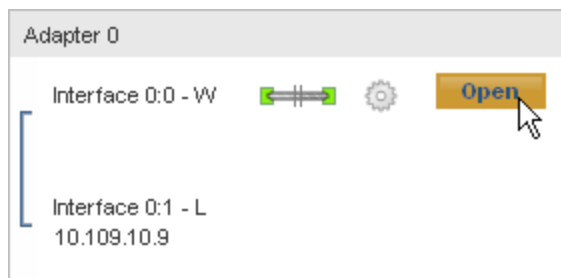
For example, to launch the Sky Management Console on the Houston appliance you would enter:

`https://10.101.10.221:8082`

9. In the Sky Management Console banner, make sure the Device health is **OK**. If the device health is **Warning** or **Critical**, click the link to view details about the health issues or click a link in the **Alerts** panel in the right side of the Sky Management Console banner.



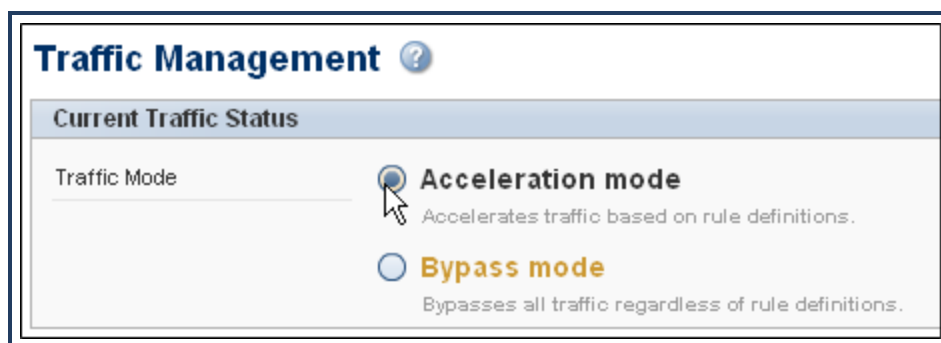
10. Verify that the configured link settings (speed/duplex) on the MACH5 interface match the configured settings on the connected switch/router interface.
 - a. Select **System Settings > Adapters & Interfaces**.
 - b. In the box that corresponds to the bridge that is connected to the switch or router in the **Adapter Overview** section of the tab, click **Open**.



- c. Verify that the **Speed** and **duplex** settings match the settings that are defined on the router or switch interface.
- d. Click **Close**.
- e. If you made any changes, click **Commit all**.

Step 3: Configure Acceleration

1. If you did not enable acceleration during initial configuration, enable it now.
 - a. Select **Configure > Acceleration > Traffic Management**.
 - b. Select **Acceleration mode**.

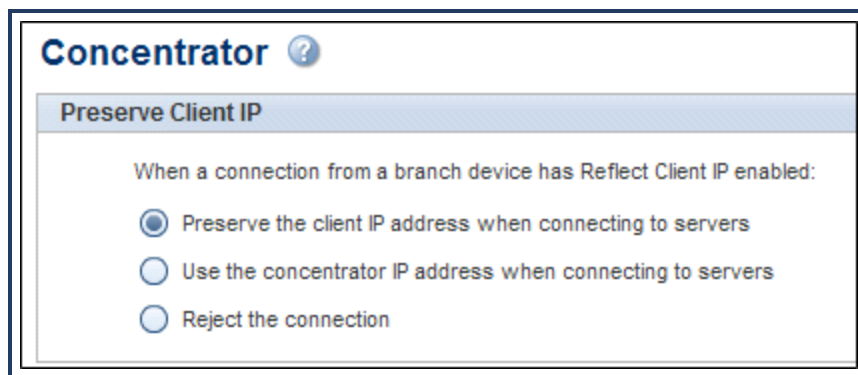


- c. Click **Commit all**.



In Open configurations such as this one, you do not need to configure an ADN manager. If you want to change this deployment to an Open Managed or a Closed deployment, see "Switch Acceleration Modes" on page 33.

2. **Preserve the client IP address for inbound connections.**
 - a. Select **Configure > ADN > Concentrator**.
 - b. Select **Preserve the client IP address when connecting to servers**.



Concentrator ?

Preserve Client IP

When a connection from a branch device has Reflect Client IP enabled:

- ☒ Preserve the client IP address when connecting to servers
- ☐ Use the concentrator IP address when connecting to servers
- ☐ Reject the connection

c. Click **Commit all**.

Plan the Configuration of the Concentrator Peers

Use the [Concentrator Peer Configuration Worksheet](#) to record the information you need to gather before installing a MACH5 appliance that will act as a Concentrator peer only (that is, it will not be intercepting client application traffic). Record the information you need to perform the initial installation and configuration of the MACH5, such as the required network addresses, the switch port and router interface to which to connect the MACH5, and the link settings you must configure on the MACH5 (they must match the settings defined on the switch/router to which you are connecting the appliance). In addition, if you use a non-native VLAN for management traffic, you should record the VLAN ID here.

Complete a separate worksheet for each Concentrator peer you plan to deploy.



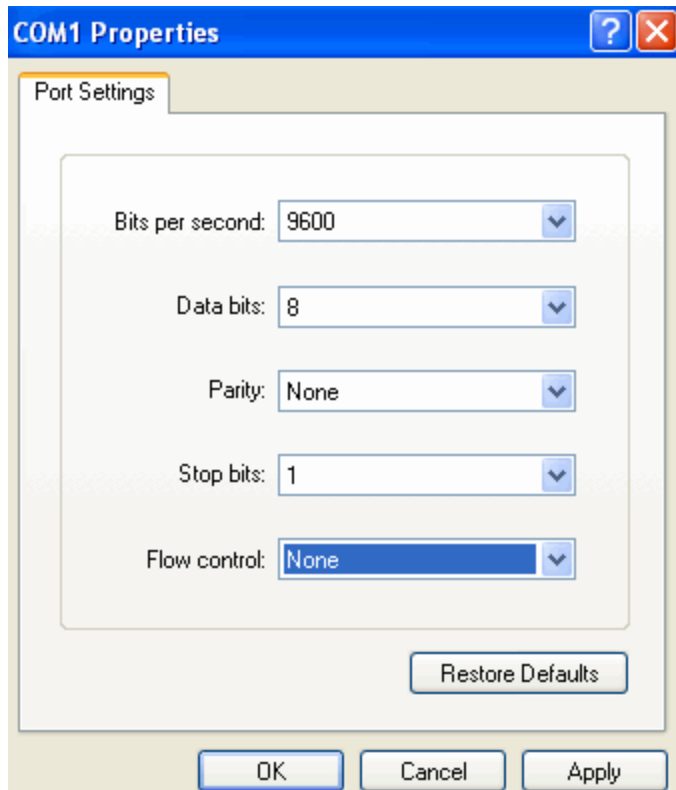
The [worksheet](#) is an interactive PDF form that you can fill in on screen before printing. You may also want to save the completed worksheet file for future reference.

Configure Basic Network Information for an In-Path Acceleration Peer (Serial Console)

Use the following procedure to connect to the MACH5 appliance serial console and configure the basic network settings on an appliance that you plan to deploy in-path as an acceleration peer. You can use whatever terminal emulation software you want. This procedure shows how to perform initial configuration using Windows HyperTerminal.

1. To launch Windows HyperTerminal, select **Start > Programs > Accessories > Communications > HyperTerminal**.
2. (Optional) Name the connection for later use.
3. Select the communication port and set the communication parameters.

For example, select COM1 and set the communication parameters as shown below:



4. Click **OK** to save your settings.
5. Activate the serial console and launch the setup console for a manual setup.
 - a. Connect the serial cable from your laptop to the MACH5 and power on the appliance. The appliance will go through a bootup process. This may take a moment.
 - b. Press **Enter** three times to activate the MACH5 serial console.
 - c. When prompted, enter **2** to launch the setup console.
 - d. When prompted, enter **a** to initiate a manual setup.
6. Enter **a** to specify that you are configuring the appliance for acceleration.

Step 2: Which solution would you like to implement?

 - a) Acceleration
 - b) Other solution

Your choice: [] **a**
7. To specify an in-path deployment, enter **a**.

Step 3: How will you deploy this device?

 - a) Physically in-path
 - b) Virtually in-path using WCCP

c) Any other
Your choice: []a

8. (optional) Enter the new name for the appliance when prompted or press **Enter** to accept the default name.
9. Configure the interface:
 - a. When prompted, enter **y** to specify that you want to configure the inactive link.
 - b. Enter the IP address.
 - c. Enter the subnet mask.
 - d. Press **Enter** to specify that you want the appliance to automatically detect speed/duplex settings.
 - e. If you use a VLAN other than the native VLAN for your management traffic, enter **y** when prompted to configure a VLAN and then enter the VLAN ID when prompted.
 - f. Press **Enter** to continue.
10. Configure other interfaces, if available. For example, if a four-port LAN option card is installed, you will need to configure the settings for each bridge pair. Each pair should be assigned a unique IP address.
11. Follow the prompts in the script to configure the default gateway address, DNS server address, and the administrator ID and password.
12. When prompted, press **Enter** to turn on acceleration immediately.
13. To save your settings, press **Enter**.

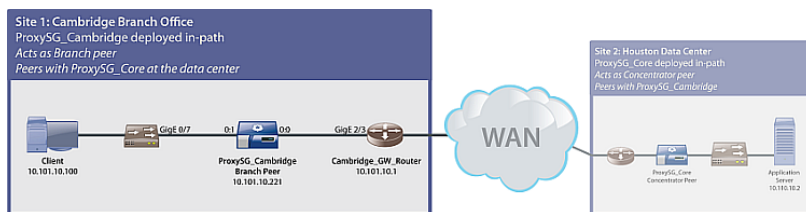


Be sure to configure IP addresses for physically-inline bridge interfaces, as well as for the management port if you are using it. If you configure an IP address for the management port only, some traffic may get inadvertently routed through this port instead of the expected interface.

Deploy a Branch Peer In-Path

This example shows how to deploy the Branch peer in a basic in-path acceleration configuration. This section shows the deployment of the Branch peer only; for an example of how to configure a Concentrator peer, see "Deploy a Concentrator Peer In-Path" on page 50.

At this site, the Branch peer, ProxySG_Cambridge, is configured as an acceleration node. It will intercept local client application traffic and establish outbound tunnel connections with the Concentrator peer at the Houston data center.



Step 1: Prepare for an Acceleration Deployment

1. Plan the configuration of branch peers. A worksheet is available to record your configuration settings. See "Plan the Configuration of Branch Peers" on page 61
2. Make sure all MACH5 appliances are running SGOS version 6.4 with the factory default settings.
 - a. Upgrade all appliances as described in Upgrade/Downgrade an SGOS Image.
 - b. After upgrading, restore the appliance to its factory default state using the `restore-defaults factory-defaults` CLI command. Note that you must be connected to the MACH5 console to issue this command.
3. Before you install the MACH5 appliance, test network connectivity to the remote sites. You will repeat this step after the appliance has been installed to reverify network connectivity.

For example, to ping a host at a remote site as shown in the [topology diagram](#), type the following commands at the command prompt on a local client:

```
ping 10.110.10.2
```

4. If you have a firewall between the ADN Concentrator peer and the ADN Branch peer, make sure the tunnel listening port is open. This port allows the creation of the control connection for the tunnel, which enables byte-cache dictionary synchronization. By default, the tunnel listening port is set to 3035 (plain) and 3037 (secure).

Step 2: Integrate the Appliance into the Network

1. Connect to the MACH5 serial console (9600, 8, N, 1) and launch the Blue Coat ProxySG configuration wizard. For detailed instructions, see "Configure Basic Network Information for an In-Path Acceleration Peer (Serial Console)" on page 54.

```

===== CONFIGURATION START =====
Welcome to the Blue Coat ProxySG 210 configuration wizard.
This appliance's serial number: 0408063522

-----
You can get field help by entering a question mark ? in the fields.
You can move backwards through the steps by pressing the UP arrow.
You can exit the wizard without saving your changes by pressing the ESC key.
-----

Step 1: How do you plan to configure this appliance?
a) Through a manual setup
b) Through a Director-managed setup
your choice: [ ] a

Step 2: Which solution would you like to implement?
a) Acceleration
b) other solution
your choice: [ ] a

Step 3: How will you deploy this appliance?
a) Physically in-path
b) Virtually in-path using WCCP
c) Any other
your choice: [ ] a

Step 4: Appliance name [ProxySG 210 0408063522] ProxySG_Cambridge

Step 5: You have the following hardware bridge interface:
Configure interface 0:0-0:1? Inactive link [No] y
IP address [ ] ..... 10.101.10.221
Subnet mask [ ] ..... 255.255.255.0
Speed and duplex undetected
Automatically detect when link exists [yes] .
Does this interface require a VLAN? [No] ....

Step 6: Default gateway [ ] 10.10
>> Pinging 10.101.10.1...FAILED

Step 7: Primary DNS server [ ] 10.101.10.100
>> Testing DNS server
>> Attempting to resolve www.bluecoat.com in the background [ ]

Step 8: Administrator ID [admin]

Step 9: Administrator password [ ] *****
Retype administrator password [ ] *****
>> Password is easily guessed. Choose another? y/n [yes] n

Step 10: Activate acceleration immediately? [yes]

```

2. Power off the MACH5 appliance.
3. Rack mount the MACH5 appliance. Refer to the *ProxySG Quick Start Guide* for instructions. Note that the appliance must have a hardware bridge card with pass-through support.



With in-path deployments, there will be some network downtime when installing the MACH5 appliance.

4. Cable the appliance as follows:
 - Connect the MACH5 LAN interface to the switch using a straight-through cable.
 - Connect the MACH5 WAN interface to the router using a crossover cable.
5. Before you power on the MACH5 appliance, test the fail open functionality, which allows traffic to pass through the appliance in the event of an outage. To do this, ping a host at the remote site (going through the MACH5 appliance).
6. Power on the MACH5 appliance.

7. Verify network connectivity to remote sites by repeating the ping test. Check adapter LEDs and cables if you cannot reach the remote sites.
8. Go to the following URL to launch the Sky Management Console: `https://<ProxySG_IP_address>:8082`.

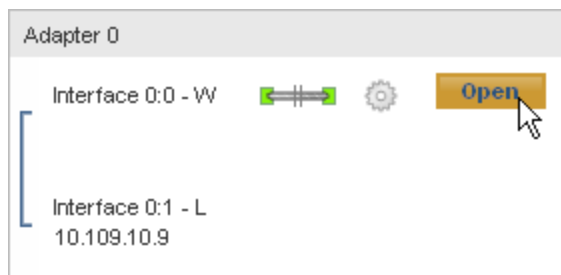
For example, to launch the Sky Management Console on the Cambridge appliance you would enter:

`https://10.101.10.221:8082`

9. In the Sky Management Console banner, make sure the Device health is **OK**. If the device health is **Warning** or **Critical**, click the link to view details about the health issues or click a link in the **Alerts** panel in the right side of the Sky Management Console banner.



10. Verify that the configured link settings (speed/duplex) on the MACH5 interface match the configured settings on the connected switch/router interface.
 - a. Select **System Settings > Adapters & Interfaces**.
 - b. In the box that corresponds to the bridge that is connected to the switch or router in the **Adapter Overview** section of the tab, click **Open**.

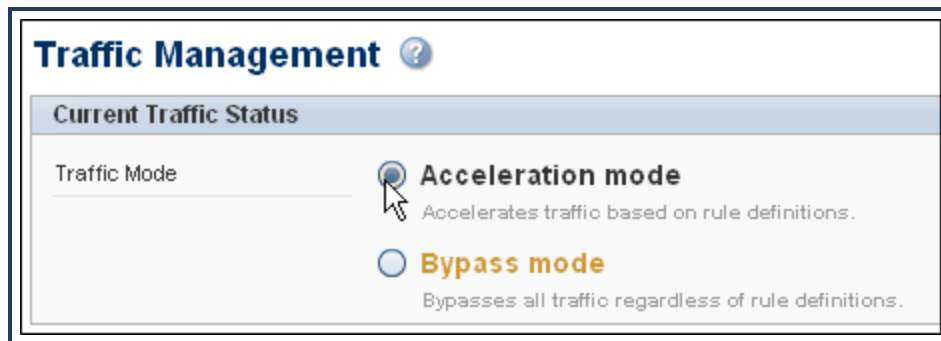


- c. Verify that the **Speed and duplex** settings match the settings that are defined on the router or switch interface.

- d. Click **Close**.
- e. If you made any changes, click **Commit all**

Step 3: Configure Acceleration

1. If you did not enable acceleration during initial configuration, enable it now.
 - a. Select **Configure > Acceleration > Traffic Management**.
 - b. Select **Acceleration mode**.



- c. Click **Commit all**.



In Open configurations such as this one, you do not need to configure an ADN manager. If you want to change this deployment to an Open Managed or a Closed deployment, see "Switch Acceleration Modes" on page 33.

Step 4: Configure Proxy Services

1. (optional) Customize what traffic the MACH5 appliance accelerates.
 - a. From Blue Coat Sky, select **Configure > Acceleration > Traffic Management**. The MACH5 automatically intercepts a default set of services based on your deployment (explicit or transparent).
 - b. Modify which services get intercepted and bypassed by selecting the radio button in the Intercept or Bypass column of the Services table as appropriate. You can only select services that can be

accelerated.

Service name	Acceleration techniques	Intercept	Bypass	Edit	Del
BGP	Monitor only	Not applicable			
Blue Coat ADN	Monitor only	Not applicable			
Blue Coat Managem...	Monitor only	Not applicable			
OPS	Application level				
Cisco IPSec VPN	Monitor only	Not applicable			
Citrix	Network level				
Default	Data level				
DNS	Application level				
Echo	Monitor only	Not applicable			
Endpoint Mapper	Application level				
Explicit HTTP	Application level				
External HTTP	Application level				
FTP	Application level				
HTTPS	Monitor only	Not applicable			
H.323	Monitor only	Not applicable			

2. Verify that the MACH5 appliances are intercepting and accelerating traffic as expected. See "Verify the Acceleration Deployment" on page 35.

Plan the Configuration of Branch Peers

Use the [Branch Peer Configuration Worksheet](#) to record the information you need to gather before installing a MACH5 appliance as a Branch peer.



The [worksheet](#) is an interactive PDF form that you can fill in on screen before printing. You may also want to save the completed worksheet file for future reference.

This worksheet includes the following sections:

Network Configuration Information—Record the information you need to perform the initial installation and configuration of the MACH5, such as the required network addresses, the switch port and router interface to which to connect the MACH5 LAN and WAN ports, and the link settings you must configure on the MACH5 (they must match the settings defined on the switch/router to which you are connecting the appliance). In addition, if you use a non-native VLAN for management traffic, you should record the VLAN ID here.

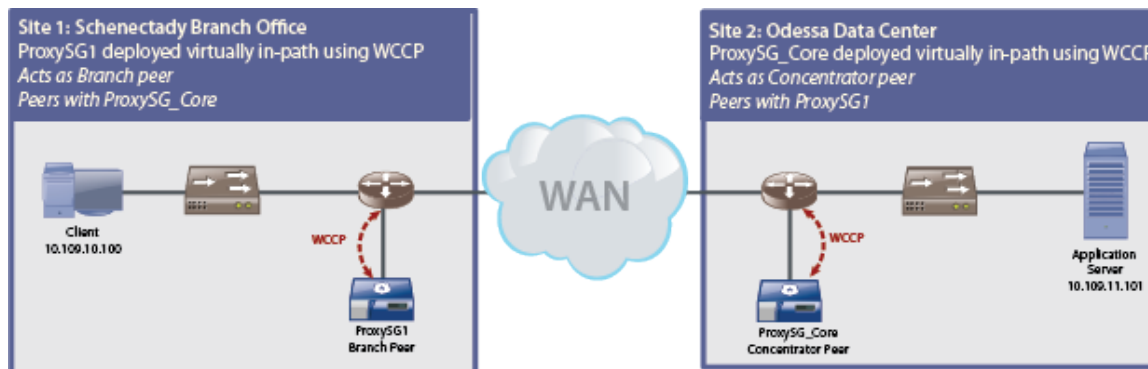
Service Configuration Information—Identify the services (and the corresponding port numbers) that the appliance needs to intercept. In addition, you must identify a client and a server to use to test whether each service is being optimized properly. For example, if you will be optimizing CIFS traffic, you should identify a Microsoft Windows client and server to use to test the file sharing operations, such as opening a file on a remote application server, modifying the file on the client, and saving the file back to the file share. You will need to identify similar types of tests for each application that you plan to intercept and you will need to identify a client and a server to use to conduct these tests.

Complete a separate worksheet for each Branch peer you plan to deploy.

Deploy Virtually In-Path Acceleration Peers

In the following example, acceleration is deployed in a network that includes a branch office with clients accessing applications located on application servers at the corporate data center. A single MACH5 appliance is deployed virtually in-path at each location as follows:

- **Site 1: Schenectady Branch Office** – The virtually in-path MACH5 appliance at this location acts as a Branch peer, intercepting client application traffic and establishing outbound transparent tunnel connections with the Concentrator peer at the data center to optimize the traffic.
- **Site 2: Odessa Data Center** – The virtually in-path MACH5 appliance at this site acts as a Concentrator peer, accepting inbound tunnel connections from the remote Branch peer at the Schenectady site. It then recreates the application request data and forwards the request to the application server. When the Concentrator peer receives the application response data from the application server it returns it to the Branch peer over the same tunnel. Because the Concentrator does not intercept client traffic, it does not need to distinguish LAN traffic from the WAN traffic. Therefore, you can configure the WCCP service groups to redirect traffic to the MACH5 appliance over a single physical interface.



When configuring acceleration, you should configure the Concentrator peers first and then configure your Branch peers.

The following sections describe how to configure each of the MACH5 appliances in this example topology and show how to verify that traffic is being accelerated as expected:

1. "Deploy a Concentrator Peer Virtually In-Path" on page 67
2. "Deploy a Branch Peer Virtually In-Path" on page 77
3. "Verify the Acceleration Deployment" on page 35

What is WCCP?

The Web Cache Communication Protocol (WCCP) is a Cisco-developed protocol that allows certain Cisco routers and switches to transparently redirect traffic to a cache engine such as a MACH5 appliance. This traffic redirection helps to improve response time and optimize network resource usage.

The MACH5 appliance can be configured to participate in a WCCP scheme, in which WCCP-capable switches or routers collaborate with MACH5 appliances to form one or more groups that service requests from clients.

Using WCCP with the MACH5

In virtually in-path deployments, when the MACH5 appliance is not in the physical path of clients and servers, a WCCP-capable router is used to redirect traffic to the MACH5 appliance for transparent proxy services.

In a transparent proxy deployment the client is not aware that it is interacting with an intermediate proxy and not the origin content server (OCS). The process works as follows:

1. The client sends a packet addressed for the OCS.
2. The WCCP-enabled router redirects the packet to the MACH5 appliance.
3. The MACH5 appliance determines what to do with it based on the transparent proxy services that have been configured for the traffic type. If it cannot service the request locally (for example by returning a page from its local cache), it sends a request to the specified OCS on behalf of the client.
4. The MACH5 appliance then forwards the response back to the client.

To implement this transparent redirection scheme, one or more MACH5 appliances and one or more routers/switches must form a service group.

The MACH5 appliance offers VLAN Support for WCCP and allows you to redirect traffic from the router over physical or virtual interfaces. If you configure multiple virtual interfaces between the MACH5 appliance and the WCCP capable router, you can segregate WAN and LAN traffic on the same physical interface by enabling a VLAN trunk between the appliances. By default, VLAN trunking is enabled on the MACH5 appliance.

Service Groups

A service group unites one or more routers/switches with one or more MACH5 appliances in a transparent redirection scheme governed by a common set of rules. The service group members agree on these rules by announcing their specific capabilities and configuration to each other in WCCP protocol packets.

The WCCP protocol packets include "Here I Am" messages between the MACH5 appliances and the routers/switches that respond with "I See You" messages. The "Here I Am" messages contain a description of the service group that the MACH5 wants to join, including the protocol, ports to redirect, method to use to forward and return packets to each other, and load balancing instructions. The "I See You" response from the routers include a Receive ID as well as a list of WCCP capabilities—such as forwarding methods or load balancing schemes that the router supports.

When the capabilities of the MACH5 appliances and the routers are compatible, they form a service group. Each MACH5 appliance then announces its presence and a list of all the routers with which it has established communications. The routers reply with their list of MACH5 appliances in the group.

There are two types of service groups:

- *Well-known service groups* are defined by a fixed set of traffic types and characteristics that are known by the routers and the MACH5 appliances in the service group. Currently there is only one well-known service, web-cache, which redirects all TCP traffic with a destination port of 80.
- *Dynamic service groups* are negotiated between the MACH5 appliances and the routers in the service group. The MACH5 instructs the router which protocol or ports to intercept, and how to distribute the traffic.

Service Group Addressing

In order to establish and maintain a service group, the MACH5 appliances and routers must be able to communicate. To specify the addresses of all the routers in a service group, you must choose one of the following methods:

- **Unicast:** Each MACH5 appliance must be explicitly configured with the IP address of every router in the service group. You will need to reconfigure each appliance whenever you add or remove a router from the group.
- **Multicast:** The routers and MACH5 appliances in the service group communicate using a single IP address in the range of 224.0.0.0 to 239.255.255.255. To configure this, each MACH5 and each router in the group must be configured with the multicast IP address. Note that if the WCCP routers and/or MACH5 appliances are more than one hop apart, IP multicast routing must also be enabled on the intervening routers.

Securing a Service Group

If you are using WCCP v2, you can secure a service group by configuring an MD5 authentication between the MACH5 appliances and the routers in the group. To configure authentication, you must define the same password on all routers and all MACH5 appliances in the service group.

When authentication is enabled, a MACH5 appliance will not be allowed to join the service group unless it knows the password.

Specifying a Forwarding and a Returning Mode

Since WCCP is used in transparent proxy deployments, when you configure the MACH5 appliance, you must specify a forwarding and a return mechanism. This mechanism defines how the router will forward packets to the MACH5 appliance as well as how the appliance will return packets that it does not intercept because of the policy or services configured on it, back to the router.

Blue Coat recommends that all service groups configured on a router use the same forwarding and packet return mechanism.

The MACH5 appliance supports the following forwarding and return methods:

- **GRE Forwarding/Return**— With Generic Routing Encapsulation (GRE) forwarding, the router encapsulates the intercepted packet in an additional IP and GRE header that shows the router address as the source IP address and the address of the MACH5 appliance as the destination IP address. When the appliance receives the packet, it strips the outside header and then determines how to process the request, either forwarding the request on to the OCS or servicing it locally.

When returning the redirected packet, the MACH5 appliance encapsulates the packet with an IP and GRE header that bears the IP address of the appliance as the source and the router IP address as the destination.

- **L2 Forwarding/Return**— With Layer 2 (L2) forwarding, the router rewrites the destination MAC address of the intercepted packet to the MAC address of the MACH5 to which it is redirecting the packet. This method is faster than GRE forwarding because the forwarding is done at the hardware level and doesn't require encapsulating and decapsulating the packet at Layer 3. However, to use L2 forwarding, the MACH5 and the routers in the service group must all be on the same L2 broadcast domain (that is, there cannot be more than one hop between them).

When returning the redirected packet, the MACH5 rewrites the destination MAC address to that of the router.

To determine whether L2 forwarding is supported on your hardware platform, refer to your Cisco documentation. For a list of the Cisco platforms on which Blue Coat has tested L2 forwarding with the MACH5, refer to the *WCCP Reference Guide*.

- **L2 Forwarding/GRE Return**— With L2 forwarding, the router rewrites the destination MAC address of the intercepted packet to the MAC address of the MACH5 to which it is redirecting the packet.

When returning the redirected packet, the MACH5 encapsulates the packet with an IP and GRE header that bears the IP address of the MACH5 as the source and the router IP address as the destination.

Note: The MACH5 does not support GRE forwarding and L2 packet return.

Assigning Service Group Redirection to the MACH5 Appliance

For every service group, you must configure how the router determines which MACH5 appliance to redirect each packet to; this is done by setting an assignment type on the MACH5. When the service group is formed, the MACH5 with the lowest IP address automatically becomes the designated cache (and if there is only one MACH5 in the service group, it is automatically the designated cache). The designated cache is responsible for communicating the assignment settings to the router, that is, which MACH5 appliance should be assigned a particular packet.

The MACH5 appliance supports two assignment types:

- **Hash Assignment** (Default)—With hash assignment, the designated cache assigns each MACH5 in the service group a portion of a 256-bucket hash table and communicates the assignment to the routers in the group. When the router receives a packet for redirection, it runs the hashing algorithm against one or more of the fields in the packet header to determine the hash value. It then compares the value to the hash assignment table to see which MACH5 is assigned to the corresponding bucket and then forwards the

packet to that appliance. When you configure the service group on the MACH5 appliances, you specify which field(s)—destination IP address, destination port, source IP address, and/or source port—should be used to calculate the hash value.

In some cases, since all of the packets are hashed using the same fields and algorithm, it is possible that one of the caches in the group can become overloaded. For example, if you have a large proportion of traffic that is directed to the same server and you are using the destination IP address to run the hashing function, it is possible that the bulk of the traffic will be redirected to the same MACH5 appliance. Therefore, you can configure an alternate field or group of fields to use to run the hashing algorithm. The router will then use this alternate hashing algorithm if the number of GRE packets or MAC addresses (depending on the forwarding method you're using) redirected to a given MACH5 exceeds a certain number.

For details on configuring a hash-weight value to adjust the proportion of the hash table that gets assigned to a MACH5, see "Load Balancing across MACH5 Appliances" below.

- **Mask Assignment**— With mask assignment, each router in the service group has a table of masks and values that it uses to distribute traffic across the MACH5 appliances in the service group. When the router receives a packet, it performs a bitwise AND operation between the mask value and the field of the packet header that is designated in the MACH5 mask assignment configuration. It then compares the result against its list of values for each mask; each value is assigned to a specific MACH5 in the service group.

Load Balancing across MACH5 Appliances

Each MACH5 in the service group is assigned roughly an even percentage of the load by default, regardless of assignment type. If you would like to adjust or balance the load across multiple MACH5 appliances, you can assign a weight value to each MACH5 in the group. MACH5 appliances with higher weight values receive a larger portion of the redirected traffic.

For example, suppose you have assigned the following weight values: MACH51=100, MACH52=100, and MACH53=50 respectively. The total weight value is 250, and so MACH51 and MACH52 will each receive 2/5 of the traffic (100/250) and MACH53 will receive 1/5 of the traffic (50/250).

If a MACH5 becomes unavailable, the load will automatically be redistributed across the remaining MACH5 appliances in the service group.

Prerequisites for Configuring WCCP on the MACH5

Before you configure WCCP on the MACH5, you must complete the following tasks:

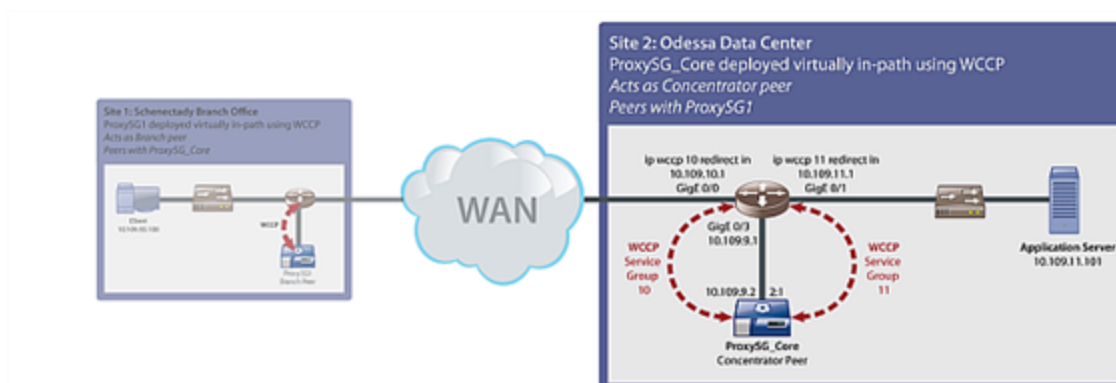
- Plan your service groups.
 - Decide which routers and which MACH5 appliances will work together in the redirection scheme.
 - If you are configuring VLAN interfaces for WCCP, the MACH5 appliance must be deployed on a VLAN trunk and you must enable VLAN trunking on the applicable interface of the MACH5.

