Chapter 1

INTRODUCTION

1.1 Wide Area Application Services

The purpose of this document is to outline how Wide Area Application Services (WAAS) technology developed by Cisco Systems optimizes the performance of any TCP-based application operating in a wide area network (WAN) environment while preserving and strengthening branch security.

It is Cisco's attempt to keep WAN optimization residing firmly in the router, eliminating the need to deploy acceleration appliances throughout the infrastructure. The technology preserves TCP information within the network while offering the performance benefits that come along with using WAN optimization technology.

There are many disadvantages of using WAN:

- LANs are typically faster and more secure than WANs.
- WANs have a lower data transfer rate compared to LANs.
- Low bandwidth is available for transmission.
- Experiences more data transmission errors as compared to LAN.
- Maintaining WAN is difficult because of its wider geographical coverage and higher maintenance costs.

To overcome these disadvantages of WAN and to enhance its use further, Cisco has found solution through Cisco Wide Area Application Service (WAAS). The WAAS system consists of a set of devices called wide area application engines (WAEs) that work together to optimize TCP traffic over your network.

When client and server applications attempt to communicate with each other, the network intercepts and redirects this traffic to the WAEs so that they can act on behalf of the client application and the destination server. The WAEs examine the traffic and use built-in application

policies to determine whether to optimize the traffic or allow it to pass through your network unoptimized.

Currently available product of Cisco WAAS is based on Common Internet File System (CIFS).CIFS is a dialect of Server Message Block (SMB).It is same as SMBv1 protocol. The Common Internet File System (CIFS) Protocol is a cross-platform, transport-independent protocol that provides a mechanism for client systems to use file and print services made available by server systems over a network.

CIFS is a dialect of the Server Message Block (SMB) protocol, which was originally developed by IBM Corporation and then further enhanced by Microsoft, IBM, Intel, 3Com, and others. There are several dialects of SMB. A standard for the SMB protocol, covering dialects prior to CIFS, was published by X/Open (now The Open Group) as [XOPEN-SMB].

The meaning of the term "CIFS" has changed since it was first introduced. It was originally used to indicate a proposed standard version of SMB based upon the design of the Windows NT 4.0 operating system and Windows 2000 operating system implementations. In some references, "CIFS" has been used as a name for the SMB protocol in general (all dialects) and, additionally, the suite of protocols that support and include SMB. In this document, the term "CIFS" is used specifically to identify the Windows NT LAN Manager (NTLM) dialect of SMB as designed for use with Windows: in particular, Windows NT Server 3.51 operating system and Windows NT Server 4.0 operating system, Windows NT Workstation 4.0 operating system, and Microsoft Windows 98 operating system.

As CIFS is an old protocol, Cisco is working on a new product based on SMBv2 and SMBv3.This protocol is important as its interoperable and found in most recent Microsoft Windows 7 and 8 OS.This is a new secure dialect negotiation used in Windows 2012 server.

The Server Message Block (SMB) Protocol Versions 2 and 3, hereafter referred to as "SMB 2 Protocol", is an extension of the original Server Message Block (SMB) Protocol. Both protocols are used by clients to request file and print services from a server system over the network. Both are stateful protocols in which clients establish a connection to a server, establish an authenticated context on that connection, and then issue a variety of requests to access files, printers, and named pipes for interprocess communication.

The SMB 2 Protocol is a major revision of the existing SMB Protocol. The packet formats are completely different from those of the SMB Protocol. However, many of the underlying concepts are carried over. The underlying transports that are used to initiate and accept connections are either Direct TCP or NetBIOS over TCP transports.

To retain compatibility with existing clients and servers, the existing SMB Protocol can be used to negotiate the use of the SMB 2 Protocol. However, the two protocols will never be intermixed on a specified connection after one is selected during negotiation.

The SMB 2 Protocol assumes the availability of the following resources:

- Either TCP or NetBIOS over TCP to support reliable, in-order message delivery. The SMB 3.x dialect family optionally supports the additional use of RDMA to support reliable, in-order message delivery with direct placement.
- An underlying local resource, such as a file system on the server side, exposing file, named pipe, or printer objects.
- Infrastructure that supports Simple and Protected GSS-API Negotiation on both the client and the server.

The variable-length buffer that contains the security buffer for the response, as specified by Security Buffer Offset and Security Buffer Length. The buffer SHOULD contain a token as produced by the GSS protocol. If Security Buffer Length is 0, this field is empty and then client-initiated authentication, with an authentication protocol of the client's choice, will be used instead of server-initiated SPNEGO authentication.