



Windows Server 2003 Remote Access Overview

Microsoft Corporation

Published: March 2003

Abstract

Remote access allows users with remote computers to create a logical connection to an organization network or the Internet. This white paper provides an overview of the remote access server features in Windows Server 2003. Windows Server 2003 includes a remote access server that supports both dial-up and virtual private network (VPN) connections and includes a set of features that provides flexibility and security for your remote access solution.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2003 Microsoft Corporation. All rights reserved.

Microsoft, Windows, and Windows logo are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Introduction	1
Remote Access and Remote Control	2
Elements of a Dial-up Remote Access Connection	2
Remote Access Client	2
Remote Access Server.....	3
Dial-up Equipment and WAN Infrastructure	3
Remote Access Protocols	3
LAN Protocols.....	3
Table 1 LAN Protocols and Their Use.....	3
Elements of a VPN Remote Access Connection	3
Remote Access VPN Client.....	4
Remote Access VPN Server	4
VPN Protocols	4
Internet	6
Advanced Remote Access Features	7
RADIUS Client Support.....	7
Multicast Forwarding Support	7
DHCP Support	8
Multilink and BAP	8
Callback	8
Security Features of Microsoft Remote Access	10
Authentication and Authorization	10
Secure User Authentication	11
Extensible Authentication Protocol	11
EAP-MD5.....	12
EAP-TLS.....	12
EAP Over RADIUS.....	12
Mutual Authentication	13
Data Encryption.....	13

Network Access Quarantine Control.....	14
Caller-ID	14
Remote Access Account Lockout	14
Packet Filtering for VPN Remote Access	15
Remote Access Policy Profile Packet Filtering	16
Setting Up a Windows Server 2003 Remote Access Server	17
Configuring a Windows XP Remote Access Client.....	18
Manual Configuration of a Dial-up Remote Access Connection.....	18
Manual Configuration of a VPN Remote Access Connection.....	18
Connection Manager and Managed Remote Access Connections	20
Connection Manager Client Dialer	20
Connection Manager Administration Kit.....	21
Connection Point Services	21
Deploying Connection Manager for Managed Remote Access	22
Summary	23
Related Links	24

Introduction

Remote access is a set of technologies that transparently connects a computer, typically located in an off-site or remote location, to a network. Remote access is typically used by organizations to connect an employee's laptop or home computer to an organization's network to read email or access shared files and by Internet service providers (ISPs) to connect a customer to the Internet.

Users run remote access client software and initiate a connection to a remote access server. The remote access server authenticates users and services sessions until terminated by the user or a network administrator. All services typically available to a LAN-connected user (including file and print sharing, Web server access, and messaging) are enabled by means of the remote access connection.

Remote access clients use standard tools to access resources. For example, on a computer running Windows 2000 Professional or Windows XP, clients can use Windows Explorer to make drive connections and to connect to printers. Connections are persistent: Users do not need to reconnect to network resources during their remote sessions. Because drive letters and universal naming convention (UNC) names are fully supported by remote access, most commercial and custom applications work without modification.

Figure 1 shows the logical equivalent for a remote access client when connected to a remote access server.

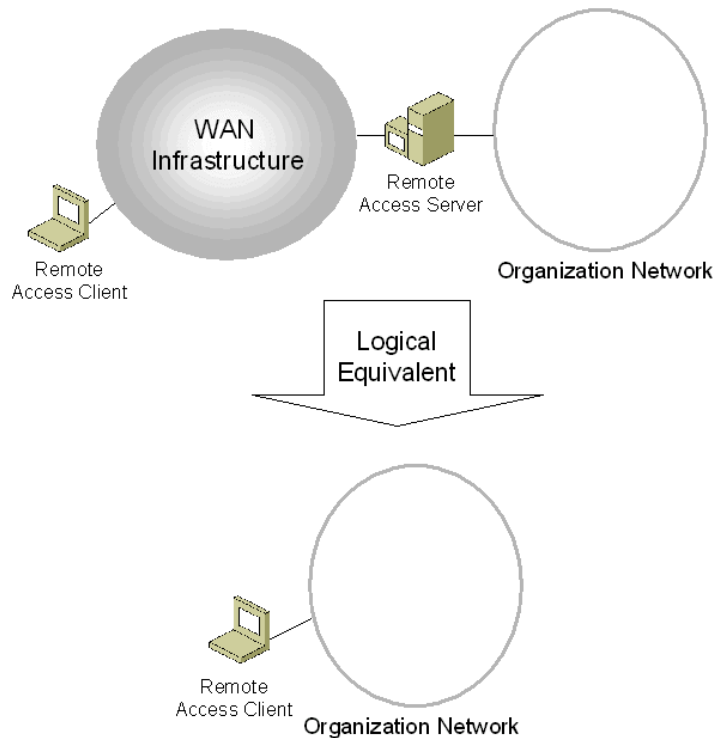


Figure 1 The logical equivalent of a remote access connection

Windows remote access provides two different types of remote access connectivity:

- **Dial-up remote access.** With dial-up remote access, a remote access client uses the telecommunications infrastructure (typically an analog phone line) to create a temporary physical circuit

or a virtual circuit to a port on a remote access server. Once the physical or virtual circuit is created, the rest of the connection parameters can be negotiated.

- **Virtual private network (VPN) remote access.** With virtual private network remote access, a VPN client uses an IP network to create a virtual point-to-point connection with a remote access server acting as the VPN server. Once the virtual point-to-point connection is created, the rest of the connection parameters can be negotiated.

Remote Access and Remote Control

Remote access is not the same as remote control. The remote access server is a software-based multi-protocol router; remote control solutions work by sharing screen, keyboard, and mouse over the remote link. The distinctions between remote access and remote control solutions are the following:

- In remote access, the applications are run on the remote access client computer. A computer running Windows Server 2003 and the Routing and Remote Access service is an example of a remote access server. A computer running Windows 2000 Professional or Windows XP is an example of a remote access client.
- In a remote control solution, users share a CPU or multiple CPUs on the server. In remote control, the applications are run on the server. The remote access server's CPU is dedicated to facilitating communications between remote access clients and network resources, not to running applications. A computer running Windows Server 2003 and the Terminal Services is an example of a remote control server. A computer running Windows 2000 Professional and the Terminal Services client is an example of a remote control client.