- Determine the WCCP capabilities that your router/switch supports.
- Refer to the documentation that came with your router for the specifics on your router/switch.
- In WCCP v1, you can only intercept TCP traffic on destination port 80, which is the default web-cache service group. In addition, you can only configure a single home router to communicate with one or more MACH5 appliances in a service group.
- Blue Coat recommends the use of version 2.0. WCCP v2 allows you to configure multiple service groups, intercepts and redirects any IP traffic, supports MD5 hash-based authentication, supports a service group with up to 32 MACH5 appliances and up to 32 routers, permits multiple hash distributions. For a complete list of WCCP v2 capabilities, refer to Cisco documentation.
- Decide what traffic you want to redirect. Do you want to redirect all traffic, or just a specific protocol or specific ports? Do you want to exclude certain hosts or traffic from redirection?
- Decide what forwarding and return method you plan to use. All service groups configured on a router must use the same forwarding and packet return method. Further, make sure that all the routers in the service group support the chosen forwarding and the return method.
- Decide how the router will assign a specific redirected packet to a MACH5 appliance. Make sure the router(s) in the service group support the assignment method you plan to use. If there is more than one MACH5 in the service group, decide whether you want to distribute traffic equally, or if you want to assign varying weights.
- Configure the routers. For information on the feature sets and the capabilities of your router and for configuring it, refer to the router documentation.

See Configure WCCP for details on configuring your MACH5 appliance for WCCP redirection.

Deploy a Concentrator Peer Virtually In-Path

This example shows how to deploy the Concentrator peer in a basic virtually in-path configuration. The Concentrator peer, ProxySG_Core, is configured as an acceleration node. It will accept inbound tunnel connections from the Branch peer at the Schenectady site.





A MACH5 appliance can act as both a Concentrator peer and a Branch peer depending on its role in a given tunnel. (See "What are the Acceleration Roles?" on page 157) In this example, ProxySG_Core does not intercept client traffic and therefore it acts as a Concentrator peer only.

Step 1: Prepare for an Acceleration Deployment

1. Plan the configuration of the concentrator peers. A worksheet is available to record your configuration settings. See "Plan the Configuration of the Concentrator Peers" on page 54.
2. Plan the WCCP configuration. See "Plan WCCP Configuration" on page 73.
3. Verify that the Cisco model hardware and IOS version supports the WCCP features required for this deployment. See "WCCP Tested Platforms" on page 74 for a list of the Cisco hardware and software platforms and WCCP capabilities that have been tested with the MACH5 appliance.
4. Make sure all MACH5 appliances are running SGOS version 6.5 with the factory default settings.
 - a. Upgrade all appliances as described in Upgrade/Downgrade an SGOS Image.
 - b. After upgrading, restore the appliance to its factory default state using the `restore-defaults factory-defaults` CLI command. Note that you must be connected to the MACH5 console to issue this command.
5. Before you install the MACH5 appliance, test network connectivity to the remote sites. You will repeat this step after the appliance has been installed to reverify network connectivity.

For example, to ping a host at a remote site as shown in the [topology diagram](#), type the following commands at the command prompt on a local client:

```
ping 10.109.10.100
```

6. If you have a firewall between the ADN Concentrator peer and the ADN Branch peer, make sure the tunnel listening port is open. This port allows the creation of the control connection for the tunnel, which enables byte-cache dictionary synchronization. By default, the tunnel listening port is set to 3035 (plain) and 3037 (secure).

Step 2: Integrate the Appliance into the Network

1. Connect to the MACH5 serial console (9600, 8, N, 1) and launch the Blue Coat ProxySG configuration wizard. For detailed instructions, see "Configure Basic Network Info for a Virtually In-Path Acceleration Peer" on page 75.

```

----- CONFIGURATION START -----
Welcome to the Blue Coat ProxySG 210 configuration wizard.
This appliance's serial number: 0

You can get field help by entering a question mark ? in the fields.
You can move backwards through the steps by pressing the UP arrow.
You can exit the wizard without saving your entries by pressing ESC.

Step 1: How do you plan to configure this appliance?
a) Through a manual setup
b) Through a Director-managed setup
Your choice:

Step 2: Which solution would you like to implement?
a) Acceleration
b) Other solution
Your choice: ☐ a

Step 3: How will you deploy this appliance?
a) Physically in-path
b) Virtually in-path using WCCP
c) Any other
Your choice: ☐ b

Step 4: Appliance name [ProxySG 210 0408063522] ProxySG_Core

Step 5: You have chosen to configure this appliance to use WCCP.
Your appliance has the following interfaces.

Interface      IP address      Subnet mask      Speed (Mbps) Duplex  Type
-----
a) 2:0-2:1     0.0.0.0         0.0.0.0          no link       HW bridge

Select an interface by entering the letter.
Your choice: ☐ a
IP address for 0:0-0:1 ☐ ..... 10.109.9.2
Subnet mask ☐ .....
Speed and duplex undetected
Automatically detect when link exists [yes] .
Does this interface require a VLAN? [no] ....

The configuration has now met the requirement for WCCP.

Interface      IP address      Subnet mask      Speed (Mbps) Duplex  Interface
-----
a) 0:0-0:1     10.109.9.2      255.255.255.0    no link

You can select another interface to configure or press enter to continue.
Your choice: ☐

Step 6: Default gateway ☐ 10.109.9.1
>> Pinging 10.109.9.1...FAILED

Step 7: Primary DNS server ☐ 10.2.2.100
>> Testing DNS server
>> DNS query failed

Step 8: Administrator ID [admin]

Step 9: Administrator password ☐
Retype administrator password ☐ *****
>> Password is easily guessed. Choose another? y/n [yes] n

Step 10: After you complete WCCP configuration in the graphical UI
do you want to activate acceleration? [yes]

```

2. Power off the MACH5 appliance.
3. Rack mount the MACH5 appliance. Refer to the *ProxySG Quick Start Guide* for instructions.
4. To cable the appliance, connect the MACH5 LAN interface to a dedicated interface on the router or switch using a crossover cable.



You must attach the MACH5 LAN interface to a dedicated network reachable by the Cisco router; do not attach the MACH5 to a network that will traverse a router interface on which you plan to configure WCCP redirection. In addition, to use L2 forwarding/return on a Cisco Layer-3 switch, you must install the MACH5 appliance on the same broadcast domain as a dedicated Layer-3 interface on the switch.

5. From the router CLI, create the WCCP service groups and apply them to the WAN and LAN interfaces.

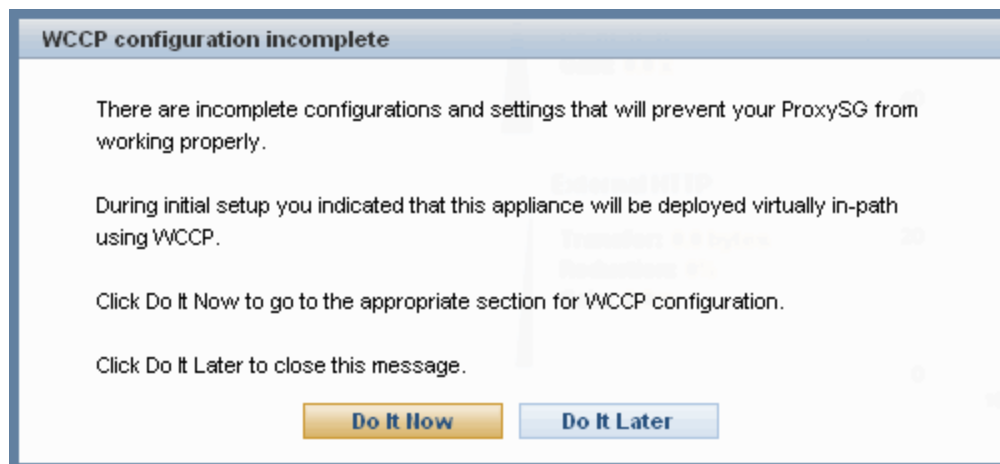
```

Router(config)#ip wccp version 2
Router(config)#ip wccp 10
Router(config)#ip wccp 11
Router(config)#interface gigabitethernet0/0
Router(config-if)#description WAN side
Router(config-if)#ip wccp 10 redirect in
Router(config-if)#exit
Router(config)#interface gigabitethernet0/1
Router(config-if)#description LAN side
Router(config-if)#ip wccp 11 redirect in

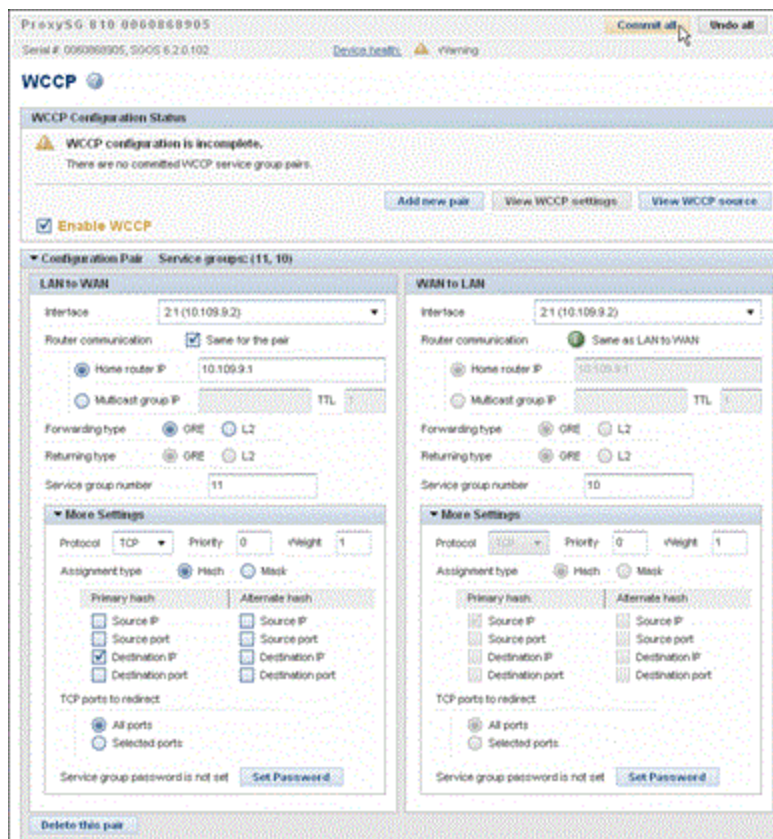
```

6. Power on the MACH5 appliance.
7. Go to the following URL to launch the Sky Management Console: `https://<ProxySG_IP_address>:8082`. Because you indicated that you are deploying the appliance virtually in-path, the interface prompts you to configure WCCP.

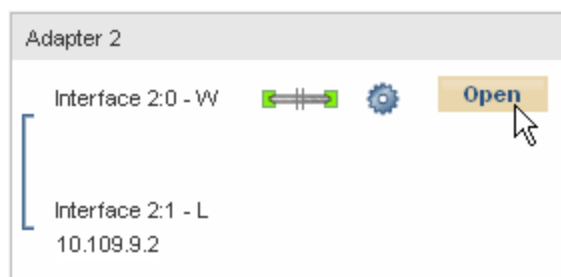
For example, to launch the Sky Management Console on the Odessa appliance you would enter:
`https://10.109.9.2:8082`



8. Create the LAN-to-WAN and WAN-to-LAN service groups on the MACH5 (known as a *WCCP pair*) as follows:
 - a. When prompted to configure WCCP, click **Do It Now**.
 - b. Select **Enable WCCP**.
 - c. Click **Add new pair**.
 - d. Create the service groups.



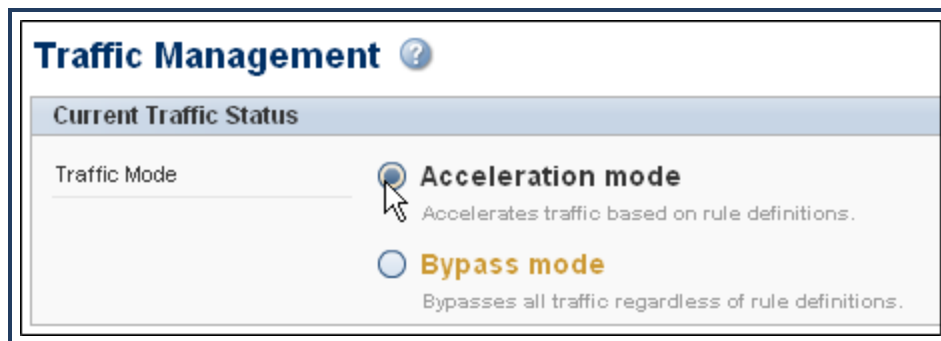
- e. Click **Commit all**.
 - f. Verify that the service groups negotiate successfully and the **State** changes to **Ready**.
9. Verify that the configured link settings (speed/duplex) on the MACH5 interface match the configured settings on the connected switch/router interface.
 - a. Select **System Settings > Adapters & Interfaces**.
 - b. In the box that corresponds to the interface that is connected to the switch or router in the Adapter Overview section of the tab, click **Open**.



- c. Verify that the **Speed and duplex** settings match the settings that are defined on the router or switch interface.
 - d. Click **Close**.
 - e. If you made any changes, click **Commit all**
10. Verify that the MACH5 appliance is bypassing traffic.
- a. Select **Report > Active Sessions**.
 - b. In the **Connection Type** field, select **Bypassed** and then click **Submit**.
 - c. Look for one-way traffic, which can indicate asymmetric routing. This can interfere with acceleration.

Step 3: Configure Acceleration

1. If you did not enable acceleration during initial configuration, enable it now.
 - a. Select **Configure > Acceleration > Traffic Management**.
 - b. Select **Acceleration mode**.

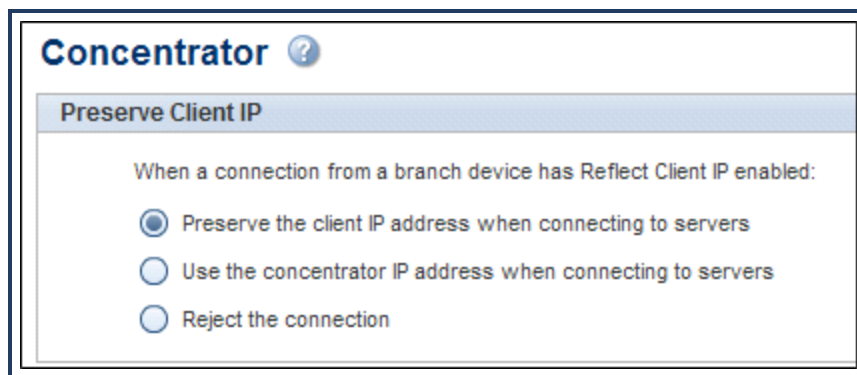


- c. Click **Commit all**.



In Open configurations such as this one, you do not need to configure an ADN manager. If you want to change this deployment to an Open Managed or a Closed deployment, see "Switch Acceleration Modes" on page 33.

2. **Preserve the client IP address for inbound connections.**
 - a. Select **Configure > ADN > Concentrator**.
 - b. Select **Preserve the client IP address when connecting to servers**.



The screenshot shows a window titled "Concentrator" with a question mark icon. Below the title bar is a section titled "Preserve Client IP". Inside this section, there is a text label: "When a connection from a branch device has Reflect Client IP enabled:". Below this label are three radio button options: "Preserve the client IP address when connecting to servers" (which is selected), "Use the concentrator IP address when connecting to servers", and "Reject the connection".

- c. Click **Commit all**.

3. Enable IP Forwarding.

- a. Click **Advanced configuration** to go to the Advanced Management Console.
- b. Select **Configuration > Network > Routing**.
- c. Select **Enable IP forwarding**.



The screenshot shows a configuration section titled "IP Forwarding". Below the title is a checkbox labeled "Enable IP forwarding", which is checked with a green checkmark.

- d. Click **Apply**.

- 4. Check the health state of the appliance in the upper right hand corner of the Advanced Management Console window. Make sure appliance Health is **OK**. If the health is **Warning** or **Critical**, click the status link to view details about the health issues.

Plan WCCP Configuration

If you are deploying the MACH5 appliance virtually in-path, you must plan your WCCP deployment. To configure WCCP, you must define settings on both the WCCP-capable Cisco router(s) and the MACH5 appliance(s) that make up the redirection service group. The WCCP service group on the router and on the MACH5 define what traffic the router should redirect, the method the router should use to forward packets to the MACH5 appliance, and the algorithm to use to choose a MACH5 to which to redirect traffic. For more detailed information about WCCP and the settings you can define, refer to the *WCCP Reference Guide*.

To simplify the WCCP configuration process, record the settings you plan to use for each service group on the [WCCP Configuration Worksheet](#).



The [worksheet](#) is an interactive PDF form that you can fill in on screen before printing. You may also want to save the completed worksheet file for future reference.

For each service group, this worksheet includes the following sections:

Router Configuration for Service Group—Define the routers that are part of the service group. For each router, record the interfaces on which you will enable redirection and the interface to which the ProxySG MACH5 appliance will connect.

ProxySG Configuration for Service Group—Define the WCCP settings for the service group, including what ProxySG interface to include in the service group, what forwarding/return method the router will use to forward redirected packets to the ProxySG, the assignment type the router will use to pick a ProxySG to receive the redirected packet, and the IP addresses of the router(s) in the service group. Note that the WCCP settings that are supported vary greatly from router to router. To determine what features are supported on your specific routing/switching platform, refer to the documentation for your specific hardware platform and IOS version.

This worksheet assumes that you have one router and one MACH5 in each service group. However, each service group may actually include multiple routers and/or MACH5 appliances (up to 32 of each). In addition, each router and each MACH5 can be configured with multiple service groups, each with a different set of redirection rules. Use as many worksheets as you need to document your planned WCCP service group settings.

WCCP Tested Platforms

The following table summarizes the Cisco hardware and software platforms that Blue Coat has tested with the MACH5 WCCP feature on SGOS 6.5. Although you can use other WCCP-capable Cisco hardware and software in your MACH5 WCCP deployment, you must check the Cisco documentation to determine the specific WCCP features that are supported on the platform.

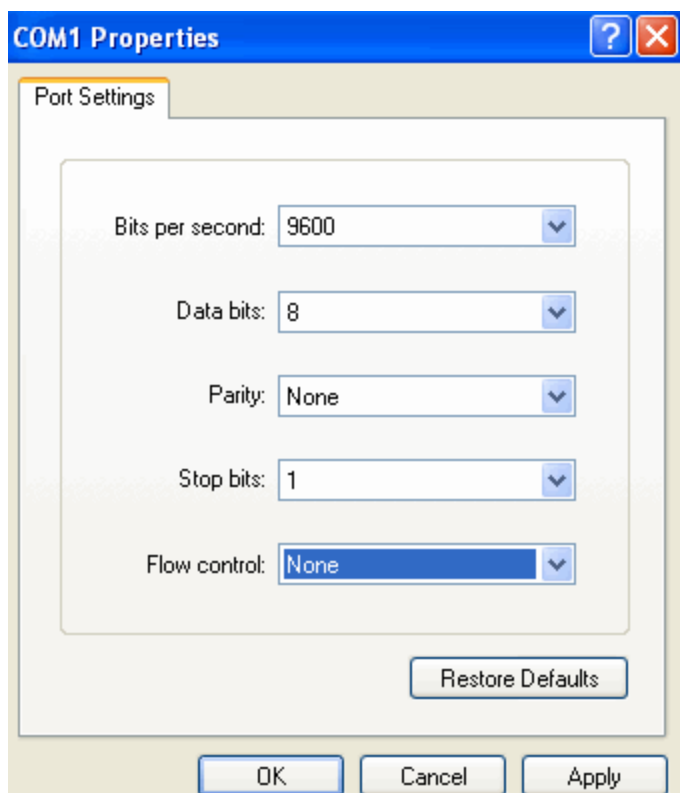
Cisco Hardware and Software Platform	Features Tested with MACH5 running SGOS 6.5				
	GRE/GRE	L2/GRE	L2/L2	Mask	Hash
Cisco 6506 Software (s72033_rp-ADVENTERPRISEK9-M), Version 12.2(33)SXH3a, RELEASE SOFTWARE (fc1)					
Cisco 2821 Version 12.4(13r)T, RELEASE SOFTWARE (fc1)					
Cisco 3825 Version 12.4(13r)T, RELEASE SOFTWARE (fc1)					
Cisco 3650E					
Version 12.2(44r)SE3 RELEASE SOFTWARE					
Cisco IOS Software, 3800 Software (C3825-ADVENTERPRISEK9-M), Version 12.4(22)T, RELEASE SOFTWARE (fc1)					
ROM: Bootstrap program is C3560 boot loader BOOTLDR: C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(44)SE5, RELEASE SOFTWARE (fc1)					
Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version 15.0(1)M3, RELEASE SOFTWARE (fc2)					

Configure Basic Network Info for a Virtually In-Path Acceleration Peer

Use the following procedure to connect to the MACH5 serial console and configure the basic network settings on an appliance that you plan to deploy virtually in-path as an acceleration peer. You can use whatever terminal emulation software you want. This procedure shows how to perform initial configuration using Windows HyperTerminal.

1. To launch Windows HyperTerminal, select **Start > Programs > Accessories > Communications > HyperTerminal**.
2. (Optional) Name the connection for later use.
3. Select the communication port and set the communication parameters.

For example, select COM1 and set the communication parameters as shown below:

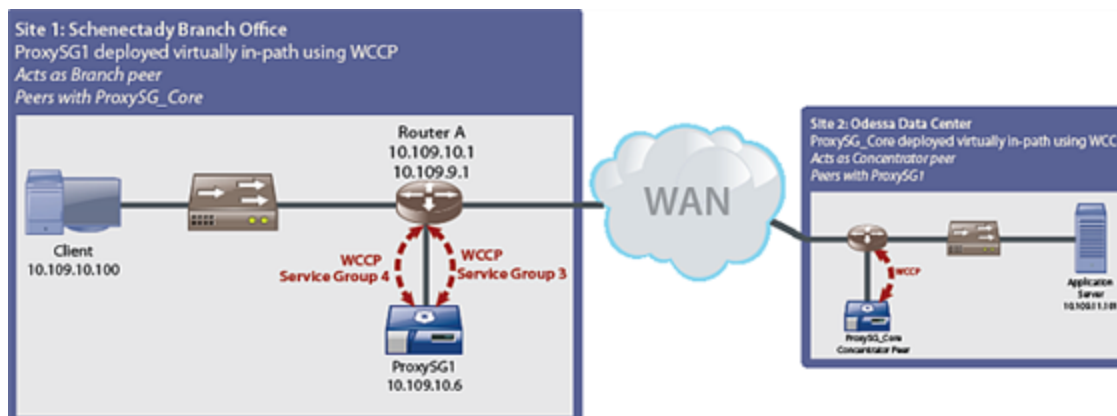


4. Click **OK** to save your settings.
5. Activate the serial console and launch the setup console for a manual setup.
 - a. Connect the serial cable from your laptop to the MACH5 and power on the appliance. The appliance will go through a bootup process. This may take a moment.

- b. Press **Enter** three times to activate the MACH5 serial console.
 - c. When prompted, enter **2** to launch the setup console.
 - d. When prompted, enter **a** to initiate a manual setup.
6. Enter **a** to specify that you are configuring the appliance for acceleration.
Step 2: Which solution would you like to implement?
a) Acceleration
b) Other solution
Your choice: [] **a**
7. To specify a virtually in-path deployment, enter **b**.
Step 3: How will you deploy this device?
a) Physically in-path
b) Virtually in-path using WCCP
c) Any other
Your choice: [] **b**
8. (optional) Enter the new name for the appliance when prompted or press **Enter** to accept the default name.
9. Configure the interface(s).
 - a. When prompted, select the interface to configure or press **Enter** to select the default interface.
 - b. Enter the IP address.
 - c. Enter the subnet mask.
 - d. Press **Enter** to specify that you want the appliance to automatically detect speed/duplex settings.
 - e. If you use a VLAN other than the native VLAN for your management traffic, enter **y** when prompted to configure a VLAN and then enter the VLAN ID when prompted.
 - f. Press **Enter** to continue.
10. Follow the prompts in the script to configure the default gateway address, DNS server address, and the administrator ID and password.
11. When prompted, press **Enter** to turn on acceleration immediately after configuring WCCP.
12. To save your settings, press **Enter**.

Deploy a Branch Peer Virtually In-Path

This example shows how to deploy the Concentrator peer in a basic virtually in-path Open configuration. The Branch peer, ProxySG1, is configured as an acceleration node. The MACH5 appliance intercepts application requests from local clients and establishes a tunnel connection with the concentrator peer at the Odessa data center to accelerate application traffic. Router A and ProxySG1 are configured with two WCCP service groups: service group 4 redirects outbound traffic from this site to the WAN (LAN-to-WAN traffic); service group 3 redirects inbound traffic heading into this site from the remote sites via the WAN to ProxySG1 (WAN-to-LAN traffic).



Step 1: Prepare for an Acceleration Deployment

1. Plan the configuration of branch peers. A worksheet is available to record your configuration settings. See "Plan the Configuration of Branch Peers" on page 61
2. Plan the WCCP configuration. See "Plan WCCP Configuration" on page 73.
3. Verify that the Cisco model hardware and IOS version supports the WCCP features required for this deployment. See "WCCP Tested Platforms" on page 74 for a list of the Cisco hardware and software platforms and WCCP capabilities that have been tested with the MACH5.
4. Make sure all MACH5 appliances are running SGOS version 6.5 with the factory default settings.
 - a. Upgrade all appliances as described in Upgrade/Downgrade an SGOS Image.
 - b. After upgrading, restore the appliance to its factory default state using the `restore-defaults` CLI command. Note that you must be connected to the MACH5 console to issue this command.
5. Before you install the MACH5 appliance, test network connectivity to the remote sites. You will

repeat this step after the appliance has been installed to reverify network connectivity.

For example, to ping a host at a remote site as shown in the [topology diagram](#), type the following commands at the command prompt on a local client:

ping 10.109.11.101

6. If you have a firewall between the ADN Concentrator peer and the ADN Branch peer, make sure the tunnel listening port is open. This port allows the creation of the control connection for the tunnel, which enables byte-cache dictionary synchronization. By default, the tunnel listening port is set to 3035 (plain) and 3037 (secure).

Step 2: Integrate the Appliance into the Network

1. Connect to the MACH5 serial console (9600, 8, N, 1) and launch the Blue Coat ProxySG configuration wizard. For detailed instructions, see "Configure Basic Network Info for a Virtually In-Path Acceleration Peer" on page 75.

```

Step 1: How do you plan to configure this appliance?
a) Through a manual setup
b) Through a Director-managed setup
Your choice: [] a

Step 2: Which solution would you like to implement?
a) Acceleration
b) Other solution
Your choice: [] a

Step 3: How will you deploy this appliance?
a) Physically in-path
b) Virtually in-path using WCCP
c) Any other
Your choice: [] b

Step 4: Appliance name [ProxySG 210 0408063522] ProxySG_Core

Step 5: You have chosen to configure this appliance to use WCCP.
Your appliance has the following interfaces.

Interface      IP address      Subnet mask      Speed
(Mbps) duplex  Type
-----
a) 0:0-0:1      0.0.0.0          0.0.0.0          no link
hw bridge

Select an interface by entering the letter.
Your choice: [] a
IP address for 0:0-0:1 [] ..... 10.109.10.6
Subnet mask [] .....255.255.255.0

Speed and duplex undetected
Automatically detect when link exists [yes] .
Does this interface require a VLAN? [No] ....

The configuration has now met the requirement for WCCP.

Interface      IP address      Subnet mask      Speed      Interface
(Mbps) duplex  Type
-----
a) 0:0-0:1      10.109.10.6      255.255.255.0    no link

You can select another interface to configure or press Enter to continue.
Your choice: []

Step 6: Default gateway [] 10.109.10.1
>> Ping 10.109.9.1...FAILED

Step 7: Primary DNS server [] 10.100.10.101
>> Testing DNS server
>> DNS query failed

Step 8: Administrator ID [admin]

Step 9: Administrator password [] *****
Retype administrator password [] *****
>> Password is easily guessed. Choose another? y/n [yes] n

Step 10: After you complete WCCP configuration in the graphical UI
do you want to activate acceleration? [yes]

```

2. Power off the MACH5 appliance.
3. Rack mount the MACH5 appliance. Refer to the *ProxySG Quick Start Guide* for instructions.
4. To cable the appliance, connect the MACH5 LAN interface to a dedicated interface on RouterA using a crossover cable.



You must attach the MACH5 LAN interface to a dedicated network reachable by the Cisco router; do not attach the MACH5 to a network that will traverse a router interface on which you plan to configure WCCP redirection. In addition, to use L2 forwarding/return on a Cisco Layer-3 switch, you must install the MACH5 on the same broadcast domain as a dedicated Layer-3 interface on the switch.

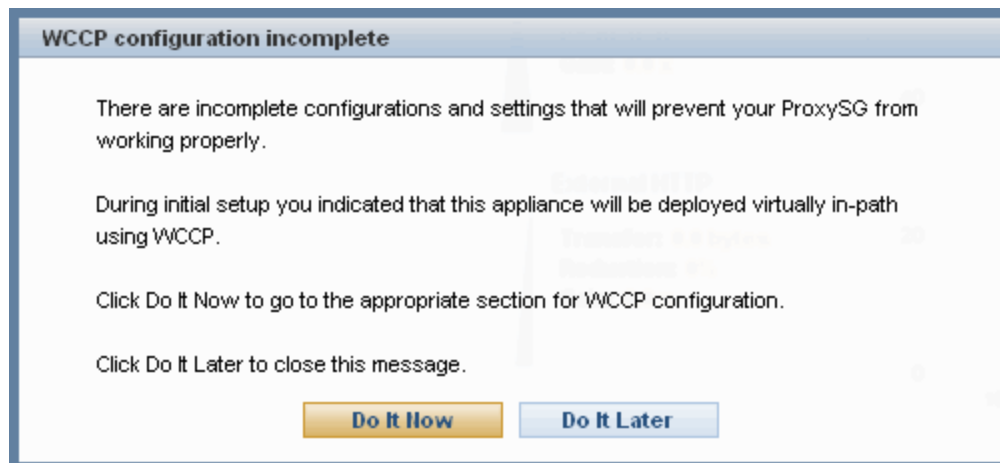
5. From the router CLI, create the WCCP service groups and apply them to the WAN and LAN

interfaces.

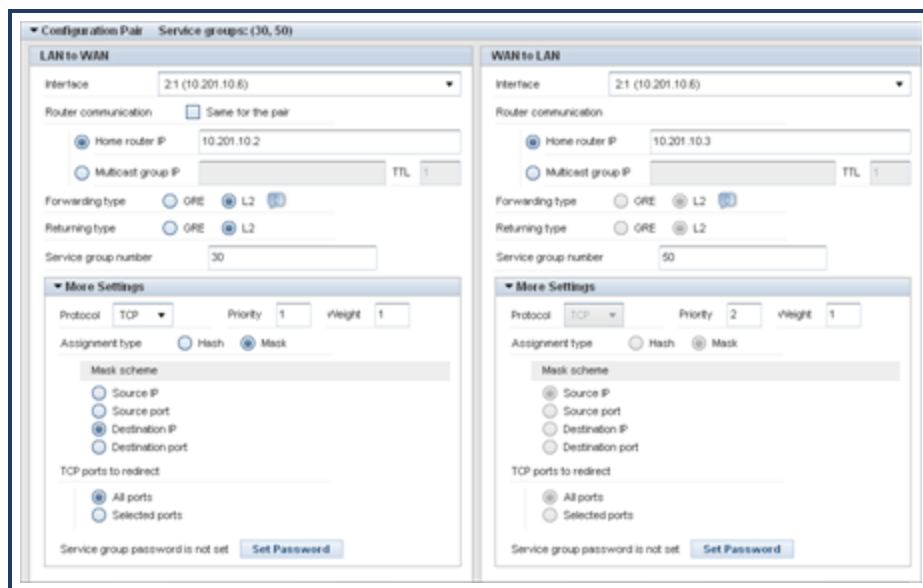
```
Router(config)#ip wccp version 2
Router(config)#ip wccp 3
Router(config)#ip wccp 4
Router(config)#interface gigabitethernet0/5
Router(config-if)#description WAN side
Router(config-if)#ip wccp 4 redirect in
Router(config-if)#exit
Router(config)#interface gigabitethernet0/6
Router(config-if)#description LAN side
Router(config-if)#ip wccp 3 redirect in
```

6. Power on the MACH5.
7. Go to the following URL to launch the Sky Management Console: https://<ProxySG_IP_address>:8082. Because you indicated that you are deploying the appliance virtually in-path, the interface prompts you to configure WCCP.

