Windows 2000 Server

Chapter 8 - Internet Authentication Service

The Internet Authentication Service (IAS) in Microsoft® Windows® 2000 is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server. IAS performs centralized authentication, authorization, auditing, and accounting (AAAA) of connections for dial-up and virtual private network (VPN) remote access and demand-dial connections, and it can be used in conjunction with the Windows 2000 Routing and Remote Access service. IAS enables the use of a single or multiple vendor network of remote access or VPN equipment.

In This Chapter

Related Information in the Resource Kit

- For more information about remote access, see "Remote Access Server" in this book.
- For more information about virtual private networks, see "Virtual Private Networking" in this book.

IAS Overview

Internet service providers (ISPs) and corporations maintaining remote access service for their employees are faced with the increasing challenge of managing all remote access from a single point of administration - regardless of the type of remote access equipment employed. The RADIUS standard supports this functionality in a homogeneous, as well as heterogeneous environment. RADIUS is a client-server protocol, which enables remote access equipment acting as RADIUS clients to submit authentication and accounting requests to a RADIUS server.

The RADIUS server has access to user account information and can check remote access authentication credentials. If the user's credentials are authentic and the connection attempt is authorized, the RADIUS server authorizes the user's access based on specified conditions and logs the remote access connections as accounting events.

The use of RADIUS allows the remote access user authentication and authorization and accounting data to be maintained in a central location, rather than on each network access server (NAS). Users connect to RADIUS-compliant NASs, such as a Windows 2000-based computer that is running the Routing and Remote Access service, which in turn, forward authentication requests to the centralized IAS server.

For more information about the RADIUS protocol, see RFCs 2138 and 2139.

IAS also allows companies to outsource remote access infrastructure to ISPs while retaining control over user authentication and authorization, as well as accounting.

Different types of IAS configurations can be created for using Internet technology, such as:

- Dial-up access to your network.
- Extranet access for business partners.
- Internet access.
- Outsourced corporate access through service providers.

Note A company might need to make certain resources on its network available to other companies with which it has partnership agreements. IAS can be used to limit partner access to the corporate network resources, based on restrictions defined for each partner.

IAS Features

The IAS features include the following:

Centralized User Authentication

The authentication of users attempting connections is an important security concern. IAS supports a variety of authentication protocols and allows you to use arbitrary authentication methods to meet your authentication requirements.

The following section describes the authentication methods supported in Windows 2000.

- Point-to-Point Protocol (PPP) is a set of industry-standard framing and authentication protocols that enables remote access solutions to be interoperable in a multivendor network. IAS supports the authentication protocols within PPP, such as Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) versions 1 and 2, and Extensible Authentication Protocol (EAP).
- Extensible Authentication Protocol (EAP) is an infrastructure that allows the addition of arbitrary authentication methods such as Smart Cards, certificates, one-time passwords, and Token Cards.
- Dialed Number Identification Service (DNIS) is an authorization method based on the number called by the user.
- Automatic Number Identification/Calling Line Identification (ANI/CLI) is an authorization method based on the number the user called from. ANI is also known as Caller ID.
- Guest authentication is an authorization method where the caller does not send a user name or password during the authentication process. If unauthenticated access is enabled, the Guest account is used as the identity of the caller by default.

Outsourced Dialing and Worldwide Remote Access

Outsourced dialing (also referred to as wholesale dialing) involves a contract between an organization or private company (the customer) and an ISP in which the ISP allows the company's employees to connect to the ISP's network before establishing the VPN tunnel to the company's private network. When an employee connects to the ISP's remote access server, the authentication and usage records are forwarded to the IAS server at the company. The IAS server allows the company to control user authentication, track usage, and manage which employees are allowed to gain access the ISP's network.

The advantage of outsourcing is the potential savings. For example, by using an ISP's routers, network access servers, and T1 lines (instead of buying your own), you can save a great deal on hardware (infrastructure) costs. You can also significantly decrease your long-distance phone bill costs by dialing into the ISP's with worldwide connections or roaming consortium's scattered Point of Presence (POPs) belonging to other ISPs. Thus, by handing off support to the provider, you can eliminate a large amount of your administrative budget.

Centralized User Authorization

To grant the connecting user-appropriate access to the network, IAS authenticates users in Microsoft® Windows NT® version 4.0 domains and Windows 2000 Local Security Accounts Manager (SAM). IAS also supports new features in Active Directory™ directory service, such as user principal names and Universal Groups.

Remote access policies are a set of conditions that network administrators can use to get more flexibility in granting remote access. They provide flexibility in controlling who is allowed to connect to your network. Although it is simple to manage remote access permission for each user account, this approach can become unwieldy as your organization grows. Remote access policies provide a more powerful and flexible way to manage remote access permission.

You can use remote access policies to control remote access based on a variety of conditions, such as:

- User membership in a Windows 2000 security group.
- The time of day, or day of the week of the connection.
- The type of media through which the user is connecting (for example, ISDN, modem, or a VPN tunnel).
- The type of VPN tunneling protocol used (Point-to-Point Tunneling Protocol or Layer Two Tunneling Protocol).
- The phone number the user calls.
- The phone number the user calls from.

Each remote access policy contains a profile of a setting from which you can control connection parameters. For example, you can:

- Permit or deny the use of certain authentication methods.
- Control the amount of time the connection can be idle.
- Control the maximum time of a single session.
- Control the number of links in a multilink session.
- Control encryption settings.
- Add packet filters to control what the user can access when connected to the network. For example, you can use filters to control which IP addresses, hosts, and ports the user is allowed to send or receive packets.
- Create a mandatory tunnel that forces all packets from that connection to be securely tunneled through the Internet and terminated in a private network.
- Allow users to request a specific IP address, or specify that the remote access server must assign an IP address.

Centralized Administration of Remote Access Servers

Support for the RADIUS standard allows IAS to control connection parameters for any network access server that implements that standard. The RADIUS standard also allows individual remote access vendors to create proprietary extensions called vendor-specific attributes. IAS has incorporated the extensions from a number of vendors in its multivendor dictionary.

Centralized Auditing and Usage Accounting

Support for the RADIUS standard allows IAS to collect the usage (accounting) records sent by a NAS at a single point. IAS logs audit information (for example, authentication Accepts and Rejects) and usage information (for example, logon and logoff records) to log files. IAS supports a log-file format that can be directly imported into a database. The data in the database can be analyzed by using third-party data-analysis software.

Integration with Routing and Remote Access Service

The Windows 2000 Routing and Remote Access service is configured to use Windows authentication and accounting, or to use RADIUS authentication and accounting. When RADIUS authentication or accounting is selected, any RFC-compliant RADIUS server can be used. However, using an IAS server is recommended to achieve the optimum level of integration in Windows 2000 environments and take advantage of centralized remote access policies.

For example, in a small network environment or branch offices with a small number of remote access servers and no requirements for centralized management of remote access, the Routing and Remote Access service can be configured to use Windows authentication and accounting.

In a global enterprise with large numbers or remote access servers deployed worldwide, centralized authentication and accounting using IAS can be beneficial. However, if a small branch office is experiencing a low bandwidth connection to the global enterprise with the centralized IAS server, the Windows authentication and accounting configuration can be copied from a central location to the remote access servers of the branch office.

IAS and the Routing and Remote Access service share the same remote access policies and authentication and accounting logging capabilities. When the Routing and Remote Access service is configured for Windows authentication, local policies, and logging are used. When the Routing and Remote Access service is configured as a RADIUS client to an IAS server, the policies and logging of the IAS server are used.

This integration provides consistent implementation across IAS and the Routing and Remote Access service. It allows you to deploy the Routing and Remote Access service in small sites without the need for a separate, centralized IAS server; it also provides the capability to scale up to a centralized remote access management model when you have multiple remote access servers in your organization. In this case, IAS in conjunction with remote access servers implements a single point of administration for remote access to your network for outsourced-dial, demand-dial, and VPN access. The policies within IAS at a central large site can be exported to the independent remote access server in a small site.

Graphical User Interface

IAS provides a graphical user interface (snap-in) that enables you to configure local or remote IAS servers.

Remote Monitoring

You can monitor IAS by using Windows 2000-based tools, such as Event Viewer or System Monitor, or by using Simple Network Management Protocol (SNMP).

Scalability

You can use IAS in a variety of network configurations of varying size, from stand-alone servers for small networks to large corporate and ISP networks.

IAS Software Development Kit

The IAS Software Development Kit (SDK) can be used to:

- Control the number of end-user network sessions.
- Extend the remote access authorizations currently provided by IAS.
- Export usage/audit data to a database.
- Create custom authentication methods for IAS (non-EAP).

EAP Software Development Kit

Provides the capability to implement arbitrary authentication methods using EAP.

Import/Export of Configuration to Manage Multiple IAS Servers

IAS configuration can be imported/exported by running **netsh** from the command prompt.

RADIUS Protocol

Remote Authentication Dial-In User Service (RADIUS) is an industry standard for providing authorization, identification, authentication, and accounting services for distributed dial-up/remote access networking. A RADIUS client, typically a dial-up server used by an ISP, sends user information to a RADIUS server. The RADIUS server validates the RADIUS client request.

For more information about the RADIUS protocol, see RFCs 2138 and 2139.

RADIUS Authentication Operation

The RADIUS authentication process begins when a remote access user presents authentication information to the RADIUS client. After the RADIUS client has obtained such information, it might authenticate by using RADIUS.

For example, when the remote access user sends their credentials using the Challenge Handshake Authentication Protocol (CHAP), the RADIUS client creates a RADIUS Access-Request packet containing such attributes as the user's name, the user's password, the ID of the client and the Port ID the user is accessing. When a password is present, CHAP encrypts the password using a method based on Rivest-Shamir-Adleman (RSA) Message Digest 5 (MD5).

The RADIUS Access-Request packet is sent to the RADIUS server. If no response is returned within a length of time, the request can be re-sent a number of times. The RADIUS client can also forward requests to an alternate server or servers in the event that the primary server is down or unreachable. An alternate server can be used either after a number of tries to the primary server fail, or in a round-robin fashion.

In the case of Routing and Remote Access service, multiple RADIUS servers can be added and prioritized as authentication providers. If a primary RADIUS server does not respond within a three-second time period, the Routing and Remote Access service automatically switches to the RADIUS server with the next highest score.

After the RADIUS server receives the request, it validates the sending RADIUS client. Validation occurs by verifying that the RADIUS Access-Request packet is sent from a configured RADIUS client. If the Access-Request packet was sent by a valid RADIUS client, and if digital signatures are enabled for the RADIUS client, the digital signature in the packet is checked using the shared secret.

A request from a RADIUS client for which the RADIUS server does not have a shared secret is silently discarded. If the RADIUS client is valid, the RADIUS server consults a database of users to find the user whose name matches the request. The user account contains a list of requirements that must be met to allow access for the user. This can include verification of the password, but can also specify whether the user is allowed access.

If any condition where the authentication or authorization is not met, the RADIUS server sends a RADIUS Access-Reject packet in response, indicating that this user request is invalid.

If all conditions are met, the list of configuration values for the user are placed into a RADIUS Access-Accept packet that is sent back to the RADIUS client. These values include a list of RADIUS attributes and all necessary values to deliver the desired service. For SLIP and PPP service types, this can include values such as IP address, subnet mask, MTU, desired compression, and desired packet filter identifiers.

RADIUS Packet Format

The following section provides information that might be useful for the following:

- Debugging a Network Monitor trace.
- Understanding the different packet formats for analyzing the accounting log.
- Entering vendor-specific attribute numbers.

RADIUS packets sent to the RADIUS server are sent as User Datagram Protocol (UDP) messages using UDP port 1812 for RADIUS authentication messages and UDP port 1813 for RADIUS accounting messages. Some older network access servers use UDP port 1645 for RADIUS authentication messages and UDP port 1646 for RADIUS accounting messages. IAS supports the receiving of RADIUS messages on both sets of UDP ports. Exactly one RADIUS packet is encapsulated in the UDP payload.

General Packet Structure

Figure 8.1 shows the general structure of a RADIUS packet.

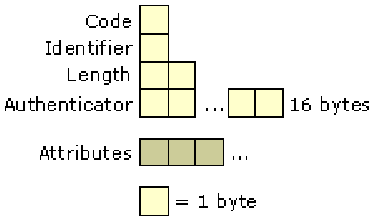


Figure 8.1 General Structure of RADIUS Packet

Code

The Code field is 1 byte long and indicates the type of RADIUS packet. A packet with an invalid Code field is silently discarded. The defined values for the RADIUS Code field are listed in Table 8.1.

Table 8.1 Values for the RADIUS Code Field

Codes (Decimal)	Packets
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

Identifier

The Identifier field is 1 byte long and is used to match a request with its corresponding response.

Length

The Length field is two octets long and indicates the entire length of the packet and RADIUS message, including the Code, Identifier, Length, and Authenticator fields, and the RADIUS Attributes. The Length field can vary from 20 to 4,096 bytes.

Authenticator

The Authenticator field is sixteen octets long and contains the information that the RADIUS client and server use to authenticate each other.

Attributes

The Attributes section of the RADIUS packet contains one or more RADIUS attributes, which carry the specific authentication, authorization, information, and configuration details for RADIUS packets. For attributes that have multiple instances, the order of the attributes must be preserved. Otherwise, attribute types do not have to have their order preserved.

RADIUS Attributes

Figure 8.2 shows the structure of each RADIUS attribute. RADIUS attributes use the common Type-Length-Value format used by other protocols.

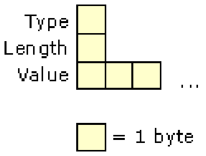


Figure 8.2 RADIUS Attribute Structure

Type

The Type field is 1 byte long and indicates the specific type of RADIUS attribute. For information about the most recent RADIUS attributes, see the Radius Types link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Some of the attributes are listed in Table 8.2. For information about other RADIUS attributes and their use, see RFCs 2138 and 2139.

Table 8.2 RADIUS Attribute Types

Type Values	Description
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
9	Framed-IP-Netmask
10	Framed-Routing
11	Filter-ID
12	Framed-MTU
13	Framed-Compression
19	Reply-Message
24	State
25	Class
26	Vendor-Specific
27	Session-Timeout

28	Idle-Timeout
29	Termination-Action
32	NAS-Identifier
61	NAS-Port-Type
62	Port-Limit

Type values 192 through 223 are reserved for experimental use, values 224 through 240 are reserved for implementation-specific use, and values 241 through 255 are reserved and must not be used. Value 26 is reserved for vendor-specific attributes (VSAs).

