Deploying Windows Server 2003 Internet Authentication Service (IAS) with Virtual Local Area Networks (VLANs)

Microsoft Corporation

Published: June 2004

Abstract

This white paper describes how to configure remote access policy in Internet Authentication Service (IAS) for use with virtual local area networks (VLANs). When you configure the profile of an IAS remote access policy for use with VLANs, you must configure the attributes Tunnel-Medium-Type, Tunnel-Pvt-Group-ID, Tunnel-Type, and Tunnel-Tag. VLANs allow network architects and administrators to logically group network resources (such as servers, printers, and client computers) even when they are not on the same physical subnet.

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

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

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

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

Contents

Introduction

By using VLAN-aware network access servers and Internet Authentication Service (IAS) in Microsoft® Windows Server™ 2003, you can provide groups of users with access only to the network resources that are appropriate for their security permissions. For example, you can provide visitors with wireless access to the Internet without allowing them access to your organization network.

In addition, VLANs allow you to logically group network resources that exist in different physical locations or on different physical subnets. For example, members of your sales department and their network resources, such as client computers, servers, and printers, might be located in several different buildings at your organization, but you can place all of these resources on one VLAN using the same IP address range; the VLAN then functions, from the end-user perspective, as a single subnet.

You can also use VLANs when you want to segregate a network between different groups of users. After you have determined how you want to define your groups, you can create security groups in Active Directory and add members to the groups. You can define groups of users in several ways:

- **By role.** You can create groups for the sales team, the finance department, and other departments.
- **By position.** You can create groups for knowledge workers, managers, executives, and other positions.
- **By access level.** You can create groups for visitors, partners, full-time employees, and other categories with different access levels.

After you have created groups in Active Directory, you can open the IAS Microsoft Management Console (MMC) snap-in and create a remote access policy for each group. Within the remote access policy configuration process, you can define the VLAN to which the group will be assigned.

Configuration of VLAN-aware network hardware, such as VLAN-aware routers, switches, wireless access points, and access controllers, is beyond the scope of this white paper. When you have one or more of these devices configured as a Remote Authentication Dial-In User Service (RADIUS) client to your IAS server, however, you can use IAS to designate which VLAN the connecting user is placed on.

For information about how to configure your VLAN-aware network access server, see your access server documentation.

IAS is included in the following products:

- Windows Server 2003, Standard Edition
- Windows Server 2003, Enterprise Edition
- Windows Server 2003, Datacenter Edition

- Microsoft Windows Server 2003, 64-Bit Enterprise Edition
- Microsoft Windows Server 2003, 64-Bit Datacenter Edition
- Microsoft Windows Small Business Server 2003, Standard Edition
- Microsoft Windows Small Business Server 2003, Premium Edition

Requirements

To deploy IAS with VLANs as described in this white paper, the following components are required:

- A computer running Windows Server 2003 and IAS
- An Active Directory® directory service user accounts database
- RADIUS clients that are VLAN-aware, such as wireless access points, switches, or access controllers

Remote access policy

When you use Active Directory as your user accounts database, IAS performs network access authentication and authorization using Active Directory user account dial-in properties and remote access policies, which are configured in the IAS snap-in.

Authentication is the process of verifying identity, while *authorization* is the process of verifying that the user or device connecting to the network has permissions to do so.

A *remote access policy* is an ordered set of rules that define how a connection is either authorized or rejected by IAS. For each rule, there are one or more conditions, a set of profile settings, and a remote access permission setting.

If a connection is authorized, the remote access policy profile settings specify a set of connection restrictions that can include the assignment of the connection to a VLAN.

Authorization by group

It is recommended that you manage authorization by security group rather than by individual user. Managing authorization by group provides the ability to create one remote access policy, or rule, for network connection attempts by all members of the group. For example, if you have a sales department that you want to place on a VLAN, you can create a security group named Sales in the Active Directory Users and Computers snap-in, and then you can add all members of the sales department as members of the group. When a member of the Sales group attempts to connect to the network, the connection attempt is processed by IAS with the remote access policy for the group.

If the user is authenticated and authorized, IAS applies connection restrictions, and can instruct a VLAN-aware access server to place the member of the Sales group onto the VLAN for the sales department.

IAS authorizes connection attempts with both the dial-in properties of the user account, which are configured in the Active Directory Users and Computers snap-in, and remote access policies, which are configured in the IAS snap-in.

User account remote access permission

One of the dial-in properties of user accounts in Active Directory is **Remote Access Permission (Dial-in or VPN)**. You can use this property to set remote access permission to be explicitly allowed, denied, or determined through remote access policies. In all cases, remote access policies are used to authorize the connection attempt.