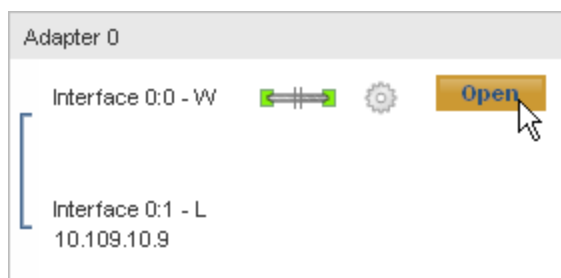
For example, to launch the Sky Management Console on the Schenectady appliance you would enter: <https://10.109.10.6:8082>



8. Create the LAN-to-WAN and WAN-to-LAN service groups on the MACH5 (known as a *WCCP pair*) as follows:
 - a. When prompted to configure WCCP, click **Do It Now**.
 - b. Select **Enable WCCP**.
 - c. Click **Add new pair**.
 - d. Create the service groups.



- e. Click **Commit all**.
 - f. Verify that the service groups negotiate successfully and the **State** changes to **Ready**.
9. Verify that the configured link settings (speed/duplex) on the MACH5 interface match the configured settings on the connected switch/router interface.
- a. Select **System Settings > Adapters & Interfaces**.
 - b. In the box that corresponds to the interface that is connected to the switch or router in the Adapter Overview section of the tab, click **Open**.

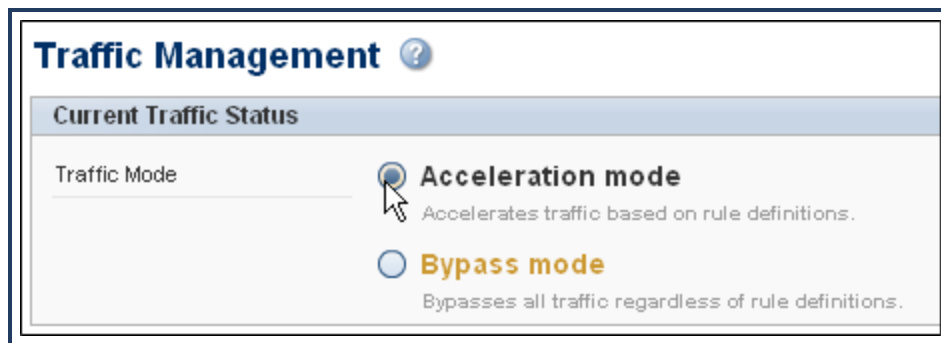


- c. Verify that the **Speed** and **duplex** settings match the settings that are defined on the router or switch interface.
 - d. Click **Close**.
 - e. If you made any changes, click **Commit all**
10. Verify that the MACH5 appliance is bypassing traffic.

- a. Select **Report > Active Sessions**.
- b. In the **Connection Type** field, select **Bypassed** and then click **Submit**.
- c. Look for one-way traffic, which can indicate asymmetric routing. This can interfere with acceleration.

Step 3: Configure Acceleration

1. If you did not enable acceleration during initial configuration, enable it now.
 - a. Select **Configure > Acceleration > Traffic Management**.
 - b. Select **Acceleration mode**.



- c. Click **Commit all**.



In Open configurations such as this one, you do not need to configure an ADN manager. If you want to change this deployment to an Open Managed or a Closed deployment, see "Switch Acceleration Modes" on page 33.

2. Enable IP Forwarding.
 - a. Click **Advanced configuration** to launch the Advanced Management Console.
 - b. Select **Configuration > Network > Routing**.
 - c. Select **Enable IP forwarding**.



- d. Click **Apply**.
3. Check the health state of the appliance in the upper right hand corner of the Advanced Management Console

window. Make sure appliance Health is **OK**. If the health is **Warning** or **Critical**, click the status link to view details about the health issues.

Step 4: Configure Proxy Services

1. (optional) Customize what traffic the MACH5 accelerates.
 - a. From the Sky Management Console, select **Configure > Acceleration > Traffic Management**. The MACH5 appliance automatically intercepts a default set of services based on your deployment (explicit or transparent).
 - b. Modify which services get intercepted and bypassed by selecting the radio button in the Intercept or Bypass column of the Services table as appropriate. You can only select services that can be accelerated.

Service name	Acceleration techniques	Intercept	Bypass	Edit	Del
BGP	Monitor only	Not applicable			
Blue Coat ACN	Monitor only	Not applicable			
Blue Coat Managem...	Monitor only	Not applicable			
OPFS	Application level	<input checked="" type="radio"/>	<input type="radio"/>		
Osco PSec VPN	Monitor only	Not applicable			
CRic	Network level	<input checked="" type="radio"/>	<input type="radio"/>		
Default	Data level	<input checked="" type="radio"/>	<input type="radio"/>		
DNS	Application level	<input checked="" type="radio"/>	<input type="radio"/>		
Echo	Monitor only	Not applicable			
Endpoint Mapper	Application level	<input checked="" type="radio"/>	<input type="radio"/>		
Explicit HTTP	Application level	<input checked="" type="radio"/>	<input type="radio"/>		
External HTTP	Application level	<input checked="" type="radio"/>	<input type="radio"/>		
FTP	Application level	<input checked="" type="radio"/>	<input type="radio"/>		
FTPS	Monitor only	Not applicable			
H.323	Monitor only	Not applicable			

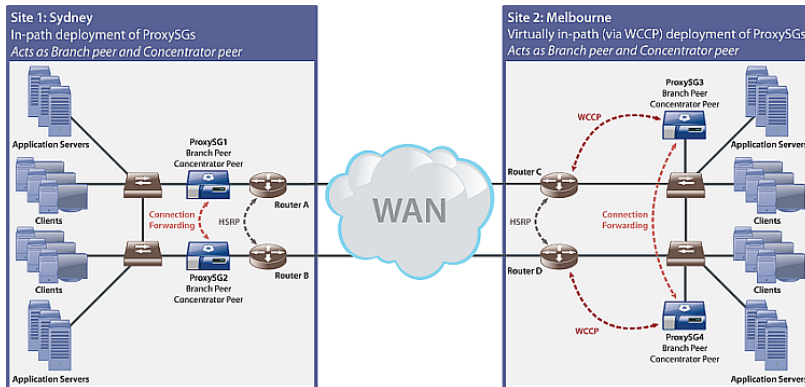
2. Verify that the MACH5 appliances are intercepting and accelerating traffic as expected. See "Verify the Acceleration Deployment" on page 35.

Redundant Acceleration Topology

In the following example, each corporate site uses one of the recommended redundant acceleration deployments:

- **Site 1: Sydney**—This site has redundant LAN and WAN links with two MACH5 appliances deployed in-path. These MACH5 appliances act as both Branch peers and Concentrator peers. As Branch peers, the MACH5 appliances intercept traffic and establish tunnel connections with Concentrator peers at the Melbourne site to optimize the traffic. As Concentrator peers, ProxySG1 and ProxySG2 terminate client connections from the Melbourne site.

- **Site 2: Melbourne**—This site has two MACH5 appliances deployed virtually in-path using WCCP. These MACH5 appliances act as both Branch peers and Concentrator peers. As Branch peers, the MACH5 appliances intercept traffic and establish tunnel connections with Concentrator peers at the Sydney site to optimize the traffic. As Concentrator peers, ProxySG3 and ProxySG4 terminate client connections from the Sydney site.



The following sections describe how to configure each of the MACH5 appliances in this example topology and show how to verify that traffic is being accelerated as expected:

1. "Deploy In-Path with Redundant Links" below.
2. "Deploy Virtually In-Path in a Redundant Layer 2 Network" on page 98.
3. "Verify the Acceleration Deployment" on page 35.

Deploy In-Path with Redundant Links

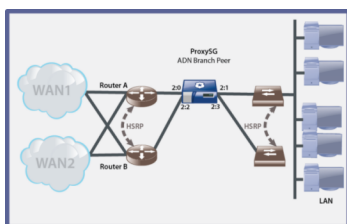
Blue Coat offers two options for setting up an in-path deployment with redundant routers and switches:

- "Deploy One MACH5 In-Path with Two Redundant Links" on the next page: A single MACH5 appliance with a four-port LAN option card installed; each bridge is connected to a separate WAN link. This option is less expensive since it uses a single MACH5 at the branch or core, but it has several drawbacks. The MACH5 becomes a single point of failure (even with fail-to-wire capability) and when the appliance goes offline for maintenance, both links will be down.
- "Deploy Two MACH5s In-Path with Redundant Links" on page 92: Two MACH5 appliances, with each appliance connected to a redundant path. This is the recommended option since it does not have the drawbacks of the single-appliance solution.

Deploy One MACH5 In-Path with Two Redundant Links

This example shows how to deploy a single MACH5 appliance in a redundant network with two routers and two switches; a four-port LAN option card is required for this deployment. The network devices in this topology are configured as follows:

- Routers are configured with Hot Standby Routing Protocol (HSRP) or Virtual Router Redundancy Protocol, which enables the standby router to take over if the primary router fails. HSRP or VRRP provides dynamic fail-over functionality between the routers by using a virtual IP address that is shared by the routers. This shared virtual IP allows the routers to appear as a single virtual router, while they share routing information and maintain connectivity with each other. HSRP/VRRP ensures that while the members of the virtual router group continually exchange information, only one of the routers is active and is forwarding packets on behalf of the virtual router. In the event the active router fails, the standby router seamlessly assumes the responsibility of routing traffic through the network.
- The switches are physically connected to one another with a cable and can sense if the other fails.
- A four-port LAN option card is installed in the MACH5 appliance. This card includes two sets of WAN and LAN interfaces; each pair of WAN and LAN interfaces is bridged to provide a network link. Each bridge is then connected to a router that participates in the HSRP/VRRP scheme, to ensure continuous network connectivity.
- Each hardware bridge is assigned a unique IP address.



Step 1: Prepare for the Acceleration Deployment

1. Plan the configuration of acceleration peers. A worksheet is available to record your configuration settings. See "Plan Configuration of Acceleration Peers" on page 90.
2. Verify that the routers are configured with HSRP or VRRP.
3. Install the four-port LAN option card on the MACH5 appliance. Note that lower-end models do not have support for these cards. Refer to the *Maintenance and Upgrade Guide* for your MACH5 model.

<https://bto.bluecoat.com/documentation/All-Documents/ProxySG>

4. Make sure the MACH5 appliance is running SGOS version 6.5 with the factory default settings.
 - a. Upgrade the appliance as described in Upgrade/Downgrade an SGOS Image.
 - b. After upgrading, restore the appliance to its factory default state using the `restore-defaults factory-defaults` CLI command. Note that you must be connected to the MACH5 console to issue this command.
5. Before you install the MACH5 appliance, test network connectivity to the remote sites. You will repeat this step after the MACH5 has been installed to reverify network connectivity.

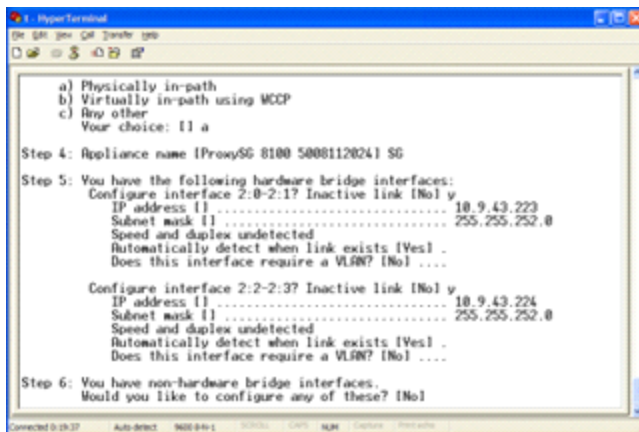
For example, to ping a host at a remote site, type the following commands at the command prompt on a local client:

ping 10.201.10.100

6. If you have a firewall between the ADN Concentrator peer and the ADN Branch peer, make sure the tunnel listening port is open. This port allows the creation of the control connection for the tunnel, which enables byte-cache dictionary synchronization. By default, the tunnel listening port is set to 3035 (plain) and 3037 (secure).

Step 2: Integrate the Appliance into the Network

1. Connect to the serial console (9600, 8, N, 1) of the MACH5 appliance and launch the Blue Coat ProxySG configuration wizard. For detailed instructions, see "Configure Basic Network Information for an In-Path Acceleration Peer (Serial Console)" on page 54. Make sure to assign a unique IP address to each bridge pair on the four-port LAN option card.



2. Power off the MACH5 appliance.
3. Rack mount the MACH5 appliance. Refer to the *ProxySG Quick Start Guide* for instructions.

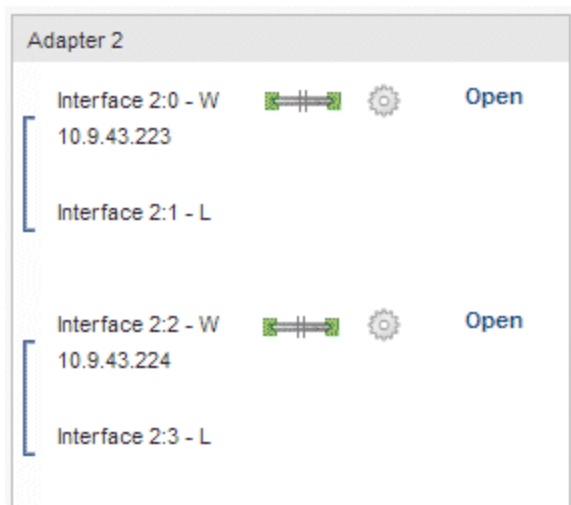


With in-path deployments, there will be some network downtime when installing the MACH5.

4. Cable the appliance as follows:
 - Connect a crossover cable from one of the routers to the first WAN interface of the four-port card.
 - Connect a straight-through cable from the switch to the corresponding LAN interface for the bridge.
 - Connect a crossover cable from the other router to the second WAN interface of the four-port card.
 - Connect a straight-through cable from the other switch to the corresponding LAN interface for the bridge.
5. Power on the MACH5 appliance.
6. Verify network connectivity to remote sites by repeating the ping test. Check adapter LEDs and cables if you cannot reach the remote sites.
7. Go to the following URL to launch the Sky Management Console: `https://<ProxySG_IP_address>:8082`.

For example:

`https://10.103.10.221:8082`
8. Verify that the configured link settings (speed/duplex) on the MACH5 interface match the configured settings on the connected switch/router interfaces.
 - a. Select **System Settings > Adapters & Interfaces**.
 - b. In the Adapter 2 box, click **Open** for the bridge you want to modify.



If you configure speed/duplex settings other than **Auto-negotiate** on either bridge interface, the other bridge interface will inherit the same settings.

- c. Verify that the **Speed and duplex** settings match the settings that are defined on the router or switch interface.
 - d. Click **Close**.
 - e. Configure other interfaces (such as a Management port).
 - f. If you made any changes, click **Commit all**
9. (Optional) Create a VLAN interface on the MACH5 for each VLAN for which the appliance must handle traffic.
- a. Click **Advanced configuration** to go to the Advanced Management Console.
 - b. Select **Configuration > Network > Adapters > Adapters**.
 - c. Select the interface that is connected to the switch (the LAN interface).
 - d. Click **New VLAN** to create a VLAN interface. See "Set Up and Verify VLAN Interfaces" on page 91 for detailed instructions on how to configure the VLAN.
10. Verify that the MACH5 appliances are bypassing traffic:
- a. Select **Statistics > Sessions > Active Sessions > Bypassed Connections**.
 - b. Look for one-way traffic (shows up in red), which can indicate asymmetric routing. This can interfere with acceleration.

Step 3: Configure Acceleration

1. If the MACH5 appliance will act as a Concentrator peer, enable client IP address reflection for inbound connections.
 - a. Select **Configuration > ADN > Tunneling > Network**.
 - b. In the Reflect Client IP for MACH5 peers section or the tab, select **Allow the request and reflect the client IP**.
 - c. Click **Apply**.
2. If the MACH5 appliance will act as a Branch peer, verify that client IP address reflection for outbound connections is enabled (this should be set by default when you specify that you are configuring an acceleration deployment during initial configuration):
 - a. Select **Configuration > Proxy Settings > General**.
 - b. Make sure **Reflect Client's Source IP when connecting to servers** is selected.
 - c. If you made a change, click **Apply**.
3. Check the health state of the appliance in the upper right hand corner of the Advanced Management Console window. Make sure appliance Health is **OK**. If the health is **Warning** or **Critical**, click the status link to view details about the health issues.

Step 4: Configure Proxy Services

1. (optional) Customize what traffic the MACH5 accelerates.
 - a. Launch Blue Coat Sky.
 - b. From the Sky Management Console, select **Configure > Acceleration > Traffic Management**. The ProxySG automatically intercepts a default set of services based on your deployment (explicit or transparent).
 - c. Modify which services get intercepted and bypassed by selecting the radio button in the Intercept or Bypass column of the Services table as appropriate. You can only select services that can be accelerated.

Service name	Acceleration techniques	Intercept	Bypass	Edit	Del
BGP	Monitor only	Not applicable			
Blue Coat ADN	Monitor only	Not applicable			
Blue Coat Managem...	Monitor only	Not applicable			
CIFS	Application level				
Cisco IPSec VPN	Monitor only	Not applicable			
Citrix	Network level				
Default	Data level				
DNS	Application level				
Echo	Monitor only	Not applicable			
Endpoint Mapper	Application level				
Explicit HTTP	Application level				
External HTTP	Application level				
FTP	Application level				
FTPS	Monitor only	Not applicable			
H.323	Monitor only	Not applicable			

2. Verify that the MACH5 appliances are intercepting and accelerating traffic as expected. See "Verify the Acceleration Deployment" on page 35.

Plan Configuration of Acceleration Peers

Use the [Acceleration Peer Configuration Worksheet](#) to record the information you need to gather before installing a MACH5 appliance.



The [worksheet](#) is an interactive PDF form that you can fill in on screen before printing. You may also want to save the completed worksheet file for future reference.

This worksheet includes the following sections:

Network Configuration Information—Record the information you need to perform the initial installation and configuration of the MACH5 appliance, such as the required network addresses, the switch port and router interface to which to connect the MACH5 LAN and/or WAN ports, and the link settings you must configure on the MACH5 appliance (they must match the settings defined on the switch/router to which you are connecting the appliance).

ADN Configuration Information—Define the primary and backup ADN managers and other ADN-related settings.

Service Configuration Information—Identify the services (and the corresponding port numbers) that the appliance needs to intercept. You only need to complete this section if the acceleration node will act as a Branch peer; if it will act as a Concentrator peer only it will not need to intercept services. In addition to recording the services to intercept, you should also use this section to identify a client and a server to use to test whether each service is being optimized properly. For example, if you will be optimizing CIFS traffic, you should identify a Microsoft Windows client and server to use to test the file sharing operations, such as opening a file on a remote application server, modifying the file on the client, and saving the file back to the file share. You will need to identify similar types of tests for each application that you plan to intercept and you will need to identify a client and a server to use to conduct these tests.

Complete a separate worksheet for each Branch and/or Concentrator peer you plan to deploy.

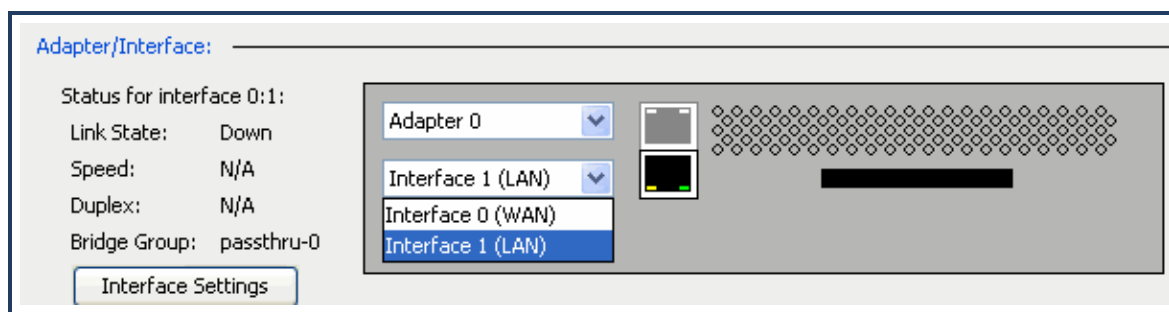
Set Up and Verify VLAN Interfaces

By default, the MACH5 appliance can only intercept traffic on the native VLAN (VLAN 1 by default). If you use VLAN-tagged traffic on your network, you must create a VLAN interface on the MACH5 for each VLAN for which the appliance must handle traffic. This includes management VLANs as well as any VLANs that carry traffic that the MACH5 appliance will intercept.

Although VLANs are logical network segments, the MACH5 appliance treats VLAN interfaces identically to traditional physical LAN interfaces. After you add a VLAN, it appears in the list of network interfaces.

The serial console setup script allows you to set up a single VLAN interface for a non-native VLAN, which you would normally use to define your management VLAN. If you plan to intercept additional VLANs, you must configure them as described in the following procedure.

1. Launch the Advanced Management Console (`https://<ProxySG_IP_address>:8082/mgmt`).
2. Select **Configuration > Network > Adapters > Adapters**.
3. Select the interface that is connected to the switch (the LAN interface).



4. Create a new VLAN.
 - a. Click **New VLAN**. The Configure Interface IPs dialog displays.
 - b. Enter the configuration details for the new VLAN:
 - Specify the **VLAN ID** number (VID) of the VLAN on this interface.
 - Click **Add IP**. The Add list item dialog displays.
 - Enter the **IP Address** and **Prefix Length or Subnet Mask** for the defined VLAN.
 - Click **OK** to save the values and close the dialog.

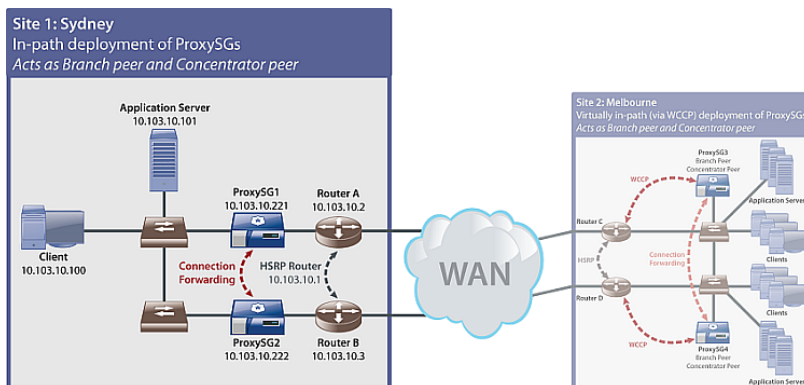
- Select the action that the MACH5 appliance must execute when intercepting traffic on this VLAN interface: **Allow transparent interception**, **Bypass transparent interception**, **Firewall incoming traffic**, or **Use physical interface settings** (default).
- Click **OK**.

c. Click **Apply**.

Deploy Two MACH5s In-Path with Redundant Links

This example shows how to deploy two MACH5 appliances in a redundant network with two routers and two switches. The network devices in this topology are configured as follows:

- Routers are configured with Hot Standby Routing Protocol (HSRP), which enables the standby router to take over if the primary router fails.
- The switches are physically connected to one another with a cable and can sense if the other fails.
- The MACH5 appliances are configured to fail to the disconnected state (also known as fail closed) so that if one MACH5 fails, WAN optimization occurs through the active MACH5.
- The MACH5 appliances are configured with Connection Forwarding to ensure that connections are serviced by the appropriate MACH5.



Step 1: Prepare for the Acceleration Deployment

1. Plan the configuration of acceleration peers. A worksheet is available to record your configuration settings. See "Plan Configuration of Acceleration Peers" on page 90.
2. Verify that the routers are configured with HSRP.
3. Make sure all MACH5 appliances are running SGOS version 6.5 with the factory default settings.
 - a. Upgrade all appliances as described in Upgrade/Downgrade an SGOS Image.
 - b. After upgrading, restore the appliance to its factory default state using the `restore-defaults factory-defaults` CLI command. Note that you must be connected to the MACH5 console to issue this command.
4. Before you install the MACH5 appliance, test network connectivity to the remote sites. You will repeat this step after the appliance has been installed to reverify network connectivity.

For example, to ping a host at a remote site as shown in the [topology diagram](#), type the following commands at the command prompt on a local client:

ping 10.201.10.100

5. If you have a firewall between the ADN Concentrator peer and the ADN Branch peer, make sure the tunnel listening port is open. This port allows the creation of the control connection for the tunnel, which enables byte-cache dictionary synchronization. By default, the tunnel listening port is set to 3035 (plain) and 3037 (secure).

Step 2: Integrate the Appliance into the Network

1. Connect to the serial console (9600, 8, N, 1) of each MACH5 and launch the Blue Coat ProxySG configuration wizard. For detailed instructions, see "Configure Basic Network Information for an In-Path Acceleration Peer (Serial Console)" on page 54.

```

===== CONFIGURATION START =====
Welcome to the Blue Coat ProxySG 210 configuration wizard.
This appliance's serial number: 0408063522

-----
you can get field help by entering a question mark ? in the fields.
you can move backwards through the steps by pressing the UP arrow.
you can exit the wizard without saving your changes
-----

Step 1: How do you plan to configure this appliance?
a) Through a manual setup
b) Through a Director-managed setup
your choice: ☐ a

Step 2: Which solution would you like to implement?
a) Acceleration
b) other solution
your choice: ☐ a

Step 3: How will you deploy this appliance?
a) Physically in-path
b) Virtually in-path using WCCP
c) Any other
your choice: ☐ a

Step 4: Appliance name [ProxySG 210 0408063522] ProxySG1

Step 5: you have the following hardware bridge interface:
Configure interface 0:0-0:1? Inactive link [No] y
IP address ☐ ..... 10.103.10.221
Subnet mask ☐ ..... 255.255.255.0
Speed and duplex undetected
Automatically detect when link exists [yes] .
Does this interface require a VLAN? [No] ....

Step 6: Default gateway ☐ 10.103.10.1
>> Pinging 10.103.10.1...FAILED

Step 7: Primary DNS server ☐ 10.101.10.100
>> Testing DNS server
>> Attempting to resolve www.bluecoat.com in the background

Step 8: Administrator ID [admin]

Step 9: Administrator password ☐ *****
Retype administrator password ☐ *****
>> Password is easily guessed. Choose another? y/n [yes] n

Step 10: Activate acceleration immediately? [yes]

```

2. Power off each MACH5 appliance.
3. Rack mount each MACH5 appliance. Refer to the *ProxySG Quick Start Guide* for instructions. Note that the appliance must have a hardware bridge card with pass-through support.



With in-path deployments, there will be some network downtime when installing the MACH5 appliance.

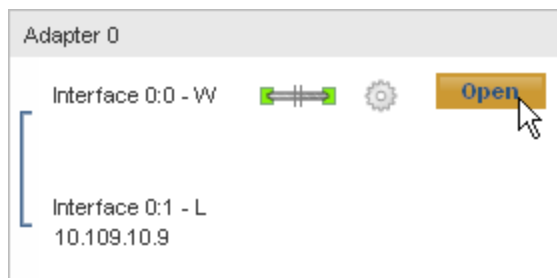
4. Cable the appliance as follows:
 - Connect the MACH5 bridge card LAN interface to the first switch using a straight-through cable.
 - Connect the MACH5 bridge card WAN interface to the corresponding router using a crossover cable.
5. Power on each MACH5 appliance.
6. Verify network connectivity to remote sites by repeating the ping test. Check adapter LEDs and cables if you cannot reach the remote sites.
7. Go to the following URL to launch the Sky Management Console: https://<ProxySG_IP_

`address>:8082.`

For example, to launch the Sky Management Console on the ProxySG1 appliance shown in this example you would enter:

`https://10.103.10.221:8082`

8. Verify that the configured link settings (speed/duplex) on the MACH5 interface match the configured settings on the connected switch/router interfaces.
 - a. Select **System Settings > Adapters & Interfaces**.
 - b. In the box that corresponds to the bridge that is connected to the switch or router in the **Adapter Overview** section of the tab, click **Open**.



If you configure speed/duplex settings other than **Auto-negotiate** on either bridge interface, the other bridge interface will inherit the same settings.

- c. Verify that the **Speed and duplex** settings match the settings that are defined on the router or switch interface.
 - d. Click **Close**.
 - e. If you made any changes, click **Commit all**
9. (Optional) Create a VLAN interface on the MACH5 for each VLAN for which the MACH5 must handle traffic.
 - a. Click **Advanced configuration** to go to the Advanced Management Console.
 - b. Select **Configuration > Network > Adapters > Adapters**.
 - c. Select the interface that is connected to the switch (the LAN interface).
 - d. Click **New VLAN** to create a VLAN interface. See "Set Up and Verify VLAN Interfaces" on page 91 for detailed instructions on how to configure the VLAN.

10. **Configure the bridge cards to block traffic in the event of failure. If one MACH5 fails, the other MACH5 appliance will optimize all traffic.**
 - a. Select **Configuration > Network > Adapters > Bridges**.
 - b. In the **Bridges** section, select the bridge you want to configure.
 - c. Click **Edit**. The Edit Bridge dialog displays.
 - d. To prevent the MACH5 from passing traffic when down, select the **Fail Closed** mode from the **Mode** drop-down list.
 - e. Click **OK** to save your changes and close the Edit Bridge dialog.
 - f. Click **Apply**.
 - g. (Optional) After both MACH5 appliances are installed and configured, test that the appliance is failing to a disconnected state by powering off one of the MACH5 appliances and ensuring that traffic fails over to the other MACH5.

For detailed instructions for configuring the function of a programmable bridge card see "Configure the Bridge Mode" on page 46.

11. **Configure each MACH5 appliance to propagate link state status:**
 - a. Select **Configuration > Network > Bridges**.
 - b. Select the bridge and click **Edit**.
 - c. Select **Propagate Failure**.
 - d. Click **OK**.
 - e. Click **Apply**.
12. **Verify that the MACH5 appliances are bypassing traffic:**
 - a. Select **Statistics > Sessions > Active Sessions > Bypassed Connections**.
 - b. Look for one-way traffic (shows up in red), which can indicate asymmetric routing. This can interfere with acceleration.

Step 3: Configure Acceleration

1. **If the MACH5 will act as a Concentrator peer, enable client IP address reflection for inbound connections.**
 - a. Select **Configuration > ADN > Tunneling > Network**.