Length

The Length field indicates the length of the attribute, including the Type, Length, and Value fields.

Value

The Value field is zero or more octets and contains information specific to the Attribute. The format and length of the Value field is based on the type of RADIUS attribute.

Vendor-Specific Attributes

VSAs are available to allow vendors to support their own proprietary attributes that are not covered by RFC 2138. IAS includes VSAs from a number of vendors in its multivendor dictionary. However, this list evolves over time and new attributes and vendors are always being added.

To accommodate for attributes that are not in the IAS multivendor dictionary, IAS allows you to add them as Vendor-Specific (attribute type 26) in the **Advanced** tab of a remote access policy profile. To use attribute type 26, an administrator needs to know the VSA format, as well as the exact information to enter. The VSA formats are documented in the following section. For information about what to enter, see your NAS documentation.

The structure of the vendor-specific attribute is shown in Figure 8.3.

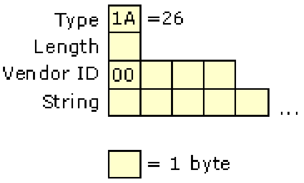


Figure 8.3 Vendor-Specific Attribute Structure

Type

The Type value is set to 26 (0x1A) to indicate a VSA.

Length

The Length value is set to the number of bytes in the VSA.

Vendor-ID

The high-order octet is 0 (0x00) and 4 octets long, and the low-order 3 octets are the Structure and Identification of Management Information (SMI) Network Management Private Enterprise Code of the vendor.

String

The String field is the VSA consisting of one or more octets. To conform with the recommendation of RFC 2138, the String field should consist of the fields as shown in Figure 8.4.

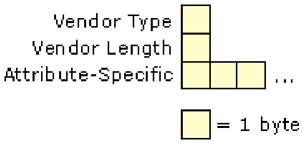


Figure 8.4 Structure of the String Field

Vendor Type

The Type value is used to indicate a specific VSA for the vendor.

Vendor Length

The Type value is set to the number of bytes in the string.

Attribute-Specific

The Attribute-Specific field contains the data for the specific vendor attribute.

Vendors that do not conform to RFC 2138 use the attribute type 26 to identify a vendor-specific attribute but do not use the Vendor Type, Vendor Length, and Attribute-Specific fields within the String field. In this case, the vendor-specific attribute format appears as shown in Figure 8.4.

When adding a VSA for a particular NAS as type 26, you need to know whether the attribute conforms to RFC 2138. For information about whether your NAS uses the VSA format documented in Figure 8.4, see your NAS documentation.

VSAs are configured from the **Vendor-Specific Attribute Information** dialog box when adding a Vendor-Specific Attribute from the **Advanced** tab of a remote access policy profile. If the VSA format conforms to RFC 2138, select the **Yes. It conforms.** option and configure the attribute with the vendor-assigned attribute number, attribute format, and attribute value as defined in NAS documentation. If the VSA format does not conform to RFC 2138, choose **No. It does not conform.**, and configure the attribute with the hexadecimal attribute value, which includes the string of the VSA format (everything after Vendor-ID) as defined in NAS documentation. For more information about configuring vendor-specific attributes, see "IAS Authorization" later in this chapter.

RADIUS Packet Example

A Windows 2000 PPTP client attempts a remote access connection to a Windows 2000 VPN server. The VPN server is at the IP address 10.10.210.13, and the IAS server is at the IP address 10.10.210.12.

Access-Request Packet

The following Network Monitor trace shows the Access-Request packet sent by the VPN server to the IAS server.

```
+ IP: ID = 0x850; Proto = UDP; Len: 248
+ UDP: Src Port: Unknown, (1327); Dst Port: Unknown (1812); Length = 228 (0xE4)
RADIUS: Message Type: Access Request(1)
RADIUS: Message Type = Access Request
RADIUS: Identifier = 2 (0x2)
RADIUS: Length = 220 (0xDC)
RADIUS: Authenticator = 8A 6F DC 03 23 5F 4B 62 CA 40 92 38 DC 75
CB 74
RADIUS: Attribute Type: NAS IP Address(4)
RADIUS: Attribute type = NAS IP Address
RADIUS: Attribute length = 6 (0x6)
RADIUS: NAS IP address = 10.10.210.13
RADIUS: Attribute Type: Service Type(6)
RADIUS: Attribute type = Service Type
RADIUS: Attribute length = 6 (0x6)
RADIUS: Service type = Framed
RADIUS: Attribute Type: Framed Protocol(7)
RADIUS: Attribute type = Framed Protocol
RADIUS: Attribute length = 6 (0x6)
RADIUS: Framed protocol = PPP
RADIUS: Attribute Type: NAS Port(5)
RADIUS: Attribute type = NAS Port
RADIUS: Attribute length = 6 (0x6)
RADIUS: NAS port = 32 (0x20)
RADIUS: Attribute Type: Vendor Specific(26)
RADIUS: Attribute type = Vendor Specific
RADIUS: Attribute length = 12 (0xC)
RADIUS: Vendor ID = 311 (0x137)
RADIUS: Vendor string = _
RADIUS: Attribute Type: Vendor Specific(26)
RADIUS: Attribute type = Vendor Specific
RADIUS: Attribute length = 18 (0x12)
RADIUS: Vendor ID = 311 (0x137)
RADIUS: Vendor string = MSRASV5.00
RADIUS: Attribute Type: NAS Port Type(61)
RADIUS: Attribute type = NAS Port Type
RADIUS: Attribute length = 6 (0x6)
RADIUS: NAS port type = Virtual
RADIUS: Attribute Type: Tunnel Type(64)
RADIUS: Attribute type = Tunnel Type
RADIUS: Attribute length = 6 (0x6)
RADIUS: Tag = 0 (0x0)
RADIUS: Tunnel type = Point-to-Point Tunneling Protocol(PPTP)
RADIUS: Attribute Type: Tunnel Media Type(65)
RADIUS: Attribute type = Tunnel Media Type
RADIUS: Attribute length = 6 (0x6)
RADIUS: Tag = 0 (0x0)
RADIUS: Tunnel media type = IP (IP version 4)
RADIUS: Attribute Type: Calling Station ID(31)
RADIUS: Attribute type = Calling Station ID
RADIUS: Attribute length = 14 (0xE)
RADIUS: Calling station ID = 10.10.14.226
RADIUS: Attribute Type: Tunnel Client Endpoint(66)
RADIUS: Attribute type = Tunnel Client Endpoint
RADIUS: Attribute length = 14 (0xE)
RADIUS: Tunnel client endpoint = 10.10.14.226
RADIUS: Attribute Type: User Name(1)
RADIUS: Attribute type = User Name
RADIUS: Attribute length = 18 (0x12)
RADIUS: User name = NTRESKIT\johndoe
RADIUS: Attribute Type: Vendor Specific(26)
RADIUS: Attribute type = Vendor Specific
RADIUS: Attribute length = 24 (0x18)
RADIUS: Vendor ID = 311 (0x137)
RADIUS: Vendor string = _¦ì1/2+-_¦e_$+fN<åN
RADIUS: Attribute Type: Vendor Specific(26)
RADIUS: Attribute type = Vendor Specific
RADIUS: Attribute length = 58 (0x3A)
RADIUS: Vendor ID = 311 (0x137)
RADIUS: Vendor string = _4
```

The RADIUS attributes sent by the VPN server include the user name, the service types, the framed protocol, various tunnel attributes for the PPTP connection, and a series of vendor-specific attributes for MS-CHAP authentication. For more information about Microsoft VSAs, see RFC 2548.

Access-Accept Packet

The following Network Monitor trace shows the Access-Accept packet sent by the IAS server to the VPN server.

```
+ IP: ID = 0xB18; Proto = UDP; Len: 248
+ UDP: Src Port: Unknown, (1812); Dst Port: Unknown (1327); Length = 228 (0xE4)
RADIUS: Message Type: Access Accept(2)
RADIUS: Message Type = Access Accept
RADIUS: Identifier = 2 (0x2)
RADIUS: Length = 220 (0xDC)
RADIUS: Authenticator = 52 E2 19 98 2E F8 E2 D3 B7 3B E1 24 5B 72
55 9E
```

```
RADIUS: Attribute Type: Framed Protocol(7)
RADIUS: Attribute type = Framed Protocol
RADIUS: Attribute length = 6 (0x6)
RADIUS: Framed protocol = PPP
RADIUS: Attribute Type: Service Type(6)
RADIUS: Attribute type = Service Type
RADIUS: Attribute length = 6 (0x6)
RADIUS: Service type = Framed
RADIUS: Attribute Type: Class(25)
RADIUS: Attribute type = Class
RADIUS: Attribute length = 32 (0x20)
RADIUS: Class = <$_@
RADIUS: Attribute Type: Vendor Specific(26)
RADIUS: Attribute type = Vendor Specific
RADIUS: Attribute length = 42 (0x2A)
RADIUS: Vendor ID = 311 (0x137)
RADIUS: Vendor string = _$Ç_DZ¦,S¯c7__æ:+RW_tÖ-qxF¦ (-+¦%p6
RADIUS: Attribute Type: Vendor Specific(26)
RADIUS: Attribute type = Vendor Specific
RADIUS: Attribute length = 42 (0x2A)
RADIUS: Vendor ID = 311 (0x137)
RADIUS: Vendor string = _$Ç_
RADIUS: Attribute Type: Vendor Specific(26)
RADIUS: Attribute type = Vendor Specific
RADIUS: Attribute length = 51 (0x33)
RADIUS: Vendor ID = 311 (0x137)
RADIUS: Vendor string = _-
RADIUS: Attribute Type: Vendor Specific(26)
RADIUS: Attribute type = Vendor Specific
RADIUS: Attribute length = 21 (0x15)
RADIUS: Vendor ID = 311 (0x137)
RADIUS: Vendor string =
```

The RADIUS attributes sent by the IAS server include the user name, the service type, the framed protocol, the service class, and a series of vendor-specific attributes for MS-CHAP authentication.

IAS Authentication

In the process of identifying dial-up users and admitting them to a secure network or site, different servers handle different aspects of the task.

A network access server (NAS) operates as a client of an IAS server. The client is responsible for passing user information to designated IAS servers, and then acting on the response.

IAS is responsible for receiving user connection requests, authenticating the user, authorizing the connection attempt, and then returning all configuration information necessary for the RADIUS client to deliver service to the user. Figure 8.5 illustrates the general IAS authentication process.

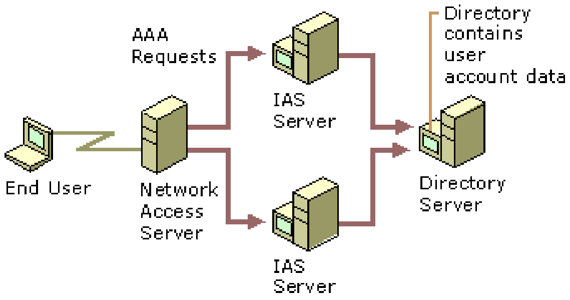


Figure 8.5 IAS Authentication Process

When a user attempts to connect to a network through a dial-up connection or virtual private network, the authentication request is processed as follows:

1. The NAS tries to negotiate a connection with the remote access client by using the most secure protocol first, then the next least secure protocol, and so on, down to the least secure protocol (for example, NAS tries to negotiate a connection by using EAP, MS-CHAP, then CHAP, and finally PAP).
2. The NAS forwards the authentication request to an IAS server in the form of a RADIUS Access-Request packet.
3. The IAS server first verifies that the RADIUS Access-Request packet is sent from a configured RADIUS client by checking the source IP address. If the Access-Request packet was sent by a valid RADIUS client, and if digital signatures are enabled for the RADIUS client, the digital signature in the packet is checked using the shared secret. A shared secret is a text string that serves as a special password between RADIUS server and the RADIUS clients connected to it. Each IAS server must have a shared secret for each NAS or other IAS server that forwards RADIUS requests to it. There are a few rules you must follow to successfully set up a shared secret:
   - The shared secret must be exactly the same at both servers.
   - Secrets are case-sensitive.
   - Secrets can use any standard alphanumeric characters or any special characters.
4. If digital signatures are enabled and the verification of the digital signature fails, IAS server silently discards the packet. When the NAS does not get a response within its time-out period, it retries and then disconnects the user. If IAS server cannot connect to the domain controller or cannot find the domain controller the user belongs to, it silently discards the packet. This allows a RADIUS proxy to retransmit the request to the backup IAS server, which would then attempt to authenticate the user against the domain's database.
5. If digital signatures are enabled and the verification of the digital signature is successful, the IAS server queries the Windows 2000-based domain controller, which validates the user credentials.
6. If the user credentials are authentic, the IAS server evaluates the connection attempt against the configured remote access policies and the dial-in properties of the user's account to decide whether to authorize the request. If the connection attempt matches the conditions of at least one policy and the user account dial-in properties, remote access policy properties and the remote access policy profile properties authorize the connection, IAS sends a RADIUS Access-Accept message to the NAS that sent the Access-

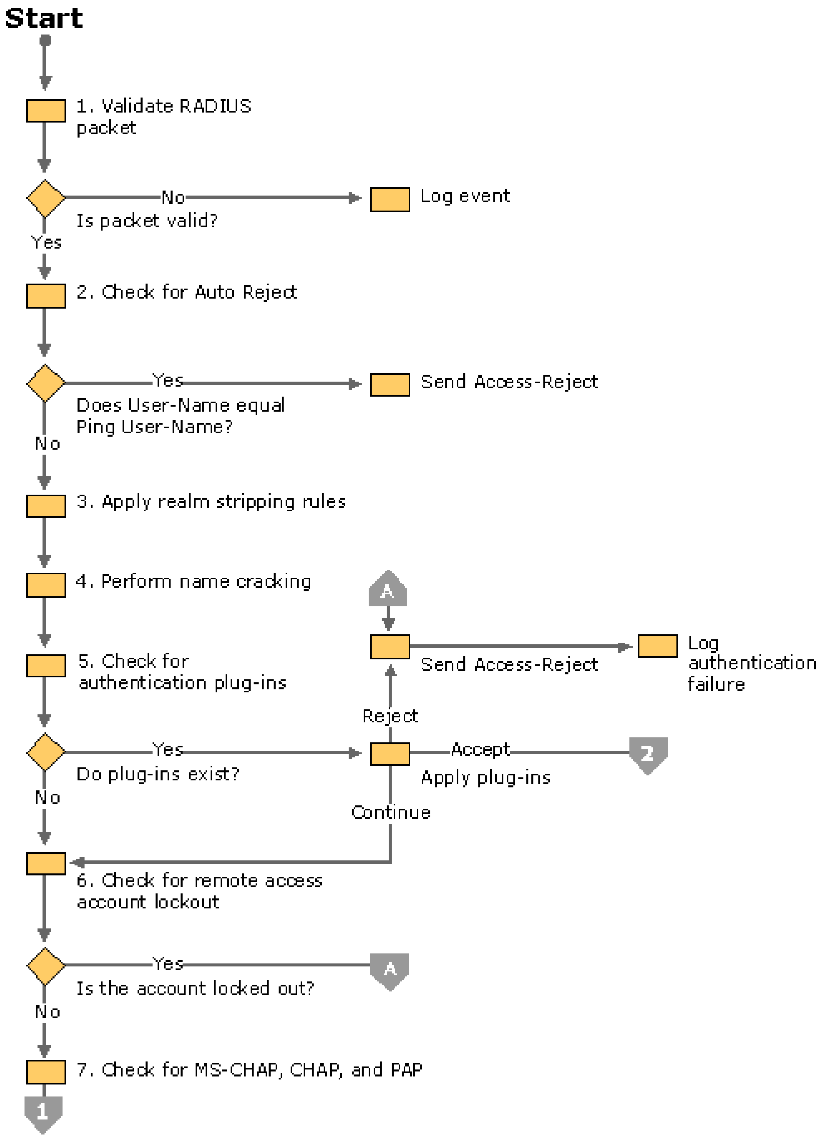
Request message. The Access-Accept message authorizes the connection but also contains connection parameters based on the remote access policy profile settings and the dial-in properties of the user account. The NAS interprets this authorization data to determine the connection parameters that the server has authorized.