Elements of a Dial-up Remote Access Connection

A dial-up remote access connection consists of a remote access client, a remote access server, and a wide area network (WAN) infrastructure as illustrated in Figure 2.

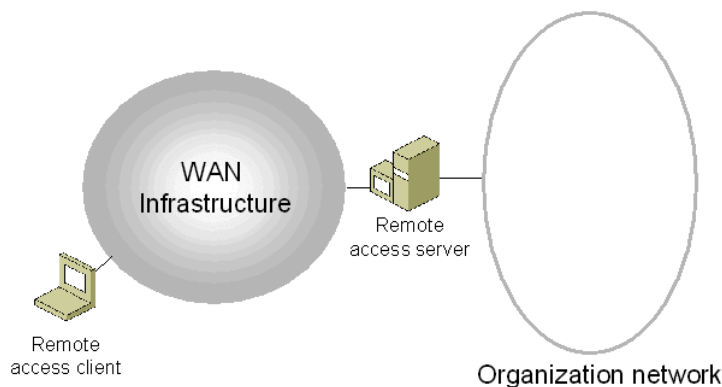


Figure 2 The elements of a dial-up remote access connection

Remote Access Client

Windows Server 2003, Windows XP, Windows 2000, Microsoft® Windows NT® 4.0, Microsoft® Windows® Millennium Edition, and Microsoft® Windows® 98 remote access clients can all connect to a Windows Server 2003 remote access server and most other dial-up remote access servers. Almost any third-party Point-to-Point Protocol (PPP) remote access clients including UNIX and Apple Macintosh can also connect to a Windows Server 2003 remote access server.

Remote Access Server

The Windows Server 2003 remote access server accepts dial-up connections and forwards packets between remote access clients and the network to which the remote access server is attached.

Dial-up Equipment and WAN Infrastructure

The physical or logical connection between the remote access server and the remote access client is facilitated by dial-up equipment installed at the remote access client, the remote access server, and the telecommunications infrastructure. The nature of the dial-up equipment and telecommunications infrastructure varies depending on the type of connection being made.

Remote Access Protocols

Remote access protocols control the connection establishment and transmission of data over wide area network (WAN) links. The operating system and LAN protocols used on remote access clients and servers dictate which remote access protocol your clients can use.

The primary remote access protocols supported by current Microsoft operating systems including Windows Server 2003, Windows XP, Windows 2000, Windows Millennium Edition, and Windows 98 is the Point-to-Point Protocol (PPP), an industry-standard set of protocols providing security, multi-protocol support, and interoperability.

LAN Protocols

LAN protocols are the protocols used by the remote access client to access resources on the network connected to the remote access server. Windows Server 2003 remote access supports TCP/IP and AppleTalk.

Table 1 lists the remote access protocols and their use.

Table 1 LAN Protocols and Their Use

Remote access protocols	Windows XP or Windows 2000 remote access client	Windows Server 2003 remote access server
TCP/IP	X	X
IPX	X	
AppleTalk		X

Note Most references to the typical remote access client in this paper are for computers running Windows XP or Windows 2000. Windows Server 2003 has the same capabilities and is configured in the same way as a Windows XP remote access client, but because a computer running Windows Server 2003 is not commonly used as a remote access client, it is not included as a typical remote access client.

Elements of a VPN Remote Access Connection

A VPN remote access connection consists of a VPN client, a VPN server, and the Internet as illustrated in Figure 3.

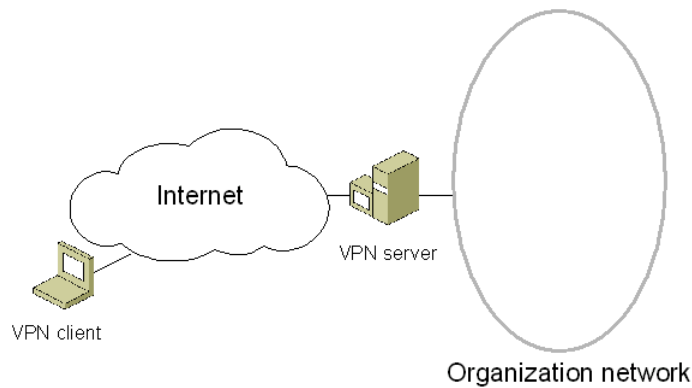


Figure 3 The elements of a VPN remote access connection

Remote Access VPN Client

VPN clients are either individual users who obtain a remote access VPN connection or routers that obtain a site-to-site (also known as router-to-router) VPN connection. Windows Server 2003, Windows XP, Windows 2000, Windows NT 4.0, Windows Millennium Edition, and Windows 98 VPN clients can create remote access VPN connections to a Windows Server 2003 VPN server and most other VPN servers. VPN clients can also be any non-Microsoft Point-to-Point Tunneling Protocol (PPTP) client or Layer Two Tunneling Protocol (L2TP) client that uses Internet Protocol security (IPSec). Computers running Windows Server 2003, Windows 2000 Server, or Windows NT Server 4.0¹ can also create site-to-site VPN connections.

Remote Access VPN Server

The Windows Server 2003 remote access server accepts PPTP and L2TP/IPSec-based VPN connections and forwards packets between remote access clients and the network to which the remote access server is attached.