If access is explicitly allowed, remote access policy conditions, user account properties, or profile properties can still deny the connection attempt. The **Control access through Remote Access Policy** option is only available on user accounts in a Windows 2000 native domain, a Windows Server 2003 domain, or for local accounts on stand-alone servers running Windows 2000; Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; or Windows Server 2003, Datacenter Edition.

New accounts that are created on a stand-alone server or in a Windows 2000 native domain are set to **Control access through Remote Access Policy**. New accounts that are created in a Windows 2000 mixed domain are set to **Deny access**.

When you manage authorization by security group, the remote access permission setting in user account dial-in properties can be set to one of the following:

- **Allow access**. Only apply this setting for users who are members of groups to whom you want to grant remote access permission. You can use this setting when your domain functional level is Windows 2000 mixed. Windows 2000 mixed supports Windows NT 4.0, Windows 2000, and Windows Server 2003 family domain controllers. With user account remote access permission set to **Allow access**, authorization is performed by IAS in circumstances where you have created a policy that matches the conditions of the connection.
- **Control access through Remote Access Policy**. This setting is recommended for domains with a functional level of Windows 2000 native or Windows Server 2003.

> **Important**
>
> To set user account dial-in properties to **Control access through remote access policy**, the domain functional level must be Windows 2000 native or higher. For more information, see "Domain and forest functionality" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=30600.

Ignoring the user account dial-in properties

You can configure IAS to ignore the dial-in properties of user accounts. This setting is useful for circumstances where you want IAS remote access policy to determine authorization for all connections to your network. For example, you can configure IAS to ignore the dial-in properties of user accounts when:

- Your domain functional level is Windows 2000 mixed.
- Changing the current settings on user accounts is not cost-effective.

For more information on configuring IAS to ignore the dial-in properties of user accounts, see “Dial-in properties of a user account” in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=30601.

For more information on remote access policies, see “Introduction to remote access policies” in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=30602.

Configuring Active Directory

If you want to create security groups in Active Directory or raise the domain functional level, perform the following procedures.

> **Important**
>
> **If you have or will have any domain controllers running Windows NT 4.0 and earlier, then do not raise the domain functional level to Windows 2000 native. After the domain functional level is set to Windows 2000 native, it cannot be changed back to Windows 2000 mixed.**
>
> **If you have or will have any domain controllers running Windows NT 4.0 and earlier or Windows 2000, then do not raise the domain functional level to Windows Server 2003. After the domain functional level is set to Windows Server 2003, it cannot be changed back to Windows 2000 mixed or Windows 2000 native.**

If you want to raise the domain functional level to either Windows 2000 native or Windows Server 2003, do the following:

1. Open the **Active Directory Domains and Trusts** snap-in. To open Active Directory Domains and Trusts, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Active Directory Domains and Trusts**.
2. In the console tree, right-click the domain for which you want to raise the domain functional level, and then click **Raise Domain Functional Level**.
3. In **Select an available domain functional level**, do one of the following:
    - To raise the domain functional level to Windows 2000 native, click **Windows 2000 native**, and then click **Raise**.

- To raise the domain functional level to Windows Server 2003, click **Windows Server 2003**, and then click **Raise**.

> **Notes**
>
> - To perform this procedure, you must be a member of the Domain Admins group in the domain for which you want to raise functionality or the Enterprise Admins group in Active Directory, or you must have been delegated the appropriate authority.
> - The current domain functional level is displayed under **Current domain functional level** in the **Raise Domain Functional Level** dialog box.

To create a group and add members to the group, do the following:

1. Open the **Active Directory Users and Computers** snap-in.
2. In the console tree, right-click the folder in which you want to add a new group.
3. Point to **New**, and then click **Group**.
4. Type the name of the new group. By default, the name you type is automatically entered in **Group name (pre-Windows 2000)**.
5. In **Group scope**, click one of the options.
6. In **Group type**, click one of the options, and then click **OK**.
7. In the details pane, right-click the group you just created, and then click **Properties**.
8. On the **Members** tab, click **Add**.
9. In **Enter the object names to select**, type the name of the user, group, or computer that you want to add to the group, and then click **OK**.

For more information, see "To create a new group" at http://go.microsoft.com/fwlink/?LinkId=20018 and "Assign user rights to a group in Active Directory" at http://go.microsoft.com/fwlink/?LinkId=20019.