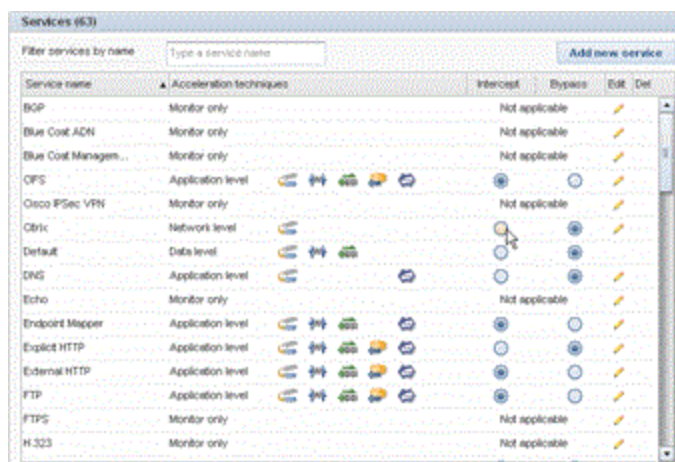
- b. In the Reflect Client IP for MACH5 peers section or the tab, select **Allow the request and reflect the client IP**.
 - c. Click **Apply**.
 2. If the MACH5 will act as a Branch peer, verify that client IP address reflection for outbound connections is enabled (this should be set by default when you specify that you are configuring an acceleration deployment during initial configuration):
 - a. Select **Configuration > Proxy Settings > General**.
 - b. Make sure **Reflect Client's Source IP when connecting to servers** is selected.
 - c. If you made a change, click **Apply**.
 3. **Configure Connection Forwarding on each MACH5 appliance.**
 - a. Select **Configuration > Network > Advanced > Connection Forwarding**.
 - b. Select the IP address of the MACH5 you are configuring from the **Local IP** drop-down list.

A blue circular icon with a white lowercase 'i' inside, representing an information or tip.

If you are configuring an appliance that has additional interfaces—such as a 600, 810, 900, or 9000—you can configure a separate IP address (on both MACH5 appliances) and directly connect those interfaces for Connection Forwarding.
 - c. Click **Add**.
 - d. In the Add IPs dialog, add the IP address of the other MACH5 to the list of forwarding peers.
 - e. Click **OK**.
 - f. Select **Enable Connection Forwarding**.
 - g. Click **Apply**.
 4. **Verify Connection Forwarding on each MACH5 appliance::**
 - a. Select **Statistics > Advanced > CCM**.
 - b. Select **Show CCM Statistics**.
 - c. Verify that the forwarding peer status displays as **Online**.
 5. Check the health state of the appliance in the upper right hand corner of the Advanced Management Console window. Make sure appliance Health is **OK**. If the health is **Warning** or **Critical**, click the status link to view details about the health issues.

Step 4: Configure Proxy Services

1. (optional) Customize what traffic the MACH5 appliance accelerates.
 - a. Launch Blue Coat Sky.
 - b. From the Sky Management Console, select **Configure > Acceleration > Traffic Management**. The MACH5 automatically intercepts a default set of services based on your deployment (explicit or transparent).
 - c. Modify which services get intercepted and bypassed by selecting the radio button in the Intercept or Bypass column of the Services table as appropriate. You can only select services that can be accelerated.



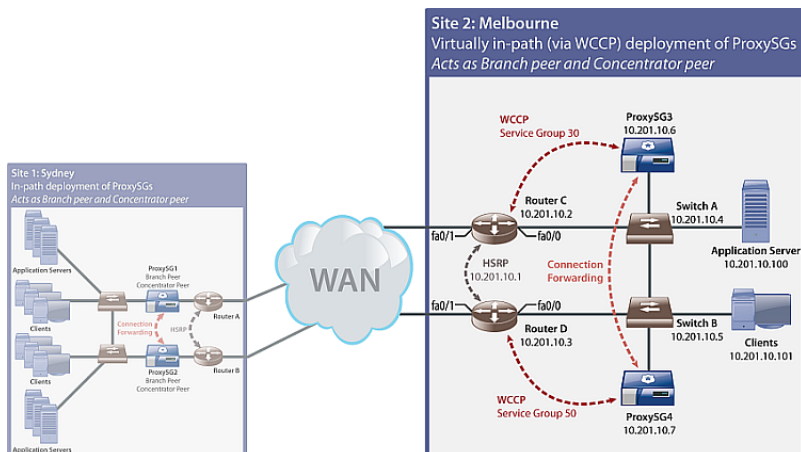
2. Verify that the MACH5 appliances are intercepting and accelerating traffic as expected. See "Verify the Acceleration Deployment" on page 35.

Deploy Virtually In-Path in a Redundant Layer 2 Network

This example shows how to deploy MACH5 appliances virtually in-path with redundant WCCP routers and redundant switches. The network devices in this topology are configured as follows:

- Routers are configured with Hot Standby Routing Protocol (HSRP), which enables the standby router to take over if the primary router fails.
- Routers and MACH5 appliances are configured with WCCP to redirect traffic for optimization. Note that if you have a Layer 3 switch that supports WCCP, you can configure redirection using the switch.

- The switches are physically connected by a cable to one another, and can sense if the other fails.
- The MACH5 appliances are configured with Connection Forwarding to ensure that connections are serviced by the appropriate MACH5.



Step 1: Prepare for the Acceleration Deployment

1. Plan the configuration of acceleration peers. A worksheet is available to record your configuration settings. See "Plan Configuration of Acceleration Peers" on page 90.
2. Plan the WCCP Configuration. See "Plan WCCP Configuration" on page 73.
3. Verify that the Cisco model hardware and IOS version supports the WCCP features required for this deployment. See "WCCP Tested Platforms" on page 74 for a list of the Cisco hardware and software platforms and WCCP capabilities that have been tested with the MACH5.
4. Verify that the routers are configured with HSRP.
5. Make sure all MACH5 appliances are running SGOS version 6.2 with the factory default settings.
 - a. Upgrade all appliances as described in Upgrade/Downgrade an SGOS Image.
 - b. After upgrading, restore the appliance to its factory default state using the `restore-defaults factory-` CLI command.
6. Before you install the MACH5, test network connectivity to the remote sites. You will repeat this step after the MACH5 has been installed to reverify network connectivity.

For example, to ping a host at a remote site as shown in the [topology diagram](#), type the following commands at the command prompt on a local client:

ping 10.103.10.101

7. If you have a firewall between the ADN Concentrator peer and the ADN Branch peer, make sure the tunnel listening port is open. This port allows the creation of the control connection for the tunnel, which enables byte-cache dictionary synchronization. By default, the tunnel listening port is set to 3035 (plain) and 3037 (secure).

Step 2: Integrate the Appliance into the Network

1. Connect to the serial console (9600, 8, N, 1) of each MACH5 and launch the Blue Coat ProxySG configuration wizard. For detailed instructions, see "Configure Basic Network Information for an In-Path Acceleration Peer (Serial Console)" on page 54.

```

----- CONFIGURATION START -----
Welcome to the Blue Coat ProxySG 210 configuration wizard.
This appliance's serial number: 0408063522

-----
You can get field help by entering a question mark ? in the fields.
You can move backwards through the steps by pressing the UP arrow.
You can exit the wizard without saving your changes
-----

Step 1: How do you plan to configure this appliance?
a) Through a manual setup
b) Through a Director-managed setup
Your choice: [ ] a

Step 2: Which solution would you like to implement?
a) Acceleration
b) Other solution
Your choice: [ ] a

Step 3: How will you deploy this appliance?
a) Physically in-path
b) Virtually in-path using WCCP
c) Any other
Your choice: [ ] a

Step 4: Appliance name [ProxySG 210 0408063522] ProxySG1

Step 5: You have the following hardware bridge interface:
Configure interface 0:0-0:1? Inactive link [NO] y
IP address [ ] ..... 10.103.10.221
Subnet mask [ ] ..... 255.255.255.0
Speed and duplex undetected
Automatically detect when link exists [yes] .
Does this interface require a VLAN? [NO] ...

Step 6: Default gateway [ ] 10.103.10.1
>> Pinging 10.103.10.1...FAILED

Step 7: Primary DNS server [ ] 10.101.10.100
>> Testing DNS server
>> Attempting to resolve www.bluecoat.com in the background

Step 8: Administrator ID [admin]

Step 9: Administrator password [ ] *****
Retype administrator password [ ] *****
>> Password is easily guessed. Choose another? y/n [yes] n

Step 10: Activate acceleration immediately? [yes]

```

2. Power off each MACH5 appliance.
3. On the first router, create the WCCP service groups for the LAN and WAN interfaces.


```

Router> enable
Router#conf t
Router(config)#ip wccp version 2
Router(config)#ip wccp 30
Router(config)#interface fa0/0
Router(config-if)#ip wccp 30 redirect in
Router(config-if)#exit
Router(config)#interface fa0/1

```

```
Router(config-if)#ip wccp 30 redirect in
Router(config-if)#exit
```

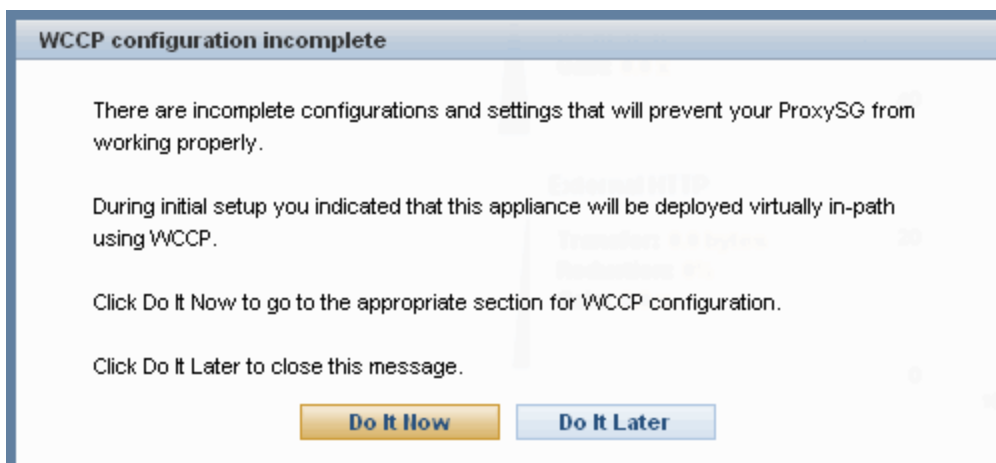
4. On the second router, create the WCCP service groups for the LAN and WAN interfaces.

```
Router> enable
Router#conf t
Router(config)#ip wccp version 2
Router(config)#ip wccp 50
Router(config)#interface fa0/0
Router(config-if)#ip wccp 50 redirect in
Router(config-if)#exit
Router(config)#interface fa0/1
Router(config-if)#ip wccp 50 redirect in
Router(config-if)#exit
```

5. Rack mount each MACH5 appliance. Refer to the *ProxySG Quick Start Guide* for instructions. Note that the appliance must have a hardware bridge card with pass-through support.
6. Cable each appliance by connecting the MACH5 LAN interface to the switch/router using a straight-through cable.
7. Power on each MACH5 appliance.
8. Go to the following URL to launch the Sky Management Console: https://<ProxySG_IP_address>:8082. Because you indicated that you are deploying the appliance virtually in-path, the interface prompts you to configure WCCP.

For example, to launch the Sky Management Console on the ProxySG3 appliance shown in this example you would enter:

<https://10.201.10.6:8082>



9. On the first MACH5, define the LAN-to-WAN and WAN-to-LAN service groups (known as a

WCCP pair).

- a. When prompted to configure WCCP, click **Do It Now**.
- b. Select **Enable WCCP**.
- c. Click **Add new pair**.
- d. Create the service groups.

This example shows the WCCP configuration for ProxySG3 in this example deployment:

The screenshot displays the WCCP configuration interface for ProxySG3, showing two service groups: LAN to WAN (Service group: 30, 50) and WAN to LAN (Service group: 30, 50).

LAN to WAN Configuration:

- Interface: 2:1 (10.201.10.8)
- Router communication: ☐ Same for the pair
- Home router IP: 10.201.10.2
- Multicast group IP: TTL: 1
- Forwarding type: ☐ GRE ☒ L2
- Returning type: ☐ GRE ☒ L2
- Service group number: 30
- More Settings:
 - Protocol: TCP
 - Priority: 1
 - Weight: 1
 - Assignment type: ☐ Hash ☒ Mask
 - Mask scheme:
 - ☐ Source IP
 - ☐ Source port
 - ☒ Destination IP
 - ☐ Destination port
 - TCP ports to redirect:
 - ☒ All ports
 - ☐ Selected ports
 - Service group password is not set [Set Password](#)

WAN to LAN Configuration:

- Interface: 2:1 (10.201.10.8)
- Router communication: ☐ Same for the pair
- Home router IP: 10.201.10.3
- Multicast group IP: TTL: 1
- Forwarding type: ☐ GRE ☒ L2
- Returning type: ☐ GRE ☒ L2
- Service group number: 50
- More Settings:
 - Protocol: TCP
 - Priority: 2
 - Weight: 1
 - Assignment type: ☐ Hash ☒ Mask
 - Mask scheme:
 - ☒ Source IP
 - ☐ Source port
 - ☐ Destination IP
 - ☐ Destination port
 - TCP ports to redirect:
 - ☒ All ports
 - ☐ Selected ports
 - Service group password is not set [Set Password](#)

- e. Click **Commit all**.
 - f. Verify that the service groups negotiate successfully and the **State** changes to **Ready**.
10. On the second MACH5, define the LAN-to-WAN and WAN-to-LAN service groups.
- a. When prompted to configure WCCP, click **Do It Now**.
 - b. Select **Enable WCCP**.
 - c. Click **Add new pair**.
 - d. Create the service groups.

This example shows the WCCP configuration for ProxySG4 in this example deployment:

The image shows two configuration windows for service groups. The left window is titled 'LAN to WAN' and the right is 'WAN to LAN'. Both windows have a 'Service groups (50, 30)' header. They contain fields for interface (2:1 (10.201.10.7)), router communication (Home router IP: 10.201.10.3 for LAN, 10.201.10.2 for WAN), forwarding type (L2), and returning type (L2). The 'More Settings' section includes protocol (TCP), priority (1 for LAN, 2 for WAN), weight (1), assignment type (Mask), and mask scheme (Source IP, Source port, Destination IP, Destination port). TCP ports to redirect are set to 'All ports'. A 'Set Password' button is at the bottom of each window.

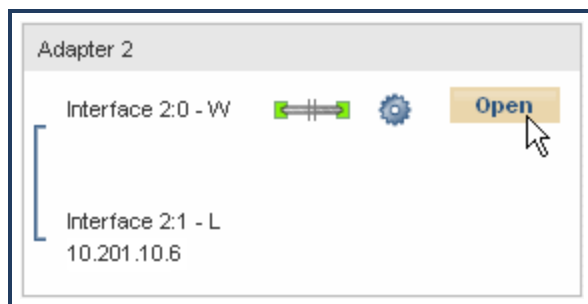
e. Click **Commit all**.

f. Verify that the service groups negotiate successfully and the **State** changes to **Ready**.

11. Verify that the configured link settings (speed/duplex) on the MACH5 interface match the configured settings on the connected switch/router interfaces.

a. Select **System Settings > Adapters & Interfaces**.

b. In the box that corresponds to the bridge that is connected to the switch or router in the **Adapter Overview** section of the tab, click **Open**.



If you configure speed/duplex settings other than **Auto-negotiate** on either bridge interface, the other bridge interface will inherit the same settings.

c. Verify that the **Speed and duplex** settings match the settings that are defined on the router or switch interface.

d. Click **Close**.

- e. If you made any changes, click **Commit all**
- 12. Verify that the MACH5 appliances are bypassing traffic.
 - a. Select **Report > Active Sessions**.
 - b. In the **Connection Type** field, select **Bypassed** and then click **Submit**.
 - c. Look for one-way traffic, which can indicate asymmetric routing. This can interfere with acceleration.

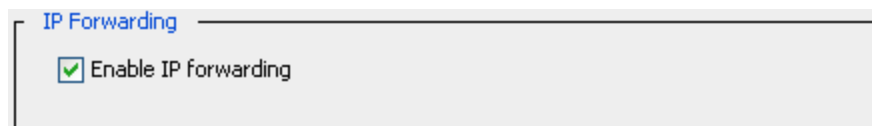
Step 3: Configure Acceleration

1. If the MACH5 will act as a **Concentrator peer**, preserve the client IP address for inbound connections.
 - a. Select **Configure > ADN > Concentrator**.
 - b. Select **Preserve the client IP address when connecting to servers**.
 - c. Click **Commit all**.



For client IP reflection to work in this deployment, the MACH5 must reside on a separate Layer 2 network (LAN or VLAN) than the interfaces to be intercepted.

2. If the MACH5 will act as a **Branch peer**, verify that client IP address reflection for outbound connections is enabled (this should be set by default when you specify that you are configuring an acceleration deployment during initial configuration):
 - a. Select **Configure > Proxy Settings > General**.
 - b. Make sure **Reflect Client's Source IP when connecting to servers** is selected.
 - c. If you made a change, click **Commit all**.
3. **Enable IP Forwarding.**
 - a. Click **Advanced configuration** to go to the Advanced Management Console.
 - b. Select **Configuration > Network > Routing**.
 - c. Select **Enable IP forwarding**.



- d. Click **Apply**.

4. **Configure Connection Forwarding on each MACH5 appliance.**

- a. In the Advanced Management Console, select **Configuration > Network > Advanced > Connection Forwarding**.
- b. Select the IP address of the MACH5 you are configuring from the **Local IP** drop-down list.



- c. Click **Add**.
- d. In the Add IPs dialog, add the IP address of the other MACH5 to the list of forwarding peers.
- e. Click **OK**.
- f. Select **Enable Connection Forwarding**.
- g. Click **Apply**.

For more detailed instructions, see "Configure Connection Forwarding" on page 107.

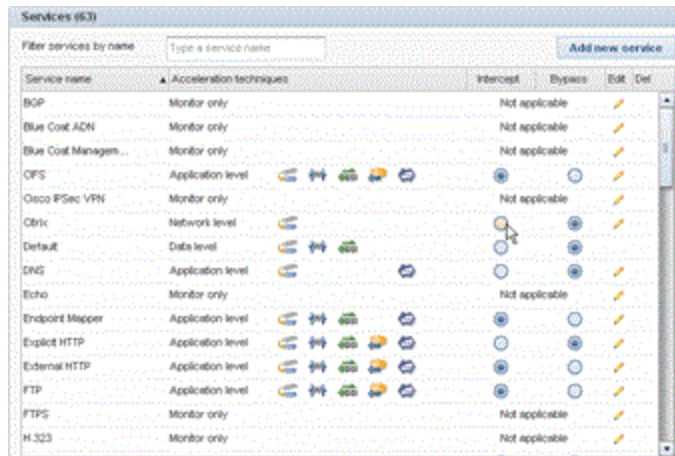
5. **Verify Connection Forwarding on each MACH5 appliance::**

- a. In the Advanced Management Console, select **Statistics > Advanced > CCM**.
 - b. Select **Show CCM Statistics**.
 - c. Verify that the forwarding peer status displays as **Online**.
6. Check the health state of the appliance in the upper right hand corner of the Advanced Management Console window. Make sure appliance Health is **OK**. If the health is **Warning** or **Critical**, click the status link to view details about the health issues.

Step 4: Configure Proxy Services

1. (optional) Customize what traffic the MACH5 accelerates.
 - a. Launch Blue Coat Sky.

- b. From the Sky Management Console, select **Configure > Acceleration > Traffic Management**. The MACH5 automatically intercepts a default set of services based on your deployment (explicit or transparent).
- c. Modify which services get intercepted and bypassed by selecting the radio button in the Intercept or Bypass column of the Services table as appropriate. You can only select services that can be accelerated.



2. Verify that the MACH5 appliances are intercepting and accelerating traffic as expected. See "Verify the Acceleration Deployment" on page 35.

What is Connection Forwarding?

TCP Connection Forwarding is a Blue Coat feature that enables MACH5 appliances to share TCP connection information and selectively forward TCP connections to other MACH5 appliances. Connection Forwarding is useful in transparent deployments where asymmetric routing conditions exist. An asymmetric route is one in which the path from client to server is different than the return path from server to client. Asymmetric routes are common in networks with external load balancing or redundant routes when client IP reflection is enabled.

In asymmetric routing conditions, Connection Forwarding is a simple solution that resolves a complex network routing problem. Using Connection Forwarding to track connections, administrators do not need to reconfigure switches and/or routers to ensure that connections are routed to the correct appliance.

The figure below illustrates the Connection Forwarding process.

Connection Forwarding requires two or more MACH5 appliances configured as peers. To create a Connection Forwarding group, each MACH5 must be configured with the IP addresses of all other MACH5 appliances in the group. This enables all of the group members to share TCP connection information, allowing them to identify which connections exist on which appliances. When a group member receives a connection it either processes it or forwards to another peer in the group using IP-in-IP encapsulation (similar to Generic Route Encapsulation).

Configure Connection Forwarding

Connection Forwarding is useful in transparent deployments where asymmetric routing conditions exist. An asymmetric route is one in which the path from client to server is different than the return path from server to client. Asymmetric routes are common in networks with external load balancing or redundant routes when client IP reflection is enabled. With Connection Forwarding, two or more MACH5 appliances are joined in a Connection Forwarding group in which each MACH5 is configured with the IP address of all other MACH5 appliances in the group. This enables all of the group members to share TCP connection information, allowing them to identify which connections exist on which appliances. When a group member receives a connection it either processes it or forwards to another peer in the group using IP-in-IP encapsulation.



If you are configuring a MACH5 510, 600, 810, 8100 or 9000 that has additional interfaces, you can configure a separate IP address (on all MACH5 appliances in the Connection Forwarding group) and directly connect those interfaces for Connection Forwarding.

Use the following procedure to enable Connection Forwarding. You must repeat this procedure for each appliance in the Connection Forwarding group.

1. Launch the Advanced Management Console (https://<ProxySG_IP_address>:8082/mgmt).
2. Select **Configuration > Network > Advanced > Connection Forwarding**.
3. Define the Connection Forwarding group:
 - a. Select the IP address of this MACH5 from the **Local IP** drop-down list.
 - b. Click **Add**. The Add IPs dialog is displayed.
 - c. In the **Peer IPs** text box, enter the IP address(es) of the other appliances in the Connection Forwarding group and then click **OK** to close the Add IPs dialog.

A screenshot of the 'Connection Forwarding' configuration tab in the Advanced Management Console. The tab is selected among 'WCCP', 'VIPs', 'Failover', and 'Connection Forwarding'. Below the tabs, there is a checkbox labeled 'Enable Connection Forwarding' which is checked. Below this, there is a 'Local IP' dropdown menu showing '10.9.59.246' and a 'Port' text box containing '3030'.

4. On the Connection Forwarding tab, select **Enable Connection Forwarding**.
5. Click **Apply**.
6. After you enable Connection Forwarding on all appliances in the forwarding group, verify that it is configured properly:

- a. Select **Statistics > Advanced > CCM**.
- b. Select **Show CCM Statistics**. A CCM Statistics page displays in a new browser window or tab.
- c. Verify that the **Status** for each peer is **ONLINE**.

Acceleration Strategies

This chapter explains basic strategies for accelerating traffic on your network. It includes the following topics:

Reduce Bandwidth Usage	109
Accelerate Applications	110
Verify Application Acceleration	111
Define Exceptions for Traffic Management	113
What are Protocols?	114
Examples of Custom Services	116
What is ADN Last Peer Detection?	117
What is the TCP Window Size?	119

Reduce Bandwidth Usage

One of the benefits of using the MACH5 appliance is reduction of bandwidth usage. The appliance is able to reduce bandwidth usage by caching content and performing protocol-specific optimizations. The appliance offers a number of ways to determine how much bandwidth the MACH5 appliance is saving.

1. The appliance is able to cache and optimize traffic for any service that it is actively managing (intercepting). Therefore, you need to make sure you are intercepting the appropriate services.

See [Intercept a Service](#).
2. To monitor how much bandwidth is going over the WAN versus the LAN, you can view the Traffic Summary report and look at the Bandwidth Usage graph. The gold area represents the rate of WAN traffic and the green area represents the rate of LAN traffic; the difference between the two areas represents savings of bandwidth. See [View Traffic Summary](#).
3. To determine how much bandwidth the MACH5 appliance is saving, you can look at overall and per-service statistics on the Bandwidth Savings report. The default time period is the last hour, but it is more interesting to look at trends over a longer duration, such as the last week or month. See [Analyze Bandwidth Savings](#).
4. To focus on savings due to object caching, view the various object caching graphs. You can look at graphs that demonstrate savings for all proxies and services or for a specific proxy or service. See [View Benefits of Object Caching](#).

5. The Active Sessions report lists how much bandwidth is being saved on each intercepted connection. See List Active Sessions, and select intercepted sessions for the connection type.

To see which acceleration techniques are being applied to the connection, look for colored icons in the **Comp**, **BC**, **OC**, **PO**, and **BWM** columns.

Column	Description	Active Icon
Comp	Compression	
BC	Byte Caching	
OC	Object Caching	
PO	Protocol Optimization	
BWM	Bandwidth Management	

Accelerate Applications

If you answered no to the *Activate acceleration immediately?* question in the configuration wizard, bypass mode is enabled in Blue Coat Sky, and the MACH5 appliance does not accelerate any services. This is a more conservative approach. It allows you to first observe the type of traffic on your network, decide which services you want to accelerate, and then enable acceleration one service at a time. With this slower, more controlled approach, you can see the effects of each small change you make to the configuration.

Follow these basic steps to use this approach:

Step 1: Determine what traffic is running on your network.

In bypass mode, all connections are bypassed. For specific information about the traffic currently flowing through the MACH5 appliance, display the Active Sessions report for bypassed connections. (See Active Sessions report.) This report lists the connections that are being bypassed, indicating the service name associated with each connection. You can sort by any of the column headings, so if you want to group together all the connections associated with a particular service, click the **Service name** heading.

Step 2: Accelerate a service.

Interception is a process in which the MACH5 appliance actively manages or controls the traffic flows associated with a particular service. Various settings, rules, and policies determine what action the MACH5 appliance takes when it encounters the service traffic. There are a number of services that are set to intercept by default, so if you want to accelerate one service at a time, you first need to clear out all the default settings.

1. On the Traffic Management screen, select **Bypass** for all services, except for the one you want to accelerate; set this application to **Intercept**. See *Modify a Service's Acceleration Setting*.
2. Switch to acceleration mode. See *Select the Traffic Mode*.

Step 3: Verify acceleration.

After some time has passed, you will want to verify that this service is being accelerated.

1. Display the Bandwidth Savings report for the service to see how much acceleration benefit the intercepted service is getting. See *Analyze Bandwidth Savings*.
2. Bring up the Active Sessions report and view intercepted sessions. It should list the sessions for the service you are intercepting (assuming that type of traffic is active on your network). It also indicates which acceleration techniques the MACH5 appliance is using.

Step 4: Accelerate other services.

Assuming you are satisfied with the acceleration results you are getting for the one service you are intercepting, you might want to gradually start enabling interception on other services. After each step, verify acceleration as described in the section above.

Step 5: Define exceptions for traffic management.

The MACH5 appliance manages traffic to and from all clients and servers for a variety of types of network traffic. To fit your specific traffic management needs and goals, you may want to define exceptions to these default settings. You can decide which clients and servers to control traffic to and from, or choose whether or not you want to actively manage a type of traffic (such as streaming). See "Define Exceptions for Traffic Management" on page 113.

Step 6: Explore other MACH5 acceleration solutions.

The MACH5 appliance offers additional tools and settings for accelerating different types of traffic. Look through the topics in the Table of Contents for ideas. For example, you can accelerate file sharing by pre-populating the MACH5 cache, or optimize Web or streaming media traffic.

Verify Application Acceleration

If you answered yes to the *Activate acceleration immediately?* question in the configuration wizard, acceleration mode is enabled in Blue Coat Sky, and the MACH5 automatically begins accelerating a set of services that typically benefit from optimization.



If you selected the virtually in-path deployment during initial configuration, you need to configure WCCP before the MACH5 appliance can accelerate traffic. See [Configure WCCP](#).

To verify that applications are being accelerated, answer the following questions.

Is acceleration enabled?

Acceleration cannot occur unless the MACH5 appliance is in acceleration mode. To check this setting, go to the Traffic Management screen. See [Select the Traffic Mode](#).

Has my MACH5 found an acceleration peer?

Acceleration peers are required for optimal acceleration results. Without a peer, the MACH5 appliance can perform object caching and protocol optimization only (no byte caching or compression). To determine whether the MACH5 has found an acceleration peer, display the Active Sessions report and see if there is an IP address listed in the **ADN Peer** column for any of the sessions. (See [List Active Sessions](#).)

What kind of traffic is running on my network?

The Traffic Summary report lists the services or proxies that are consuming the most bandwidth on your network. You can select different time periods to see how the list of top services/proxies varies over time. See [View Traffic Summary](#).

For more specific information about the traffic currently flowing through the MACH5 appliance, the Active Sessions report lists the current intercepted and/or bypassed sessions, indicating the service name and proxy type associated with each session. See [List Active Sessions](#).

How much benefit am I getting from MACH5 acceleration?

You can see the acceleration benefit from several different angles:

- The Bandwidth Savings report shows the percent of bandwidth saved due to various acceleration techniques on the MACH5. You can view reports that show bandwidth savings for all traffic or for a single service or proxy. See [Analyze Bandwidth Savings](#).
- Use the Bandwidth Usage graph on the Traffic Summary report to verify reduction in WAN traffic. See [View Traffic Summary](#).
- The Object Caching report shows the bandwidth savings gained from object caching. See [View Benefits of Object Caching](#).
- The Active Sessions report lists the savings for each open session. See [List Active Sessions](#).

What methods of optimization are being used?

The MACH5 can apply five different acceleration methods, depending on the type of traffic: compression, byte caching, object caching, protocol optimization, and bandwidth management. The Active Sessions report shows which techniques are active on each intercepted session: look for colored icons in the **Comp**, **BC**, **OC**, **PO**, and **BWM** columns.

Compression (Comp)

Byte Caching (BC)

Object Caching (OC)

Protocol Optimization (PO)

Bandwidth Management (BWM)

After you have verified that applications are being accelerated, you may want to fine-tune what traffic is being optimized.

Do you want to define any exceptions to traffic management?

The MACH5 appliance manages traffic to and from all clients and servers for a variety of types of network traffic. To fit your specific traffic management needs and goals, you may want to define exceptions to these default settings. You can decide which clients and servers to control traffic to and from, or choose whether or not you want to actively manage a type of traffic (such as streaming). See "Define Exceptions for Traffic Management" below.

Are there additional services you want to optimize?

The MACH5 appliance is pre-configured to identify and control a set of services that typically benefit from optimization. If you want to optimize additional services, you can set these services to **Intercept**. See Intercept a Service.

Are there any services you don't want to manage?

If you don't care about managing a certain type of traffic or if you want to troubleshoot issues with a particular service, you can set the service to **Bypass**. See Bypass a Service.

Define Exceptions for Traffic Management

By default, the MACH5 appliance manages traffic to all clients and servers for a variety of types of network traffic, such as Web, secure Web, file transfers, and streaming protocols. To fit your specific traffic management needs

and goals, you may want to define exceptions to these default settings. You can decide which clients and servers to control traffic to and from, or choose whether or not you want to actively manage a type of traffic (such as streaming).

1. Do you want to bypass traffic from a particular client subnet or to a specific server? If so, you can add static bypass rules. See [Add Static Bypass Rules](#).
2. Do you want to control traffic from certain clients or to a particular server? If so, you can add restricted intercept rules. See [Add Restricted Intercept Rules](#).
3. Do you *not* want the MACH5 appliance to manage a particular type of traffic? Traffic that you want to pass through the appliance without processing should be set to bypass. See [Bypass a Service](#).
4. Do you want the MACH5 appliance to manage a type of traffic that it currently is passing through without processing? If so, set the service to intercept the traffic. See [Intercept a Service](#).

What are Protocols?

You can create custom services based on the following protocols.