If the user is not authentic or the user's attempt to connect does not match conditions in at least one policy, or matches conditions in a policy that denies access, IAS sends a RADIUS Access-Reject message to the NAS, and the NAS disconnects the user.

IAS Step-by-Step Authentication and Authorization

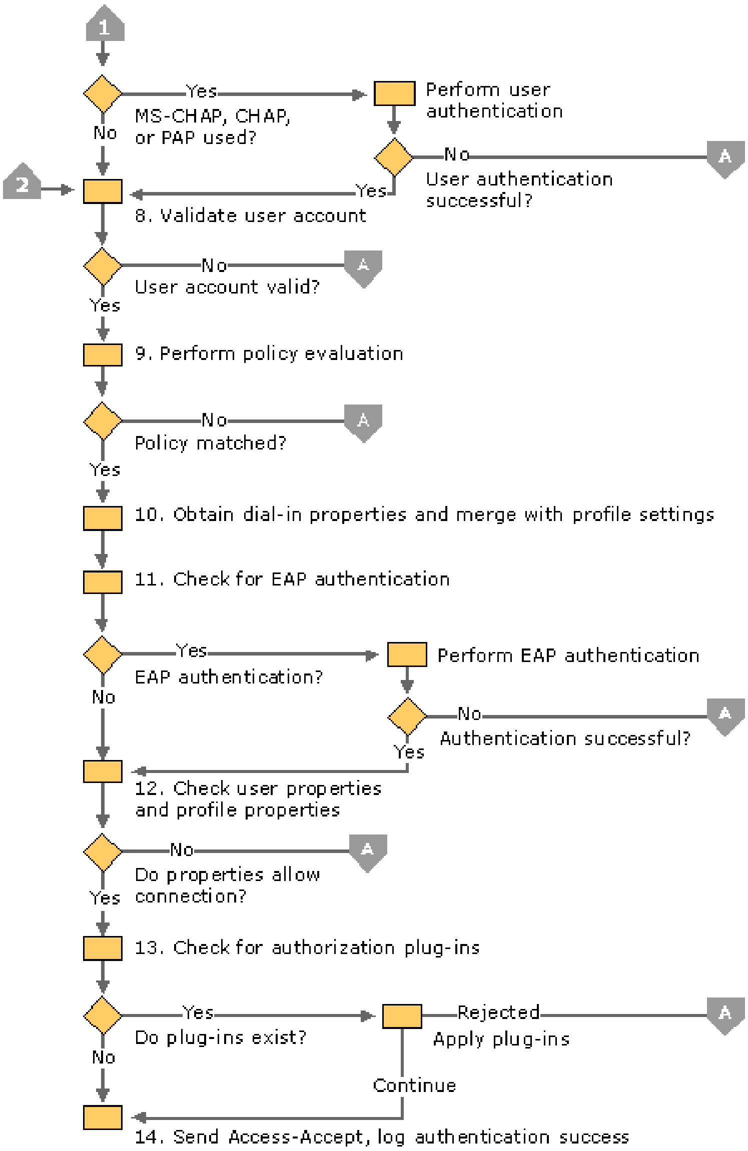
The diagram shown in Figure 8.6a and Figure 8.6b demonstrates the step-by-step IAS authentication and authorization process.

Note The authentication and authorization process for the Routing and Remote Access service, when configured for Windows authentication, uses steps 4 through 14 of this process. In all steps, no RADIUS packets are sent. The authentication and authorization success and failure are the return values of functions called by the Routing and Remote Access service. Local event or authentication logging depends on the configured logging settings of the Routing and Remote Access service. For more information, see "Routing and Remote Access Service" in this book.


Start
1. Validate RADIUS packet
No
Log event
Is packet valid?
Yes
2. Check for Auto Reject
Yes
Send Access-Reject
Does User-Name equal Ping User-Name?
No
3. Apply realm stripping rules
4. Perform name cracking
A
5. Check for authentication plug-ins
Send Access-Reject
Log authentication failure
Reject
Yes
Accept
2
Do plug-ins exist?
Apply plug-ins
No
Continue
6. Check for remote access account lockout
Yes
A
Is the account locked out?
No
7. Check for MS-CHAP, CHAP, and PAP
1

If your browser does not support inline frames, click here to view on a separate page.

Figure 8.6a IAS Authentication and Authorization Process


1
Yes
MS-CHAP, CHAP, or PAP used?
No
Perform user authentication
No
User authentication successful?
Yes
A
2
8. Validate user account
No
User account valid?
Yes
A
9. Perform policy evaluation
No
Policy matched?
Yes
A
10. Obtain dial-in properties and merge with profile settings
11. Check for EAP authentication
Yes
EAP authentication?
No
Perform EAP authentication
No
Authentication successful?
Yes
A
12. Check user properties and profile properties
No
Do properties allow connection?
Yes
A
13. Check for authorization plug-ins
Yes
Do plug-ins exist?
No
Rejected
Apply plug-ins
A
Continue
14. Send Access-Accept, log authentication success

If your browser does not support inline frames, click here to view on a separate page.

Figure 8.6b IAS Authentication and Authorization Process

1. Validate RADIUS packet

   The incoming Access-Request packet is validated for source IP address, the digital signature, valid attributes, and so on.

   If the RADIUS packet is not valid, an event is logged in the system event log and the RADIUS Access-Request packet is discarded. An Access-Reject message is not sent.

2. Check for Auto Reject

   Auto Reject is used to send an immediate Access-Reject packet when the User-Name attribute in the Access-Request packet matches a specific value. The periodic sending of an Access-Request packet and reception of an Access-Reject packet assures the RADIUS client that the RADIUS server is still present on the network. An Auto Reject Access-Request message requires special handling because it does not need to be evaluated for authentication and authorization. No authentication log entry is created for Auto Reject requests. This is done to prevent Auto Reject messages from filling up the authentication log file.

   To configure IAS for Auto Reject, configure the **Ping User-Name** registry setting (HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \IAS \Parameters) with the user name for Auto Reject packets. If the User-Name attribute of the Access-Request packet matches the Ping User-Name registry setting, an Access-Reject message is sent.

3. Apply realm stripping rules

   If the User-Name attribute in the Access-Request packet is not the Auto Reject name, then the user identity is determined. User identity is how IAS identifies the user for the purposes of authentication and authorization. Normally, the user identity is the string value of the User-Name RADIUS attribute. If the User-Name attribute is not present, the user identity is set to the Guest account or the account specified by the **Default User Identity** registry value (HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \RemoteAccess\Policy).

   However, IAS can use any RADIUS attribute to identify the user. The RADIUS attribute that IAS uses to identify the user is configurable by setting the **User Identity Attribute** registry setting (HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \RemoteAccess \Policy) to the number of the RADIUS attribute that is used for the user identity. By default, **User Identity Attribute** is set to 1, the RADIUS type value for the User-Name RADIUS attribute. For more information about the use of the **User Identity Attribute** registry setting, see "Unauthenticated Access" later in this chapter.

   Realm stripping rules are then applied and define how the user identity is manipulated before the name is checked for existence. The realm stripping rules consist of an ordered set of <Original string to match>, <Replacement String>. IAS applies the realm stripping rules to the user identity in the configured order. For information about how to configure realm stripping and examples of using pattern syntax to create realm stripping rules, see Windows 2000 Server Help.

4. Perform name cracking

   Name cracking is the resolution of the user identity to a user account using user principal names, Lightweight Directory Access Protocol (LDAP), distinguished names (DNA), Canonical Names, and so on. If a user principal name is encountered by IAS, IAS performs a query to the Active Directory Global Catalog in an attempt to resolve the name. To speed up this process, a copy of the Global Catalog must be located on a domain controller within the same site as the IAS server.

   When the user identity does not contain a domain name, IAS supplies a domain name. By default, the IAS-supplied domain name is the domain for which the IAS server is a member. You can specify the IAS-supplied domain through the DefaultDomain registry setting (HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \RasMan \PPP \ControlProtocols \BuiltIn).

5. Check for authentication plug-ins

   The existence of authentication plug-ins is checked. Authentication plug-ins are optional components created using the IAS SDK. Each plug-in can return either Accept, Reject, or Continue. If an authentication plug-in returns an Accept, the user is considered to be authenticated and the account is then validated. If the authentication plug-in returns a Reject, an Access-Reject packet is sent and the authentication failure event is logged in the system event log or the IAS authentication log, depending on the configured logging settings. If the authentication plug-in returns a Continue, the next plug-in is checked. If there are no more plug-ins, the user still needs to be authenticated.

   The authentication plug-in can also return RADIUS attributes to be included in the Access-Accept packet.

6. Check for remote access account lockout

   After the authentication plug-ins are checked, the registry on the IAS server is read for the remote access account lockout entry for the user account. If the account is locked out through remote access account lockout, IAS sends an Access-Reject message back to the NAS and logs an authentication event.

Note Remote access account lockout is a security feature that is enabled through the Windows 2000 registry. Remote access account lockout is used to prevent dictionary attacks against user accounts. For more information about remote access account lockout, see "Remote Access Server" in this book. Remote access account lockout is not related to account lockout on the Windows 2000 user account and the implementation of account lockout policies by using Windows 2000 Group Policy.

1. Check for MS-CHAP, CHAP, and PAP

   If the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) version 1 or version 2, CHAP, or Password Authentication Protocol (PAP) are used to authenticate the remote access client, IAS consults an authentication submodule based on the authentication protocol to perform the authentication. The user's credentials, the user name and password, are authenticated against the user name and password of the accounts database (a domain or the local accounts database) and the group membership of the user account is determined. The exact method of authentication varies depending on the authentication protocol.

   If the authentication of the credentials is not successful, an Access-Reject packet is sent and the authentication failure event is logged in the system event log or the IAS authentication log depending on the configured logging settings.

   If either EAP or unauthenticated access is being used, then the user authentication process is bypassed. EAP authentication takes place later in this process. For unauthenticated access, no user authentication is performed.

2. Validate user account

   Based on the user account determined through name cracking, the user account is validated to check whether the account is locked out (which is not the same as remote access account lockout), whether the account is disabled, and whether the user account's password has expired. If the user account is not valid, an Access-Reject packet is sent and the authentication failure event is logged in the system event log or the IAS authentication log depending, on the configured logging settings.

3. Perform policy evaluation

   Remote access policies configured on the IAS server are evaluated to find a policy that matches the parameters of the connection. If a matching policy is not found, an Access-Reject packet is sent and an event is logged. For more information about remote access policies and policy evaluation logic, see "Remote Access Policies" later in this chapter.

4. Obtain dial-in properties and merge with profile settings

   The dial-in properties for the user account associated with the connection and the profile properties from the matching policy are merged into a set of properties for the connection.

5. Check for EAP authentication

   If EAP is the authentication protocol used for the connection attempt, EAP authentication takes place. The initial negotiation for EAP consists of selecting EAP as the PPP authentication protocol and negotiating an EAP type. Based on the EAP type, the profile settings for the matching policy are checked to ensure that the EAP type is allowed. If the EAP type is not allowed with the profile settings, an Access-Reject packet is sent and the authentication failure event is logged in the system event log or the IAS authentication log, depending on the configured logging settings.

   If the EAP type is allowed with the profile settings, EAP authentication for the EAP type occurs. IAS sends an EAP challenge to NAS asking it to start EAP negotiation. Communications between EAP dynamic-link libraries (DLLs) on a client and server side are tunneled between the client and the IAS server using the RADIUS protocol. After complete, an EAP provider can return attributes that are sent back to the NAS in the Access-Accept packet. If EAP authentication fails, an Access-Reject packet is sent and the authentication failure event is logged in the system event log or the IAS authentication log, depending on the configured logging settings.

6. Check user properties and profile properties

   The dial-in properties of the user account and the profile properties of the matching remote access policy are evaluated against the parameters of the connection attempt to ensure that the connection attempt is allowed. If the connection attempt is not allowed, an Access-Reject packet is sent and the authentication failure event is logged in the system event log or the IAS authentication log, depending on the configured logging settings.

7. Check for authorization plug-ins

   The existence of authorization plug-ins is checked. Authorization plug-ins are optional components created using the IAS SDK. Each plug-in can return either Reject or Continue. If the authorization plug-in returns a Reject, an Access-Reject packet is sent and the authentication failure event is logged in the system event log or the IAS authentication log, depending on the configured logging settings. If the authorization plug-in returns Continue, the next plug-in is checked. If there are no more plug-ins, the user is considered to be authorized.

   The authorization plug-in can also return RADIUS attributes to be included in the Access-Accept packet.

8. Send Access-Accept

   If the dial-in properties of the user account, the profile properties of the matching remote access policy, and the conditions imposed by authorization plug-ins allow the connection attempt, an Access-Accept packet is sent back to the NAS with the set of RADIUS attributes for the restrictions on the connection and an authentication success event is logged in the system event log or the IAS authentication log, depending on the configured logging settings.