Configuring IAS

To configure IAS for use with VLANs, do the following:

1. Install Internet Authentication Service on a computer running Windows Server 2003. For more information, see "To install IAS" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20028.
2. Register IAS in Active Directory. In order for IAS to have permission to read user accounts in Active Directory, IAS must be registered with Active Directory. For more information, see "To enable the IAS server to read user accounts in Active Directory" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=20030.

3. Add RADIUS clients. In the IAS snap-in, right-click **RADIUS Clients**, and then click **New RADIUS Client**. Use the **New RADIUS Client Wizard** to both add and configure your network access servers as RADIUS clients.
4. Delete the default remote access policies. To delete the policies, open the IAS snap-in, and then click **Remote Access Policies**. Select each existing policy, right-click the policy, and then click **Delete**.
5. Create a new remote access policy. In the console tree of the IAS snap-in, right-click **Remote Access Policies**, and then click New **Remote Access Policy**. Use the **New Remote Access Policy Wizard** to create a policy.

As an example policy, you can choose the following:

- For **How do you want to set up this policy?** select **Use the wizard to set up a typical policy for a common scenario**.
- For **Policy name**, type a name for your policy. For example, type **Sales policy**.
- For **Select the method of access for which you want to create a policy**, select the appropriate type of access, such as **Wireless** or **Ethernet**.
- For **Grant access based on the following**, click **Group**, and then click **Add**. In **Enter the object name to select**, type the name of a security group that you defined when configuring Active Directory. For example, if you created a group named Sales, type **Sales**, and then click **OK**.
- In **Authentication Methods**, select the authentication method that you would like to enforce for users who will be placed on this VLAN. Your choices will differ based upon the access method you have chosen for the policy, such as Wireless or VPN. When you have completed configuring an authentication method, click **Finish**.

After you have completed creating the policy and have closed the wizard, you need to configure additional items for the remote access policy. In the IAS snap-in, click **Remote Access Policies**, and then double-click the policy you just created. Make the following configuration changes to the policy:

1. In the policy **Properties** dialog box, for **Policy conditions**, click **Add**.
2. In **Attribute Types**, click **Day-And-Time-Restrictions**, and then click **Add**. In **Time of day restraints,** select **Permitted**, configure the days and times that access is permitted, and then click **OK**.
3. In the policy **Properties** dialog box, click **Grant remote access permission**.
4. Click **Edit Profile**, and then click the **Advanced** tab. By default, the **Service-Type** attribute appears in **Attributes** with a value of **Framed**. By default, for policies with access methods of VPN and dial-up, the **Framed-Protocol** attribute appears in **Attributes** with a value of **PPP**. To specify additional connection attributes required for VLANs, click **Add**, and then add the following attributes:
    - **Tunnel-Medium-Type**. Select a value appropriate to the previous selections you have made. For example, if the remote access policy you are configuring is a wireless policy, select: **Value: 802 (Includes all 802 media plus Ethernet canonical format)**.

- **Tunnel-Pvt-Group-ID**. Enter the integer that represents the VLAN number to which group members will be assigned. For example, if your Sales VLAN is on VLAN 4, type the number **4**.
- **Tunnel-Type**. Select the value **Virtual LANs (VLAN)**.
- **Tunnel-Tag**. Obtain this value from your hardware documentation.

5. Configure IAS connection request policies as you require.

> **Important**
>
> IAS evaluates remote access policies in the order in which they appear in the IAS snap-in under **Remote Access Policies.**

For more information about remote access policies, see "Elements of a remote access policy" in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=30605.

For more information about connection request processing, see “Introduction to connection request processing” in Help and Support Center for Windows Server 2003 or on the Web at http://go.microsoft.com/fwlink/?LinkId=30607.

Summary

When you use VLAN-aware network hardware, such as routers, switches, and access controllers, you can configure remote access policy in Internet Authentication Service in Windows Server 2003 to instruct the access servers to place members of Active Directory groups on VLANs. When you configure the profile of an IAS remote access policy for use with VLANs, you must configure the attributes Tunnel-Medium-Type, Tunnel-Pvt-Group-ID, Tunnel-Type, and Tunnel-Tag. This ability to group network resources logically with VLANs provides flexibility when designing and implementing network solutions.

Related Links

For more information about IAS, see the following:

- The Internet Authentication Service home page at http://go.microsoft.com/fwlink/?LinkId=16171.
- “Deploying IAS” in the *Windows Server 2003 Deployment Kit* at http://go.microsoft.com/fwlink/?LinkId=30603.
- “Internet Authentication Service” in Windows Server 2003 Help on the Web at http://go.microsoft.com/fwlink/?LinkId=30604.