Protocol	Description	Available Acceleration Techniques
CIFS	Common Internet File System The MACH5 can optimize/accelerate file sharing across the WAN to users in branch offices.	TCP optimization
		Byte caching
		Compression
		Object caching
		Protocol optimization
DNS	Domain Name Service The MACH5 can speed up domain name resolution by looking up domain names in its DNS cache. If the name isn't found in the cache, the MACH5 forwards the request to the configured DNS server list. The MACH5 also has the ability to rewrite DNS requests and responses.	Object caching
		Protocol optimization

Protocol	Description	Available Acceleration Techniques
Endpoint Mapper	<p>Protocol used by Microsoft Outlook (client) to communicate with Microsoft Exchange (server)</p> <p>The MACH5 can accelerate the following Outlook processes: sending/receiving e-mail, accessing message folders, changing calendar elements.</p>	<p>TCP optimization</p> <p>Byte caching</p> <p>Compression</p> <p>Protocol optimization</p>
FTP	<p>File Transfer Protocol</p> <p>The MACH5 can control, secure, and accelerate file transfer requests. Additionally, it caches FTP objects.</p>	<p>TCP optimization</p> <p>Byte caching</p> <p>Compression</p> <p>Object caching</p> <p>Protocol optimization</p>
HTTP	<p>Hyper Text Transfer Protocol</p> <p>The MACH5 can control, secure, and accelerate web traffic. It also caches copies of frequently requested web pages and objects.</p>	<p>TCP optimization</p> <p>Byte caching</p> <p>Compression</p> <p>Object caching</p> <p>Protocol optimization</p>
MMS	<p>Microsoft Media Services; streaming protocol</p> <p>The MACH5 can monitor, control, limit, or block streaming media traffic that uses Microsoft's proprietary streaming protocol. It also reduces stutter and improves the quality of streaming media, and logs streaming connections.</p>	<p>TCP optimization</p> <p>Object caching</p> <p>Protocol optimization</p>

Protocol	Description	Available Acceleration Techniques
RTMP	Real Time Messaging Protocol (Flash)	TCP optimization
	The MACH5 appliance fetches a live Flash stream once from the OCS and serves it to all users behind the appliance.	Object caching Protocol optimization
	As Flash clients stream pre-recorded content from the OCS through the MACH5, the content is cached on the appliance. After content gets cached on the MACH5, subsequent requests for the cached portions are served from the appliance; uncached portions are fetched from the OCS.	
RTSP	Real Time Streaming Protocol	TCP optimization
	The MACH5 can monitor, control, limit, or block streaming media traffic that uses Internet standard RTSP protocol. It also reduces stutter and improves the quality of streaming media, and logs streaming connections.	Object caching Protocol optimization
TCP Tunnel	A tunnel for any TCP-based protocol for which a more specific protocol isn't available.	TCP optimization
	The MACH5 can compress and accelerate tunneled traffic.	Byte caching Compression

Examples of Custom Services

Here are several situations when you might want to create a custom service:

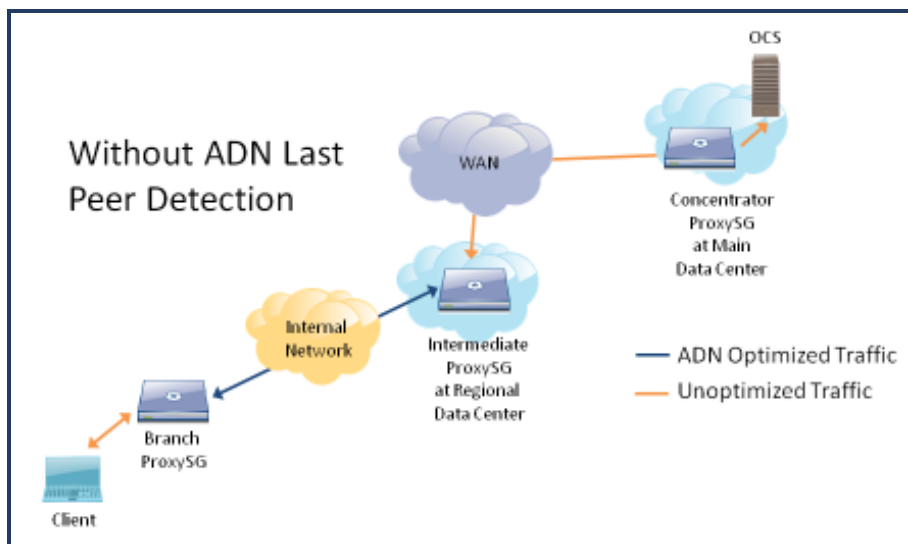
- A service doesn't exist for a type of traffic that you want to monitor or control. For example, if a significant amount of the traffic on your network is for a specific port, you can create a custom service for this port so that it doesn't get classified as Default.
- A particular server could benefit from a different proxy or acceleration techniques than other servers on the same subnet.
- You want to monitor traffic on a specific server, separating it out from other traffic using the same proxy. For

example, the predefined FTP service monitors traffic on all servers; you can create a custom service for FTP traffic on internal servers and another custom service for FTP traffic on external servers. By creating a custom service for a certain type of traffic on a server, you can create reports for this service and track its utilization over time.

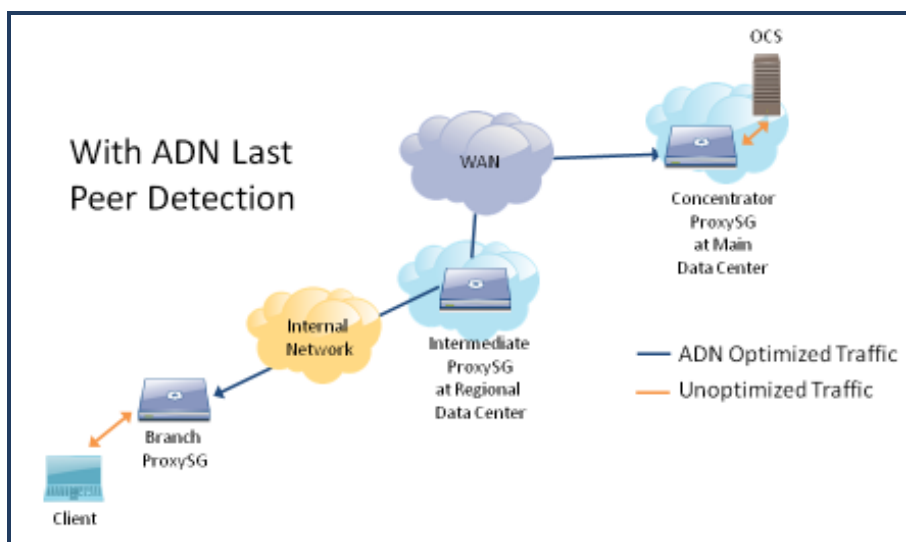
- A particular protocol may have several business level uses. For example, HTTP can be used for general web traffic, as well as an internal business application. By using distinct services, you can treat the HTTP application differently from general HTTP traffic.
- Your network uses a different port for a service than the predefined service does.
- You want to have named services that correspond to your servers. Custom services allow you to apply appropriate acceleration techniques and policies to each server.
- If you don't need the detail provided by separate services for a category of traffic, you can create a custom service that consolidates them into a single service. For example, you can delete the predefined AOL, Yahoo, and MSN services, and create a custom service called Instant_Messaging with three protocols in its traffic definition.

What is ADN Last Peer Detection?

In transparent ADN deployments where branch office traffic goes through multiple concentrators on its way to and from an origin content server (OCS), you will want to ensure that the ADN tunnel extends across the entire path, allowing the ADN traffic to be optimized from end to end. To achieve this benefit, you enable the *last peer detection* feature on the intermediate concentrators. This feature sends out probes to locate the last qualified peer—the upstream concentrator that has a valid SSL license, closest to the connection's destination address; an ADN tunnel is formed between the branch MACH5 appliance and the last peer en route to the OCS. If there is a concentrator in the path that does not support last peer detection or has it disabled, the transparent tunnel is formed with that concentrator.



Without this feature, the ADN tunnel ends at the first qualified concentrator in the path, as shown in the topology below. The traffic is optimized over this partial segment of the path to the origin content server (OCS). Traffic is not optimized over the rest of the path to the OCS.



Contrast the above illustration with the one shown below. The second illustration shows how the ADN tunnel is lengthened when the last peer detection feature is enabled on the intermediate concentrators. This feature results in the longest ADN tunnel, allowing the traffic to be optimized over the entire path.

Supported ADN Deployments

Last peer detection can be used in transparent ADN deployments including the ones listed below:

- Physically inline or virtually inline (WCCP) transparent deployments
- Open ADN mode, managed or unmanaged
- Closed ADN mode
- Transparent load balancing deployments
- Secure ADN
- SGRP redundancy support on concentrator side

Limitations

- When using last peer detection in a deployment where traffic to an OCS is distributed by a load balancer, there should be a concentrator in each potential path to the OCS. This allows the traffic to be optimized irrespective of the path that the load balancer decides upon.

- This feature is not operational when the concentrator is performing HTTP proxy processing. For accelerated HTTP traffic, an intermediate concentrator with HTTP proxy processing enabled will not attempt to detect any upstream concentrators and will terminate any inbound transparent tunnels carrying HTTP traffic. Note that the HTTP proxy processing feature has been deprecated.

What is the TCP Window Size?

TCP window size is the number of bytes that can be buffered on a system before the sending host must wait for an acknowledgement from the receiving host. The TCP window size for ADN tunnel connections is set and updated automatically, based on current network conditions and on the receiving host's acknowledgement. In most situations, you do not need to modify the TCP window size. You might need to modify it only if your network environment has intervening network equipment that makes the delay appear lower than it actually is. These environments are sometimes found on satellite links that have high bandwidth and high delay requirements. In this case, the automatically adjusted window size would be smaller than optimal.

If you know the bandwidth and round-trip delay, you can approximate the value to use:

$$2 * \text{bandwidth} * \text{delay}$$

For example, if the bandwidth of the link is 8 Mbits/sec and the round-trip delay is 0.75 seconds:

$$\text{window} = 2 * 8 \text{ Mbits/sec} * 0.75 \text{ sec} = 12 \text{ Mbits} = 1.5 \text{ Mbytes}$$

The window-size setting in this example would be 1500000 bytes. This number goes up as either bandwidth or delay increases, and goes down as they decrease. You can decrease or increase the window size based on the calculation; however, decreasing the window size below 64Kb is not recommended. The window-size setting is a maximum value; the normal TCP/IP behaviors adjust the window-size setting downward as necessary. Setting the window size to a lower value might result in an artificially low throughput.

General Proxy Settings

Blue Coat provides certain settings that apply to all proxy services:

HTTP Proxy

This chapter explains how to use the HTTP proxy. It includes the following topics:

What is the HTTP Proxy?	121
Optimize Users' Web Experience	121

What is the HTTP Proxy?

The HTTP proxy controls the delivery of Web traffic on your network. After the proxy identifies HTTP traffic, the appliance uses the following techniques to control these connections:

- Object caching
- Byte caching
- Compression
- TCP optimization
- Protocol optimization

Together, these techniques minimize latency and improve response times for Web page requests. (See "Acceleration Techniques" on page 16 for descriptions.)

The HTTP proxy functions when the HTTP proxy service is being intercepted on the Branch peers. (See Intercept a Service.)

Optimize Users' Web Experience

By having the MACH5 appliance manage Web traffic, you can improve users' Internet experience. The appliance caches copies of frequently requested Web pages and objects, so instead of the user having to wait for the object to be fetched from the original content server (OCS), it can be retrieved locally, from the MACH5 cache. In addition, the appliance optimizes the HTTP protocol using a variety of other techniques that minimize latency and improve response times for Web page requests.

1. The MACH5 appliance is pre-configured to control Web traffic, but if you want to verify that the appliance is configured to intercept the HTTP service, see Intercept a Service.

2. To monitor active Web traffic on your network, display current connections for the Web service you are intercepting (HTTP). See [List Active Sessions](#).
3. If the appliance is caching Web pages and optimizing Web protocols, you will see an increase in bandwidth savings for the HTTP service. See [Analyze Bandwidth Savings](#) and [View Benefits of Object Caching](#).
4. Although not a scientific measurement, talk to users to find out anecdotal information about Web response times after deploying the MACH5 appliance.

Streaming Media Proxies

This chapter explains how to use the streaming media proxies. It includes the following topics:

What are the Streaming Media Proxies?	123
Fine Tune Streaming Proxy Settings	125
Improve Quality of Streaming Media	126
Control Streaming Media Traffic	126
Limit Bandwidth of Streaming Media	127
Accelerate Encrypted Flash Traffic	128

What are the Streaming Media Proxies?

The streaming media proxies identify various types of streaming video and audio traffic that use real-time streaming protocol (RTSP), real-time messaging protocol (RTMP), or HTTP as transport. This allows the MACH5 appliance to filter, monitor, or limit streaming media traffic on your network. The streaming proxies use several optimization techniques to improve the quality of the streaming media.

Because video, audio, and other streaming media use a considerable amount of bandwidth—much more than Web traffic—you will probably want to use the streaming proxies to control this type of traffic. Without the proxy on a congested network, users are likely to experience problems such as jagged video, patchy audio, and unsynchronized video and audio as packets are dropped or arrive late. By using the proxy, you can save bandwidth, increase quality of service, and reduce pauses and buffering during playback.

The MACH5 appliance uses the following techniques to control streaming delivery:

- **Caching** – The appliance stores frequently requested media content in its cache and distributes it upon client requests. Because the appliance is closer to the client than the origin media server, the data is served locally at nearly LAN speed.
- **Live splitting** – The appliance supports the splitting of a live stream to multiple local users.
- **TCP optimization** – On high-latency networks or networks experiencing packet loss, the appliance is able to optimize streaming traffic by reducing stutter and static.
- **Bandwidth limits** – The appliance includes options for limiting the amount of streaming media traffic on your network.

Streaming Media Support

The MACH5 appliance offers five proxies for streaming media: Flash, MS Smooth, Windows Media, QuickTime, and Real Media. The following streaming media clients are supported:

- **Adobe Flash Player** – The appliance can fetch a live Flash stream once from the OCS and serve it to all users behind the appliance. In addition, the appliance caches content as Flash clients stream pre-recorded content from the OCS through the MACH5 appliance. The Flash proxy is able to accelerate unencrypted connections that use the RTMP (Real Time Messaging Protocol) or RTMPT (RTMP tunneled over HTTP) protocol as well as encrypted connections that use the RTMPE (RTMP encrypted) or RTMPTE (RTMP encrypted, tunneled over HTTP) protocol. Note that the Flash streaming proxy does not support bandwidth limits or bandwidth management for any RTMP-based protocol, such as RTMP, RTMPT, RTMPE, or RTMPTE.
- **MS Smooth Streaming** – The MACH5 appliance caches on-demand Smooth Streaming video content delivered over HTTP. Silverlight is the typical player used for Smooth Streaming and is available as a plug-in for web browsers running under Microsoft Windows and Mac OS X.
- **Adobe HTTP Dynamic Streaming** – The MACH5 appliance caches Adobe HDS on-demand and live adaptive bit-rate video delivery of MP4 media over HTTP.
- **Apple HTTP Live Streaming** – The MACH5 appliance caches Apple HLS on-demand and live video content delivered over HTTP. This protocol was developed for iOS and Apple TV devices.
- **Microsoft Windows Media Player** – The appliance caches Windows Media-encoded video and audio files. The standard extensions for these file types are .wmv, .wma, and .asf.
- **Real Networks Real Media Player** – The appliance caches Real Media-encoded files, such as RealVideo and RealAudio. The standard extensions for these file types are .ra, .rm, and .rmvb. Other content served from a Real Media server through RTSP is also supported, but it is not cached; this content is served in pass-through mode only. (Pass-through mode offers TCP optimization but does not support caching.)
- **Apple QuickTime Player** – The appliance does not cache QuickTime content (.mov files). All QuickTime content is served in pass-through mode only.

Streaming media can be delivered in a real-time live media stream or a previously-recorded on-demand media stream. The MACH5 appliance supports both types of streaming media.

The streaming proxies function when the RTMP, RTSP, and HTTP proxy services are being intercepted. See Intercept a Service.

Fine Tune Streaming Proxy Settings

You can configure settings for each of the supported streaming media clients: Flash, Windows Media, Real Media, and QuickTime, as well as the protocols that deliver over HTTP (MS Smooth Streaming, Apple HLS, Adobe HDS).

Go to the Advanced Management Console.

1. In Blue Coat Sky, click **Advanced configuration**.
2. Select **Configuration > Proxy Settings > Streaming Proxies**.
3. Click the tab of the streaming client you want to configure: **Flash**, **HTTP**, **Windows Media**, **Real Media**, or **QuickTime**.
4. The **Enable HTTP handoff** option is enabled by default. When a Flash, MS Smooth Streaming, Apple HLS, Adobe HDS, Windows Media, Real Media, or QuickTime client requests a stream from the MACH5 appliance over port 80 (typically the only port that allows traffic through a firewall), the HTTP module passes control to the streaming module so HTTP streaming can be supported through the HTTP proxy port. This is the HTTP handoff.

Disable this option only if you do not want the appliance to cache HTTP streams or split a live stream to multiple local users; typically there is no reason to do this unless Support requests you to do so for troubleshooting purposes.

5. The **Forward client-generated logs to origin media server** option is enabled by default.

The MACH5 appliance logs information, such as client IP address, the date, and the time, to the origin server for Windows Media and Real Media content. This option is not applicable to QuickTime or Flash. You will need to forward client logs to the origin server for any auditing functionality on the server to work correctly; some servers might disconnect clients if they don't get logs upon expected events.

6. For Windows Media and Real Media proxies, specify how often the appliance checks cached streaming content for freshness:
 - **Never check freshness** – This is the default setting.
 - **Check freshness every (hours)** – The MACH5 appliance checks content freshness every *n.nn* hours.
 - **Check freshness every access** – Every time cached content is requested, it is checked for freshness.
7. Leave the bandwidth limit settings at their default settings; it's preferable to set global bandwidth limits for all streaming clients. See "Limit Bandwidth of Streaming Media" on page 127.
8. Click **Apply**.

Improve Quality of Streaming Media

The MACH5 appliance's streaming proxies are able to improve the quality of streaming media, reducing artifacts such as frozen playback and dropped frames.

1. To control streaming media traffic, the appliance must be configured to intercept the following services:

RTMP (for Flash)

Explicit HTTP and External HTTP (for Microsoft Smooth Streaming, Apple HLS, Adobe HDS)

RTSP and MMS (for Windows Media, Real Media, and QuickTime)

See Intercept a Service; make sure the applicable services are set to intercept.

2. Verify player-specific settings and adjust if necessary. Make sure the HTTP handoff is enabled. See "Fine Tune Streaming Proxy Settings" on the previous page.

3. To monitor streaming media traffic on your network:

- Display the Traffic Summary report, select the Proxy view, and look at the table underneath the graphs. (See View Traffic Summary.) Locate the streaming proxy you are interested in (such as Flash or Windows Media) and observe the amount of WAN and LAN traffic.

Note: By default, the top 10 proxies are listed in the table; if the proxy of interest isn't displayed, click the **View all** link.

- Display current connections and filter the list for the streaming proxy you are interested in (Adobe HDS, Apple HLS, Flash, MS Smooth, Windows Media, Real Media, or QuickTime). See List Active Sessions.

4. Although not a scientific measurement, talk to users to find out anecdotal information about the quality of streaming traffic after deploying the MACH5 appliance.

Control Streaming Media Traffic

Without controls, streaming media can easily cause congestion on your network and disrupt mission-critical traffic.



This solution does not apply to Flash streaming or protocols that stream over HTTP. For an alternate solution for HTTP, see "Limit Bandwidth for Protocols that Stream over HTTP" on the facing page below.

1. To control streaming media traffic, the appliance must be configured to intercept the following services:

RTSP and MMS

See Intercept a Service; make sure the applicable streaming services are set to intercept.

2. Decide how much of your WAN bandwidth you are willing to set aside for streaming media traffic; this number (in kilobits per second) is the gateway bandwidth limit. ¹



If you want to block all streaming media traffic, you can specify a gateway bandwidth limit of 0.

3. Using the value determined in step 2, specify the gateway bandwidth limit for connections to streaming servers. See "Limit Bandwidth of Streaming Media" below.
4. To see how much bandwidth the streaming-based services are using, you can look at Traffic History utilization graphs. See "Monitor Bandwidth Utilization" on page 164. and select the service you are interested in: RTSP or MMS.
5. When the appliance is caching video and audio files and optimizing the delivery of streaming media, you will see an increase in bandwidth savings for the streaming proxies. See Analyze Bandwidth Savings and select the proxy you are interested in: Windows Media, Real Media, or QuickTime.

Limit Bandwidth for Protocols that Stream over HTTP

The global bandwidth limits for streaming protocols do not apply to MS Smooth Streaming, Apple HLS, and Adobe HDS because they are essentially treated just like HTTP traffic. However, you can write policy to limit bandwidth of these clients. For example:

```
<proxy>
streaming.client=ms_smooth limit_bandwidth.client_outbound(bw_class)
```

The streaming.client condition can also be adobe_hds or apple.hls.

Limit Bandwidth of Streaming Media

So that your network doesn't get overloaded with users watching recreational streaming videos, you may want to limit bandwidth from the streaming media clients to the MACH5 appliance or from the appliance to the servers that contain streaming content.

¹Suppose you have a 10 Gbps link and you know that you regularly have 7 Gbps of business-related traffic; you may then decide that it's acceptable to have up to 3 Gbps of streaming traffic without disrupting business traffic.

Note: These bandwidth limits do not apply to Flash streaming or Smooth Streaming over HTTP traffic.

Go to the Advanced Management Console.

1. In Blue Coat Sky, click **Advanced statistics** or **Advanced configuration**.
2. Select **Configuration > Proxy Settings > Streaming Proxies > General**.
3. To limit the bandwidth for streaming client connections, select **Client bandwidth limit** and enter the maximum number of kilobits per second that the appliance allows for all streaming client connections.
4. To limit the bandwidth for connections to streaming servers, select **Gateway bandwidth limit**, and enter the maximum number of kilobits per second that the appliance allows for all streaming connections to media servers.



To determine what value to enter for the gateway bandwidth limit, think in terms of how much of your link you are willing to allocate to streaming traffic. For example, suppose you have a 10 Gbps link and you know that you regularly have 7 Gbps of business-related traffic; you may then decide that it's acceptable to have up to 3 Gbps of streaming traffic without disrupting business traffic.

5. Click **Apply**.

You can also specify bandwidth limits for a particular streaming client: Windows Media, Real Media, or QuickTime. However, it typically is sufficient to limit bandwidth for all types of streaming clients, as described in the above procedure.



Once a limit is reached, any additional streaming connections will be denied. Clients attempting to connect may receive an error message, depending on the media player they are using. They will not be able to make a streaming media connection until the total streaming bandwidth is under the maximum limit.

Accelerate Encrypted Flash Traffic

The Flash proxy is able to process encrypted protocols (RTMPE and RTMPTE), allowing this traffic to take full advantage of the MACH5 byte caching, compression, object caching, and protocol-specific optimizations. The proxy decrypts incoming encrypted Flash data, accelerates the connection, and then re-encrypts the outgoing data.

Configuring Encrypted RTMP for Acceleration

If your MACH5 appliance is already set up to accelerate Flash traffic, no additional configuration is necessary. Just verify the following service configuration:

- **Transparent deployment** You need to have an RTMP proxy service configured to listen on port 1935 (the typical RTMP port), and this service must be set to intercept. This service controls RTMP and RTMPE traffic.
- **Explicit deployment** You should have an Explicit HTTP proxy service configured to listen on ports 8080 and 80, and this service must be set to intercept. This service controls plain and encrypted Flash connections tunneled over HTTP.

Verifying Encrypted Flash Traffic is Accelerated

The Active Sessions report indicates which Flash connections are encrypted and whether they have been optimized.

1. In Blue Coat Sky, select the **Report** tab.
2. Select **Active Sessions**.
3. In the **Filtered by** drop-down list, select **Individual proxy**.
4. In the **Individual Proxy** drop-down list, select **Flash**.
5. Click **Submit**.

Encrypted Flash connections will show one of the following three messages in the Details column:

- **Encrypted**—The encrypted connection was decrypted, optimized, and reencrypted. In this case, you should also see icons in the compression, byte caching, object caching, and protocol optimization columns, indicating that these acceleration techniques have been applied to the connection.
- **Encrypted, tunneled by policy**—The encrypted connection was not decrypted or optimized because a policy dictated that the connection should be tunneled. The policy property that controls whether encrypted Flash connections are tunneled is `streaming.rtmp.tunnel_encrypted()`.
- **Encrypted, tunneled as unknown protocol version**—The encrypted connection could not be decrypted or optimized because the RTMPE protocol version was not recognized.

SSL Proxy

This chapter explains how to use the SSL proxy. It includes the following topics:

What is the SSL Proxy?	130
Requirements	130
Accelerate SSL Traffic	131

What is the SSL Proxy?

The SSL proxy controls HTTPS and other SSL traffic so that security measures and performance enhancements can be applied to secure web content. With the appropriate configuration, the SSL proxy will:

- hand off HTTPS traffic to the HTTP proxy for protocol optimization and other acceleration techniques.
- hand off traffic from intercepted SSL-based services to the STunnel proxy which will accelerate the traffic with compression and byte caching (but no protocol optimization).
- tunnel other types of SSL traffic for which an intercepted service is not configured; this traffic will not be accelerated

One of the functions of the SSL proxy is to emulate server certificates; that is, present a certificate that appears to come from the origin content server (OCS). The MACH5 appliance emulates the certificate and signs it using the issuer keyring. The keyring includes the public and private key pair for encrypted communication, as well as the certificate that is signed by an authority that the browser trusts.

STunnel supports SSLv2, SSLv3, TLS 1.0, TLS1.1, and TLS 1.2.

Requirements

The SSL proxy in an application delivery network requires the following configuration:

- The Branch and Concentrator peers must have SSL licenses installed.
- Secure ADN must be enabled and configured on all ADN nodes.

- The Branch peer needs to specify how it proves to the browser that it's a trusted authority; this is done by specifying a keyring. In addition, you need to specify a server CA Certificate List (CCL) that provides the list of CA certificates the Branch peer should trust. See [Configure the SSL Proxy](#).
- On the Branch peers, proxy services must be configured to intercept HTTPS and other SSL-based traffic.
- On the Branch peers, policy must be configured to intercept SSL using the STunnel proxy; protocol detection must be enabled in the policy as well.

Accelerate SSL Traffic

The MACH5 appliance is able to optimize HTTPS and other types of SSL traffic. This optimization requires that the appliance is intercepting SSL-based services and that there is a policy to intercept SSL with automatic protocol detection.

1. Secure the application delivery network. See [Secure a Managed ADN](#) or [Secure an Unmanaged ADN](#).
2. In the Advanced Management Console on each Branch peer, edit the HTTPS service and make sure it is configured with the following settings:
 - Proxy: SSL
 - Enable ADN
 - Enable byte caching
 - Enable compression
 - Listener action: Intercept
3. Create (or edit) a service for the SSL-based traffic (such as POP3S or SMTPS) that you want to accelerate. Configure the following settings:
 - Proxy: SSL
 - Enable ADN
 - Enable byte caching
 - Enable compression
 - Listener action: Intercept

4. Create a policy to intercept SSL with automatic protocol detection.
 - a. Launch the Visual Policy Manager (VPM).
 - b. Create an SSL Intercept layer.
 - c. In a new rule, right-click in the Action column.
 - d. Select **Set > New > Enable SSL Interception**.
 - e. In the Add SSL Interception Object window, choose **Enable SSL interception with automatic protocol detection**.
 - f. Install the policy.
5. To test that SSL connections are being intercepted and accelerated, list Active Sessions. Use the following report settings:

Connection type: Intercepted sessions
Filtered by: Individual proxy
Individual proxy: HTTPS Forward Proxy
6. Assuming you have HTTPS traffic currently running on your network, the Active Sessions report should list connections with HTTPS listed in the Proxy Type column. To confirm the connection is being accelerated, you should see a value in the Savings column, as well as in the Comp (Compression) column and in the BC (Byte Caching) column. In addition, HTTPS connections should have in the PO (Protocol Optimization) column.
7. Repeat steps 5 and 6 to test the STunnel proxy. Note that STunnel connections cannot be accelerated with protocol optimization so you will not see the in the PO column.
8. Another way to see the benefit you are getting from accelerating SSL traffic is to look at the Bandwidth Savings report. (See Analyze Bandwidth Savings.) First, choose the **HTTPS Forward Proxy** to see the benefit from accelerating HTTPS. Then choose **STunnel** to see the bandwidth savings from accelerating other intercepted SSL services.

Note: The **SSL** proxy controls the tunneled (unintercepted) SSL traffic—there is no need to look at the Bandwidth Savings report for the SSL proxy since this traffic is not accelerated.

Encrypted MAPI Proxy

This chapter explains how to use the encrypted MAPI proxy. It includes the following topics:

What is Encrypted MAPI?	133
Accelerate Encrypted MAPI Traffic	134
Identify CAS Array to Optimize MAPI	135

What is Encrypted MAPI?

Blue Coat's encrypted MAPI solution provides the ability to transparently accelerate encrypted MAPI traffic between the Outlook client and the Exchange server. The ability to decrypt and encrypt MAPI is transparent to the user, with no knowledge of the user's password.

This feature assumes your acceleration network is set up as follows.

The encrypted MAPI acceleration feature expects the Outlook client to use the Simple and Protected Negotiation (SPNEGO) security protocol, and as a result the proxy will negotiate NTLM protocol on the client side and Kerberos on the server side. SPNEGO is used when a client application wants to authenticate to a remote server, but neither end is sure what authentication protocols the other supports.

Encrypted MAPI Requirements

The Blue Coat encrypted MAPI feature has the following requirements:

- ADN must be configured with at least one Branch and one Concentrator peer. The peers must be running SGOS 6.2+ and be configured to use an SSL device profile and secure ADN.
- An SSL license is required for secure ADN on the Branch and the Concentrator peers.
- The Outlook clients must be configured to use Kerberos/NTLM Password Authentication (Outlook 2003) or Negotiate Authentication (Outlook 2007, Outlook 2010) logon network security. The Exchange server must be enabled to support Kerberos security protocol and the Domain Controller must be enabled to support both Kerberos and NTLM LAN authentication protocols. In load balanced solutions, extra configuration is required; see *Configure Client Access Server Array* or *Load Balanced Solutions to Support Encrypted MAPI*.
- The clocks on the Branch and Concentrator peers must be synchronized with the Domain Controller clock.

- The Branch peer must be joined to each Windows domain to which your Exchange server(s) and Outlook users belong. For example, if users are created in domain A and the Exchange server resides in domain B (which has a trust relationship with domain A), the MACH5 appliance must be joined to both domains.
- The Branch peer must be configured to be trusted for delegation for exchangeMDB services and must act as an Active Directory member host.
- If you are using a third-party load balancer for your Exchange servers, you need to configure the virtual IP address of your Client Access Server (CAS) array.

Encrypted MAPI Limitations

The encrypted MAPI feature has the following limitations on the MACH5 appliance:

- The encrypted MAPI solution on the MACH5 does not support batching.
- Encrypted MAPI 2000 is not supported on the MACH5 appliance .
- Non-secure ADN can be reported in the Active Sessions at the branch even though secure ADN is enabled on the Branch and Concentrator peers. This can happen when Outlook establishes a plain connection with the Exchange server and then switches to the secure authentication level in the middle of a MAPI conversation. When this happens, the encrypted MAPI session goes through a plain ADN tunnel, without acceleration benefits.

To prevent this, enable the **Secure all ADN routing and tunnel connections** option.

- Encrypted MAPI is not supported if the Branch peer fails to authenticate the user by using NTLM and Kerberos authentication protocols within the Exchange domain.

Accelerate Encrypted MAPI Traffic

Accelerating encrypted MAPI traffic requires that you perform the following tasks. If you skip any of these steps, the MACH5 appliance tunnels MAPI traffic without optimization. Some of these tasks are performed on the Domain Controller, some on the Branch peer, and others on the Concentrator peer.