VPN Protocols

The Windows Server 2003 remote access server and client support two VPN protocols for remote access VPN connections:

- Point-to-Point Tunneling Protocol
- Layer Two Tunneling Protocol with Internet Protocol security

Point-to-Point Tunneling Protocol

The Point-to-Point Tunneling Protocol (PPTP) is a tunneling protocol first supported in Windows NT 4.0. PPTP is an extension of the Point-to-Point Protocol (PPP) and leverages the authentication, compression, and encryption mechanisms of PPP. PPTP is automatically installed with the TCP/IP protocol. PPTP and Microsoft Point-to-Point Encryption (MPPE) provide the primary VPN services of encapsulation and encryption of private data.

¹ With the Routing and Remote Access Service (RRAS) for Windows NT 4.0 Server installed.

A PPP frame (an IP datagram) is wrapped with a Generic Routing Encapsulation (GRE) header and an IP header. In the IP header is the source and destination IP address that correspond to the VPN client and VPN server.

The PPP frame is encrypted with MPPE by using encryption keys generated from the MS-CHAP, MS-CHAP v2, or EAP-TLS authentication process. PPTP clients must use the MS-CHAP, MS-CHAP v2, or EAP-TLS authentication protocol in order for the payloads of PPP frames to be encrypted.

Figure 4 shows PPTP encapsulation and encryption for a PPP frame.

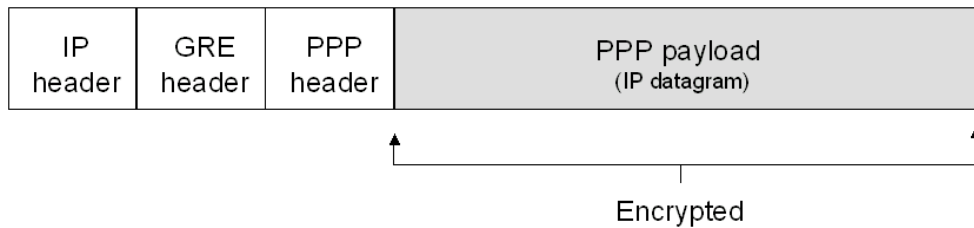


Figure 4 PPTP encapsulation and encryption for a PPP frame

Layer Two Tunneling Protocol with Internet Protocol security

The Layer Two Tunneling Protocol (L2TP) is an Internet Engineering Task Force (IETF) standard tunneling protocol. Unlike PPTP, L2TP in Windows Server 2003 does not utilize MPPE to encrypt PPP frames. L2TP relies on Internet Protocol security (IPSec) for encryption services. The combination of L2TP and IPSec is known as L2TP/IPSec. Both the VPN client and the VPN server must support L2TP and IPSec. For Windows Server 2003, L2TP is automatically installed with the Routing and Remote Access service. For Windows XP and Windows 2000, L2TP is automatically installed with the TCP/IP protocol.

L2TP/IPSec provides the primary VPN services of encapsulation and encryption of private data.

Encapsulation for L2TP over IPSec packets consists of two layers:

- **L2TP encapsulation.** A PPP frame (an IP datagram) is wrapped with a L2TP header and a UDP header.
- **IPSec encapsulation.** The resulting L2TP message is then wrapped with an IPSec Encapsulating Security Payload (ESP) header and trailer, an IPSec ESP Authentication trailer that provides message integrity and authentication, and a final IP header. In the IP header is the source and destination IP address that corresponds to the VPN client and VPN server. The L2TP message is encrypted with IPSec encryption mechanisms by using encryption keys generated from the IPSec authentication process.

Figure 5 shows L2TP/IPSec encapsulation and encryption for a PPP datagram.

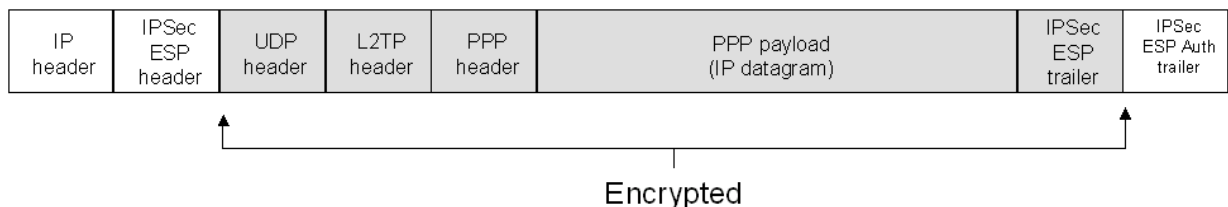


Figure 5 L2TP/IPSec encapsulation and encryption for a PPP frame

Internet

The medium between the VPN remote access client and the VPN remote access server is any TCP/IP-based network, although, typically it is the Internet. VPN remote access clients often use a dial-up remote access connection to an ISP access the Internet. Then, they use a VPN remote access connection to access their organization's network.

Advanced Remote Access Features

Current Microsoft operating systems support the following advanced features for remote access connections:

- RADIUS client support
- Multicast forwarding support
- DHCP support
- Multilink and BAP
- Callback

RADIUS Client Support

The Routing and Remote Access service for Windows Server 2003 can use Windows or Remote Authentication Dial-In User Service (RADIUS) as its authentication or accounting provider.

- When Windows is used as the authentication and accounting provider, the remote access server uses native Windows functions to validate the security credentials of the remote access client (typically, the remote access user's user name and password) and access the remote access client's user account dial-in properties. Locally configured remote access policies authorize the remote access connection and locally written accounting log files log connection accounting information.
- When RADIUS is used as the authentication and accounting provider, the remote access server acts as a RADIUS client and sends the users credentials and other connection settings to a RADIUS server. The RADIUS server validates the credentials of the remote access client, authorizes the connection attempt, and store remote access connection accounting information.

Windows Server 2003 includes a RADIUS server and proxy with the Internet Authentication Service (IAS), an optional networking component. When IAS is used as the RADIUS server, the IAS server uses native Windows functions to validate the security credentials of the remote access client and access the remote access client's user account dial-in properties. Remote access policies configured on the IAS server authorize the remote access connection and connection accounting information is written to accounting log files stored on the IAS server.