Compulsory Tunneling with IAS

The benefit of using IAS with tunnels is that IAS can be configured to direct the traffic from the client through a tunnel to a particular location. Depending on the category of authenticating user, a tunnel can be created to different parts of the corporate network.

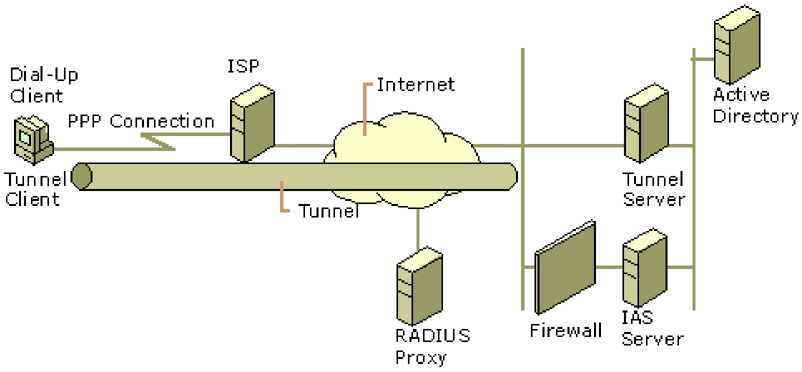
Note For information about tunneling and the use of tunneling in Windows 2000, see "Virtual Private Networking" in this book.

Tunnels can be created in different ways. The following sections describe the two main tunnel types: voluntary tunneling and compulsory tunneling.

Voluntary Tunneling

A user or client computer can issue a VPN request to configure and create a voluntary tunnel. In this case, the user's computer is a tunnel endpoint and acts as the tunnel client. Voluntary tunneling occurs when a workstation or router uses tunneling client software to create a VPN connection to the target tunnel server. In order to accomplish this, the appropriate tunneling protocol must be installed on the client computer.

In a dial-up situation, the client must establish a dial-up connection to the internetwork before the client can set up a tunnel. This is the most common case. The best example of this is the dial-up Internet user, who must dial an ISP and obtain an Internet connection before a tunnel over the Internet can be created. Figure 8.7 shows a voluntary tunnel created between a dial-up user and a tunnel server.



If your browser does not support inline frames, click here to view on a separate page.

Figure 8.7 Voluntary Tunnel Created by a Dial-Up User

Figure 8.7 shows IAS as it is used in an outsourced bulk dial scenario for voluntary tunneling. A dial-up client establishes a dial-up connection to an ISP. In the outsourced bulk, dial scenario, the dial-up client calls an ISP that is providing Internet access for all the employees of an organization. Based on the dial-up connection parameters, the NAS dialed by the dial-up client sends an Access-Request packet to a configured RADIUS proxy computer. The RADIUS proxy, based on the realm name in the User-Name attribute, forwards the Access-Request packet to the IAS server of the organization that is reachable on the Internet through a firewall. The organization IAS server authenticates and authorizes the connection attempt of the dial-up client and sends an Access-Accept packet back to the RADIUS proxy. The RADIUS proxy forwards the Access-Accept packet to the ISP NAS and the ISP NAS connects the dial-up client to the Internet.

After on the Internet, the dial-up client initiates a tunnel connection with the organization tunnel server on the Internet. Based on the tunnel connection parameters, the tunnel server sends an Access-Request packet to the organization IAS server. The organization IAS server authenticates and authorizes the connection attempt of the tunnel client and sends an Access-Accept packet back to the tunnel server. The tunnel server completes the tunnel creation and the tunnel client can now send packets to the organization intranet through the tunnel.

Note The authentication type and level of encryption might be different for the dial-up connection and the tunnel. For example, the dial-up connection to the ISP might use CHAP, but the tunnel might choose a more secure authentication type such as MS-CHAP v2 or EAP-TLS.

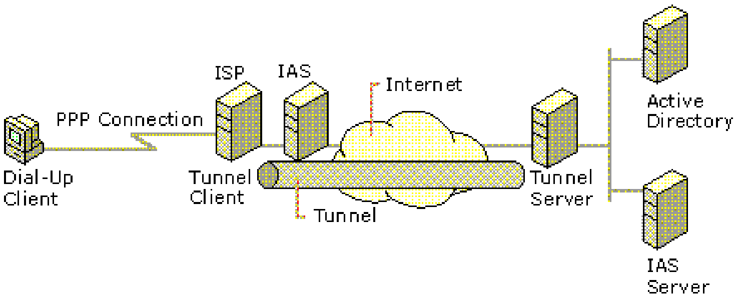
Compulsory Tunneling

Compulsory tunneling is the creation of a secure tunnel by another computer or network device on the client computer's behalf. Compulsory tunnels are configured and created automatically for the user without their knowledge or intervention. With a compulsory tunnel, the user's computer is not a tunnel endpoint. Another device between the user's computer and the tunnel server is the tunnel endpoint, acting as the tunnel client. The dial-up access server dialed by the client computer is the tunnel endpoint, acting as the tunnel client.

A number of vendors that sell dial-up access servers have implemented the ability to create a tunnel on behalf of a dial-up client. The computer or network device providing the tunnel for the client computer is known as a Front End Processor (FEP) in PPTP, an L2TP Access Concentrator (LAC) in L2TP, or an IP Security Gateway in IPSec. For the purposes of this chapter, the term FEP is used to describe this functionality, regardless of the tunneling protocol. To carry out its function, the FEP must have the appropriate tunneling protocol installed and must be capable of establishing the tunnel when the client computer attempts a connection.

A corporation can contract with an ISP to deploy a nationwide set of FEPs. These FEPs can establish tunnels across the Internet to a tunnel server connected to the corporation's private network, thereby consolidating calls from geographically diverse locations into a single Internet connection at the corporate network.

Figure 8.8 shows the client computer placing a dial-up call to a tunneling-enabled NAS at the ISP, in order to authenticate against an IAS server on the other side of the tunnel.



If your browser does not support inline frames, click here to view on a separate page.

Figure 8.8 Compulsory Tunnel Created by a Tunneling-Enabled NAS

Figure 8.8 shows IAS as it is used in an outsourced bulk dial scenario for compulsory tunneling.

A dial-up client establishes a dial-up connection to an ISP. In the outsourced bulk dial scenario, the dial-up client calls an ISP that is providing tunneled access across the Internet for all the employees of an organization. Based on the dial-up connection parameters, the NAS dialed by the dial-up client sends an Access-Request packet to a configured IAS server. The ISP IAS server authorizes the tunnel connection and sends back an Access-Accept packet with a series of tunnel attributes. If needed, the IAS NAS creates a tunnel to the organization tunnel server on the Internet.

Note Normally IAS provides both authentication and authorization. In this case, however, it is common for the ISP IAS server to provide authorization only. Because the dial-in client is performing authentication against the organization tunnel server, authentication against the ISP NAS is not necessary.

The ISP NAS then sends a PPP message to the dial-up client to restart the authentication process so that the dial-up user can be authenticated against the organization tunnel server. The dial-up client sends its authentication information to the IAS NAS, which encapsulates it and sends it through the tunnel to the tunnel server.

After the authentication credentials are received by the tunnel server, the tunnel server sends an Access-Request packet to the organization IAS server. The organization IAS server authenticates and authorizes the connection of the dial-up client to the tunnel server and sends an Access-Accept packet to the tunnel server. The tunnel server then completes the connection to the dial-up client.

All data that is sent by the dial-up client is automatically sent through the tunnel to the tunnel server by the ISP NAS.

This configuration is known as compulsory tunneling because the client is compelled to use the tunnel created by the FEP. After the initial connection is made, all network traffic to and from the client is automatically sent through the tunnel. IAS can be configured to instruct a FEP to tunnel different dial-up clients to different tunnel servers.

Unlike the separate tunnels created for each voluntary client, a compulsory tunnel between the FEP and tunnel server can be shared by multiple dial-up clients. When a second client dials into the access server (the FEP) to reach a destination for which a tunnel already exists, the data traffic for the new client is carried over the existing tunnel.

Note Using a RADIUS proxy in compulsory tunnels is not recommended. A proxy can decrypt a tunnel's password because it uses the shared secret between the proxy and IAS to encrypt the password.

The following RADIUS Attributes are used to carry the tunneling information from the IAS server to the NAS.

Used in authorization only:

- Tunnel-Private-Group-ID
- Tunnel-Assignment-ID
- Tunnel-Preference
- Tunnel-Password (not for use with proxies)

Used in authorization and accounting:

- Tunnel-Type (PPTP, L2TP, and so on)
- Tunnel-Medium-Type (X.25, ATM, Frame Relay, IP, and so on)
- Tunnel-Client-Endpoint
- Tunnel-Server-Endpoint

Used for accounting only:

- Acct-Tunnel-Connection

The Windows 2000 Routing and Remote Access service cannot be used as a FEP for compulsory tunneling.

Authentication Methods

There are a number of PPP authentication protocols that are supported by the RADIUS protocol. Each protocol has advantages and disadvantages in terms of security, usability, and breadth of support. The protocol used is determined by the configuration of the NAS device. See your NAS documentation if you are configuring a dial-up network, or consult your ISP if you are using an ISP for dial-up access to your LAN.

The following sections focus on the advantages and disadvantages of the authentication protocols currently supported by IAS. The information is also useful in configuring a particular authentication method for remote access.

Password Authentication Protocol

Password Authentication Protocol (PAP) passes a password as a string from the user's computer to the NAS device. When the NAS forwards the password, it is encrypted using the RADIUS shared secret as an encryption key. PAP is the most flexible protocol because passing a plaintext password to the authentication server enables that server to compare the password with nearly any storage format. For example, UNIX passwords are stored as one-way encrypted strings that cannot be decrypted. PAP passwords can be compared to these strings by reproducing the encryption method.

Because it uses a plaintext version of the password, PAP has a number of security vulnerabilities. Although the RADIUS protocol encrypts the password, it is transmitted as plaintext across the dial-up connection.

Enabling PAP

To enable PAP-based authentication, you must do the following:

1. Enable PAP as an authentication protocol on the remote access server. For information about a default setting on a particular NAS, see your NAS documentation. On the Routing and Remote Access service, PAP is disabled by default.
2. Enable PAP on the appropriate remote access policy. PAP is disabled by default.
3. Enable PAP on a remote access client.

Note Enabling PAP as an authentication protocol means that user passwords are sent from a client to a NAS in plaintext form. The NAS encrypts the password using the shared secret and sends it in an Access-Request packet. Because a RADIUS proxy must encrypt the PAP password using the shared secret of its forwarding RADIUS server, a RADIUS proxy must decrypt the PAP password using the shared secret between the RADIUS proxy and the NAS. A malicious user at a RADIUS proxy can record user names and passwords for PAP connections. For this reason, the use of PAP is highly discouraged, especially for virtual private network connections.

Challenge Handshake Authentication Protocol

Challenge Handshake Authentication Protocol (CHAP) is designed to address the concern of passing passwords in plaintext. By using CHAP, the NAS sends a random number challenge to the user's computer. The challenge and the user's password are then hashed by using MD5. The client computer then sends the hash as a response to the NAS challenge and the NAS forwards both the challenge and response in the RADIUS Access-Request packet.

When the authenticating server receives the RADIUS packet, it uses the challenge and the user's password to create its own version of the response. If the version of the server matches the response supplied by the user's computer, the access request is accepted.

CHAP responses cannot be reused because NAS devices send a unique challenge each time a client computer connects to them. Because the algorithm for calculating CHAP responses is well known, it is very important that passwords be carefully chosen and sufficiently long. CHAP passwords that are common words or names are vulnerable to dictionary attacks if they can be discovered by comparing responses to the CHAP challenge with every entry in a dictionary. Passwords that are not sufficiently long can be discovered by brute force by comparing the CHAP response to sequential trials until a match to the user's response is found.

Historically, CHAP is the most common dial-up authentication protocol used. When the server does not store the same password that was used to calculate the CHAP response, it cannot calculate an equivalent response. Because standard CHAP clients use the plaintext version of the password to create the CHAP challenge response, passwords must be stored in plaintext on the server to calculate an equivalent response.

Although the IAS server supports CHAP, a Windows NT 4.0-based domain controller cannot validate CHAP requests without support for storing reversibly encrypted passwords. This support is available in Windows 2000; in Windows NT 4.0, this support is available through an update to the Windows NT 4.0-based domain controller.

Enabling CHAP

To enable CHAP-based authentication, you must do the following:

1. Enable CHAP as an authentication protocol on the remote access server. For information about a default setting on a particular NAS, see your NAS documentation. For the Routing and Remote Access service, CHAP is enabled by default.
2. Enable CHAP on the appropriate remote access policy. CHAP is enabled by default.
3. Enable storage of a reversibly encrypted form of the user's password. For a Windows 2000-based stand-alone server, use machine Group Policy to enable storage of reversibly encrypted passwords for all users of the computer. For Windows 2000 domains, Group Policy at the domain or Organizational Unit (OU) level can be used. For information about enabling reversibly encrypted passwords in a Windows 2000 domain, see Windows 2000 Server Help.
4. Force a reset of user's passwords so that the new password is in a reversibly encrypted form. When you enable passwords to be stored in a reversibly encrypted form, the current passwords are in a nonreversibly encrypted form and are not automatically changed. You must either reset user passwords or set user passwords to be changed the next time you log on. After the password is changed, it is stored in a reversibly encrypted form.

   If you set user passwords to be changed at the next attempt to log on, the user must log on using a LAN connection and change their password before they attempt to log on with a remote access connection using CHAP. CHAP does not support the changing of passwords during the authentication process and the logon attempt fails. One workaround for the remote access user is to temporarily log on using MS-CHAP to change their password.
5. Enable CHAP on the remote access client.

Microsoft Challenge Handshake Authentication Protocol

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is a variant of CHAP that does not require a plaintext version of the password on the authenticating server. In MS-CHAP the challenge response is calculated with an MD4 hashed version of the password and the NAS challenge. This enables authentication over the Internet to a Windows 2000 domain controller (or a Windows NT 4.0 domain controller on which the update has not been installed).

MS-CHAP passwords are stored more securely at the server but have the same vulnerabilities to dictionary and brute force attacks as CHAP. When using MS-CHAP, it is important to ensure that passwords are well chosen (not found in a standard dictionary) and long enough that they cannot be calculated readily. Many large customers require passwords to be at least six characters long with upper and lower case characters and at least one numeral.

See your NAS documentation, or consult your ISP to see whether the ISP currently supports MS-CHAP.