1. Prepare the Domain Controller to support the Trust Delegation feature. See [Prepare the Domain Controller to Support Trust Delegation](#).
2. Ensure that the MACH5 clocks are synchronized with the Domain Controller. See [Synchronize the Appliances and DC Clocks](#).

3. On the Domain Controller, configure Trust Delegation for the MACH5 appliance at the branch office. See [Configure the Domain Controller to Trust the Host](#).
4. Configure secure ADN between the Branch and Concentrator peers. See [Verify Secure ADN](#).
5. Join the Branch peer to the Windows domain. See [Join the Branch Peer to the Windows Domain](#).
6. Make sure the Endpoint Mapper service is being intercepted. See [Intercept a Service](#).
7. If you are using a third-party load balancer for your Exchange servers, you need to configure the virtual IP address of your Client Access Server (CAS) array. See [Identify CAS Array to Optimize MAPI](#).
8. Verify optimization of encrypted MAPI traffic. See [Verify Optimization of Encrypted MAPI](#).



In load balanced solutions, extra configuration is required for successful Kerberos authentication; see [Configure Client Access Server Array or Load Balanced Solutions to Support Encrypted MAPI](#).

Identify CAS Array to Optimize MAPI

To optimize MAPI connections when Microsoft Exchange 2010 servers are load balanced with hardware, such as Kemp, you need to identify the virtual IP address of the Client Access Server (CAS) array that fronts the Exchange Mailbox servers.

The configuration of the CAS array virtual IP (VIP) address is currently available in the command line interface (CLI) only. After the VIP is configured, the MACH5 appliance can create a new listener for this IP address, allowing the MAPI connections to the CAS array virtual host to be intercepted and optimized. This setting must be configured on each Branch peer that will handle MAPI traffic to an Exchange server with a third-party load balancer, and must be set before Outlook connects to the Exchange Server.

1. Access the CLI of the MACH5, in enable mode.
2. Type the following CLI commands to define the virtual IP address of the CAS array:

```
SGOS# conf t
```

```
SGOS# mapi
```

```
SGOS#(config mapi) cas-virtual-ip ip_address
```

where *ip_address* is the virtual IP address of the CAS array. Note that only one VIP can be configured per MACH5 appliance .

CIFS Proxy

This chapter explains how to use the CIFS proxy. It includes the following topics:

What is the CIFS Proxy?	136
What is SMB Signing?	137
SMBv1	137
SMBv2	137
Accelerate CIFS	138
Accelerate CIFS by Pre-Populating the Cache	138

What is the CIFS Proxy?

The Common Internet File System (CIFS) protocol is based on the Server Message Block (SMB) protocol used for file sharing, printers, serial ports, and other communications. It is a client-server, request-response protocol that allows computers to share files and printers, supports authentication, and is popular in enterprises because it supports all Microsoft operating systems, clients, and servers.

More than one client can access and update the same file, while not compromising file-sharing and locking schemes. However, CIFS communications are inefficient over low bandwidth lines or lines with high latency, such as in enterprise branch offices. This is because CIFS transmissions are broken into blocks of data. When using SMBv1, the client must stop and wait for each block to arrive before requesting the next block. Each stop represents time lost instead of data sent. Therefore, users attempting to access, move, or modify documents experience substantial, work-prohibiting delays.

The second version of SMB (SMBv2) alleviates some of the inefficiencies in CIFS communication and improves performance over high latency links. Servers that support SMBv2 pipelining can send multiple requests/responses concurrently which improves performance of large file transfers over fast networks. While SMBv2 has some improvements, it does not address all of the performance issues of CIFS; for example, it cannot reduce payload data transferred over low bandwidth links.

The CIFS proxy on the MACH5 appliance combines the benefits of the CIFS protocol with the abilities of the MACH5 appliance to improve performance, reduce bandwidth, and apply basic policy checks. This solution is designed for branch office deployments because network administrators can consolidate their Windows file servers (at the core office) instead of spreading them across the network.

After the proxy identifies CIFS traffic, the appliance uses the following techniques to control these connections:

- Object caching
- Byte caching
- Compression
- TCP optimization
- Protocol optimization

See "Acceleration Techniques" on page 16 for descriptions.



If there are CIFS files or folders you know many users are going to be accessing frequently, you can pre-populate the cache with this content. See "Accelerate CIFS " on the facing page.

What is SMB Signing?

Server Message Block (SMB) signing is a Microsoft-devised security mechanism that attempts to prevent man-in-the-middle attacks. If a network administrator configures SMB signing on clients and servers, signatures are added to the packet header. A decrypted signature by the recipient server or client indicates a valid packet. If the signature is malformed or not present, or if the SMB packet is compromised, the client or server rejects and drops the packet.

However, security signatures prevent the CIFS proxy from providing its full acceleration capabilities. Additionally, security signatures require a considerable amount of processing on both clients and servers. As their benefits are often superseded by link-layer security measures, such as VPNs and restricted network topology, the benefits are minimal and the drawbacks are high.

SMBv1

In order for the CIFS proxy to fully optimize SMBv1 traffic, the Windows clients cannot be configured with a requirement that security signatures always be used. For instructions on verifying this Windows setting, see *Verify Security Settings in Windows*.

In addition, if signing is required on the server, you must enable and configure SMB signing on the ADN concentrator. See *Enable SMB Signing for SMBv1 Connections*.

SMBv2

For SMBv2, if security signatures are always required on the client or the server, the CIFS proxy cannot fully optimize SMBv2 traffic. The proxy can perform byte caching and compression on this traffic, but it cannot perform object caching or protocol acceleration. If you want to fully optimize SMBv2 traffic, you must disable the setting that controls whether digital signing must always be used; this must be configured on clients and servers. If either

side requires signing always be used, the SMBv2 connections will be passed through the proxy without full optimization.

Accelerate CIFS

The CIFS proxy on the MACH5 appliance improves response times and reduces bandwidth in deployments where files are stored on a file server at the data center and accessed from a branch office.

Configure the CIFS Proxy

[Accelerate CIFS by Pre-Populating the Cache](#)

Accelerate CIFS by Pre-Populating the Cache

Pre-population refers to the process of copying files from the origin server to the MACH5 cache. Using the pre-population feature, you can cache CIFS content on the MACH5 *before* users attempt to open files the first time, resulting in faster initial access.

1. Determine which files and folders users are likely to access frequently; these are good candidates for pre-population.
2. Identify the CIFS URL of the content. You will need to know the following details:
 - Server name
 - Share name
 - Directory path to the file or files (Note: this needs to be provided only if you don't want the entire share to be pre-populated.)
 - Content access credentials (domain, user name, password)
3. Initiate the pre-population request. See Pre-Populate Content.
4. Repeat the above steps for other CIFS content you want to pre-populate.
5. Monitor the pre-population requests. See Monitor Content Pre-Population Requests.



The CIFS pre-population feature cannot pre-populate from DFS shares.

Thin Client Processing

This chapter explains how to apply special treatment to application traffic from thin client applications and virtual desktop infrastructure environments such as RDP, VNC, Citrix, and VDI. It includes the following topics:

What is Thin Client Processing?	139
Accelerate Citrix Traffic	140
Enable Thin Client Processing	141
Disable Compression and Encryption on Citrix	141
Accelerate Microsoft RDP Traffic	143
Disable Compression and Lower Encryption on RDP	143
Disable Compression and Encryption on RealVNC	145
Disable Compression and Encryption on NX	146

What is Thin Client Processing?

Thin client connections are those controlling remote desktop management and the execution of remote applications. You can apply special treatment to application traffic from thin client applications and virtual desktop infrastructure environments such as RDP, VNC, Citrix, and VDI. The MACH5 appliance has the ability to handle thin client data in a more latency-aware manner, as well as allowing the byte cache to use a low priority for retaining this type of traffic. The result of these changes is improved responsiveness of thin client actions and more efficient use of the byte cache for other types of traffic that can better leverage it.

A fresh installation of SGOS 6.4 will have the following services marked for thin client processing: MS Terminal Services, VNC, Citrix, and X-Windows; however, none will be marked for interception. Systems that are upgraded to SGOS 6.4 will not have thin client processing enabled for any services; this configuration must be done manually.

For instructions on configuring a service for thin client processing, see "Enable Thin Client Processing" on page 141.

Feature Requirements

- Thin client processing is an option for only those services that use TCP Tunnel proxies.
- This option is available only when ADN is enabled and byte caching is enabled for the service.

- Thin client processing and retention priority are mutually exclusive settings; you cannot enable both options for a service.
- The service must be marked for interception in order for thin client processing to occur.
- For thin client processing to be most effective, you must deactivate the thin client's software-based encryption and compression. For instructions, see:
 - "Disable Compression and Lower Encryption on RDP" on page 143
 - "Disable Compression and Encryption on Citrix" on the facing page
 - "Disable Compression and Encryption on RealVNC" on page 145
 - "Disable Compression and Encryption on NX" on page 146

Accelerate Citrix Traffic

By using the MACH5 appliance to accelerate Citrix thin client traffic, Citrix users will notice improved performance and responsiveness of their Citrix desktop, and branch locations will be able to support more users.

1. Edit the Citrix service so that it uses the Data Level acceleration techniques; Data Level includes byte caching and compression techniques. See [Edit a Service](#).
2. Intercept the Citrix service. See [Intercept a Service](#).
3. Enable thin client processing on the Citrix service. See ["Enable Thin Client Processing"](#) on the facing page.
4. Disable compression and encryption on the Citrix clients and lower the encryption level on the XenApp server. See ["Disable Compression and Encryption on Citrix"](#) on the facing page.
5. To test that Citrix connections are being intercepted and accelerated, connect a Citrix client to a XenApp server and list Active Sessions. Use the following report settings:

Connection type: Intercepted sessions
Filtered by: Individual service
Individual service: Citrix
6. If the Citrix connection appears in the list of intercepted sessions, the connection is being intercepted. If the connection has a value in the **Savings** column, and colored icons in the **Comp** and **BC** columns, the connection is being accelerated.

Enable Thin Client Processing

You can apply special treatment to application traffic from thin client applications and virtual desktop infrastructure environments such as RDP, VNC, Citrix, and VDI. This processing improves responsiveness of thin client actions. For example, end-users will notice that the desktop displays significantly faster.

1. In the MACH5 Management Console, edit a thin client service that uses the TCP Tunnel proxy.
 - a. Select **Configuration > Services > Proxy Services**.
 - b. Select the service. Examples: MS Terminal Services, VNC, Citrix, X-Windows.
 - c. Click **Edit Service**. The Edit Service window displays.
2. Select the following settings:
 - **Enable ADN**
 - **Enable byte caching**
 - **Enable compression** (not required)
 - **Enable thin client processing**
3. Click **OK**.
4. Select **Intercept** for the service.
5. Click **Apply** to save the settings.

For thin client processing to be most effective, you must deactivate the thin client's software-based encryption and compression.



"Disable Compression and Lower Encryption on RDP" on page 143

"Disable Compression and Encryption on Citrix" below

"Disable Compression and Encryption on RealVNC" on page 145

"Disable Compression and Encryption on NX" on page 146

Disable Compression and Encryption on Citrix

For [thin client processing](#) to be most effective, you must deactivate the thin client's software-based encryption and compression. By default, Citrix uses compression and encryption between the desktop client and the XenApp server.

Disable Compression and Encryption on the Citrix Clients

To change the compression and encryption level, you must edit the Windows registry on each client:

1. Select **Start > Run** and enter **regedit**.

Open the following registry key:

2. \HKLM\SOFTWARE\Citrix\ICAClient\Engine\Configuration\Advanced\Modules\TCP/IP
3. Change the value of **Compress** from On to Off.
4. Change the value of **Encrypt** from On to Off.
5. Save the registry.

If you are using Program Neighborhood:

1. Select **Start > All Programs > Citrix > Program Neighborhood**.
2. Right click on the desired connection and choose **Properties**.
3. In the **Options** tab, set **Encryption Level** to **Basic**.
4. Uncheck **Use data compression** and uncheck **Use disk cache for bitmaps**.

Change the Encryption Level on the XenApp Server

1. On the XenApp server, open the Registry Editor: select **Start > Run** and enter **regedit**.

Open the following registry key:

2. \HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\ICA-Tcp
3. Change the value of **MinEncryptionLevel** from 1 to 0.
4. Save the registry.
5. If you are using the XenApp web plugin:
 - a. Open the Citrix Access Management Console
 - b. Right click on the desired connection and choose **Properties**.
 - c. In the left pane, open **Advanced** and select **Client options**.
 - d. Set **Encryption** to **Basic**.

Accelerate Microsoft RDP Traffic

By using the MACH5 appliance to accelerate Microsoft Remote Desktop Protocol (RDP) thin client traffic, RDP users will notice improved performance and responsiveness, and branch locations will be able to support more users.

1. Edit the MS Terminal Services service so that it accelerates (not monitors) and uses the Data Level acceleration techniques; Data Level includes byte caching and compression techniques. See [Edit a Service](#).
2. Intercept the MS Terminal Services service. See [Intercept a Service](#).
3. Enable thin client processing on the MS Terminal Services service. See "Enable Thin Client Processing" on page 141.
4. Disable compression on the RDP clients and lower the encryption level on the Windows server. See "Disable Compression and Lower Encryption on RDP" below.
5. To test that RDP connections are being intercepted and accelerated, connect to a remote desktop and list Active Sessions. Use the following report settings:

Connection type: Intercepted sessions

Filtered by: Individual service

Individual service: MS Terminal Services

6. If the RDP connection appears in the list of intercepted sessions, the connection is being intercepted. If the connection has a value in the **Savings** column, and colored icons in the **Comp** and **BC** columns, the connection is being accelerated.

Disable Compression and Lower Encryption on RDP

For [thin client processing](#) to be most effective, you must deactivate the thin client's software-based encryption and compression. With Microsoft Remote Desktop Protocol (RDP), compression is controlled by the client and encryption is controlled by the Windows server. Microsoft does not allow encryption to be completely disabled, although it can be set to a lower level. At this low level of encryption, server --> client traffic is not encrypted but client --> server traffic is encrypted in order to protect the transmission of user login information.

Disable Compression on the RDP Clients

The RDP client does not include an option for disabling compression; you must edit the configuration file to disable compression.

1. Create the .rdp configuration file (if you haven't already configured the RDP client):
 - a. Select **Start > Programs > Accessories > Remote Desktop Connection**.
 - b. Click **Options** and go to the **General** tab.
 - c. Provide appropriate server details and access credentials.
 - d. Click **Save As** in the Connection Settings area and name the file.

2. Locate the .rdp file and open it in a text editor.

3. Locate the following parameter:

```
compression:i:1
```

4. And change it to:

```
compression:i:0
```

5. Save the file and close the text editor.
6. Double-click the .rdp file to start your RDP session.

If you are using Windows Server 2008 R2 and clients are running Microsoft Vista SP1 or higher, you can disable compression via group policy:

Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Session Environment > Set compression algorithm for RDP data

Lower the Encryption Level on the Windows Server

The default encryption setting on the server is set to Client Compatible, which uses the highest level the client can support. This setting should be set to Low.

Windows Server 2003

1. Select **Start > All Programs > Administrative Tools > Terminal Services Configuration**.
2. In the left pane, click **Connections**.
3. In the right pane, right-click **RDP-tcp** and choose **Properties**.
4. Click the **General** tab.
5. Select **Low** for the encryption level and click **OK**.

Windows Server 2008

1. On the RD Session Host server, select **Start > Administrative Tools > Remote Desktop Services > Remote Desktop Session Host Configuration**.
2. Under Connections, right-click the name of the connection and choose **Properties**.
3. Click the **General** tab.
4. Select the server authentication settings that are appropriate for your environment and select **Low** for the encryption level.
5. If you select SSL (TLS 1.0), either select a certificate that is installed on the RD Session Host server, or click **Default** to generate a self-signed certificate. If you are using a self-signed certificate, the name of the certificate will display as **Auto generated**.
6. Click **OK**.

Windows XP

Microsoft has provided a patch to customers using Windows XP as their Terminal Services Server. This patch fixes the issue that Windows XP would not let clients establish RDP connections to it with encryption levels set to Low. The Microsoft patch is located at:

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;95607>

Disable Compression and Encryption on RealVNC

For [thin client processing](#) to be most effective, you must deactivate the thin client's software-based encryption and compression. With RealVNC, compression is controlled by the client and encryption is controlled by the server. The following instructions are based on RealVNC Version 4 running on Windows.

Disable Compression on the RealVNC Clients

1. In the RealVNC viewer program, select **Options**.
2. In the **Colour & Encoding** tab, disable **Auto select** and choose **Raw** as the preferred encoding method.

Disable Encryption on the Server Component

1. Open the VNC Server properties GUI (usually via the VNC icon residing within the system tray).
2. In the **Authentication** tab, set **Encryption** to **Always Off**.

Disable Compression and Encryption on NX

For [thin client processing](#) to be most effective, you must deactivate the thin client's software-based encryption and compression. These settings are both disabled via the NX client. The following instructions are based on NX version 3.5 running on Ubuntu Linux.

1. Start the NX Client.
2. Click **Configure**.
3. In the Advanced tab, select **Disable encryption of all traffic** and **Disable ZLIB stream compression**.

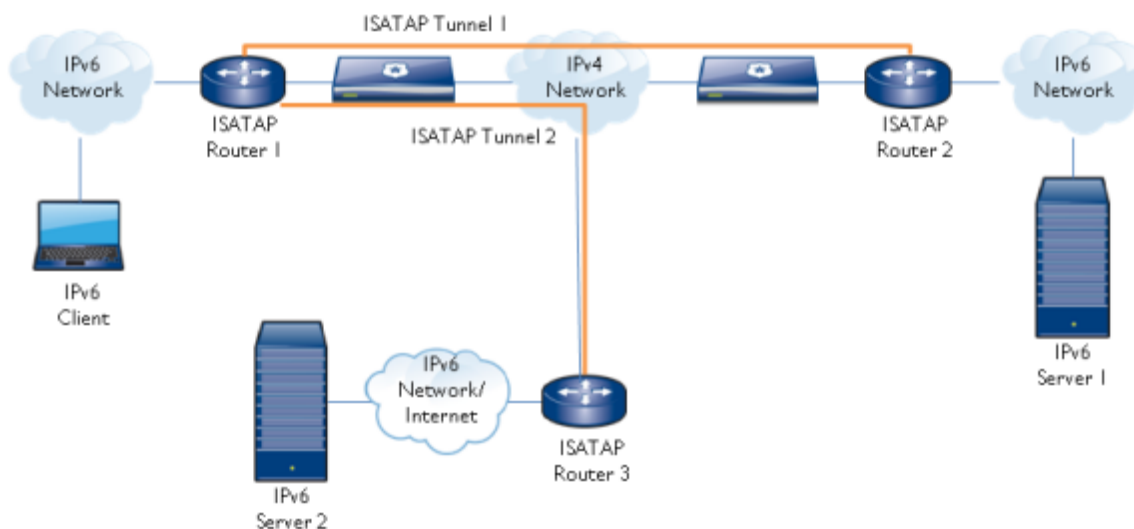
ISATAP Proxy

This chapter explains how to use the ISATAP proxy to optimize IPv6 packets and payloads over an ADN tunnel. It includes the following topics:

What is ISATAP?	147
What is the ISATAP Proxy?	150
Accelerate ISATAP Traffic	151
Configure the ISATAP Proxy	151
Verify ISATAP	152
Verify ISATAP Processing	153
Verify ISATAP Optimization	153

What is ISATAP?

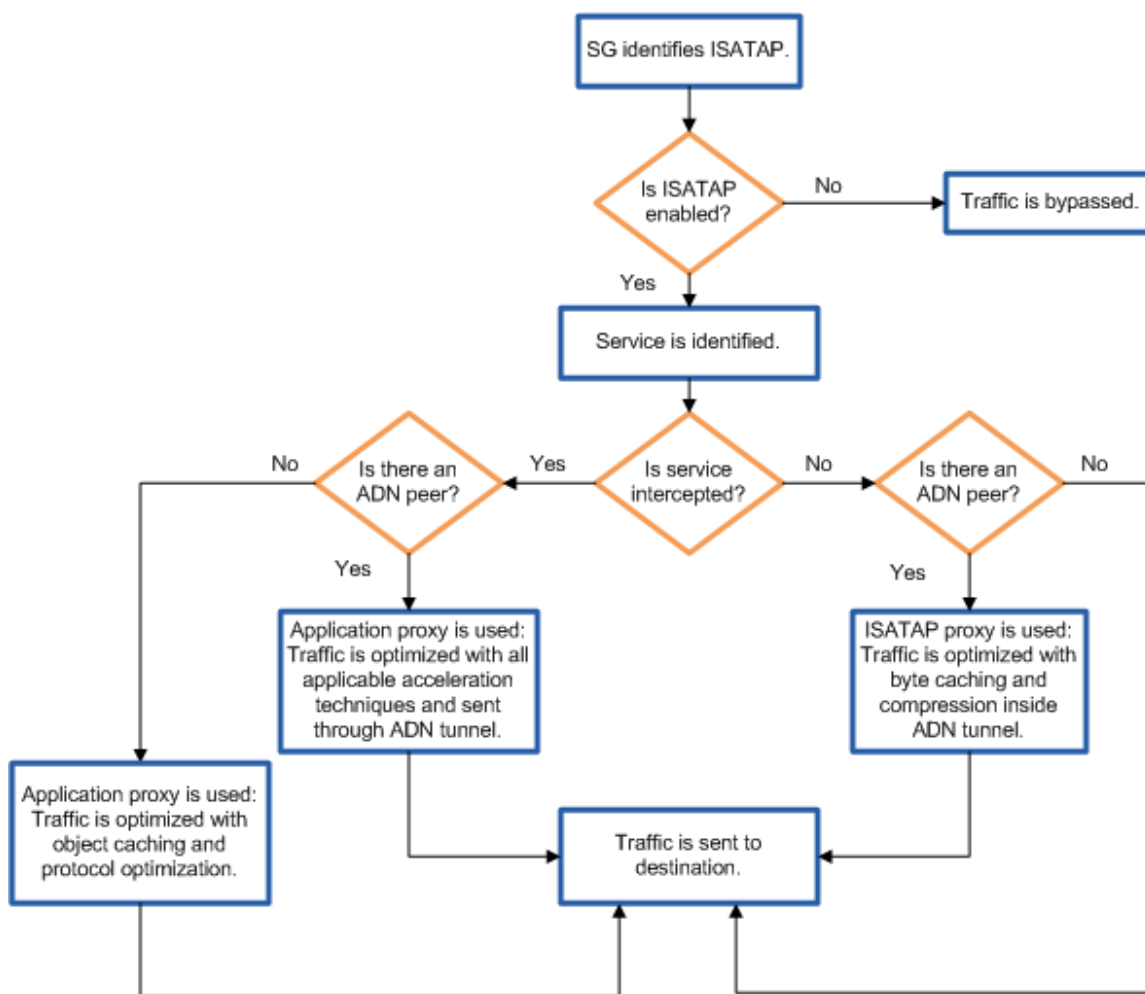
One way to transition a network from IPv4 to IPv6 is with the Intra-Site Automatic Tunnel Addressing Protocol (ISATAP). ISATAP uses a tunneling approach to transport IPv6 traffic across an existing IPv4 infrastructure by encapsulating IPv6 packets with an IPv4 header. ISATAP-based connectivity can immediately be used to deliver IPv6 services while the IPv4-only infrastructure is gradually migrated to integrate native IPv6 capabilities. The tunneling of IPv6 traffic through the use of IPv4 encapsulation is called *6-in-4*.



In this example of an ISATAP topology, remote IPv6 clients need to access IPv6 servers over the enterprise IPv4 network. To accomplish this, IPv6 traffic from the client is encapsulated by the ISATAP router before traversing the IPv4 network. For example, IPv6 packets destined for IPv6 Server 1 in the data center are encapsulated with the IPv4 tunnel address of ISATAP Tunnel 1. IPv6 packets destined for the Internet are encapsulated with the IPv4 tunnel address of ISATAP Tunnel 2.

How Does the MACH5 Handle ISATAP Traffic?

After the appliance identifies ISATAP traffic, it determines the service inside the encapsulated packet, then uses the appropriate proxy to optimize the traffic. For example, the HTTP proxy optimizes web traffic with object caching, byte caching, compression, TCP optimization, and protocol optimization (assuming an ADN peer is found). For non-TCP, non-UDP, and services that are not intercepted (such as ICMPv6), the MACH5 appliance uses the ISATAP proxy; this proxy optimizes the IPv6 packet and payload using byte caching and compression over an ADN tunnel (assuming a peer is found). The following flow diagram describes how the MACH5 appliance processes ISATAP traffic.



Notes:

- If the requested object is in cache or if the security policy determines that the request should not be allowed, the response is sent back to the client immediately over the encapsulated client-side connection.
- ISATAP is disabled by default.
- Reflect Client IP settings do not apply to the outer encapsulation header (the IPv4 address). Reflect Client IP settings are honored only for inner IPv6 source addresses for connections intercepted by application proxies, not the ISATAP proxy.

Feature Requirements

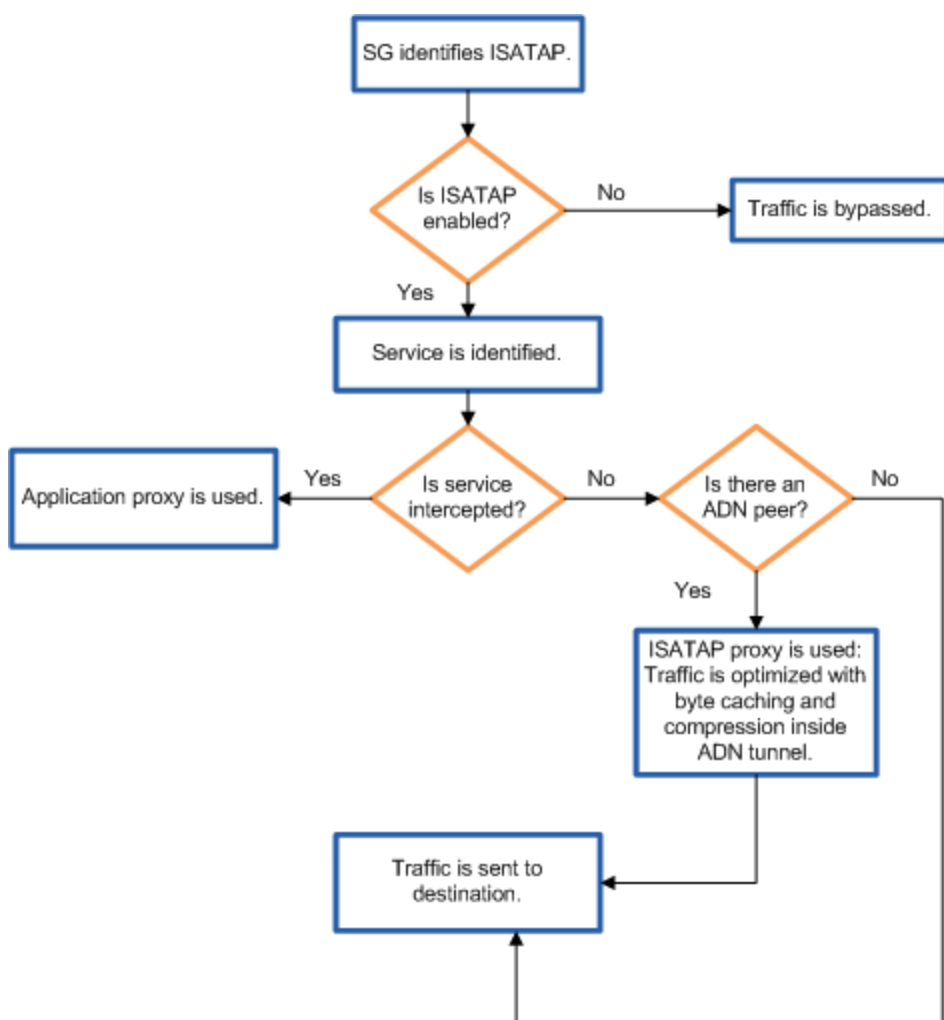
- The routers must support ISATAP.
- The MACH5 appliances must be inline between the ISATAP-capable routers.
- As shown in the topology above, the MACH5s need to be situated inside of the ISATAP tunnel. This position in the network allows the MACH5 to see and optimize traffic in ISATAP tunnels.
- When load balancing is done via an external VIP, the concentrator should have SGOS 6.5 or later.
- ISATAP must be enabled. See "Configure the ISATAP Proxy" on page 151.

Feature Limitations

- Features that modify the destination address, such as URL rewrites and advanced forwarding, can cause issues with ISATAP processing because the IP encapsulation information must be preserved. If the destination address gets modified, users will see TCP connection errors because the server cannot be found. However, if these actions change the destination to IPv4, there is no problem.
- Only explicit ADN deployments are supported for ISATAP encapsulated traffic. The MACH5 uses the destination address in the encapsulation header to perform the route lookup for establishing the explicit ADN tunnel.
- In a virtually inline (WCCP) deployment, the MACH5 is able to handle the ISATAP traffic and optimize the services for which application proxies are available, but the ISATAP proxy is not able to optimize the remaining ISATAP traffic, as it can in an inline deployment. This limitation occurs because the remaining traffic will likely not be redirected to the MACH5.

What is the ISATAP Proxy?

When the MACH5 appliance encounters Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) traffic, it decides whether to process the 6-in-4 packets with the ISATAP proxy or one of the traditional application proxies (HTTP, FTP, CIFS, etc.). To make the decision on which proxy to use, the MACH5 appliance identifies the service inside the encapsulated packet. If the MACH5 appliance is intercepting this service, the traffic is processed by one of the traditional application proxies. If the service is not intercepted, the MACH5 appliance uses the ISATAP proxy to optimize the IPv6 packet and payload over an ADN tunnel, assuming an ADN peer is found. Note that this proxy processes and optimizes all ISATAP traffic that is not handled by application proxies, including ICMP, UDP, TCP, and routing protocols. If an ADN peer is not found, the packet cannot be optimized; it is simply sent to its destination.



The ISATAP proxy uses the following techniques to optimize the IPv6 packets:

- Byte caching
- Compression

See "Acceleration Techniques" on page 16 for descriptions.

The ISATAP proxy works differently than the application proxies: it processes individual packets instead of entire streams. It does not inspect the contents of the payload; it optimizes the entire packet.

Traffic that is processed by the ISATAP proxy appears in Active Sessions as the ISATAP tunnel service and the ISATAP proxy type. The Active Sessions report lists the IPv4 tunnel address (not the IPv6 destination) as the server address since the ISATAP proxy has no insight into the payload of the packet.

The ISATAP proxy is not enabled by default. Until you enable ISATAP, 6-in-4 packets will be bypassed. See "Configure the ISATAP Proxy" below.

Accelerate ISATAP Traffic

The MACH5 appliance can see inside a 6-in-4 encapsulated packet so that it can identify the service and use the appropriate proxy to optimize the traffic. For example, the Flash proxy optimizes Flash streaming traffic with object caching, TCP optimization, and protocol optimization (assuming an ADN peer is found). For services that are not intercepted (such as ICMPv6 and UDP), the MACH5 appliance uses the ISATAP proxy; this proxy optimizes the IPv6 packet and payload using byte caching and compression over an ADN tunnel (assuming a peer is found).

1. Make sure your MACH5 appliances are inline between ISATAP-capable routers.
2. Enable both ISATAP options in the CLI. See [Configure the ISATAP Proxy](#).
3. Verify ISATAP traffic is being processed by the appropriate proxy: ISATAP or the applicable application proxy. See "Verify ISATAP" on the next page.
4. Verify ISATAP traffic is being optimized. See "Verify ISATAP Optimization" on page 153.
5. If ISATAP isn't being processed properly, refer to the ISATAP troubleshooting topics. See "Solve a Problem" on page 178.