Multicast Forwarding Support

If your network supports IP multicasting, a Windows Server 2003 remote access server can act as a multicast gateway between remote access clients and your multicast-enabled network. Remote access client notifications to receive IP multicast traffic are passed from the remote access client to a multicast-enabled router on the network segment to which the remote access server is attached. When multicast traffic destined for a remote access client is forwarded to the network segment to which the remote access server is attached, the remote access server forwards the multicast packet to the appropriate remote access client. Remote access clients can even send IP multicast traffic to each other. Multicast forwarding support is enabled by default when you run the Routing and Remote Access Server Setup Wizard. For more information, see "Setting up a Windows Server 2003 Remote Access Server" in this article.

DHCP Support

Dynamic Host Configuration Protocol (DHCP) is a protocol that automates TCP/IP address assignment and configuration and is typically used in organization networks. Windows Server 2003 supports DHCP for remote access in the following ways:

- The Windows Server 2003 remote access server can be configured to use DHCP to obtain IP addresses that are assigned to remote access clients during the PPP connection process. Remote access clients use PPP negotiation to obtain IP addresses from the remote access server. Remote access clients do not use DHCP to obtain IP addresses from a DHCP server. By using DHCP, address allocation for remote access clients can use the existing TCP/IP management infrastructure and the use of DHCP-obtained addresses simplifies the routing of traffic destined to remote access clients.
- After completing a PPP connection, Windows Server 2003, Windows XP, and Windows 2000 remote access clients send the remote access server a special DHCP message known as a DHCPInform. A DHCPInform message is sent to request a specific set of configuration parameters. The Windows Server 2003 remote access server can be configured to forward the DHCPInform message to a DHCP server on the organization network and the response is forwarded back to the remote access client. The end result is that the remote access clients can obtain configuration settings that are not provided during the negotiation of the PPP connection, such as the name of the DNS domain to which the remote access client belongs.

Multilink and BAP

For dial-up links, Windows Server 2003 remote access supports Multilink and the Bandwidth Allocation Protocol (BAP). With Multilink, multiple physical links to appear as a single logical link over which data is sent and received. A good example is the aggregation of both B channels of an ISDN Basic Rate Interface (BRI) connection. Multilink is the recommended method of combining multiple B channels of a BRI connection because the support for bonding, the combining of ISDN B channels through hardware support, is specific to the ISDN adapter. You can use Multilink for any ISDN adapter. Multilink must be supported on both sides of the connection.

While Multilink allows for multiple physical links to be aggregated, it does not provide a mechanism to adapt to changing bandwidth conditions by adding extra links when needed or terminating extra links when unneeded. The Bandwidth Allocation Protocol (BAP) provides this additional capability. BAP uses a Multilink connection to dynamically manage links.

For example, a Multilink and BAP-enabled remote access client and remote access server create a Multilink connection that consists of a single physical link. As the utilization of the single link rises to a configured level, the remote access client uses a BAP request message to request an additional link. The BAP request message specifies the type of link desired, such as analog phone, ISDN, or X.25. The remote access server then sends a BAP response message that contains the phone number of an available port on the remote access server of the same type as specified by the remote access client in the BAP request.

Callback

With callback, the remote access server calls the remote access client after the user credentials have been verified. Callback can be configured on the server to call the remote access client back at a number specified by the user of the remote access client during the time of the call. This allows a traveling user to dial-in and have the remote access server call them back at their current location,

saving phone charges. Callback can also be configured to always call the remote access client back at a specific location, which is the secure form of callback.

Security Features of Microsoft Remote Access

Because remote access is designed to transparently connect a remote access client to a network and its potentially sensitive data, security of remote access connections is an important consideration. Microsoft remote access offers a wide range of security features including:

- Authentication and authorization
- Secure user authentication
- Extensible Authentication Protocol
- Data encryption
- Network Access Quarantine Control
- Caller ID
- Remote access account lockout
- Remote access policy profile packet filtering
- Packet filtering for VPN remote access

Authentication and Authorization

The distinction between authentication and authorization is important in understanding why connection attempts are either accepted or denied:

- Authentication is the verification of the credentials of the connection attempt. This process consists of sending the credentials from the remote access client to the remote access server by using an authentication protocol.
- Authorization is the verification that the connection attempt is allowed. Authorization occurs after successful authentication.

For a connection attempt to be accepted, it must be both authenticated and authorized. It is possible for the connection attempt to be authenticated by using valid credentials, but not authorized. In this case, the connection attempt is denied.

If a remote access server is configured for Windows authentication, Windows security is used to verify the credentials for authentication, and the dial-in properties of the user account and locally stored remote access policies are used to authorize the connection. If the connection attempt is both authenticated and authorized, the connection attempt is accepted.

Remote access policies are an ordered set of rules that define how connections are authorized. For connections that are authorized, remote access policies can also define connection restrictions. Connection attempts are evaluated against the remote access policies in order, trying to determine whether the connection attempt matches all of the conditions of each policy. If the connection attempt does not match all of the conditions of any policy, the connection attempt is rejected.

If a connection matches all the conditions of a remote access policy and is granted remote access permission, the remote access policy profile specifies a set of connection restrictions. The dial-in

properties of the user account also provide a set of restrictions. Where applicable, user account connection restrictions override the remote access policy profile connection restrictions.

One of the most useful conditions that you can configure on a remote access policy is membership in a specific Windows group. By using this condition, you can specify authorization and connection restraints based on the group membership of the user account of the remote access user. For example, you can:

- Prevent members of the Contactors group from making connections during non-business hours.
- Specify that connections made by members of the Employees group have a maximum session time of 10 minutes and a 5-minute idle time-out.
- Specify that connections made by members of the Executives group have no maximum session time and no idle time-out.