Note By default, MS-CHAP v1 for Windows 2000 supports LAN Manager authentication. If you want to prohibit the use of LAN Manager authentication with MS-CHAP v1 for older Microsoft operating systems such as Windows NT 3.5*x* and Windows 95, you must set Allow LM Authentication (HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \RemoteAccess\Policy) to 0 on the authenticating server.

If a user attempt authenticates using MS-CHAP using an expired password, MS-CHAP prompts the user to change the password while connecting to the server. Other authentication protocols do not support this feature effectively locking out the user who used the expired password.

Enabling MS-CHAP

To enable MS-CHAP-based authentication, you must do the following:

1. Enable MS-CHAP as an authentication protocol on the remote access server. MS-CHAP is enabled by default on the Routing and Remote Access service. For information about default settings on other NASs, see your NAS documentation.
2. Enable MS-CHAP on the appropriate remote access policy. MS-CHAP is enabled by default.
3. Enable MS-CHAP on a remote access client.

Microsoft Challenge Handshake Authentication Protocol Version 2

Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) provides mutual authentication, stronger initial data encryption keys, and different encryption keys for sending and receiving. For VPN connections, Windows 2000 servers offer MS-CHAP v2 before offering the legacy MS-CHAP. Updated Windows clients accept MS-CHAP v2 when it is offered.

MS-CHAP v2 is a one-way encrypted password, mutual authentication process that works as follows:

1. The remote access server sends a challenge to the remote access client that consists of a session identifier and an arbitrary challenge string.
2. The remote access client sends a response that contains:
   - The user name.
   - An arbitrary peer challenge string.
   - A one-way encryption of the received challenge string, the peer challenge string, the session identifier, and the user's password.
3. The remote access server checks the response from the client and sends back a response containing:
   - An indication of the success or failure of the connection attempt.
   - An authenticated response based on the sent challenge string, the peer challenge string, the encrypted response of the client, and the user's password.
4. The remote access client verifies the authentication response and, if correct, uses the connection. If the authentication response is not correct, the remote access client terminates the connection.

If a user authenticates by using MS-CHAP v2 and attempts to use an expired password, MS-CHAP prompts the user to change the password while connecting to the server. Other authentication protocols do not support this feature effectively locking out the user who used the expired password.

Enabling MS-CHAP v2

To enable MS-CHAP v2-based authentication, you must do the following:

1. Enable MS-CHAP v2 as an authentication protocol on the remote access server. MS-CHAP v2 is enabled by default on the Routing and Remote Access service. For information about default settings on other NASs, see your NAS documentation.
2. Enable MS-CHAP v2 on the appropriate remote access policy. MS-CHAP v2 is enabled by default.
3. Enable MS-CHAP v2 on the Windows 2000 remote access client.

Note Windows 95 and Windows 98 support MS-CHAP v2 only for virtual private network (VPN) connections. Windows 95 and Windows 98 do not support MS-CHAP v2 for dial-up connections.

Extensible Authentication Protocol

Extensible Authentication Protocol (EAP) is an extension to the Point-to-Point protocol (PPP) that works with dial-up, PPTP, and L2TP clients. EAP allows the addition of new authentication methods known as EAP types. Both the dial-in client and the remote access server must support the same EAP type for successful authentication to occur.

Windows 2000 includes an EAP infrastructure and two EAP types, EAP-MD5 CHAP and EAP-TLS. The IAS implementation in Windows 2000 has the ability to pass EAP messages to a RADIUS server (EAP-RADIUS).

EAP-MD5 CHAP

Message Digest 5 Challenge Handshake Authentication Protocol (EAP-MD5 CHAP) is a required EAP type that uses the same challenge-handshake protocol as PPP-based CHAP, but the challenges and responses are sent as EAP messages. A typical use for EAP-MD5 CHAP is to authenticate the credentials of remote access clients by using user name and password security systems. You can use EAP-MD5 CHAP to test EAP interoperability.

EAP-TLS

EAP-Transport Level Security (EAP-TLS) is an EAP type that is used in certificate-based security environments. If you are using smart cards for remote access authentication, you must use the EAP-TLS authentication method. The EAP-TLS exchange of messages provides mutual authentication, negotiation of the encryption method, and secured private key exchange between the remote access client and the authenticating server. EAP-TLS provides the strongest authentication and key exchange method. EAP-TLS is supported only on a remote access server that is running Windows 2000 and is a member of a Windows 2000 mixed or native domain.

EAP-RADIUS

EAP-RADIUS is not an EAP type, but the passing of EAP messages of any EAP type by a 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.

EAP-RADIUS is used in environments where RADIUS is used as the authentication provider. An advantage of using EAP-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-RADIUS, a remote access server is configured to use EAP and to use RADIUS as its authentication provider. When a connection 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. In this configuration, the remote access server is only a pass-through device. All processing of EAP messages occurs at the remote access client and the RADIUS server.

Enabling EAP

To enable EAP-based authentication, you must do the following:

1. Enable EAP as an authentication protocol on the remote access server.
2. Enable EAP; if needed, configure the EAP type on the appropriate remote access policy.
3. Enable and configure EAP on a remote access client.

In addition to the EAP types defined and supported in Windows 2000, new EAP authentication methods can be included through the use of EAP Software Development Kit.

Unauthenticated Access

The unauthenticated access method allows remote access users to log on without checking their credentials. For example, IAS does not verify the user's name and password. The only user validation performed in the unauthenticated access method is authorization. Enabling unauthenticated access presents security risks that must be carefully considered when deciding whether to enable this authentication method.

This section discusses three scenarios of unauthenticated access:

- Guest Access
- Dialed Number Identification Service (DNIS) authorization
- Automatic Number Identification/Calling Line Identification (ANI/CLI) authorization

Guest Access for PPP Users

Guest access is the ability to log on to a domain without a user name and/or a password. Both Routing and Remote Access service and IAS must be configured to support unauthenticated access.

When a remote access server receives a connection attempt, it negotiates with the user different authentication types enabled at the server. If the client accepts one of them, it sends the appropriate credentials for the accepted authentication type. It the user refuses authentication, Routing and Remote Access service checks its properties to verify if unauthenticated access is enabled and, if enabled, forwards the Access-Request packet to IAS. This Access-Request packet does not contain a User-Name attribute or any other credentials.

When IAS receives the packet without a User-Name attribute, it assumes that the user wants to dial in using guest access. In this case, IAS uses the name of the guest account in a domain as the user identity. It proceeds to evaluate policies in order to determine the right profile. If a match is found, and unauthenticated access is enabled in the profile, other authorizations are validated, and an Access-Accept packet is returned. The accounting log file logs the user identity and authentication type, which can be used to determine whether the user was logged on with guest access.

Enabling Guest Access

To enable Guest access, perform the following steps:

1. Enable unauthenticated access on the remote access server.
2. Enable unauthenticated access on the appropriate remote access policy.
3. Enable the Guest account.
4. Set the remote access permission on the Guest account to either **Allow access** or **Control access through Remote Access Policy** depending on your remote access policy administrative model.

If you do not want to enable the Guest account, create a user account and set the remote access permission to either **Allow access** or **Control access through Remote Access Policy**. Then set the **Default User Identity** registry value (HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \RemoteAccess \Policy) on the authenticating server (either the remote access server or the IAS server) to the name of the account.

For more information about enabling authentication protocols, configuring authentication, and enabling a disabled user account, see Windows 2000 Server Help.

Guest Access Example

1. During PPP negotiation, the dial-in client rejects all of the PPP authentication protocols of the NAS.
2. If the NAS is configured to allowed unauthenticated access, the NAS sends an Access-Request packet without the User-Name attribute and without a password. For the Windows 2000 Routing and Remote Access service, unauthenticated access is enabled from the **Authentication** tab on the properties of a server in the Routing and Remote Access snap-in.
3. Because the User-Name attribute is not included in the Access-Request packet and by default the IAS user identity is using the User-Name attribute, the user identity is set to Guest (or the value of Default User Identity).
4. With the user identity of Guest and an unauthenticated connection attempt, the authentication and authorization process as discussed earlier in the chapter is performed. If the connection attempt matches a policy whose profile settings have unauthenticated access enabled and the Guest account is enabled and has the appropriate remote access permission, IAS sends an Access-Accept packet to the NAS.

DNIS Authorization

Dialed Number Identification Service (DNIS) authorization is the authorization of a connection attempt based on the number called. This attribute is referred to as Called Station ID. DNIS is used by standard telecommunication companies. This service returns the number called to the called party. Based on the Called Station ID attribute, IAS can deliver different services to dial-up/remote access users.

Enabling DNIS Authorization

The following steps are required in order to enable DNIS authorization:

1. Enable unauthenticated access on the remote access server.
2. Create a remote access policy on the authenticating server (remote access server or IAS server) for DNIS-based authorization with the Called-Station-ID condition set to the phone number.
3. Enable unauthenticated access on the remote access policy for DNIS-based authorization.

ANI Authorization

ANI authorization is based on the number the user called from. This attribute is referred to as Calling Station ID, or Caller ID. Based on the Calling-Station-ID attribute, IAS can deliver different services to dial-up/remote access users.

Using ANI authorization is different from using the Caller ID dial-in property of a user account. ANI authorization is performed when the user does not type in any user name or password, and refuses to use any valid authentication method. In this case, IAS receives Calling-Station-ID, and no user name and password. To support ANI authorization, the Active Directory must have user accounts with Caller IDs as user names. This kind of authentication is used with the cellular phone authentication and by ISPs in Germany and Japan.

When using the Caller ID property on a user account, the user types in his credentials, such as a user name and password, and uses a valid authentication method to log on. IAS uses the user name and password to authenticate the user, and then compares the Calling-Station-ID attribute in the Access-Request to the Caller ID property of the user account as a way of authorizing the connection attempt.

Enabling ANI Authorization

1. Enable unauthenticated access on the remote access server.
2. Enable unauthenticated access on the appropriate remote access policy for ANI/CLI-based authentication.
3. Create a user account for each number calling, for which you want to provide ANI/CLI authorization. The name of the user account must match the number that the user is dialing from. For example, if a user is dialing in from 555-0100, create a "5550100" user account.
4. Set the **User Identity Attribute** registry value (HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services RemoteAccess\Policy) to 31 on the authenticating server.

This registry setting tells the authenticating server to use the calling number (RADIUS attribute 31, Calling-Station-ID) as the identity of the calling user. The user identity is set to the calling number only when there is no user name being supplied in the connection attempt.

To always use the calling number as the user identity, set the **Override User-Name** registry value:

HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \RemoteAccess\Policy

to 1 on the authenticating server.

However, if you set Override User-Name to 1 and the User Identity Attribute to 31, the authenticating server can perform only ANI/CLI-based authentication. Normal authentication by using authentication protocols such as MS-CHAP, CHAP, and EAP is disabled.

ANI Example

The following example explains how ANI/CLI authorization works for an dial-up client dialing in from the phone number 555-0100 and a user account called 5550100 exists.

1. During PPP negotiation, the dial-in client rejects all of the PPP authentication protocols of the NAS.
2. If the NAS is configured to allowed unauthenticated access, the NAS sends an Access-Request packet without the User-Name attribute and without a password. For the Windows 2000 Routing and Remote Access service, unauthenticated access is enabled from the **Authentication** tab on the properties of a server in the Routing and Remote Access snap-in.
3. Because the User-Name attribute is not included in the Access-Request packet and the IAS user identity is set to use the Calling-Station-ID attribute, the user identity is set to 5550100.
4. With the user identity of 5550100 and an unauthenticated connection attempt, the authentication and authorization process as discussed earlier in the chapter is performed. If the connection attempt matches a policy whose profile settings have unauthenticated access enabled and the 550100 account has the appropriate remote access permission, IAS sends an Access-Accept packet to the NAS.

IAS Authorization

An administrator can use the authorization feature of IAS to allow or deny connection attempts that are based on the connection parameters. The following sections include in-depth information about configuring remote access policies and vendor-specific attributes.

Remote Access Policies

In Windows NT 4.0, remote access privileges were granted based solely on a dial-in permission assigned to a user. In Windows 2000, remote access connections are granted based on the dial-in properties of a user object and remote access policies. Remote access policies are a set of conditions and connection parameters that administrators can use to get more flexibility in granting remote access permissions and usage. Remote access policies are stored on the local computer and are shared between the Routing and Remote Access service and IAS.

By using remote access policies, an administrator can specify remote access permissions by the time of day and day of the week, by the Windows 2000 group to which the remote access user belongs, by the type of connection being requested (dial-in or virtual private network connection), and so on. You can configure settings that limit the maximum session time, specify the authentication and encryption methods, set Bandwidth Allocation Protocol (BAP) policies, and so on.

It is important to remember that a remote connection is accepted only if the settings of the connection attempt match at least one of remote access policies (subject to the conditions of the dial-in properties of the user object and the profile properties of the remote access policy). If the settings of the connection attempt do not match at least one of the remote access policies, the connection attempt is rejected regardless of the dial-in properties of the user account.

For Windows 2000 IAS servers, remote access policies are administered from the Routing and Remote Access administrative tool (when configured for Windows authentication) or the Internet Authentication Service administrative tool.

Note Windows 2000 supports customized authorization through the use of the Software Development Kit.

Local vs. Centralized Policy Management

Because remote access policies are stored locally on either a remote access server or an IAS server, for centralized management of a single set of remote access policies for multiple remote access or VPN servers, you must do the following steps:

1. Install the Windows 2000 Internet Authentication Service (IAS) as a Remote Authentication Dial-In User Service (RADIUS) server on a computer.
2. Configure IAS with RADIUS clients that correspond to each of the Windows 2000 remote access or VPN servers.
3. On the IAS server, create the central set of policies that all Windows 2000 remote access servers are using.
4. Configure each of the Windows 2000 remote access servers as a RADIUS client to the IAS server.

After you configure a Windows 2000 remote access server as a RADIUS client to an IAS server, the local remote access policies stored on the remote access server are no longer used.

Centralized management of remote access policies are also used when you have remote access servers that are running Windows NT 4.0 with the Routing and Remote Access Service (RRAS). You can configure the server that is running Windows NT 4.0 with RRAS as a RADIUS client to an IAS server. You cannot configure a remote access server that is running Windows NT 4.0 without RRAS to take advantage of centralized remote access policies.