Configure the ISATAP Proxy

The ISATAP proxy is disabled by default, so until you enable ISATAP, all 6-in-4 packets are bypassed. You can enable and configure the ISATAP proxy via the command-line interface (CLI). To use the ISATAP proxy, enable the following commands:

```
isatap adn-tunnel
isatap allow-intercept
```

If both of these settings are disabled, ISATAP traffic is bypassed. When both of these settings are enabled:

- If the service is intercepted, the ISATAP traffic is processed by the appropriate application proxy (HTTP, CIFS, FTP, etc.).
- If the service is not intercepted, the traffic is processed by the ISATAP proxy. Note that this proxy processes all ISATAP traffic that is not handled by application proxies, including ICMP, UDP, TCP, and routing protocols.

To enable full ISATAP functionality:

1. Access the MACH5 CLI, with enable (write) access.
2. Type **conf t** to go into configuration mode.
3. At the #(config) prompt, type the following CLI commands:

```
isatap adn-tunnel enable
isatap allow-intercept enable
```

Typically, you would enable both CLI commands to process ISATAP traffic. Enabling one command but not the other results in different behavior, but you might want to do this for testing purposes.

- If `adn-tunnel` is enabled but `allow-intercept` is disabled, the ISATAP proxy processes all ISATAP traffic; the application proxies aren't used.
- If `allow-intercept` is enabled but `adn-tunnel` is disabled, the ISATAP proxy is not used; ISATAP traffic is either processed by the appropriate application proxy (if the service is intercepted) or is bypassed (if the service is not intercepted).

Byte caching and compression are automatically enabled for the ISATAP proxy. To disable them, use the following CLI commands:

```
isatap adn-tunnel adn-byte-cache disable
isatap adn-tunnel adn-compress disable
```

You can also change the priority of the ISATAP byte cache:

```
isatap adn-tunnel byte-cache-priority normal (default)
isatap adn-tunnel byte-cache-priority high
isatap adn-tunnel byte-cache-priority low
```

Verify ISATAP

The MACH5 appliance offers two ways to verify that the ISATAP traffic is being processed and optimized.

Verify ISATAP Processing

Included in the output of the `show ip-stat ip` CLI command are several ISATAP statistics that you can use to verify that ISATAP traffic is being processed. The interesting statistics are:

- **ISATAP encapsulated connections accepted** –the number of ISATAP connections intercepted by the application proxies
- **ISATAP packets delivered to ISATAP proxy** – the number of ISATAP packets sent to the ISATAP proxy for optimization.

Verify ISATAP Optimization

You can use the Active Sessions report to verify that the appropriate proxy is processing ISATAP traffic and see which acceleration techniques are being used to optimize the traffic.

For Intercepted Services:

- The Service name and Proxy type listed for the session correspond to the applicable application proxy (for example, HTTP or CIFS)
- An IPv6 address is listed for the Server.
- Colored icons should appear for the acceleration techniques that are applicable to the proxy: Compression , Byte Caching , Object Caching , Protocol Optimization

For Non-TCP, Non-UDP, and Bypassed Services:

- The Service name listed for the session is ISATAP_tunnel, and the Proxy type is ISATAP.
- An IPv4 address is listed for the Server.
- Colored icons should appear for Compression and Byte Caching

Secure the ADN

To secure the application delivery network, you need to decide whether the ADN should be open or closed, managed or unmanaged, and then configure the ADN managers and nodes accordingly. This chapter includes the following topics:

What is Secure ADN?	154
Unmanaged ADN Security	154
Managed ADN Security	155
What are the Acceleration Modes?	156
What are the Acceleration Roles?	157

What is Secure ADN?

How you secure your application delivery network depends on several factors:

- Acceleration mode (open vs. closed); see "What are the Acceleration Modes?" on page 156
- Presence of an ADN manager (managed vs. unmanaged); see "What are the Acceleration Roles?" on page 157

Many of the ADN security features rely on the ADN manager for enforcement; therefore if your ADN is operating without a manager, you will not be able to use all of the security features. By default, none of the ADN security features are enabled.

Unmanaged ADN Security

If your ADN is operating in Open-Unmanaged mode, any ADN node can form transparent tunnel connections with any other ADN node. Thus, your ADN nodes are at risk for attack from systems outside your network.

To ensure that your ADN nodes only connect to authorized ADN nodes, you must deploy your own public key infrastructure (PKI) within your ADN and then secure the tunnel connections the ADN peers use. By issuing certificates to authorized ADN nodes only, you ensure that your ADN nodes will only be able to form tunnel connections with other authorized ADN nodes.

For more information on securing an Open-Unmanaged ADN, see [Secure an Unmanaged ADN](#).

Managed ADN Security

If you are using an ADN manager, you can use the secure ADN features. Secure ADN requires an appliance certificate for each ADN peer—including the ADN manager and backup manager—for identification. You can provide your own device appliance certificates or obtain Blue Coat-issued appliance certificates from the Blue Coat CA server. To enable secure ADN, you must enable the appliance authentication profile for the ADN to use before configuring any other security parameters. Secure ADN provides the following features:

- ADN Peer Authentication
- ADN Peer Authorization
- ADN Connection Security

For more information, see [Secure a Managed ADN](#).

ADN Peer Authentication

In secure ADN mode, full mutual authentication can be supported between the ADN manager and the nodes that are connected to it and between ADN peers. To use authentication, each node must have an SSL certificate and have an SSL device profile configured.

For information on enabling device authentication on your ADN nodes, see [Enable Device Authentication for Secure ADN](#).

ADN Peer Authorization

If authorization is enabled, the ADN manager must authorize a node before it is allowed to join the ADN as follows:

- When an ADN peer comes up, it contacts the ADN manager for routing information.
- The ADN manager extracts the device ID from the connecting ADN peer's appliance certificate and looks for the device ID in its approved list of ADN peers.
 - If the device is on the approved list, a REQUEST-APPROVED response is sent, followed by the route information, and the peer joins the network.
 - If the **Pending Peers** option is enabled and the device is not on the approved list, the ADN manager adds the connecting peer's device ID to a pending-peers list and sends a REQUEST-PENDING response. After the peer is moved to the Approved list by the administrator, a REQUEST-APPROVED response is sent, followed by the route information, and the peer joins the network.
 - If the **Pending Peers** option is not enabled and a peer is not on the approved list, the ADN manager sends a REQUEST-DENIED response and closes the connection. The connecting peer closes the connection and updates its connection status.

- If a peer is deleted from the approved list, the ADN manager broadcasts a REJECT-PEER to all peers to delete this peer and terminate any existing ADN connections to it. No new connections are routed through the deleted ADN peer.

See Enable Device Authorization for Secure ADN.

ADN Connection Security

By default, ADN routing and tunnel connection requests are unauthenticated and all ADN protocol messaging and compressed application data are transferred in plaintext. For maximum security, you can configure the ADN to secure ADN routing and tunnel connections using standard SSL protocol, which provides authentication, message privacy, and message authenticity security services, regardless of the application traffic that is being accelerated or tunneled.

In secure ADN mode, you can specify that the ADN manager and tunnel use secure mode to listen for routing and tunnel requests. When ADN connection security is enabled, any existing plain outbound connections are dynamically secured by activating SSL according to the secure-outbound setting.

The following table describes secure outbound behavior with various applications.

Secure-Outbound Setting	Routing Connections	Application Connections		
		CIFS	SSL Proxy Intercept Mode	SSL Proxy Tunnel Mode
None	Plain Text	Plain Text	Bypass ADN	Bypass ADN
Secure Proxies	Encrypted	Plain Text	Encrypted	Encrypted by application
All	Encrypted	Encrypted	Encrypted	Encrypted by application

See Configure Connection Security.

What are the Acceleration Modes?

The acceleration mode determines which peers an acceleration node can form tunnel connections with. There are two acceleration modes as follows:.

- **Closed**—Acceleration nodes can only establish tunnel connections with peers that have been authenticated by the ADN manager. In this mode, you must configure a Primary ADN manager and, optionally, a Backup ADN manager to manage acceleration peer connections. The ADN manager(s) can be also be configured as acceleration nodes or they can be dedicated MACH5 appliances. In Closed mode, each node must connect to the ADN manager(s) before it will be will be allowed to connect to other acceleration peers.
- **Open**—An acceleration node is allowed to form a tunnel connection with any other acceleration node. Open acceleration only works with transparent tunnels. There are two sub-modes in an

Open acceleration network: Open, unmanaged mode and Open, managed mode. In Open, unmanaged mode there is no ADN manager. However, because the management functions are not available in Open, unmanaged mode, the following are not supported in this configuration:

- Explicit tunnel connections (including ProxyClient and out-of-path deployments)
- Load balancing (explicit or transparent)
- Internet Gateway
- Peer authorization and secure routing connections

To enable any of these services, you must configure an ADN manager and connect the MACH5 appliances that require the services to it. You do not need to connect all MACH5 appliances to the ADN manager. Mixed acceleration networks in which some open nodes connect to a manager and some do not is called Open, managed acceleration. The acceleration mode is defined on the ADN manager, if there is one.

What are the Acceleration Roles?

Acceleration requires a MACH5 appliance or ProxyClient at each location where you want to achieve WAN optimization. There are several roles that a MACH5 can play in an acceleration deployment as described in the table below. Note that a single MACH5 may assume multiple roles in an acceleration deployment. In addition, not every role is required to deploy acceleration.

Acceleration Role	Description
Branch Peer	When a MACH5 appliance is acting as a Branch peer, it intercepts application traffic initiated by local clients and establishes an outbound tunnel connection with the acceleration peer at the site hosting the application servers (these peers are acting as Concentrator peers). The MACH5 appliances at each end of the connection work together to optimize the traffic as appropriate for the specific application and the configuration settings you have defined.
Concentrator Peer	When a MACH5 appliance is acting as a Concentrator peer, it accepts inbound tunnel connections from remote Branch peers. The Concentrator peer recreates the application request data, and forwards the request to the application server. When the Concentrator peer receives the application response data from the application server, it returns it to the Branch peer over the same tunnel. Note that the only difference between the Branch peer and the Concentrator peer is whether it is initiating the connection (Branch peer) or terminating the connection (Concentrator peer) in a given tunnel. A MACH5 appliance that is local to clients only will always act as a Branch peer. A MACH5 appliance that is local to application servers only will always act as a Concentrator peer. A MACH5 appliance that is local to both clients and application servers can act as both a Branch peer (when it is intercepting local client requests) and as a Concentrator peer (when it is terminating tunnel connections from remote Branch peers).

Acceleration Role	Description
Primary ADN Manager	<p>The Primary ADN manager performs the following management functions:</p> <ul style="list-style-type: none"> ■ Provides authorization for acceleration peers and enables secure routing connections ■ Advertises connection information to acceleration peers in explicit and/or ProxyClient deployments ■ Enables load balancing <p>You must be operating in a managed acceleration mode (either Closed or Open, managed) in order to use any of these management functions. For more information, see "What are the Acceleration Modes?" on page 156</p>
Backup ADN Manager	<p>The Backup ADN manager provides redundancy for the ADN management functions. If the Primary ADN manager goes down, the Backup ADN manager takes over the management duties until the Primary ADN manager becomes available again. Although it is not required, Blue Coat recommends that you configure a Backup ADN manager when operating in a managed acceleration mode.</p>
Client Manager/ProxyClient	<p>For mobile users and remote deployments (such as a micro-branch or home office) in which users connect directly to the Internet through a corporate-controlled VPN, Blue Coat offers the ProxyClient solution. When installed on user systems, ProxyClient provides WAN optimization and Web content filtering.</p> <p>A Client Manager is a MACH5 appliance that provisions software and configuration updates. The ProxyClient application connects to the ADN manager and obtains the advertised routes from the ADN manager.</p> <p>The Client Manager can be the same MACH5 appliance as the ADN manager; a separate device is not required.</p> <p>Note: The ProxyClient component is outside the scope of this WebGuide.</p>

Monitor WAN Optimization

The MACH5 appliance offers a variety of reports for monitoring WAN optimization on your network. This chapter includes the following topics:

Get Visibility into your Network Traffic	159
Refresh Intervals for Sky Reports	159
Session Report Column Descriptions	160
Monitor Bandwidth Utilization	164
Create Consolidated Traffic Reports using NetFlow	165
Configure NetFlow	165
What is NetFlow?	166

Get Visibility into your Network Traffic

For the traffic that the MACH5 appliance is managing, it's interesting to see what types of traffic are on your network, and how much bandwidth each traffic type is consuming. For example, you can see the percentage of bandwidth, as well as the number of bytes, devoted to CIFS during the last week.

1. To find out what services are most active on your network right now, look at the Top Services pie chart on the Traffic Summary report. Try different time ranges to see if and how the top services change over time. See [View Traffic Summary](#).
2. Look at the statistics at the bottom of the Traffic Summary report to observe bandwidth utilization and savings for each service or proxy. This information can tell you, for example, how much FTP traffic there is on your network and how much bandwidth was saved.
3. To monitor active connections on your network, you can display the Active Sessions report and filter the list to show current connections for a particular service or proxy. See [List Active Sessions](#).

Refresh Intervals for Sky Reports

When auto-refresh is enabled on a Blue Coat Sky report, the refresh interval depends on the report time range.

Time Range for Report	Refresh Interval
Last 5 minutes	10 seconds
Last hour	60 seconds

Time Range for Report	Refresh Interval
Last 24 hours	15 minutes
Last 7 days	6 hours
Last 30 days	1 day

For example, if the **Time range** is set to **Last hour**, the report automatically refreshes every 60 seconds.

Session Report Column Descriptions

The following table describes all the possible columns available on the Session reports. The actual columns you see in a report depends on the connection type you are viewing (Intercepted Sessions, Bypassed Connections, Both), and the level of detail (Summary or Detail).

Column	Description
Client	<p>IP address and port of the client PC (or other downstream host).</p> <p>When the session has multiple client connections, a tree view is provided.</p>
Server	<p>Final destination of the request.</p> <p>The host name is displayed unless a user entered an IP address in the URL, in which case the IP address is displayed.</p> <p>If a server connection was never made (a pure cache hit case), the Server column displays the host name (or IP address) of the requested server.</p>
Connection type	Indicates whether the connection is Intercepted, Bypassed, Inbound ADN, or Outbound ADN.
Savings	<p>Displays a horizontal progress bar that indicates bandwidth savings. A bar that is shaded all the way represents 100% savings and a bar that is shaded half way represents 50% savings.</p> <p>When the request results in a pure cache hit, this column displays 100%.</p>
Service name	<p>Displays the service used by the session.</p> <p>Even if a client connection is handed off to a different application proxy, this column shows the service name of the original service that intercepted the client connection.</p> <p>The Default service counts all traffic that doesn't match any other existing service. In other words, when the MACH5 appliance sees traffic destined to a port that is not associated with an existing service, it counts the traffic against the Default service.</p>
Proxy type	Displays the proxy used for the intercepted session.

Column	Description
ADN	<p>Indicates with an icon if an ADN connection is encrypted:</p> <p>Secure ADN connection</p> <p>Plain ADN connection</p> <p>No icon is displayed for non-ADN connections.</p>
ADN peer	IP address of acceleration peer.
LAN bytes	<p>Represents the number of bytes (to and from the client) at the socket level on the client connection. All application-level bytes are counted, including application overhead such as HTTP headers, CIFS headers, and so on.</p> <p>TCP and IP headers, packet retransmissions, and duplicate packets are not counted.</p>
WAN bytes	<p>Represents the number of bytes (to and from the server) at the socket level on the server connection. All application-level bytes are counted, including application overhead such as HTTP headers, CIFS headers, and so on.</p> <ul style="list-style-type: none"> ■ For bypassed connections, WAN bytes equals LAN bytes. ■ If the traffic is flowing through an ADN tunnel, the bytes are counted after ADN optimization, meaning that compressed byte counts are displayed. ■ TCP and IP headers, packet retransmissions, and duplicate packets are not counted.
Comp	<p>Compression. When displayed in color, this icon indicates that an acceleration tunnel is in use and gzip compression is active in either direction on that tunnel.</p> <p>This method has three states:</p> <p>Configured (color icon)</p> <p>Unconfigured (gray icon)</p> <p>Not applicable (not displayed)</p>

Column	Description
BC	<p>Byte Caching. When displayed in color, this icon indicates that an acceleration tunnel is in use and byte-caching is active in either direction on that tunnel. Byte caching replaces byte sequences in traffic flows with reference tokens; by eliminating repeated patterns of data from being sent across the WAN, byte caching allows further reduction in WAN bandwidth.</p> <p>This method has three states:</p> <p>Configured (color icon)</p> <p>Unconfigured (gray icon)</p> <p>Not applicable (not displayed)</p> <p>Note: If the control connection fails to establish, the two ADN peers cannot synchronize their byte cache dictionaries. This can happen, for example, in a transparent unmanaged ADN if the concentrator peer sends a control IP address that is not accessible from the branch peer. When a control connection with the peer is not established and the dictionaries are out of sync, a warning icon displays in the BC column to alert you of the problem. Although byte caching is enabled, it is not in use. If you see this icon, you can fix the issue by specifying preferred IP addresses on the concentrator. See the preferred-ip-addresses command in the <i>SGOS Command Line Reference Guide</i> for more information.</p>
OC	<p>Object Caching. When displayed in color, this icon indicates that an HTTP, HTTPS, CIFS, Streaming, or FTP proxy is in use and the content is cacheable. The MACH5 appliance caches objects (HTML pages, images, streaming content, and CIFS file data) so that it can serve this data directly to clients; object caching saves time and bandwidth since the content needn't be accessed repeatedly across the WAN.</p> <p>This method has three states:</p> <p>Configured (color icon)</p> <p>Unconfigured (gray icon)</p> <p>Not applicable (not displayed)</p> <p>The icon:</p> <ul style="list-style-type: none"> ■ Is unavailable if the content is non-cacheable (or for CIFS, when the entire connection is non-cacheable—not on an object-by-object basis). ■ Is not displayed for Endpoint Mapper and TCP-Tunnel traffic. ■ Does not indicate a cache hit; it indicates only that the object is cacheable.

Column	Description
PO	<p>Protocol Optimization. When displayed in color, this icon indicates that a proxy is in use that is capable of performing optimization. These proxies include HTTP, HTTPS, CIFS, and MAPI.</p> <p>This method has three states:</p> <p>Configured (color icon)</p> <p>Unconfigured (gray icon)</p> <p>Not applicable (not displayed)</p>
BWM	<p>Bandwidth Management. When displayed in color, this icon indicates that either the client or server connection has been assigned to a bandwidth class.</p> <p>This icon has two states:</p> <p>Active (color icon)</p> <p>Inactive (gray icon)</p>
SOCKS	<p>SOCKS. Indicates that the upstream connection is being sent through a SOCKS gateway. If the icon does not display, it indicates that a SOCKS gateway is not in use.</p> <p>Active</p>
FWD	<p>Forwarding. Indicates that the upstream connection is being sent through a forwarding host. If the icon does not display, it indicates that forwarding is not in use.</p> <p>Active</p>
ICAP	<p>Indicates an ICAP-enabled session. If the icon does not display, ICAP is not supported for that session.</p> <p>Active</p>
Duration	Displays the amount of time the session has been established.

Column	Description
Details	<p>Provides additional information. For example, it can indicate that a CIFS connection is "pass-through" due to SMB signing.</p> <p>The Details column also displays the following errors:</p> <ul style="list-style-type: none"> ■ Errors connecting upstream (TCP errors, ADN network errors) ■ Unexpected network errors after connecting (e.g., read errors) ■ Request-handling errors (parse errors, unknown method or protocol, unsupported feature) ■ Response-handling errors (parse errors, unknown method or protocol, unsupported feature, unexpected responses such as HTTP 500 errors from OCS) ■ Unexpected internal errors ■ DNS errors and DNS resolve failures

Monitor Bandwidth Utilization

As part of the traffic management process, you will want to monitor bandwidth utilization on your network: how much and of what type. Using various built-in charts, you can see how much traffic is going through the MACH5 appliance as well as the utilization of each proxy or service, during a specified time period. You can use this information to validate WAN link sizing and expenses.

1. **Go to the Advanced Management Console.**

In Blue Coat Sky, click **Advanced statistics** or **Advanced configuration**.

2. **Select **Statistics > Traffic History**.**

3. **From the **Service** or **Proxy** drop-down list, select the type of traffic for which you want to analyze bandwidth utilization. For example, you can select the RTSP service or the Windows Media proxy.**

4. **Select the time period you are interested in: From the **Duration** drop-down, select **Last Hour**, **Last Day**, **Last****

Week, Last Month, or Last Year.

The graphs and statistics automatically update to reflect the time period you selected. The **BW Usage** tab displays an area graph showing the rate (in kilobits per second) of client, server, and bypassed traffic in the selected service/proxy during the time period.

5. (Optional) Clear the **Include bypassed bytes** checkbox if you don't want to include bypassed traffic in the graphs, statistics, and calculations; this would allow you to get a clearer view of traffic that is intercepted.
6. If you are interested in other time periods or other services/proxies, repeat steps 3-5.

Create Consolidated Traffic Reports using NetFlow

By exporting flow data from all your MACH5 appliances to a third-party flow collector, you can then create consolidated reports that can provide visibility into traffic load, usage, and bandwidth savings on a per-device or enterprise-wide basis.

1. Configure NetFlow. you will need to define the port and IP address of the flow collector(s), specify which interfaces you want to monitor, and enable NetFlow processing. See "Configure NetFlow" below.
2. Use the **show netflow** CLI command to verify that the MACH5 appliance is sending flow records.
3. Go to your NetFlow collector and verify that it is receiving flow records from your MACH5 appliance.
4. Repeat the above steps to set up other MACH5 appliances for NetFlow processing.
5. In your third-party flow collector, design/generate reports that consolidate data from your MACH5 appliances. For example, depending on the capabilities of your collector, you may be able to create Top Talker/Listener reports or Bandwidth Savings reports.

Configure NetFlow

To configure NetFlow, you need to define the port and IP address of the flow collector(s), specify which interfaces you want to monitor, and enable NetFlow processing.

1. Access the MACH5 CLI, with enable (write) access.
2. Type **conf t** to go into configuration mode.

3. Type the following CLI commands to define a flow collector:

```
#(config) netflow
```

```
#(config netflow) collectors
```

```
#(config netflow collectors) add <IP-address> <port>
```

Enter the collector's IPv4 or IPv6 address and the port on which it is listening.

4. Define additional collectors, if available. You can define up to four collectors.
5. (Optional) If you want to limit the number of flow detail records that are sent to the collector, specify the MACH5 interface(s) that you want to monitor:

```
#(config netflow collectors) exit
```

```
#(config netflow) add <adaptor>:<interface> [in|out|inout]
```

NetFlow input (in), output (out), or both (inout). If no parameter is specified, the default is used (inout).

6. Enable NetFlow processing:

```
#(config netflow) enable
```

The MACH5 appliance will now send flow detail records of data seen on the specified interface to the defined flow collectors. Flow records are actually bundled together into *NetFlow packets*; the MACH5 appliance sends a packet to the collector after it reaches the maximum of 30 flow records, or two minutes after the first flow record is collected, whichever comes first.

What is NetFlow?

NetFlow is a network protocol developed by Cisco Systems® to monitor and export IP traffic information. If you enable NetFlow on the MACH5 appliance (while collectors are configured), the appliance observes network flows on all interfaces and keeps track of flow statistics such as source and destination IP addresses, the size of the flows (in terms of packets and bytes), and when the flows were sent.

Currently, SGOS supports NetFlow v5, which is restricted to collecting flow statistics for IPv4 packets only.

After the appliance gathers the flow statistics, it exports the NetFlow records to a remote system called a *collector*. Blue Coat has tested the NetFlow feature with ManageEngine® NetFlow Analyzer.

The following figure shows a NetFlow deployment with:

- The MACH5 appliance acting as the NetFlow record exporter.
- Two collectors, configured on separate remote machines.

NetFlow Terminology

Blue Coat documentation uses the following terms to describe the NetFlow feature in SGOS.

Network flow—A sequence of packets from a source application to a destination application. A network flow has attributes such as IP address, port, protocol, and ingress/egress interfaces.

A flow is exported to the collectors when:

- it has been inactive for a period of time exceeding the inactive-timeout value
- it has been active for a period of time exceeding the active-timeout value
- it is reported as being finished
- it exceeds the byte count limit of 32 bytes

Flow records—Contain information about a flow, such as source and destination IP addresses, the amount of data transferred (in terms of packets and bytes), and the flow start and end times.

NetFlow packets—NetFlow-formatted packets, which contain copies of expired flows. These packets are sent to a collector once they reach the maximum of 30 records, or two minutes after the first flow record is collected.

Benefits of Using NetFlow

The MACH5 appliance can look at a flow, identify its application or protocol, gather statistics about it, include flow information in the NetFlow flow record, and then send the record to a collector. In the collector's report generator, you can analyze and summarize data to view reports.

The NetFlow feature offers:

- Enhanced troubleshooting and forensic capabilities. Collector reports can aid in troubleshooting network problems and help determine the source of a DoS attack.
- Integration with accounting/billing programs. For example, broadband service providers can bill customers by application usage and, if desired, have different billing rates for different types of applications (such as P2P, VoIP, email, and web surfing). Or, enterprises can track each department's application usage and bill them accordingly.
- Historical Top Talker and Top Listener data. For example, you may want to keep hourly data for six weeks and monthly data for two years.

Maintain the MACH5 Appliance

You can perform a variety of maintenance tasks on your MACH5 appliance. This chapter includes the following topics:

What is Health Monitoring?	168
Alert Messages	169
Device Health Alerts	170
Other Alerts	172

What is Health Monitoring?

Keeping tabs on the health of your MACH5 appliance is important. If a component is not functioning properly, you will want to know about it to take action before it fails or causes other problems. Or if an interface is frequently nearing capacity, you will want to be informed so that you can consider upgrading to a higher capacity.

The MACH5 appliance monitors the health of a variety of components (disk drives, fan operation, fan temperature, CPU temperature, memory, bus voltage, and so on) and determines the state of each component at one-minute intervals. The state indicates the condition of the monitored component:

- **OK**—The monitored component is behaving within normal operating parameters.
- **WARNING**—The monitored component is outside typical operating parameters and may require attention.
- **CRITICAL ERROR**—The monitored component is failing or has exceeded its critical threshold, as discussed in the following paragraph.

The current state of a component is determined by the relationship between its current value and its monitoring thresholds. The Warning and Critical Error states have thresholds associated with them. For example, by default, CPU utilization has a warning threshold of 80% of capacity and a critical threshold of 95%. Thresholds of some components are user configurable (in the Advanced Management Console); other components have manufacturer-defined thresholds.

Depending on the component, the state may simply be OK or Critical. For example, fans are either OK or Critical; there is no Warning.

Each component's health status begins in the OK state. If the value exceeds the Warning threshold and remains there for the threshold's specified interval, the component's health transitions to the Warning state and the MACH5 appliance issues a warning alert. Similarly, if the Critical threshold is exceeded for the specified interval, the component health transitions to the Critical state and an error alert is issued. Later (for example, if the problem is




resolved), the value will drop back down below the Warning threshold. If the value stays below the Warning threshold longer than the specified interval, the state returns to OK.

If the value fluctuates above and below a threshold, no state change occurs until the value stays above or below the threshold for the specified interval of time. This behavior helps avoid unwarranted notifications when values vary widely without having any definite trend.

Because of the importance of knowing about the MACH5 appliance's health state, alerts are prominently displayed in a panel on the Monitor tab.



Device Health

The overall device health status appears in the banner (for example, **Device health: Warning**). The following icons are used to indicate the state of the device health:

Icon	State
	OK
	Warning
	Critical

The device health is an aggregate health status based on a variety of potential situations (such as hardware, licensing, and configuration issues) and is tied to the presence of alerts. For example, the existence of an error alert would cause the device health to be in a critical state. Clicking the Device Health link displays the Health Checks window in the Advanced Management Console. While you are in the Management Console, you may also want to take a look at the Health Monitoring screen.

Alert Messages

The Alerts panel notifies you when the MACH5 appliance has operational issues. The messages are categorized as warnings or errors. The MACH5 appliance issues warning messages (flagged with ) when a predefined warning threshold has been exceeded on the device. Error messages (flagged with ) are issued when there is a connectivity problem or a critical threshold has been exceeded on the device. Errors are more severe than warnings. For example, when CPU consumption exceeds 80% of capacity, the warning threshold is exceeded and the MACH5 appliance issues a warning alert; when consumption reaches 95% of capacity, the critical threshold is exceeded and an error alert is issued.



Thresholds for CPU, memory, and interface utilization can be modified in the Advanced Management Console, in the Maintenance > Health Monitoring tab.

Messages are hyperlinks that take you to an applicable configuration or report page when clicked. For example, the *License expiry approaching* error message opens the Licensing page.

When there aren't any alert messages, a green flag appears.

Device Health Alerts

These types of alerts are related to the health of the MACH5 hardware components; they vary by model, depending on the hardware present.

Message	Description	Message Type	Action
Bus voltage fluctuations: +5V bus reached x +12 V bus reached x +3.3V bus 2 (Vcc) reached x	The bus voltage has crossed a manufacturer-defined warning or error threshold. Possible causes are malfunctioning chips or an issue with the motherboard power regulation. Bus voltage measurements are not available on all models.	Warning or Error (depending on the value)	This message may indicate a need for hardware maintenance.
Committed memory consumption reached x %	Committed memory utilization has crossed a predefined warning (90% of capacity) or critical (95%) threshold for a predefined duration (120 seconds).	Warning or Error (depending on the value)	Frequent occurrences of this message may indicate the need for a larger capacity device.
CPU consumption reached x %	CPU utilization has crossed a predefined warning (80% of capacity) or critical (95%) threshold for a predefined duration (120 seconds). When the model has multiple CPUs, the CPU number is identified in the message.	Warning or Error (depending on the value)	Frequent occurrences of this message may indicate the need for a larger capacity device.
CPU core voltage reached x	The voltage of the CPU core has crossed a manufacturer-defined warning or error threshold. CPU core voltage measurements are not available on all models.	Warning or Error (depending on the value)	This message may indicate a need for hardware maintenance.
CPU fan speed reached x RPM	The CPU fan speed has crossed a manufacturer-defined warning or error threshold. When the model has multiple fans, the fan number is identified in the message. Fan speed measurements are not available on all models.	Warning or Error (depending on the value)	This message may indicate a need for hardware maintenance.

Message	Description	Message Type	Action
CPU temperature reached x C	<p>The temperature in Celsius of the CPU has crossed a manufacturer-defined warning or error threshold.</p> <p>When the model has multiple CPUs, the CPU number is identified in the message.</p>	Warning or Error (depending on the value)	<ul style="list-style-type: none"> - Check for fan alerts. - Check operational environment and adjust HVAC systems.
Disk in negative state	<p>The disk has failed or failure is imminent.</p> <p>When a model has multiple disks, the disk number is identified in the message.</p>	Error	This message may indicate a need for hardware maintenance.
Fan in negative state	<p>The fan has failed.</p> <p>When the model has multiple fans, the fan number is identified in the message.</p>	Error	This message may indicate a need for hardware maintenance.
Fan speed reached x RPM	<p>The fan speed has crossed a manufacturer-defined warning or error threshold.</p> <p>When the model has multiple fans, the fan number is identified in the message. Fan speed measurements are not available on all models.</p>	Warning or Error (depending on the value)	This message may indicate a need for hardware maintenance.
Interface x.x capacity reached x %	The utilization on a single-port interface (such as 0.0 or 1.0) or a bridged interface (such as 0:0-0:1) has crossed a predefined warning (60% of capacity) or critical (90%) threshold for a predefined duration (120 seconds).	Warning or Error (depending on the value)	Frequent occurrences of this message may indicate the need for a larger capacity device.
Motherboard temperature reached x C	<p>The temperature in Celsius of the motherboard has crossed a manufacturer-defined warning or error threshold.</p> <p>Measurement of motherboard temperatures are not available on all models.</p>	Warning or Error (depending on the value)	<ul style="list-style-type: none"> - Check for fan alerts. - Check operational environment and adjust HVAC systems.