If the remote access server is configured for RADIUS authentication, the credentials of the connection attempt are passed to the RADIUS server for authentication and authorization. If the connection attempt is both authenticated and authorized, the RADIUS server sends an accept message back to the remote access server and the connection attempt is accepted. If the connection attempt is either not authenticated or not authorized, the RADIUS server sends a reject message back to the remote access server and the connection process is denied.

If the RADIUS server is a computer running Windows Server 2003 and the Internet Authentication Service (IAS), the IAS server performs authentication through Windows security and authorization through the dial-in properties of the user account and remote access policies stored on the IAS server.

Secure User Authentication

Secure user authentication is obtained through the encrypted exchange of user credentials. This is possible with the PPP remote access protocol using the following PPP authentication protocols:

- Extensible Authentication Protocol (EAP)
- Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
- MS-CHAP version 2 (MS-CHAP v2)
- Challenge Handshake Authentication Protocol (CHAP)
- Shiva Password Authentication Protocol (SPAP)

The remote access server can be configured to require specific secure authentication methods. If the remote access client cannot perform the required secure authentication methods, the connection is denied.

Extensible Authentication Protocol

The Extensible Authentication Protocol (EAP) is a new standard that allows for arbitrary authentication mechanisms to be employed for the validation of a PPP connection. With PPP authentication protocols such as MS-CHAP and SPAP, a specific authentication mechanism is chosen during the link establishment phase. Then, during the connection authentication phase, the negotiated authentication protocol is used to validate the connection. The authentication protocol itself is a fixed series of messages sent in a specific order.

With EAP, the specific authentication mechanism is not chosen during the link establishment phase. Instead, each PPP peer negotiates to perform EAP during the connection authentication phase. Once the connection authentication phase is reached, the PPP peers must first negotiate the use of a specific EAP authentication scheme known as an EAP type. Once the EAP type is agreed upon, EAP allows for an open-ended conversation between the remote access client and the remote access server that can vary based on the parameters of the connection. The conversation consists of requests for authentication information and the responses. The length and detail of the authentication conversation is dependent upon the EAP type.

For example, when EAP is used with security token cards, the remote access server could separately query the remote access client for a name, PIN, and card token value. As each query is asked and answered, the user passes through another level of authentication. When all questions have been answered satisfactorily, the user is authenticated and permitted access to the network.

Architecturally, EAP is designed to allow authentication plug-in modules at both the client and server ends of a connection. By installing an EAP type library file on both the remote access client and the remote access server, a new EAP type can be supported. This presents vendors with the opportunity to supply a new authentication scheme at any time. EAP provides the highest flexibility in authentication uniqueness and variations.

Windows 2000 and Windows XP include support for the EAP-MD5 and EAP-TLS EAP types for the remote access client. The Routing and Remote Access service for Windows Server 2003 includes support for the EAP-MD5 and EAP-TLS EAP types and the sending of EAP messages to a RADIUS server.

EAP-MD5

EAP-MD5 is the CHAP authentication mechanism used within the EAP framework. EAP-MD5 is a required EAP type and can be used to test EAP interoperability. Like CHAP, EAP-MD5 is difficult to use because it requires the authenticating server to store user passwords in a reversibly encrypted form.

EAP-TLS

The Transport Level Security (TLS) protocol, based on the Secure Sockets Layer (SSL), allows applications to communicate securely. With EAP-TLS, mutual authentication between the PPP client and the authenticating server is done through the exchange and verification of certificates. The client attempting the connection sends a user certificate, and the authenticating server sends a computer certificate.

EAP-TLS is the most secure form of user authentication and is supported by Windows XP and Windows 2000 remote access clients.

EAP Over RADIUS

EAP over RADIUS is not an EAP type, but the passing of EAP messages of any EAP type by the remote access server to a RADIUS server for authentication. The EAP messages sent between the remote access client and remote access server are encapsulated and formatted as RADIUS messages between the remote access server and the RADIUS server. The remote access server becomes a pass-through device passing EAP messages between the remote access client and the RADIUS server. All processing of EAP messages occurs at the remote access client and the RADIUS server.

EAP over RADIUS is used in environments where RADIUS is used as the authentication provider. An advantage of using EAP over RADIUS is that EAP types do not need to be installed at each remote access server, only at the RADIUS server.

In a typical use of EAP over RADIUS, the remote access server is configured to use EAP and to use RADIUS as its authentication provider. When a connection attempt is made, the remote access client negotiates the use of EAP with the remote access server. When the client sends an EAP message to the remote access server, the remote access server encapsulates the EAP message as a RADIUS message and sends it to its configured RADIUS server. The RADIUS server processes the EAP message and sends a RADIUS-encapsulated EAP message back to the remote access server. The remote access server then forwards the EAP message to the remote access client.

Mutual Authentication

Mutual authentication is obtained by authenticating both ends of the connection through the encrypted exchange of user credentials. This is possible using either the EAP-TLS or MS-CHAP v2 authentication protocols. During mutual authentication, the remote access client authenticates itself to the remote access server, and then the remote access server authenticates itself to the remote access client.

It is possible for a remote access server to not request authentication from the remote access client. However, in the case of a Windows XP or Windows 2000 remote access client configured for only MS-CHAP v2 or only EAP-TLS, the remote access client will enforce the authentication of the server. If the remote access server does not respond to the authentication request, the client terminates the connection.

Data Encryption

Data encryption encrypts the data sent between the remote access client and the remote access server. Remote access data encryption only provides data encryption on the communications link between the remote access client and the remote access server. If end-to-end encryption is needed, use IPsec to create an encrypted end-to-end connection after the remote access connection has been made.

Data encryption on a remote access connection is based on a secret encryption key known to the remote access server and remote access client. This secret key is generated during the connection authentication process. The remote access server can be configured to require data encryption. If the remote access client cannot perform the required encryption, the connection attempt is rejected.