Dial-in Properties of a User Object

In Windows 2000, the user object for a stand-alone or Active Directory-based server contains a set of dial-in properties that are used when allowing or denying a connection attempt made by a user. For a stand-alone server, the dial-in properties are available on the **Dial-in** tab of the user object in the local User Manager. For an Active Directory-based server, the dial-in properties are available on the **Dial-in** tab of the user object in Active Directory Users and Computers snap-in. The Windows NT 4.0 User Manager for Domains administrative tool cannot be used for Active Directory-based servers.

The dial-in properties for a user object are the following:

- Remote Access Permission (Dial-in or VPN)

  Use this property to set whether remote access is explicitly allowed, denied, or determined through remote access policies. If access is explicitly allowed, remote access policy conditions or user object or profile properties can override the setting. The **Control access through Remote Access Policy** option is available only on user objects for stand-alone Windows 2000 Routing and Remote Access service servers or members of a native Windows 2000 domain.

  By default, the Administrator and Guest accounts on a stand-alone remote access server or in a Windows 2000 native-mode domain are set to **Control access through Remote Access Policy** and for a Windows 2000 mixed-mode domain are set to **Deny access**. New accounts created on a stand-alone remote access server or in a Windows 2000 native-mode domain are set to **Control access**

through Remote Access Policy. New accounts created in a Windows 2000 mixed-mode domain are set to **Deny access**.

- Verify Caller ID

  If this property is enabled, the server verifies the caller's phone number. If the caller's phone number does not match the configured phone number, the connection attempt is denied.

  Caller ID must be supported by the caller, the phone system between the caller and the Routing and Remote Access service server, as well as by the Routing and Remote Access service server. Caller ID on the Routing and Remote Access service server consists of call answering equipment that supports the passing of Caller ID information and appropriate driver inside Windows 2000 that support the passing of Caller ID information to the Routing and Remote Access service.

  If you configure a Caller ID phone number for a user and you do not have support for the passing of Caller ID information all the way from the caller to the Routing and Remote Access service, the connection attempt is denied.

- Callback Options

  If this property is enabled, the server calls the caller back during the connection establishment at a phone number set by the caller or a specific phone number set by the administrator.

- Assign a Static IP Address

  If this property is enabled, the administrator assigns a specific IP address to the user when the connection is made.

- Apply Static Routes

  If this property enabled, the administrator defines a series of static IP routes that are added to the routing table of the remote access server when a connection is made. This setting is designed for user accounts that Windows 2000 routers use for demand-dial routing.

If a Windows 2000 Routing and Remote Access service server is a member of a Windows NT 4.0 domain or a Windows 2000 mixed domain, then:

- Only the Remote Access Permission (Allow access and Deny access options) and Callback Options dial-in properties are available.
- The User Manager for Domains administrative tool can be used to grant or deny dial-in access and set callback options.

If the Windows 2000 Routing and Remote Access service server is a stand-alone server or a member of a Windows 2000 native domain, the callback number can be of unlimited size. If a Windows 2000 Routing and Remote Access service server is a member of a Windows NT 4.0 domain or a Windows 2000 mixed domain, the callback number can only be 128 characters long. Callback numbers that are long than 128 characters are truncated during a callback connection attempt, which results in a failed callback connection.

When a Windows NT 4.0 RAS server uses a native 2000 domain to obtain the dial-in properties of a user account, the **Control access through Remote Access Policy** option is interpreted as **Deny access**. Callback settings are interpreted correctly.

User accounts upgraded to Windows 2000 that were configured with dial-in permission enabled are set to **Allow access**. User accounts upgraded to Windows 2000 that were configured with dial-in permission disabled are set to **Control access through Remote Access Policy**.

A Windows NT 4.0 RAS server does not use remote access policies. It is recommended that you upgrade Windows NT 4.0 RAS servers to take advantage of remote access policies.

Elements of a Remote Access Policy

A remote access policy is a named rule that consists of the following elements:

Conditions

Remote access policy conditions are one or more attributes that are compared to the settings of the connection attempt. If there are multiple conditions, all of the conditions must match the settings of the connection attempt in order for the connection attempt to match the policy.

Table 8.3 shows the condition attributes that you can set for a remote access policy.

Table 8.3 Condition Attributes for a Remote Access Policy

Attribute Name	Description
NAS IP Address	The IP address of the network access server (NAS). This attribute is a character string. You can use pattern matching syntax to specify IP networks. This attribute is designed for the IAS server.
Service Type	The type of service being requested. Examples include framed (such as PPP connections) and login (such as Telnet connections). For more information about RADIUS service types, see RFC 2138. This attribute is designed for the IAS server.
Framed Protocol	The type of framing for incoming packets. Examples are PPP, AppleTalk, SLIP, Frame Relay, and X.25. This attribute is designed for the IAS server.
Called Station ID	The phone number of the NAS. This attribute is a character string. You can use pattern matching syntax to specify area codes. In order to receive called station ID information during a call, the phone line, the hardware, and the Windows 2000 driver for the hardware must support the passing of the called ID. Otherwise, the called station ID is manually set for each port.
Calling Station ID	The phone number used by the caller. This attribute is a character string. You can use pattern matching syntax to specify area codes.
NAS Port Type	The type of media used by the caller. Examples are analog phone lines (also known as "asynch"), ISDN, and tunnels or virtual private networks (known as virtual).
Day and Time Restrictions	The day of the week and the time of day of the connection attempt of the server.
Client IP Address	The IP address of the network access server (the RADIUS client). This attribute is a character string. You can use pattern matching syntax to specify IP networks. This Attribute is designed for the IAS server.
NAS Manufacturer	The vendor of NAS requesting authentication. The Windows 2000 remote access server is the Microsoft RAS NAS manufacturer. You can use this Attribute to configure separate policies for different NAS manufacturers who are RADIUS clients to an IAS server. This Attribute is designed for the IAS server.
Client Friendly Name	The name of the RADIUS client computer that is requesting authentication. This Attribute is a character string. You can use pattern matching syntax to specify client names. This Attribute is designed for the IAS server.

Windows Groups	The names of the Windows groups to which the user attempting the connection belongs. There is no condition attribute for a specific user name. It is not necessary to have a separate remote access policy for each group. Instead, you can use nested groups to consolidate group membership and delegate administration of group membership. For a Windows 2000 native mode domain-based remote access or IAS server, it is recommended that you use universal groups.
Tunnel Type	The type of tunnel being created by the requesting client. Tunnel types include the Point-to-Point Tunneling Protocol (PPTP) and the Layer Two Tunneling Protocol (L2TP) used by Windows 2000 remote access clients and demand-dial routers. You can use this condition to specify profile settings such as authentication methods or encryption strengths for a specific type of tunneling technology.

Note If conditions that use an Attribute designed for the IAS server are evaluated against a remote access server connection attempt, the result is no match and the policy is not applied.

Not all network access servers send all of the IAS server-specific attributes.

You cannot use the built-in local groups of a stand-alone remote access server that is running Windows 2000 for the Windows Groups attribute.

Remote Access Permission

If all the conditions of a remote access policy are met, remote access permission is either granted or denied. Use the **Grant remote access permission** option or the **Deny remote access permission** option to set remote access permission for a policy.

Remote access permission is also granted or denied for each user account. The user remote access permission overrides the policy remote access permission. When remote access permission on a user account is set to the **Control access through Remote Access Policy** option, the policy remote access permission determines whether the user is granted access.

Granting access through the user account permission setting or the policy permission setting is only the first step in accepting a connection. The connection attempt is then subjected to the settings of the user account properties and the policy profile properties. If the connection attempt does not match the settings of the user account properties or the profile properties, the connection attempt is rejected.

By default, the **Deny remote access permission policy** permission is selected.

Profile

A remote access policy profile is a set of properties that are applied to a connection when the connection is granted remote access permission, either through the user account permission setting or the policy permission setting. A profile consists of the following groups of properties:

- Dial-in constraints
- IP
- Multilink
- Authentication
- Encryption
- Advanced

Dial-In Constraints

You can set the following dial-in constraints:

- Idle disconnect time

  The time after which a connection is disconnected when there is no activity. By default, this property is not set and the remote access server does not disconnect an idle connection.

- Maximum session length

  The maximum amount of time that a connection is connected. The connection is disconnected by the remote access server after the maximum session length. By default, this property is not set and the remote access server has no maximum session limit.

- Day and time limits

  The days of the week and hours of each day that a connection is allowed. If the day and time of the connection attempt do not match the configured day and time limits, the connection attempt is rejected. By default, this property is not set and the remote access server has no day or time limits. The remote access server does not disconnect active connections that are connected at a time when connection attempts are not allowed.

- Dial-in number

  The specific phone number that a caller must call for a connection to be allowed. If the dial-in number of the connection attempt does not match the configured dial-in number, the connection attempt is rejected. By default, this property is not set and the remote access server allows all dial-in numbers.

- Dial-in media

  The specific types of media, such as modem (known as asynch), ISDN, or virtual private network (known as virtual) that a caller must use for a connection to be allowed. If the dial-in medium of the connection attempt does not match the configured dial-in media, the connection attempt is rejected. By default, this property is not set and the remote access server allows all dial-in media types.

IP

You can set IP properties to specify whether a particular IP address for a connection can be requested by the client. By default, the remote access server automatically allocates an IP address and the client is not allowed to request a specific IP address.

You can also use the IP properties to define remote access policy profile filtering. To define the allowed traffic across the connection after the connection had been made, you can configure IP packet filters for remote access policy profiles. You can use profile packet filters to configure IP traffic that is allowed out of the connection (to client) or into the connection (from client) on an exception basis: either all traffic except traffic specified by filters or no traffic except traffic specified by filters. Remote access policy profile filtering applies to all connections that match the remote access policy.

Multilink

You can set Multilink properties that enable Multilink and determine the maximum number of ports that a Multilink connection can use. Additionally, you can set Bandwidth Allocation Protocol (BAP) policies that determine BAP usage and when extra BAP lines are dropped. The Multilink and BAP properties are specific to Microsoft Windows 2000 remote access. By default, Multilink and BAP are disabled.

The remote access server must have Multilink and BAP enabled in order for the Multilink properties of the profile to be enforced.

Authentication

You can set authentication properties to enable the types of authentication that are allowed for a connection and specify the EAP type that must be used. Additionally, you can configure the EAP type. By default, **Microsoft Encrypted Authentication (MS-CHAP)** and **Microsoft Encrypted Authentication version 2 (MS-CHAPv2)** are enabled.

The remote access server must have the corresponding authentication types enabled in order for the authentication properties of the profile to be enforced.

Encryption

You can set encryption properties for the following encryption strengths:

- No Encryption

  When selected, this option allows an unencrypted connection. To require encryption, clear the **No Encryption** option.
- Basic

  For dial-up and PPTP-based VPN connections, Microsoft Point-to-Point Encryption (MPPE) with a 40-bit key is used. For L2TP over IPSec-based VPN connections, 40-bit DES encryption is used.
- Strong

  For dial-up and PPTP-based VPN connections, MPPE with a 56-bit key is used. For L2TP over IPSec-based VPN connections, 56-bit DES encryption is used.
- Strongest

  For dial-up and PPTP-based VPN connections, MPPE with a 128-bit key is used. For L2TP over IPSec-based VPN connections, triple DES (3DES) encryption is used.

Advanced

You can set advanced properties to specify the series of RADIUS Attributes that are sent back to the RADIUS client by the IAS server. RADIUS Attributes are specific to performing RADIUS authentication and are ignored by the remote access server. By default, Framed-Protocol is set to PPP and Service-Type is set to Framed.

The only attributes that are used by the remote access server are **Account-Interim-Interval**, **Framed-Protocol**, **Framed-MTU**, **Reply-Message**, and **Service-Type**.

Default Remote Access Policy

A default remote access policy named **Allow access if dial-in permission is enabled** is created. The default policy has the following configuration:

- The Day-and-Time-Restrictions condition is set to all times and all days.
- Permission is set to Deny remote access permission.
- All profile properties are set to default values.

Note Elements of a remote access policy correspond to RADIUS attributes that are used during RADIUS-based authentication. For an IAS server, verify that the network access servers that you use are sending the RADIUS attributes that correspond to the configured remote access policy conditions and profile settings. If a NAS does not send a RADIUS attribute that corresponds to a remote access policy condition or profile setting, all RADIUS authentications from that NAS are denied.

Vendor Profiles

Some vendors use vendor-specific attributes (VSAs) to provide functionality that is not supported in standard attributes. IAS enables you to create or modify vendor-specific attributes to take advantage of the proprietary functionality that is supported by some NAS vendors.

If you need to configure more than one VSA for a specific profile, you must arrange them in the appropriate order. If you are using filters and the order of the filters is important, use the arrow buttons to rearrange the attributes.

Example 1

The following example demonstrates the procedure of adding a Cisco VSA to a profile. The example illustrates only the mechanism of adding a standard-conforming VSA to a profile. Cisco VSAs are readily available through the IAS multi-vendor dictionary.

Cisco vendor-specific attributes conform to the RADIUS RFC for Vendor-Specific Attributes (type 26). The following information is for a Cisco attribute to specify a primary DNS server:

- Vendor ID: 9. This is the unique ID for Cisco. When you specify that vendor, this is automatically supplied.
- Vendor Type: 1. This is the vendor-type number for vendor-specific attributes that take the attribute-value pair form, referred to in Cisco documentation as "cisco-avpair."
- Data Type: String.
- Format: If the attribute is mandatory, the format is: <protocol>: attribute=value

If the attribute is optional, the attribute-value pair is separated by an asterisk (*) instead of an equal sign (=). In this example, <protocol> is a value of the Cisco "protocol" attribute for a particular type of authorization. "Attribute" and "value" represent an appropriate attribute/value (AV) pair defined in the Cisco TACACS+ specification. This allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

The Cisco attribute used to specify a primary DNS server appears as follows:

```
ip:dns-servers=10.10.10.10
```

To add the vendor-specific attribute to a dial-in profile

1. In IAS, click **Remote Access Policies**.
2. Right-click the policy for which you want to configure a vendor-specific attribute, and then click **Properties**.
3. Click **Edit Profile**, click the **Advanced** tab, and then click **Add**.
4. In the list of available RADIUS attributes, double-click **Vendor-Specific**.
5. Click **Add**.
6. In **Network access server vendor**, click **Cisco**.

7. Click **Yes, It conforms**, and then click **Configure Attribute**. In **Vendor-assigned attribute number**, type **1**.
8. In **Attribute format**, click **String**.
9. In **Attribute value**, type the following:

   ip:dns-servers=10.10.10.10

Example 2

The following example demonstrates how to add a 3Com/U.S. Robotics VSA to a profile.