Message	Description	Message Type	Action
Power supply failure	This message appears only when redundant power supplies are installed.	Error	This message may indicate a need for hardware maintenance.
Standby voltage +5V standby reached x	<p>The standby voltage has crossed a manufacturer-defined warning or error threshold.</p> <p>Standby voltage measurements are not available on all models.</p>	Warning or Error (depending on the value)	This message may indicate a need for hardware maintenance.

Other Alerts

The following table lists other alert messages you may see in the Alerts panel. Note that this list is not exhaustive—it includes the messages you are most likely to see.

Message	Description	Message Type	Action
ADN Connection Status Disconnected	The ADN peer is not connected to the ADN manager (perhaps due to network or configuration issues) and cannot receive route/peer information.	Error	To verify configuration of the ADN manager, select Configure > ADN > General .
Health check warning	One or more external services used by the MACH5 are in a warning state, for example, the DNS server is experiencing response time or connectivity problems.	Warning	To see which external service is unhealthy, click the hyperlink. This opens the Health Checks page in the Advanced Management Console.
Health check critical	One or more external services used by the MACH5 are in an error state.	Error	To see which external service is unhealthy, click the hyperlink. This opens the Health Checks page in the Advanced Management Console.
License expiry approaching	The MACH5 has a device license that has reached a predefined warning period (15 days), prior to expiration. Note that the device is fully operational until the expiration date is reached.	Warning	Click the hyperlink message to install a valid license. This opens the Licensing page.

Message	Description	Message Type	Action
License expired. All traffic is now bypassed.	The MACH5 has a device license that has reached its predefined expiration date. Traffic cannot be accelerated until the license is renewed.	Error	Click the hyperlink message to install a valid license. This opens the Licensing page.
Trial period expires	The MACH5 is currently running during the trial period after initial configuration of the appliance. The alert indicates the number of days left in the trial period.	Warning	Click the hyperlink message to install a valid license. This opens the Licensing page.
WCCP configuration incomplete	The virtually in-path deployment was selected during initial configuration, but you haven't yet configured WCCP. Traffic cannot be redirected to the MACH5 until you have finished WCCP configuration.	Error	Click the message hyperlink to go to the WCCP Configuration page.

Manage SGOS Images and Licenses

This chapter explains how to upgrade and downgrade the SGOS software, and manage licenses. It includes the following topics:

What is Software Version Management?	174
What is the Physical Appliance License?	175
Trial Licenses	175
About License Expiration	176
Installing Permanent Licenses	176
What is the Virtual Appliance License?	176

What is Software Version Management?

The MACH5 software is called the Secure Gateway Operating System (SGOS). You can install up to five SGOS versions and you can upgrade or downgrade between these versions. When an image is a higher version number than the currently running system, it is considered an *upgrade*. When an image is a lower version than the running system, it is considered a *downgrade*.

The Operating System configuration page provides information about your currently running version, and provides details on any other installed versions on the MACH5 appliance.

The list of installed operating systems is sorted by SGOS version number, with the highest version appearing at the top of the list. For each version, the table indicates the date and time that version was last booted and the boot status (successful or failed). The currently running system is highlighted in gold.

Using New SGOS Versions

Using a new version of SGOS is a two-step process:

1. Download the image to the MACH5 appliance. You can either download the image from the Blue Coat download site or a web server. (See Download an SGOS Image.)
2. Upgrade or downgrade to that image. This process reboots the appliance and runs the selected version. (See Upgrade/Downgrade an SGOS Image.)

Notes:

- There are five available slots for operating systems. If all slots are full when you download a new image, the new image replaces the lowest SGOS version. The selected button in the **Replace** column indicates which image will be replaced. If you want the new image to replace a different image, select its **Replace** button before downloading a new image.
- To protect an image from this automatic removal process, you can lock it. The currently running system is automatically locked. (See Lock an Image.)
- You cannot download a system image that is already installed. If you attempt to do this, an error message displays and the operation will be canceled.
- Refer to the release notes for the recommended upgrade paths.

Blue Coat Sky Updates

Blue Coat Sky can be updated independent of the operating system. When a Blue Coat Sky update is available, Blue Coat will post the gzipped tar archive file on its download site. The currently running Sky version and release ID are shown on the Operating System configuration page.

Installing a Sky update is a single-step process and does not require a reboot of the appliance. It automatically replaces the currently running Sky version. (See Install a Update.)

What is the Physical Appliance License?

For the ProxySG VA, see "What is the Virtual Appliance License?" on the facing page.

After initial configuration of a new MACH5, the appliance operates with a *trial license*. Initial system boot-up triggers the 60-day trial, during which time you can evaluate the MACH5 functionality. If you require more time to explore the MACH5 features, a *demo license* is available; contact your reseller or Blue Coat Sales to request a demo license. At some point, preferably before the trial or demo license expires, you will want to install a non-expiring, fully functional license.

Trial Licenses

For the trial license period, all licensable components are active and available to use. You have the option to not let users access features that are currently running in the trial period. Note that you cannot selectively disable trial period features; you must either enable all of them or disable all of them. The **Disable trial components** option is on the Licensing page.

In the trial period, the number of concurrent users is unlimited. When a full license is installed, any user limits imposed by that license are enforced, even if the trial period is still valid.

About License Expiration

If your trial or demo license expires before installing a permanent license, all traffic will be bypassed. Although the setting for concurrent users may still say *unlimited* because this was the setting for the trial or demo license, traffic cannot be intercepted with an expired license.

When a license expires, users might not receive notification, depending upon the application they are using. Notifications do occur for the following:

- **HTTP (Web browsers)**—An HTML page is displayed stating the license has expired.
- **SSL**—An exception page appears when an HTTPS connection is attempted.
- **Instant Messaging clients**—Users do not receive a message that the license has expired. Any IM activity is denied, and to the user it appears that the logon connection has failed.
- **FTP clients**—If the FTP client supports it, a message is displayed stating the license has expired.
- **Streaming media clients**—If the Windows Media Player, RealPlayer, or QuickTime player version supports it, a message is displayed stating the license has expired.—
- **ProxyClient**—After the trial license has expired, clients cannot connect to the ADN network.

You can still perform configuration tasks through the CLI, SSH console, serial console, or Telnet connection. Although the component is disabled, feature configurations are not altered. Also, policy restrictions remain independent of component availability.

Installing Permanent Licenses

The ProxySG offers two types of base licenses:

- **MACH5 Edition**—Used for acceleration deployments. Security-related features are not included. The MACH5 base license (also known as the *Acceleration Edition*) allows acceleration of HTTP, FTP, CIFS, DNS, email, and streaming protocols.
- **Proxy Edition**—Used for security and/or acceleration deployments. Use the full proxy edition to secure Web communications and accelerate the delivery of business applications.

Some time during the trial/demo period, you should install the permanent license. See [Install a License via BTO](#) or [Install a License Manually](#).

What is the Virtual Appliance License?

The ProxySG VA offers two types of licenses:

- A *subscription-based license* is valid for a set period of time (such as one year). After you have installed the license, the ProxySG VA will have full functionality, and you will have access to software upgrades and product support for the subscription period.
- A *perpetual license* is a permanent license. For software upgrades and product support, you need to purchase a support contract.

The ProxySG VA license uses the MACH5 Edition for acceleration deployments. The MACH5 base license (also known as the Acceleration Edition) allows acceleration of HTTP, FTP, CIFS, DNS, email, and streaming protocols. Security-related features are not included. The ProxySG VA also includes an SSL license for intercepting SSL traffic and a Flash license for optimizing RTMP traffic.

For a period of time before a subscription-based license expires, Blue Coat Sky will alert you that the license will be expiring. If your license expires before you have renewed the subscription, all traffic will be bypassed: Traffic will not be accelerated. Therefore, it's important that you renew your license during the warning period so that you do not lose functionality.

For instructions on installing the license, see [Install a License via BTO](#) or [Install a License Manually](#).

Solve a Problem

If you are experiencing an issue with your MACH5 appliance, select one of the topics below to help troubleshoot the problem.

What tools are available to troubleshoot appliance issues?	178
How can I troubleshoot problems with TCP connections?	179
Troubleshoot Bypassed Connections	179
Troubleshoot Intercepted Sessions	181
Why is my network slow?	182
Why is all traffic being bypassed?	183
Why is ISATAP traffic being bypassed?	183
Why is all ISATAP traffic using the ISATAP Proxy?	184
Why are users seeing TCP connection errors in an ISATAP deployment?	184
Why is some traffic getting routed through the management port?	185
About Preferred IP Selection	185
Configure a Preferred IP List	186
Why is the device health reporting as Warning or Critical?	187
Why is the CPU usage so high?	187
Configure Adaptive Compression	188
Why is there a byte cache warning for a connection?	189
Why are old peers showing up in my byte-cache dictionary?	189
Why isn't the Flow Collector receiving NetFlow records?	190
Troubleshoot Duplicate Serial Numbers	191
Resolving the Duplicate Serial Number Error Message	191
Troubleshoot Stolen Time	192
Recovering from Excessive Stolen Time Accumulation	192

What tools are available to troubleshoot appliance issues?

Blue Coat Sky facilitates the collection of service information required for Technical Support to troubleshoot issues

with the MACH5 appliance.

How can I troubleshoot problems with TCP connections?

If you are experiencing an undiagnosed network problem, you can use the Active Sessions lists to help troubleshoot the issue. Errors are generally a result of configuration issues on the MACH5 appliance. If a particular proxy service is experiencing a problem, you can look at the list to see if that service has any errors or special messages.

You might also want to periodically peruse the list to see if there are any new, yet unreported problems so that you can address an issue before it becomes more widespread.

- "Troubleshoot Intercepted Sessions" on page 181
- "Troubleshoot Bypassed Connections" below

Troubleshoot Bypassed Connections

Bypassed connections are those that pass through the MACH5 appliance without any processing. This procedure describes how to see a list of current bypassed connections and how to interpret the information to troubleshoot a network problem.

1. Display the Active Sessions report in Blue Coat Sky. See [List Active Sessions](#).
2. Choose **Bypassed connections** for the **Connection type**.
3. (Optional) To display a specific category of connections in the report, choose a filter on the **Filtered by** drop-down:

Filter	Information to Enter
Client IP	Enter the client's IP address or IP address and subnet mask.
Client port	Enter a client port number.
Server IP	Enter the IP address or host name of the server. Host name filters automatically search for suffix matches. For example, if you filter for example.com, test.example.com is included in the results.

Filter	Information to Enter
Server port	Enter a server port number.
Individual service	Select a service from the drop-down list.
Individual proxy	Select a proxy name from the drop-down list.

4. Locate the **Service name** and **Details** columns.

The **Service name** is the proxy service associated with the connection and the **Details** provide a brief description of any errors. To sort by error type, click the **Details** column heading.

5. Scroll down and look at the variety of services that have bypassed connections.

- You would expect to see all the services that are configured for bypass, as well as the client/server pairs configured with static bypass rules.
- The Default service includes all traffic that the appliance does not have an existing service for.
- You should *not* see any connections for services that are being intercepted unless you have configured restricted intercept or static bypass rules.
- If you don't see any connections for a service you have configured for bypass, it's possible that there isn't that type of traffic on the network at this point in time. Verify that the service is configured for bypass and then check back later to see if there are any connections for that service type. See Bypass a Service.

6. Here are a few things you can explore according to the type of error in the **Details** column:

- **TCP errors** – The origin content server may not be available, the user may have entered the wrong URL, or a firewall may be blocking the connection.
- **Read errors** – The origin content server may be misconfigured or a firewall may be blocking the protocol.
- **Unexpected internal errors** – Contact Blue Coat Customer Support.
- **DNS errors** – Verify the local DNS server is configured properly.
- **BCAAA errors** – Make sure the BCAA service is running and verify its configuration. Confirm that there isn't a blocking firewall between the MACH5 appliance and the BCAA server.

7. If the list has been displayed on your screen for a period of time, you can manually refresh the list by clicking **Refresh**.

Troubleshoot Intercepted Sessions

Intercepted sessions are those that are intercepted by the MACH5 appliance. This procedure describes how to see a list of current intercepted sessions and how to interpret this information to troubleshoot a network problem.

1. Display the Active Sessions report in Blue Coat Sky. See [List Active Sessions](#).
2. Choose **Intercepted connections** for the **Connection type**.
3. (Optional) To display a specific category of connections in the report, choose a filter on the **Filtered by** drop-down:

Filter	Information to Enter
Client IP	Enter the client's IP address or IP address and subnet mask.
Client port	Enter a client port number.
Server IP	Enter the IP address or host name of the server. Host name filters automatically search for suffix matches. For example, if you filter for example.com, test.example.com is included in the results.
Server port	Enter a server port number.
Individual service	Select a service from the drop-down list.
Individual proxy	Select a proxy name from the drop-down list.

4. Locate the **Service name** and **Details** columns.

The **Service name** is the proxy service associated with the connection and the **Details** provide a brief description of any errors. To sort by error type, click the **Details** column heading.

5. Scroll down and look at the variety of services that have intercepted connections.
 - You would expect to see all the services that are configured for interception.
 - If you don't see any connections for an intercepted service, it's possible that there isn't that type of traffic on the network at this point in time. Verify that the service is configured for interception and then check back later to see if there are any connections for that service type. See [Intercept a Service](#).

6. Here are a few things you can explore according to the type of error in the **Details** column:
 - **TCP errors** – The origin content server may not be available, the user may have entered the wrong URL, or a firewall may be blocking the connection.
 - **Read errors** – The origin content server may be misconfigured or a firewall may be blocking the protocol.
 - **Unexpected internal errors** – Contact Blue Coat Customer Support.
 - **DNS errors** – Verify the local DNS server is configured properly.
 - **BCAAA errors** – Make sure the BCAA service is running and verify its configuration. Confirm that there isn't a blocking firewall between the MACH5 appliance and the BCAA server.
7. If the list has been displayed on your screen for a period of time, you can manually refresh the list by clicking **Refresh**.

Why is my network slow?

Problem: Internet access is slow and users experience delays in loading Web pages.

Resolution: DNS slowness is a leading cause for a sluggish response to user Web requests. While the MACH5 appliance cannot help resolve the issue, it provides information on the health and connectivity of the DNS server and tracks average and maximum DNS response times. After you corroborate this information, contact your Internet Service Provider for resolving the DNS slowness issue.

1. **Go to the Advanced Management Console.**

In Blue Coat Sky, click **Advanced statistics** or **Advanced configuration**.

2. Select **Statistics > Health Checks**.

3. View the details of the DNS server health check. The MACH5 appliance displays the following information for the DNS server health check:

- **Name:** The name of the health check uses the prefix **dns** and the IP address of the DNS server
- **State:** The health check state is represented by an icon and a status message that reads **OK**, **Check Failed**, or **DNS Failed**

- Information on the last completed health check probe.
 - When: Time of the last check.
 - Time: Response time of the last check.
 - Since last transition: Displays aggregate values since the last transition between healthy and unhealthy.
 - Duration: Length of time since the last transition.
 - #Checks: Number of health checks performed since the last transition.
 - Response times: The average response time, the minimum response time and the maximum response time since the last transition.

In the following example, the DNS health check for dns 10.2.2.100 reports healthy and is functioning for 11.7 hours now. The max response time of 38,567 milliseconds indicates that the DNS response is slow.

Why is all traffic being bypassed?

Problem: All traffic is being bypassed. The acceleration reports don't show any data being optimized.

Resolution: The following situations can cause all traffic to be bypassed:

- On a physical appliance, if your trial or demo license expires before installing a permanent license, all traffic is bypassed. See [Install a License Manually](#) or [Install a License via BTO](#).
- On a virtual appliance with a subscription-based license, if your license expires before you have renewed the subscription, all traffic is bypassed. See [Install a License Manually](#) or [Install a License via BTO](#).
- If the appliance is in bypass mode, intercept settings are ignored, and all traffic is bypassed. To switch to acceleration mode, see [Select the Traffic Mode](#).
- If all services are set to bypass, all traffic is bypassed. Change the desired services to intercept traffic; see [Intercept a Service](#)

Why is ISATAP traffic being bypassed?

Problem: Some or all of the ISATAP traffic is being bypassed.

- The ISATAP connections are listed on the Bypassed Connections list on the Active Sessions report.
- In addition, in the output of the `show ip-stat ip` CLI command, the ISATAP packets delivered to ISATAP proxy counter shows 0 (zero) packets.

Resolution: If all ISATAP traffic is being bypassed, you have not yet enabled the two ISATAP options: `allow-intercept` and `adn-tunnel`. If only some of the ISATAP traffic is being bypassed, it is likely that you enabled `allow-intercept` but did not enable the `adn-tunnel` option. When `adn-tunnel` is disabled, the ISATAP proxy is not used: any traffic that would have been processed by this proxy is bypassed. For instructions on enabling ISATAP, see "Configure the ISATAP Proxy" on page 151.

ISATAP traffic destined for the ISATAP proxy would also be bypassed if the MACH5 appliance was unable to establish an ADN tunnel connection.

Why is all ISATAP traffic using the ISATAP Proxy?

Problem: The MACH5 appliance isn't sending any of the ISATAP traffic to the application proxies; the appliance is sending all of the ISATAP through the ISATAP proxy.

- The Active Sessions report indicates that the IPv6 connections are using the `ISATAP_tunnel` service, but no application proxies are being used for other IPv6 connections.
- The output of the `show ip-stat ip` CLI command shows 0 (zero) for the ISATAP encapsulated connections accepted counter.

Resolution: With full ISATAP functionality on the MACH5 appliance, packets that belong to a service that is being intercepted (such as RTMP or CIFS) are processed by the applicable application proxy (such as Flash or CIFS), and all other ISATAP traffic is processed by the ISATAP proxy. To have the full ISATAP functionality, you must enable both ISATAP options: `allow-intercept` and `adn-tunnel`. If you enable the `adn-tunnel` option but fail to enable the `allow-intercept` option, you will experience the situation described here.

For instructions on enabling ISATAP, see "Configure the ISATAP Proxy" on page 151.

Why are users seeing TCP connection errors in an ISATAP deployment?

Problem: We have enabled ISATAP on the MACH5 appliance and now users are seeing TCP connection errors (HTTP Error 503 - Service unavailable).

Resolution: Features that modify the destination address, such as URL rewrites and advanced forwarding, can cause issues with ISATAP processing because the IP encapsulation information must be preserved. If the destination address gets changed, users will likely see TCP connection errors because the server cannot be found.

Why is some traffic getting routed through the management port?

Problem: In an inline deployment, some of the traffic is getting routed through the MACH5 management port instead of the expected interface. Some packets from a remote site come to the firewall via the firewall interface that faces the management port, instead of the firewall port that faces the LAN. The firewall drops this traffic as “spoofed” because it is not coming through the correct interface. This happens to random packets, several times per minute.

Resolution: Be sure to configure IP addresses for physically-inline bridge interfaces, as well as for the management port if you are using it. If you configure an IP address for the management port only, some traffic may get inadvertently routed through this port. You can then specify the bridge interface as the preferred IP address on the concentrator. This is configured via the CLI as described in "Configure a Preferred IP List" on the facing page.

About Preferred IP Selection

By setting up a list of preferred IP addresses on the concentrator, administrators can avoid control connection and explicit tunnel connection issues between acceleration peers; avoiding these types of issues can, in turn, prevent byte caching issues. In the case of a managed ADN, administrators can designate preferred IP addresses on the concentrator, effectively excluding management IP addresses that shouldn't be advertised to other peers. In the case of an unmanaged ADN, the preferred IP list can prevent problems caused by the concentrator trying to establish a control connection with the first configured IP address on the arriving interface; the arriving interface may not have any IP addresses configured or the first IP address may be a management IP address.

By default, the list is empty; this means that all IP addresses configured on the MACH5 appliance are eligible to be used for inbound ADN control connections and explicit tunnel connections. Note that this list indicates a preference only; if the concentrator gets an inbound ADN connection on an IP address that is not in the preferred list, that connection is still accepted.



A Byte Cache Warning icon for a connection in the Active Sessions report indicates that a control connection with an acceleration peer is not established and the dictionaries are out of sync. If you see this icon, you can fix the issue by specifying preferred IP addresses on the concentrator.

Preferred IP lists are configured in the CLI. See "Configure a Preferred IP List" on the facing page.

How the Concentrator Uses the Preferred List

In a managed ADN:

- Only the preferred IP addresses are advertised to the ADN manager, which will forward the information to other ADN nodes in the network.
- Other ADN nodes will establish explicit or control connections only to these preferred IP addresses.

In an open, unmanaged transparent ADN deployment, the concentrator looks at the list of preferred IP addresses and determines which IP address to send to the branch peer by following the guidelines below:

- The concentrator's first choice is to use a preferred IP address of the same address family as the source address on the interface that the connection came on.
- If that's not possible, it uses a preferred IP address of the same address family as the source address, on an interface that is different from the interface that the connection came on.
- If the concentrator can't use an IP from the same address family, the concentrator uses a preferred IP address of a different address family on the interface that the connection came on.
- If the same interface isn't possible, it uses a preferred IP address of a different address family, on an interface that is different from the interface that the connection came on.
- If none of the above are applicable, the concentrator uses the first data IP address in the preferred IP list.



If there isn't a preferred list, the concentrator selects the first IP configured on the incoming tunnel connection interface.

Configure a Preferred IP List

By setting up a list of preferred IP addresses on the concentrator, administrators can avoid control connection and explicit tunnel connection issues between acceleration peers; avoiding these types of issues can, in turn, prevent byte caching issues.

The preferred IP list is configured in the command-line interface.

1. Telnet to the concentrator and go into enable mode.
2. Enter the following CLI commands:

```
#conf t
#(config)adn
#(config adn)tunnel
#(config adn tunnel)preferred-ip-addresses
```

3. From the available IP addresses on the concentrator, add the addresses you want to specify as preferred, using the following command:

```
 #(config adn tunnel preferred-ip-addresses)add <ip-address>
```

4. Repeat step 3 for each preferred address.
5. To view the list of preferred IP addresses, enter the following command:

```
 #(config adn tunnel preferred-ip-addresses)view
```

In a managed ADN, this preferred list is communicated to ADN peers so that they can form explicit tunnels and control connections. In an unmanaged ADN, the concentrator chooses one of the preferred IPs based on the guidelines described in "About Preferred IP Selection" on page 185.

Why is the device health reporting as Warning or Critical?

Problem: The **Device health** shows Warning or Critical. For example:

Resolution: The MACH5 appliance issues warning messages (flagged with) when a predefined warning threshold has been exceeded on the device. Error messages (flagged with) are issued when there is a connectivity problem or a critical threshold has been exceeded on the device. Errors are more severe than warnings. For example, when CPU consumption exceeds 80% of capacity, the warning threshold is exceeded and the MACH5 appliance issues a warning alert; when consumption reaches 95% of capacity, the critical threshold is exceeded and an error alert is issued.

Messages are hyperlinks that take you to an applicable configuration or report page when clicked. For example, the *License expiry approaching* error message opens the Licensing page. For more information about the messages and the action you can take to solve the problem, see "Alert Messages" on page 169.

Why is the CPU usage so high?

Problem: CPU utilization is higher than I would expect it to be.

Resolution: If the ADN adaptive compression feature is enabled, the MACH5 appliance will adjust its compression level based on its internal compression index, resulting in higher or lower CPU usage. When extra CPU is available, it will adapt compression to use these additional resources, resulting in higher CPU usage.

Therefore, when this feature is enabled, you should monitor adaptive compression in addition to CPU usage statistics when making capacity planning decisions.

To see if adaptive compression could be the cause of high CPU utilization, look at the Adaptive Compression graph. The presence of a green bar indicates that the MACH5 appliance has adjusted compression to operate at a higher level to take advantage of available CPU resources. For more information, see "Configure Adaptive Compression" below.



To display a list of other reasons for high CPU usage along with troubleshooting steps, see the [Knowledge Base article](#).

Configure Adaptive Compression

Adaptive compression enables the MACH5 appliance to adjust its compression level based on CPU usage. When adaptive compression is enabled, the MACH5 automatically increases its compression level when CPU usage is low and decreases its compression level when CPU usage is high.

All MACH5 platforms that are manufactured or remanufactured with SGOS 6.2 or higher have adaptive compression enabled by default. In the case of an upgrade to SGOS 6.2 or higher, the setting matches the configuration before the upgrade. For example, if adaptive compression was disabled in SGOS 6.1, it will be disabled after upgrading to SGOS 6.2.

1. **Go to the Advanced Management Console.**

In Blue Coat Sky, click **Advanced statistics** or **Advanced configuration**.

2. Select **Configuration > ADN > Byte Caching**.

3. Select (or deselect) the **Enable adaptive compression** option to enable (or disable) adaptive compression

4. Click **Apply**.

5. To monitor adaptive compression, select **Statistics > ADN History > Adaptive Compression**. A graph detailing adaptive compression over the last hour is displayed. The bars on the graph display in three colors, indicating if or how compression has been adapted:

- **Green**—Indicates that the MACH5 appliance has adapted compression to operate at a higher level to take advantage of available CPU resources.
- **Yellow**—Indicates that compression is operating at the ideal level.

- **Red**—Indicates that the MACH5 appliance has adapted compression to operate at a lower level due to a lack of CPU resources; any additional load may impact performance. If you notice that adaptive compression displays red consistently, your appliance may be undersized; consider a hardware upgrade.

Why is there a byte cache warning for a connection?

Problem: The Active Sessions report displays a warning icon that indicates when byte caching is enabled, but not functional, for a connection. The warning icon looks like this:

Resolution: This icon displays in the Byte Caching (BC) column in the Active Sessions list when a control connection with an acceleration peer is not established and the dictionaries are out of sync. This can happen, for example, in a transparent unmanaged ADN if the concentrator peer sends a control IP address that is not accessible from the branch peer. If you see this icon, you can fix the issue by specifying preferred IP addresses on the concentrator. This is configured via the CLI as described in "Configure a Preferred IP List" on page 186.

Why are old peers showing up in my byte-cache dictionary?

Problem: The byte-cache dictionary list old peers that aren't being used anymore. These peers are consuming valuable space in the byte-cache dictionary, so I want to remove them.

Resolution: The MACH5 appliance allocates space in its byte-cache dictionary for each ADN peer that forms a tunnel connection with it. If the maximum number of ADN peers is reached (the maximum number of peers that is supported depends on the size of the system), any new peer that forms a tunnel connection with the MACH5 appliance cannot be allocated dictionary space. Therefore, traffic to and from this peer cannot be accelerated using byte caching; instead only GZIP compression is used.

To prevent this, each day after it updates its traffic history, the MACH5 appliance automatically deletes peers that meet the following criteria:

- The dictionary for the peer is empty and is automatically sized
- The peer has been idle for at least eight days
- There is no active connection (data or control) with the peer.

As long as your system is sized properly, the automatic peer deletion process will prevent you from reaching the maximum number of peers. However, there may be times when you want to manually delete a peer that you know is no longer valid (and is therefore taking up dictionary space unnecessarily) and that will not get deleted automatically, either because its dictionary is manually sized or because it has not yet been idle for at least eight days.

Delete ADN Peers

1. **Go to the Advanced Management Console.**

In Blue Coat Sky, click **Advanced statistics** or **Advanced configuration**.

2. Select **Statistics > ADN History > Peer Dictionary Sizing**.
3. Select the peer you want to delete and click **Delete**.

Note: All ProxyClient peers are displayed in a single line and cannot be deleted. You must delete ProxyClient peers using the CLI.

4. When prompted to confirm the deletion, click **Yes**.

Why isn't the Flow Collector receiving NetFlow records?

Problem: Third-party flow collectors are not receiving flow detail records from a MACH5 appliance that is configured for NetFlow.

Resolution: If your collectors are not receiving NetFlow records, perform the following troubleshooting steps. At each step, correct the settings as needed. If you do not have to change any settings, or if you still have issues after making the changes, proceed to the next step.

1. Check NetFlow configuration. Use the **show netflow** CLI command to verify that NetFlow is enabled and that collectors have been added and are configured correctly (IP address and port).
2. Verify communication with collectors. Use the **ping** CLI command to verify that the collector is reachable across the network.
3. Check firewall settings. If the collector is behind a firewall that is blocking the NetFlow packets, configure the firewall to allow UDP traffic for the port that the collector is using.

4. Record a packet capture (PCAP). Verify that there is traffic in the interfaces as well as NetFlow packets being exported. You can filter the captured packets using the collector ports. See [Record a Packet Capture](#).

Troubleshoot Duplicate Serial Numbers

An appliance serial number is a unique identifier and can be used in only one instance of a ProxySG Virtual Appliance (ProxySG VA). You are receiving this error because two in your ADN network have identical serial numbers.

When an ADN manager receives a connection request from an ADN node with a duplicate serial number, the following measures are taken:

- The connection to the ProxySG VA that first established a connection with the ADN Manager is terminated. This connection is terminated to prevent a routing storm in the network. All traffic that is currently intercepted on this ProxySG VA is bypassed, since ADN is effectively disabled. No traffic will be accelerated on this ProxySG VA.
- A message recording the duplicate serial number error is written to the event log of the ProxySG VA that has been disconnected.
- The health state of the ProxySG VA transitions to Critical, and the following alerts appear: *License expired. All traffic is now bypassed* and *ADN Connection Status Disconnected*.

Resolving the Duplicate Serial Number Error Message

To resolve the duplicate serial number error, you must take the following steps:

1. Identify which ProxySG VA's in your network are using identical appliance serial numbers. The serial number is displayed on the Blue Coat Sky banner and on the Management Console banner.
2. Decide which ProxySG VA to retain.
3. (Optional) Back up the configuration of the duplicate ProxySG VA. You can later restore this configuration to another ProxySG VA (one that has a unique serial number).
4. Delete the duplicate ProxySG VA. To delete the duplicate ProxySG VA on the ESX host, select it, right click and choose **Delete from Disk**.



You cannot edit the serial number on a ProxySG VA. To replace this instance of the ProxySG VA, you must purchase a new appliance serial number and recreate a ProxySG VA. Contact your Blue Coat Sales Representative for purchasing a new appliance serial number.

5. To resume acceleration, reboot the ProxySG VA. You need to reboot the appliance only if the ProxySG VA that you selected was initially disconnected from the ADN network. Booting up the appliance re-establishes the connection between the ProxySG VA and the ADN Manager.

Troubleshoot Stolen Time

Traffic is currently being bypassed because too much stolen time has been accumulated on your ProxySG VA. *Stolen time* is the difference between "real time" (as measured on the host server's clock) and "apparent time" (as measured on the ProxySG); small amounts of stolen time is an inevitable occurrence on virtual machines. Stolen time can become excessive when the ProxySG VA is running at 100% CPU utilization, the ESX server is overloaded, and the recommended resources for the ProxySG VA are not reserved.

Because excessive stolen time can create issues with ProxySG VA reporting and operations, the following actions are taken when the accumulated stolen time on your ProxySG VA has exceeded a predefined threshold:

- The ProxySG VA license is temporarily disabled, and all traffic is bypassed.
- The health state of the ProxySG VA transitions to Critical, and the following alerts appear: *License expired. All traffic is now bypassed* and *Virtual appliance stolen time threshold exceeded*.

Recovering from Excessive Stolen Time Accumulation

Because incorrect virtual appliance resource reservations created this situation, your first task is to adjust your resource settings for the ProxySG VA. Once this is done, you should reboot the ProxySG VA to re-enable the license in order to start accelerating traffic again.

To recover from excessive stolen time accumulation:

1. Use the VI Client to access the ESX server.
2. Specify the following resource settings for the ProxySG VA:
 - **CPU reservation** should be the full CPU frequency of one core.
 - **Memory reservation** should be the value recommended for your model:
VA-5: 1024 MB; VA-10: 1536 MB; VA-15: 2048 MB; VA-20: 3072 MB

Refer to the *ProxySG VA Initial Configuration Guide* for additional information.

3. Restart the ProxySG VA.

After the ProxySG VA reboots, the expired license and stolen time alerts will no longer appear in the Alerts panel. Assuming acceleration mode is enabled, traffic will immediately begin accelerating.