There are two types of data encryption technologies for remote access connections:

- Microsoft Point-to-Point Encryption (MPPE)
MPPE uses the Rivest-Shamir-Adleman (RSA) RC4 stream cipher with 40-bit, 56-bit, or 128-bit encryption keys and is supported by Windows Server 2003, Windows XP, Windows 2000, Windows NT 4.0, Windows Millennium Edition, and Windows 98 dial-up and PPTP-based VPN clients and servers. MPPE keys are generated from the MS-CHAP, MS-CHAP v2, or EAP-TLS user authentication process.
- Data Encryption Standard (DES) and Triple DES (3DES)

DES with a 56-bit key and 3DES with three 56-bit keys are block ciphers that are supported by Windows XP and Windows 2000 (with Service Pack 2 and above) L2TP/IPSec-based VPN clients and Windows Server 2003 VPN servers. DES keys are generated from the IPSec authentication process.

Network Access Quarantine Control

Network Access Quarantine Control, a new feature in the Windows Server 2003 family, delays normal remote access to a private network until the configuration of the remote access computer has been examined and validated by an administrator-provided script. When a remote access computer initiates a connection to a remote access server, the user is authenticated and the remote access computer is assigned an IP address. However, the connection is placed in quarantine mode, with which network access is limited. The administrator-provided script is run on the remote access computer. When the script completes successfully, it runs a notifier component that notifies the remote access server that the remote access computer complies with current network policies. The remote access server removes quarantine mode and the remote access computer is granted normal remote access.

Network Access Quarantine Control is a combination of the following:

- A remote access server running Windows Server 2003 and a quarantine notification listener service
- A RADIUS server running Windows Server 2003 and Internet Authentication Service (IAS), configured with a quarantine remote access policy that specifies quarantine settings
- A Connection Manager profile created with the Windows Server 2003 Connection Manager Administration Kit that contains a network policy compliance script and a notifier component
- A remote access client that is running Windows Server 2003, Windows XP, Windows 2000, Windows Millennium Edition, or Windows 98 Second Edition.

For more information, see Windows Server 2003 Help and Support and the [Windows Server 2003 Network Access Quarantine Control](#) white paper at <http://www.microsoft.com/windowsserver2003/techinfo/overview/quarantine/>.

Caller-ID

Caller-ID can be used to verify that the incoming call is coming from a specified phone number. Caller-ID is configured as part of the dial-in properties of the user account. If the Caller-ID number of the incoming connection for that user does not match the configured Caller-ID, the connection attempt is rejected.

Caller-ID requires that the caller's phone line, the phone system, the remote access server's phone line, and the Windows driver for the dial-up equipment all support Caller-ID. If a Caller-ID is configured for a user account and the Caller-ID is not being passed from the caller to the Routing and Remote Access service, then the connection is denied.

Caller-ID is a feature designed to provide a higher degree of security for network that support telecommuters. The disadvantage of configuring Caller-ID is that the user can only dial-in from a single phone line.

Remote Access Account Lockout

The remote access account lockout feature is used to specify how many times a remote access authentication fails against a valid user account before the user is denied remote access. Remote

access account lockout is especially important for remote access virtual private network (VPN) connections over the Internet. Malicious users on the Internet can attempt to access an organization intranet by sending credentials (valid user name, guessed password) during the VPN connection authentication process. During a dictionary attack, the malicious user sends hundreds or thousands of credentials by using a list of passwords based on common words or phrases. With remote access account lockout enabled, a dictionary attack is thwarted after a specified number of failed attempts.

The remote access account lockout feature does not distinguish between malicious users who attempt to access your intranet and authentic users who attempt remote access but have forgotten their current passwords. Users who have forgotten their current password typically try the passwords that they remember and might have their accounts locked out.

If you enable the remote access account lockout feature, a malicious user can deliberately force an account to be locked out by attempting multiple authentications with the user account until the account is locked out, thereby preventing the authentic user from being able to log on.

As the network administrator, you must decide on two remote access account lockout variables:

1. The number of failed attempts before future attempts are denied.

After each failed attempt, a failed attempts counter for the user account is incremented. If the user account's failed attempts counter reaches the configured maximum, future attempts to connect are denied.

A successful authentication resets the failed attempts counter when its value is less than the configured maximum. In other words, the failed attempts counter does not accumulate beyond a successful authentication.

2. How often the failed attempts counter is reset.

You must periodically reset the failed attempts counter to prevent inadvertent lockouts due to normal mistakes by users when typing in their passwords.

You configure the remote access account lockout feature by changing settings in the registry on the computer that provides the authentication. If the remote access server is configured for Windows authentication, modify the registry on the remote access server computer. If the remote access server is configured for RADIUS authentication and Internet Authentication Service (IAS) is being used, modify the registry on the IAS server computer. For more information, see the topic titled "Remote access account lockout" in Windows Server 2003 Help.

Note: The remote access account lockout feature is not related to the **Account locked out** setting on the **Account** tab on the properties of a user account and the administration of account lockout policies using group policies.

Packet Filtering for VPN Remote Access

For VPN-based remote access, the VPN remote access server is either directly connected to the Internet or connected to network segment between your network and the Internet known as the perimeter network (also known as a demilitarized zone [DMZ] or a screened subnet). In either configuration, the VPN remote access server is vulnerable to attacks from malicious Internet users. To prevent the VPN remote access server from receiving or sending any traffic that is not PPTP or

L2TP/IPSec-based, IP packet filters for PPTP and L2TP/IPSec traffic are configured on the interface of the VPN remote access server that is connected to either the Internet or the perimeter network.

When you run the Routing and Remote Access Server Setup Wizard and choose the "Remote access (dial-up or VPN)" option and select the VPN remote access type, these filters by default are automatically configured. For more information, see "Setting up a Windows Server 2003 Remote Access Server" in this article.

Remote Access Policy Profile Packet Filtering

Remote access policies that define authorization and connection constraints can be used to specify a set of IP packet filters that are applied to remote access connections. When the connection is accepted, the packet filters define the types of IP traffic that are allowed from the remote access client and to the remote access client.