Note Example 2 is included only to illustrate the mechanism of adding a standard nonconforming VSA to a profile. 3Com/U.S. Robotics VSAs are readily available through the IAS multivendor dictionary.

U.S. Robotics vendor-specific attributes do not conform to the recommended format for Vendor-Specific Attributes (type 26) in RADIUS RFC 2138. Therefore, all U.S. Robotics VSAs must be entered in hexadecimal format.

The following information is for a U.S. Robotics attribute to specify a primary DNS/NBNS server:

- Vendor ID: 429. This is the unique ID for U.S. Robotics. When you specify that vendor, this ID is automatically supplied.
- Indicator: 0x900F
- Data Type: String
- Format: The VSA must be entered in hexadecimal format.

To specify an IP address of 10.10.10.10 for a primary DNS/NBNS server

1. In IAS, click **Remote Access Policies.**
2. Right-click the policy for which you want to configure a vendor-specific attribute, and then click **Properties.**
3. Click **Edit Profile**, click the **Advanced** tab, and then click **Add.**
4. In the list of available RADIUS attributes, double-click **Vendor-Specific**, and then click **Add.**
5. Click **Select** from the list, and then click **US Robotics.**
6. Click **No**. It does not conform, and then click **Configure Attribute.**
7. In Hexadecimal attribute value, type the following:

   0x900f31302e31302e31302e31302e

For more information about the proprietary attributes of U.S. Robotics, see your U.S. Robotics documentation.

Accepting a Connection Attempt

When a user attempts a connection, the connection attempt is accepted or rejected based on the following:

1. The first policy in the ordered list of remote access policies is checked. If there are no policies, reject the connection attempt.
2. If all the conditions of the policy do not match the connection attempt, go to next policy. If there are no more policies, reject the connection attempt.
3. If all the conditions of the policy match the connection attempt, check the remote access permission setting for the user attempting the connection. For example:
   - If **Deny access** is selected, reject the connection attempt.
   - If **Allow access** is selected, apply the user account properties and profile properties.
   - If the connection attempt does not match the settings of the user account properties and profile properties, reject the connection attempt.
   - If the connection attempt matches the settings of the user account properties and profile properties, accept the connection attempt.
   - If the remote access permission is not set to **Allow access** or **Deny access**, the remote access permission must be set to **Control access through Remote Access Policy**. Therefore, check the remote access permission setting of the policy.
   - If **Deny remote access permission** is selected, reject the connection attempt.
   - If **Grant remote access permission** is selected, apply the user account properties and profile properties.
   - If the connection attempt does not match the settings of the user account properties and profile properties, reject the connection attempt.
   - If the connection attempt matches the settings of the user account properties and profile properties, accept the connection attempt.

Remote Access Policy Administrative Models

In Windows 2000, there are three primary models for administering remote access permissions and connection settings:

- Access by user.
- Access by policy in a Windows 2000 native-mode domain.
- Access by policy in a Windows 2000 mixed-mode domain.

Access by User

In the access-by-user administrative model, remote access permissions are determined by the remote access permission on the **Dial-in** tab of the user account. You enable or disable remote access permission on a per-user basis by setting the remote access permission to either **Allow access** or **Deny access**.

The remote access permission setting on the remote access policy is effectively overridden if the user account's remote access permission is set to either **Allow access** or **Deny access**. However, you can modify remote access policy conditions and profile properties to enforce connection settings, such as encryption requirements and idle time-outs.

You can administer access-by-user remote access with multiple remote access policies. Each remote access policy has its own profile settings. You must configure these settings carefully because a connection attempt might be rejected even when the remote access permission on the user account is set to **Allow access**. If a connection attempt matches the conditions of a policy but does not match the profile settings or does not match any of the remote access policies, the connection attempt is rejected.

In the access-by-user administrative model, you can control three behaviors:

- Explicit allow

  The remote access permission for the user account is set to Allow access and the connection attempt matches the conditions of a policy subject to the settings of the profile and the dial-in properties of the user account.

- Explicit deny

  The remote access permission for the user account is set to Deny access.

- Implicit deny

  The connection attempt does not match the conditions of any remote access policies.

In Windows 2000, the access-by-user administrative model is equivalent to administering remote access on a Windows NT 4.0 RAS server.

You can use the access-by-user administrative model on a stand-alone remote access server, a remote access server that is a member of a Windows 2000 native-mode domain, a remote access server that is a member of a Windows 2000 mixed-mode domain, or a remote access server that is a member of a Windows NT 4.0 domain. You can also use the access-by-user administrative model if you have Windows NT 4.0 RAS or IAS servers.

Access by Policy in a Windows 2000 Native-Mode Domain

In the access-by-policy administrative model for a Windows 2000 native-mode domain, the remote access permission on every user account is set to **Control access through Remote Access Policy** and remote access permissions are determined by the remote access permission setting on the remote access policy. Therefore, the remote access permission setting on the remote access policy determines whether remote access permission is allowed or denied.

In the access-by-policy administrative model for a Windows 2000 native-mode domain, you can control three behaviors:

- Explicit allow

  The remote access permission on the remote access policy is set to **Grant remote access permission** and the connection attempt matches the conditions of the policy subject to the settings of the profile and the dial-in properties of the user account.

- Explicit deny

  The remote access permission on the remote access policy is set to **Deny remote access permission** and the connection attempt matches the conditions of the policy.

- Implicit deny

  The connection attempt does not match the conditions of any remote access policies.

If you use this administrative model and do not add any remote access policies and do not change the default remote access policy (named **Allow access if dial-in permission is enabled**), no users are allowed remote access. By default, the remote access permission on the default remote access policy is set to **Deny remote access permission**. If you change the setting to **Grant remote access permission**, all users are allowed remote access.

The access-by-policy administrative model for a Windows 2000 native-mode domain also applies to stand-alone remote access servers that are not a member of a domain.

You cannot use the access-by-policy administrative model for a Windows 2000 native-mode domain if you have Windows NT 4.0 RAS or IAS servers.

If you use the access-by-policy administrative model for a Windows 2000 native-mode domain and do not use groups to specify which users get access, verify that the Guest account is disabled and its remote access permission is set to **Deny access**.

Access by Policy in a Windows 2000 Mixed-Mode Domain

In the access-by-policy administrative model for a Windows 2000 mixed-mode domain, the remote access permission on every user account is set to **Allow access**, the default remote access policy is deleted, and separate remote access policies are created to define the types of connections that are allowed. On a remote access server that is running Windows 2000 that is a member of a Windows 2000 mixed-mode domain, the **Control access through Remote Access Policy** option is not available for remote access permission on the user account. If a connection attempt matches the conditions of a policy subject to the profile and user account dial-in settings, the connection is accepted.

This administrative model also applies to a remote access server that is running Windows 2000 that is a member of a Windows NT 4.0 domain.

In the access-by-policy administrative model for a Windows 2000 mixed-mode domain, you can control three behaviors:

- Explicit allow

  The connection attempt matches the conditions of a policy subject to the settings of the profile and the dial-in properties of the user account.

- Explicit deny

  The connection attempt matches the conditions of a policy but not the settings of the profile. You can do an explicit deny in this administrative model by enabling the **Restrict Dial-in to this number only** dial-in constraint and typing a number that does not correspond to any dial-in number being used by the remote access server.

- Implicit deny

  The connection attempt does not match the conditions of any remote access policies.

If you do not delete the default remote access policy named **Allow access if dial-in permission is enabled**, all users can obtain a remote access connection.

If you have Windows NT 4.0 Routing and Remote Access service (RRAS) servers, you can use the access-by-policy only in a Windows 2000 mixed-mode domain administrative model if the RRAS servers are configured as RADIUS clients to a Windows 2000 IAS server. You cannot use the access-by-policy in a Windows 2000 mixed-mode domain administrative model for Windows NT 4.0 RAS servers.

Note The administrative models described here are recommended ways of controlling remote access. You can administer remote access through a mixture of these models. However, you must do so carefully to produce the intended results. Improper configuration might lead to connection attempts that are rejected when they must be accepted and connection attempts that are accepted when they must be rejected. To troubleshoot these complex configurations, you can apply the logic the remote access server uses when processing connection attempts or enable authentication logging and check the authentication log.

For more information about remote access policies and scenarios using remote access policies, see Windows 2000 Server Help.

IAS Accounting

The following section describes IAS accounting features, as well as different formats of the IAS log file.

RADIUS Accounting

IAS supports RADIUS Accounting, which an administrator can use to track network usage for auditing and billing purposes. RADIUS Accounting provides the following benefits:

- Real-time data collection.
- Accounting data can be collected at the centralized place.
- Third-party products can be used to analyze RADIUS accounting data to provide charge-back, performance, and exception reports.

When a client is configured to use RADIUS Accounting, at the start of service delivery it generates an Accounting Start packet describing the type of service being delivered and the user it is being delivered to. The packet is then sent to the RADIUS Accounting server, which sends back an acknowledgment that the packet has been received. At the end of service delivery, the client generates an Accounting Stop packet describing the type of service that was delivered and statistics (optional), such as elapsed time, input and output octets, or input and output packets. It then sends that data to the RADIUS Accounting server, which sends back an acknowledgment that the packet has been received.

The Accounting-Request packet (whether for the Start or Stop packet) is submitted to the RADIUS accounting server through the network. If no response is returned within a length of time, the request is re-sent a number of times. The client can also forward requests to an alternate server or servers in the event that the primary server is down or unreachable. An alternate server can be used either after a number of tries to the primary server fail, or in a round-robin fashion. If the RADIUS accounting server is unable to successfully record the accounting packet, it does not send an Accounting-Response acknowledgment to the client. For example, when the log file gets filled up, IAS starts discarding accounting packets. This prompts the NAS to switch to the backup IAS server.

IAS Log File

IAS can create a log file based on the data returned by the network access servers. This information is useful for keeping track of usage and correlating authentication information with accounting records (for example, to discover missing records or instances of over-billing).

IAS supports two formats of the log file: IAS format and database.

Database format allows you to keep track of a predetermined set of attributes, and IAS format is more detailed and can contain information about all attributes.

Use database format if you want to import the data directly into a database. The IAS format can be used if you need to record more detailed information than the database log format allows.

Note The IAS log file contains all the IAS user-related events. IAS service and system-related events are recorded in the Event log files.

IAS Authentication and Windows Domain Modes

This section concentrates on IAS authentication features and behavior in different Windows domain modes. The information is useful when making decision about a particular domain mode in which IAS is deployed.

IAS is capable of authenticating access requests received through the RADIUS protocol against Windows 2000 native mode domains, Windows 2000 mixed-mode domains, Windows NT 4.0 domains, or Windows 2000 local accounts database for a stand-alone IAS server. The IAS authentication features and capabilities available to administrators depends on a mode of a particular domain against which the users authenticate.

Windows 2000 Native-Mode Domains

Windows 2000 native mode provides the most flexibility in managing remote access through groups. From the remote access management perspective, the following benefits are available in the native mode domain:

- Full ability to manage remote access permissions through groups. An administrator can use the universal group feature to create a single policy for users in different domains. Nested groups can be used to organize extremely large numbers of users into smaller groups for better management.
- An ability to connect remote network to office network. You can specify routes for the remote network through Static Routes.
- Support for User Principal Names (UPNs).
- End users can have the same UPN regardless of what domain the user belongs to. This indirection provides scalability that might be required in organizations that have large number of domains.

The following is a detailed list of authentication and remote management features available for an IAS server that is a member of a Windows 2000 native domain.

- Dial-in User Account Properties
  - All Remote Access Permissions, including Allow access, Deny access, and Control access through Remote Access Policy
  - Caller-ID
  - Callback Options
  - Static IP Address
  - Static Routes
- Support for UPNs and Universal Groups
- Support for EAP-TLS

In order for the IAS server to access user account dial-in properties stored in Active Directory, IAS must run in the security context of a computer account that is a member of the **RAS and IAS Servers** security group. This assignment can be implemented through the Active Directory Users and Computers snap-in or by registering the IAS server in the Internet Authentication Service snap-in. You can also use the **netsh ras add registeredserver** command.

Windows 2000 Mixed-Mode Domains or Windows NT 4.0 Domains

Windows 2000 mixed-mode domains are mainly used for migration from Windows NT 4.0 to Windows 2000. For IAS, a mixed-mode domain acts exactly like a Windows NT 4.0 domain.

For an IAS server that is a member in a Windows 2000 mixed-mode domain, the following authentication and remote access management features are available:

- Dial-in User Account Properties
  - Remote Access Permissions include only Allow access and Deny access

    Missing the "Control access through Remote Access Policy" option makes it more difficult to use groups with Policy-based management because the user's remote access permission overrides remote access policy permissions. For more information about managing through policy in a mixed-mode domain, see "Remote Access Policies" earlier in this chapter.
  - Callback options

Just as in Windows 2000 native mode domains, in order for the IAS server to access user account dial-in properties stored in Active Directory, the Internet Authentication service must run in the security context of a computer account that is a member of the **RAS and IAS Servers** security group. This assignment can be implemented through the Active Directory Users and Computers or by registering the IAS server in the Internet Authentication Service snap-in. You can also use the **netsh ras add registeredserver** command.

If IAS is a member of Windows NT 4.0 domain but has to authenticate users against a trusted Active Directory domain, it is not able to gain access to Active Directory because its computer account cannot become a member of the RAS and IAS Servers security group. In this case, verify that the Everyone group is added to the Pre-Windows 2000 Compatible Access group with the **net localgroup** "**Pre-Windows 2000 Compatible Access**" command. If not, issue the **net localgroup** "**Pre-Windows 2000 Compatible Access**" **everyone /add** command on a domain controller computer and then restart the domain controller computer.

Windows 2000 Stand-Alone Servers

Windows 2000 stand-alone servers can be used in very small networks with no domains. All the users need to be defined in the local accounts database of a stand-alone server.

The following authentication features are available for granting remote access permissions to an IAS server on a Windows 2000 stand-alone server:

- Dial-in User Account Properties
  - Remote Access Permission (includes Allow access, Deny access, and Control access through Remote Access Policy)
  - Caller-ID
  - Callback Options
  - Static IP Address
  - Static Routes

Support for UPNs, Universal Groups, and EAP-TLS is not available in IAS running on a stand-alone Windows 2000 server.

User account dial-in properties can be administered through the Network and Dial-Up Connections folder or through Local Users and Groups.

Behavior Differences Between Windows 2000 and Windows NT 4.0 IAS

A previous version of IAS was released with the Windows NT 4.0 Option Pack. The following section describes the differences in behavior between the two versions.