This feature can be used for extranet connections. An extranet is a portion of your organization network that is accessible to users outside the organization, such as business partners and vendors. By using remote access policy profile packet filtering, you can create a remote access policy that specifies that members of the Partners group can only access the Web servers at specific IP addresses or on a specific subnet.

Setting Up a Windows Server 2003 Remote Access Server

Setting up a Windows Server 2003-based remote access server is easy. Use the Routing and Remote Access Server Setup Wizard to set up the **Remote access (dial-up or VPN)** configuration using the following procedure:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. Right-click your server name, and then click **Configure and Enable Routing and Remote Access**. Click **Next**.
3. In **Configuration**, click **Remote access (dial-up or VPN)** and then click **Next**.
4. In **Remote Access**, select **VPN, Dial-up**, or both as needed. Click **Next**.
5. In **VPN Connection**, click the connection that corresponds to the interface connected to the Internet or your perimeter network, and then click **Next**.
6. In **IP Address Assignment**, click **Automatically** if the remote access server should use DHCP to obtain IP addresses for remote access clients. Alternately, click **From a specified range of addresses** to use one or more static ranges of addresses. When IP address assignment is complete, click **Next**.
7. In **Managing Multiple Remote Access Servers**, if you are using RADIUS for authentication and authorization, click **Yes, set up this server to work with a RADIUS server**, and then click **Next**.
 - In **RADIUS Server Selection**, configure the primary (mandatory) and alternate (optional) RADIUS servers and the shared secret, and then click **Next**.
8. Click **Finish**.

Configuring a Windows XP Remote Access Client

You can configure a Windows XP dial-up or VPN remote access client either manually or by using Connection Manager.

Manual Configuration of a Dial-up Remote Access Connection

If you have a small number of dial-up remote access clients, you can manually configure dial-up connections for each client. For Windows XP dial-up clients, use the following instructions to create the dial-up connection:

1. From the Windows XP desktop, click **Start**, click **Control Panel**, click **Network and Internet Connections**, and then click **Network Connections**.
2. Under **Network Tasks**, click **Create a new connection**, and then click **Next**.
3. Click **Connect to the network at my workplace**, and then click **Next**.
4. Click **Dial-up connection**, and then click **Next**.
5. Type the name of the dial-up connection, and then click **Next**.
6. Type the phone number for the modem to dial, and then click **Next**.
7. Click **Anyone's use** if you want this dial-up connection to be available to all users who log on to this computer. Otherwise, click **My use only**. Click **Next**. You will only see this choice if the computer running Windows XP is a member of a domain.
8. If you want to have a shortcut on the desktop for this dial-up connection, click **Add a shortcut to my desktop**. Click **Finish**.
9. In the **Connect** dialog box, type the user name and password that will be sent as your security credentials when you connect. If you want to save the password so that it does not have to be typed for each connection attempt, click **Save this user name and password for the following users**.
10. To make a dial-up connection, click **Connect**.

To create a dial-up connection on a computer running Windows 2000, double-click the **Make New Connection** icon in the Network and Dial-up Connections folder and select the **Dial to private network** connection type.

Manual Configuration of a VPN Remote Access Connection

If you have a small number of VPN remote access clients, you can manually configure VPN connections for each client. For Windows XP VPN clients, use the following instructions to create the VPN connection:

1. From the Windows XP desktop, click **Start**, click **Control Panel**, click **Network and Internet Connections**, and then click **Network Connections**.
2. Under **Network Tasks**, click **Create a new connection**, and then click **Next**.
3. Click **Connect to the network at my workplace**, and then click **Next**.
4. Click **Virtual Private Network connection**, and then click **Next**.

5. Type the name of the VPN connection, and then click **Next**.
6. Click **Automatically dial this initial connection** and select the correct dial-up connection that connects this computer to the Internet. If your computer is already connected to the Internet through a DSL, cable modem, or other type of LAN connection, click **Do not dial the initial connection**. Click **Next**.
7. Type either the IP address or the DNS name of the VPN server (for example: vpn.example.microsoft.com), and then click **Next**.
8. Click **Anyone's use** if you want this dial-up connection to be available to all users who log on to this computer. Otherwise, click **My use only**. Click **Next**. You will only see this choice if the Windows XP computer is a member of a domain.
9. If you want to have a shortcut on the desktop for this dial-up connection, click **Add a shortcut to my desktop**. Click **Finish**.
10. In the **Connect** dialog box, type the user name and password that will be sent as your security credentials when you connect. If you want to save the password so that it does not have to be typed for each connection attempt, click **Save this user name and password for the following users**.
11. To make a VPN connection, click **Connect**.

To create a VPN connection on a computer running Windows 2000, double-click the **Make New Connection** icon in the Network and Dial-up Connections folder and select the **Connect to a private network through the Internet** connection type.

Connection Manager and Managed Remote Access Connections

To deploy the configuration of remote access clients, each client must be configured to make a connection with the deployed servers. For a small business with a small number of clients, each can be configured manually. When configuring the dial-up or connections for an enterprise that consists of hundreds or thousands of clients, the following issues arise:

- The exact procedure used to configure a dial-up or VPN connection varies, depending on the version of Windows running on the client computer.
- To prevent configuration errors, it is preferable to have the information technology (IT) staff—not end users—configure the dial-up or VPN connection.
- To best utilize IT staff resources, a configuration method must be able to scale to hundreds or thousands of client computers.
- A VPN connection might need a double-dial configuration, in which the user must access the Internet through a dial-up connection before creating a VPN connection with the organization intranet.

Even more issues arise when an organization outsources dial-up or VPN access to a third party dial-up or Internet service provider (ISP). In this case, there might not be a single phone number used to reach the Internet or organization intranet (such as a toll-free number). In a multi-site organization or an outsourced dial configuration, there might be multiple local phone numbers that employees of an organization can use, depending upon physical location. A number of companies are taking advantage of the Internet by contracting with ISPs to utilize their worldwide access points so that users can make a local dial-up connection to the Internet, and then create a VPN connection to their organization intranet.

Connection Manager (CM) is the solution for issues associated with configuring dial-up or VPN connections for an enterprise and for outsourced dial configurations. CM is a set of components included with Windows Server 2003 that consist of the following:

- Connection Manager (CM) client dialer
- Connection Manager Administration Kit (CMAK)
- Connection Point Services (CPS)

Connection Manager Client Dialer

The Connection Manager (CM) client dialer is software that is installed on each remote access client. It includes advanced features that make it a superset of basic dial-up networking. At the same time, CM presents a simplified dialing experience to the user. It limits the number of configuration options that a user can change, ensuring that the user can always connect successfully. For example, with the CM client dialer, a user can:

- Select from a list of phone numbers to use, based on physical location.
- Use customized graphics, icons, messages, and help.
- Automatically create a dial-up connection before the VPN connection is made.
- Run custom actions during various parts of the connection process, such as pre-connect and post-connect actions (executed before or after the dial-up or VPN connection is completed).

A customized CM client dialer package, also known as a profile, is a self-extracting executable file that is created by a network administrator with the Connection Manager Administration Kit (CMAK). The CM profile is distributed to VPN users via CD-ROM, e-mail, Web site, or file share. When the user runs the

CM profile, it automatically configures the appropriate dial-up and VPN connections. The Connection Manager profile does not require a specific version of Windows—it will configure connections for computers running Windows Server 2003, Windows XP, Windows 2000, Windows NT 4.0, Windows Millennium Edition, and Windows 98.

Connection Manager Administration Kit

The Connection Manager Administration Kit (CMAK) is an optional management tool installed from:

- **Add/Remove Programs (in Control Panel) on a computer running Windows Server 2003.** You must specify Connection Manager Components in the Management and Monitoring Tools category of Windows components.
- **Windows Server 2003 Administration Tools on a computer running Windows XP Professional.** You must run the Adminpak.msi file from the \i386 folder on a Windows Server 2003 CD-ROM. After it is installed, you can run Connection Manager Administration Kit from Administrative Tools.

CMAK is a Wizard that guides you through a variety of options when configuring a CM profile and creates the profile to distribute to your dial-up and VPN users.

Connection Point Services

Connection Point Services (CPS) allows you to create, distribute, and update custom phone books. Phone books contain one or more Point of Presence (POP) entries. Each POP has a telephone number used to access a dial-up network or the Internet. Phone books give users complete POP information, so when they travel, they can connect to different corporate or Internet access points based on location, rather than having to use a toll-free or long distance number.

Without the ability to update phone books, users would not only have to contact their organization's technical support staff to obtain changes in POP information; they would also have to reconfigure their client dialer software.

CPS is a combination of:

- **Phone Book Administrator.** A tool used to both create and maintain phone book files, and publish new or updated phone book files on the phone book server.
- **A phone book server.** A computer running Windows Server 2003 and Internet Information Services (IIS) (including the FTP Publishing Service) and an Internet Server Application Programming Interface (ISAPI) extension that processes phone book update requests from CM clients.

The Phone Book Administrator is a tool that is installed by running Pbainst.exe from the Valueadd\Msft\Mgmt\Pba folder on the Windows Server 2003 CD-ROMs. Once installed, you can run Phone Book Administrator from Administrative Tools. It is not required to run the Phone Book Administrator on the phone book server.

You can use the Phone Book Administrator to create phone book entries and regions and publish them in the *SystemRoot\Program Files\Phone Book Service\Data\PhoneBookFileName* folder of the phone book server.

After the phone book is configured and published, the CM profile is created with CMAK and configured with:

- The **Automatically download phone book updates** standard post-connect action (on the **Post-**

Connect Actions page in the CMAK Wizard).

- The name of the phone book file (on the **Phone Book** page in the CMAK Wizard).
- The names of the phone book file and the phone book server (on the **Phone-Book Updates** page in the CMAK Wizard).

Deploying Connection Manager for Managed Remote Access

The following are the basic steps for deploying Connection Manager for Windows Server 2003:

1. Designate a computer running Windows Server 2003 and IIS with the FTP Publishing Service as the phone book server. This computer can be an existing IIS server or a low-end computer that will be a dedicated phone book server.
2. Install Connection Manager Components on the phone book server.
3. Install the Phone Book Administrator on a computer running Windows Server 2003 or Windows XP Professional.
4. Use the Phone Book Administrator to configure a phone book.
5. Use the Phone Book Administrator to publish the phone book files on the phone book server.
6. Install the Connection Manager Administration Kit on the computer running Windows Server 2003 or Windows XP Professional that will be used to create CM profiles. Use CMAK to create a CM profile with the appropriate phone book file and instructions to obtain updated phone books.
7. Distribute the CM profile to dial-up or VPN users.

ISPs can also use Connection Manager to create custom dialers for their customers—complete with a phone book of local ISP POPs.

For more information about Connection Manager, see the topic titled "Before you start: Understanding Connection Manager and the Administration Kit" in Windows Server 2003 Help.

Summary

Remote access is the logical connection of a remote access client computer to a network. Sometimes the network is an organization network and sometimes the Internet. Remote access connections can use a dial-up WAN media or the Internet. Microsoft operating systems include feature-rich remote access clients and remote access servers. The remote access client is configured through the Network Connections folder. The remote access server is configured through the Routing and Remote Access service. To facilitate wide scale deployment of remote access clients, Windows Server 2003 also includes the Connection Manager components to easily create and distribute a custom dialer to computers running many versions of Windows.

Related Links

See the following resources for further information:

- [Virtual Private Networks](http://www.microsoft.com/vpn) at <http://www.microsoft.com/vpn>

For the latest information about Windows Server 2003, see the [Windows Server 2003 Web site](http://www.microsoft.com/windowsserver2003/) at <http://www.microsoft.com/windowsserver2003/>.