Windows NT 4.0 IAS Behavior

- If no domain name is specified during authentication, the IAS server authenticates the user against only the local SAM database.
- IAS does not use the callback permissions for all user objects. IAS
- IAS log files are written in ASCII.

Windows 2000 IAS Behavior

- IAS resolves a user name with no domain specified by using the following sequence:
  1. IAS determines a default domain from the registry, if one is specified there.
  2. If the IAS server is a member of a domain, IAS authenticates the user against that domain.
  3. If the IAS server is not a member of a domain, IAS authenticates the user against the local SAM database.
- IAS uses the callback permissions for all user objects.
- IAS log files are multi-language and are written in UTF-8.

Security Considerations

This section covers possible IAS security-related issues and recommendations on how to overcome them.

RADIUS Proxy Security Issues

It is not anticipated that a particular named user would be authenticated by multiple methods. This would make the user vulnerable to attacks that negotiate the least secure method from among a set. Instead, for each named user, there must be an indication of exactly one method used to authenticate that user name. If a user needs to make use of different authentication methods under different circumstances, distinct user names must be employed, each of which identifies exactly one authentication method. Passwords and other secrets must be stored at the respective ends, such that access to them is as limited as possible.

Ideally, the secrets must be accessible only to the process requiring access, in order to perform the authentication. The secrets must be distributed with a mechanism that limits the number of entities that handle (and gain knowledge of) the secret. Ideally, no unauthorized person must ever gain knowledge of the secrets.

Firewall Protection

A firewall provides additional security and protection to the services that are running on any operating system. The firewall might be a Windows NT-based or Windows 2000-based computer with the Proxy Server, or a third-party firewall package. The firewall can run on the same computer as the IAS server.

One option is to use the Proxy Server to hide the IP address of the server. In this way, the proxy IP address is exposed as the IAS address. You can also use a third-party firewall and enable the UDP traffic for the IAS server only for those ports used by the RADIUS server. For more security, allow traffic to come in only from specific IP Addresses, of NAS or RADIUS proxy, to the RADIUS server.

Remote Access Account Lockout

You can use the remote access account lockout feature to specify how many times an remote access authentication fails against a valid user account before future connection attempts using the user account name are denied. For more information about remote access account lockout, see "Remote Access Server" in this book.

Performance Tuning and Optimization

This section contains recommendations on IAS performance fine-tuning and monitoring. It also includes sample performance information that can be helpful in determining your IAS server performance and health conditions.

Consider the following points when fine-tuning the performance of an IAS server.

- If IAS authenticates users against a Windows 2000-based domain controller that is running in native mode, the domain controller should also contain the Global Catalog.
- High latency connections between the NAS and IAS server, or IAS server and the domain controller, can negatively impact authentication times, and cause retries and time-outs.

In very large ISP environments (millions of remote access users) with extremely heavy load conditions, where a large number of authentication requests, as well as accounting packets are being handled within seconds, the following items must be considered:

- As a general rule of thumb, number of authentications/second you get would depend on the hardware used for the domain controller. A faster domain controller should yield a better throughput.

- Consider using separate IAS servers for authentication and accounting.
- Consider running the IAS server on a domain controller with a Global Catalog. This would minimize network latency and would improve throughput.
- To achieve better throughput, use a registry entry to tune the number of concurrent authentication calls in progress at one time, between the IAS server and the domain controller. For information about registry entry details, see Windows 2000 Server Help.
- An administrator can deploy multiple IAS servers and use Windows Load Balance Service to point NASs to a single IP address representing a pool of IAS servers.

Monitoring Performance and Health of the IAS Server

The RADIUS authentication protocol distinguishes between the client function and the server function. In RADIUS authentication, clients send Access-Request packets, and servers reply with Access-Accept, Access-Reject, and Access-Challenge packets. Typically, NAS devices perform the client function and implement the RADIUS authentication client MIB, and RADIUS authentication servers perform the server function and implement the RADIUS authentication server MIB.

The two most commonly used counters for IAS performance monitoring are:

- Access Requests/sec
- Accounting Requests/sec

The most common counters used for health monitoring are described in the following section.

For more information about SNMP MIBs supported by IAS, see "Simple Network Management Protocol Service" in the *TCP/IP Core Networking Guide*.

Troubleshooting

The following sections provide information about troubleshooting for IAS installation and configuration problems, including common IAS problems reported from the field, and about advanced troubleshooting with Network Monitor traces.

Troubleshooting IAS Installation

The most common problems with IAS installation and their solutions are outlined here. In all cases, a valid user cannot log on and a Windows 2000 Event Viewer error message appears.

The error messages appear in bold type, and the possible solutions are described in the following paragraphs.

"Unknown user name or bad password."

"The specified user does not exist."

"The specified domain does not exist."

The user might have entered the wrong user name or password. Check the user's Windows 2000 user name and account password to make sure they are typed correctly and that the account is valid for the domain IAS is authenticating the user against.

Realm replacement might be set up incorrectly, or in the wrong order, so that the domain controller cannot recognize the user name. Adjust the realm replacement rules. For more information about realm names or configuring realm replacement, see your Windows 2000 Server information.

If the remote access server is a member of domain and the user response does not contain a domain name, the domain name of the remote access server is used. To use a domain name that is different from that of the IAS server, on the computer that is running IAS, set the following registry value to the name of the domain that you want to use:

HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \RasMan \PPP\ControlProtocols\BuiltIn\DefaultDomain

Caution Do not use a registry editor to edit the registry directly unless you have no alternative. The registry editors bypass the standard safeguards provided by administrative tools. These safeguards prevent you from entering conflicting settings or settings that are likely to degrade performance or damage your system. Editing the registry directly can have serious, unexpected consequences that can prevent the system from starting and require that you reinstall Windows 2000. To configure or customize Windows 2000, use the programs in Control Panel or Microsoft Management Console (MMC) whenever possible.

Some NASs automatically strip the domain name from the user name before forwarding the user name to a RADIUS server. Turn off the feature that strips the domain name from the user name. For more information, see your NAS documentation.

"The authentication type is not supported on this system."

The user is trying to authenticate by using an authentication method that is not supported on this computer. For example, the user might be using an EAP type that has not been installed. Modify the dial-in profile to allow the protocol in question.

If a remote access policy denies access to the user, the following error messages might appear:

"The user's information did not match a remote access policy."

"The user is not allowed dial-in access to the network."

"User attempted an unauthorized authentication method."

"User tried to connect from an unauthorized calling station."

"User tried to dial-in outside of permitted hours."

"User tried to connect by calling an unauthorized NAS phone number."

"User tried to connect using an invalid port type."

"A constraint defined in the remote access policy failed."

A remote access policy might be denying access to the user. Check the policy list to make sure that you have not excluded users who must be granted access. Check the event log to see if the user is trying to connect with parameters not permitted by a remote access policy (for example, during an unauthorized time period, using an unauthorized wrong port type, calling from an unauthorized wrong phone number, or calling an unauthorized NAS phone number). You might have to revise the remote access policies accordingly to grant the user access.

Remote access policies might be in the wrong order. Authorization is granted or denied by the first policy whose conditions match the connection attempt. Use the **Move Up** button to move the policy that grants access to the users who are having trouble so that it is higher in the list.

"The user has exceeded the dial-in lockout count."

If remote access account lockout is enabled, previous failed access attempts might have caused the user account to be locked out. If so, increase the dial-in lockout count.

"The user's account is currently locked out and might not be logged on to."

The user's account is locked out and cannot be validated.

"The user is not allowed dial-in access to the network."

The user might be denied dial-in access. Check the user's information about the domain controller (or in Local Users and Groups) to see that dial-in access is granted for the user. If dial-in access is denied, this overrides any remote access policy that grants access.

"The current configuration supports only local user accounts."

IAS is set up to authenticate against the local SAM, and the user is not a member of the local user database. In this case, add the IAS server to Active Directory.

"The user's account domain is unreachable."

"The server is unavailable."

"The specified domain did not exist."

"IAS could not access the Global Catalog."

There might be a communication problem between the NAS and IAS, or between IAS and the domain controller or Global Catalog server. Use the **ping** command to check the communication with the domain controller or Global Catalog server. If **ping** works, try to connect to the server by using the command **net use \\servername\share**. If no packet information appears in the IAS log, check the Windows 2000 event log to see whether the attempt times out.

The user might be using CHAP, but Active Directory might not be configured to use plaintext passwords. To use CHAP authentication with IAS, configure the dial-in profile for a user or group to use CHAP. The NAS and the user's dialing program (such as Connection Manager) must also be configured to use CHAP authentication. You also need to enable CHAP on the domain controller.

Certain NASs do not recognize all the characters that IAS accepts for the shared secret. Try to change the shared secret to one with only alphanumeric characters.

The NAS might be sending packets that do not correspond to the format expected by IAS.

Right-click **Internet Authentication Service** and then click **Properties**. Make sure **Log rejected or discarded authentication requests** is selected, and then display the command to see if unexpected or malformed packets are being sent. If this is the case, you might need to set some vendor-specific attributes in IAS to solve communication problems with your NAS.

IAS cannot connect to the domain. Make sure IAS is authenticating against the correct domain name. If the domain name is correct, make sure that the IAS server is a member of that domain, or that there is a trust relationship between that domain and the domain to which the IAS server belongs.

IAS does not have permission to view user objects in Active Directory. Add the IAS server to Active Directory.

The user account is in an Active Directory forest that is different from the forest of which the IAS server is a member. Use a RADIUS proxy to route the authentication request to an IAS server that is a member of the other Active Directory forest.

The user is trying to use 128-bit encryption enabled, IAS has it enabled in a remote access policy, but Routing and Remote Access does not. Enable the Strongest security setting on the Routing and Remote Access server. (If you have not enabled it on this server before, you might need to install the Microsoft Encryption Pack.)

Your NAS might require framed routing; but on IAS, framed routing is not set by default. Enable framed routing.

To enable framed routing

1. In IAS, click **Remote Access Policies**, and then double-click the policy that applies to the users who cannot log on.
2. Click **Edit Profile**, click the **Advanced** tab, and then click **Add**.
3. In the list of available RADIUS attributes, double-click **Framed-Routing**.
4. In **Attribute value**, click **None**.

Your NAS might require Van Jacobsen TCP/IP compression. Configure IAS to work with Van Jacobsen TCP/IP compression.

To configure IAS to work with Van Jacobsen TCP/IP header compression

1. In IAS, click **Remote Access Policies**, and then double-click the policy that applies to the users who cannot log on.
2. Click **Edit Profile**, click the **Advanced** tab, and then click **Add**.
3. In the list of available RADIUS attributes, double-click **Framed-Compression**.
4. In **Attribute value**, click **Van Jacobsen TCP/IP header compression**.

If framed MTU is set on the NAS and not on IAS, users are not able to log on. Check your framed MTU settings on IAS, and make sure that they match the settings on your NAS.

To change framed MTU settings

1. In IAS, click **Remote Access Policies**, and then double-click the policy that applies to the users who cannot log on.
2. Click **Edit Profile**, click the **Advanced** tab, and then click **Add**.
3. In the list of available RADIUS attributes, double-click **Framed-MTU**.
4. Click **Attribute value**, and then type the value that matches the settings for your NAS.

If IAS is returning the Access-Accept packet by using a different network adapter than the one by which the Access-Request packet was received, the NAS does not recognize the packet. In this event, check your IAS settings.

If the request is returned through a RADIUS proxy, the proxy might not support certain extensions that are necessary to support some features. For example:

- If you want your users to use EAP authentication, the RADIUS proxy must support digital signatures (according to RADIUS extensions).

- If you want your users to connect using compulsory tunnels, the RADIUS proxy must support encryption of the tunnel password.
- If you want connections to use Microsoft Encryption, the RADIUS proxy must support encryption of MPPE keys.

See your RADIUS proxy documentation to make sure that it supports the extensions necessary for the features that you want to use.

A remote access policy might be granting access to the user. Check the policy list to make sure that you have not included users who must be denied access.

Dial-in properties for the user object might be set to override the remote access policy. Check the dial-in properties for the user object.

Remote access policies might be in the wrong order. Authorization is granted or denied by the first policy whose conditions apply to the user who is trying to connect. Use the **Move Up** button to move the policy that denies access to the users so that it is higher in the list.

IAS is not set up to log rejected or discarded authentication requests. Set up IAS to log rejected or discarded authentication requests in the and see if any malformed packets are being logged. The NAS might require a different shared secret for RADIUS accounting. Make sure the shared secret for accounting is the same as the one used for authentication.

The dial-in profile for the remote access policy might not be set up to permit CHAP encryption. Check dial-in profile settings to be sure that IAS is set up for CHAP authentication. Check to see whether your NAS is set up for CHAP. For more information, see your NAS documentation. Also check to make sure the domain controller is configured to store reversibly encrypted passwords.

Passwords are not stored in a reversibly encrypted form until they are reset. Perform the following:

- After you enable passwords to be stored in a reversibly encrypted form, the current passwords are not in a reversibly encrypted form and are not automatically changed. You must either reset user passwords or set user passwords to be changed the next time each user logs on.
- After you switch a domain controller from mixed mode to native mode, every domain controller in the domain must be restarted so that the change replicates.
- Restart the domain controllers so that the servers can regain access to the domain controller.

When a Routing and Remote Access server is set to use RADIUS authentication, Remote Access Policies are accessible only from Internet Authentication Service. This is intentional behavior.

Troubleshooting by Using Network Monitor

If a problem still exists after checking basic IAS configuration, the Network Monitor (NetMon) tool can be used to record a trace of the problem for further analysis.

When you use Network Monitor for IAS troubleshooting, consider the following:

- NetMon must be installed on a computer that is running IAS server.
- If you use NetMon in a switched network environment, you see only the traffic addressed to the computer that is running NetMon.

  For more information about setting up and using Network Monitor, see "Monitoring Network Performance" in the *Microsoft® Windows® 2000 Server Resource Kit Server Operations Guide*.

Set up Network Monitor for RADIUS troubleshooting by filtering NetMon on RADIUS packets in a trace.

Perform the following steps:

To filter NetMon on RADIUS packets in a trace

1. Capture trace of a problem.
2. In the **Display** menu, select **Filter**.
3. Select **Protocol = Any** and then click **Edit Expression**. Click **Disable All** to disable all of the protocols. In the right pane, select **RADIUS protocol** and then click **Enable**.
4. Click **OK**.

Send feedback to Microsoft

© 2004 Microsoft Corporation. All rights reserved.