



WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE 802.1X DYNAMIC VLANS WITH MICROSOFT IAS

Written By: Michael Hong

May 2004



Summary

This installation guide provides step-by-step instructions for configuring 802.1x Dynamic VLANs on Foundry Networks IronPoint 200 with Microsoft Windows Server 2000. This installation guide is a continuation of *IronPoint 200 Installation Guide: WPA 802.1x PEAP with Microsoft IAS*. This installation guide maybe useful for proof-of-concept testing, customer demonstrations or hands-on training.

Contents

Before You Begin **3**
Related Publications 3
This installation guide requires the following: 3
Physical Network Configuration 4
IronPoint 200 Configuration **5**
Configuring from the CLI 5
Configuring from the Web Interface..... 6
Windows 2000 Server Configuration **7**
Configuring a Remote Access Policy for VLAN 101..... 7
Testing the Configuration for VLAN 10117
Configuring a Remote Access Policy for VLAN 201.....20
Testing the Configuration for VLAN 20135
Configuring Active Directory User Groups37
Configuring IAS.....45
Testing the Configuration for "Guest" User on VLAN 10154
Testing the Configuration for "Test" User on VLAN 20163

Figures

Figure 1 – Physical Network Configuration..... 4

Before You Begin

Related Publications

The following Foundry Networks document is required before reading this installation guide:

- *IronPoint 200 Installation Guide: WPA 802.1x PEAP with Microsoft IAS*

You must complete the instructions from *IronPoint 200 Installation Guide: WPA 802.1x PEAP with Microsoft IAS* before starting the instructions in this installation guide.

This installation guide requires the following:

- A Foundry Networks IronPoint 200 (IP 200) access point with firmware version 01.2.12.00Tw8 (or newer).
- An 802.1q supported Ethernet switch.
- Two computers each with an Ethernet NIC.
- Microsoft Windows XP computer with SP1 (or newer) with the support patch for WPA (Knowledge Base Article 826942) and a wireless NIC that is Wi-Fi certified for WPA - Enterprise¹.
- Microsoft Windows 2000 Server (or Advanced Server) with SP4 (or newer).
- Basic knowledge of wired and wireless LANs, Microsoft Windows operating systems and Foundry Networks IP 200 access points.

¹ To see if your wireless NIC is Wi-Fi certified for WPA – Enterprise, look for the Wi-Fi certification logo or check the list of Wi-Fi certified products at www.wi-fi.org/certified_products.

Physical Network Configuration

This installation guide uses the network configuration shown in Figure 1.

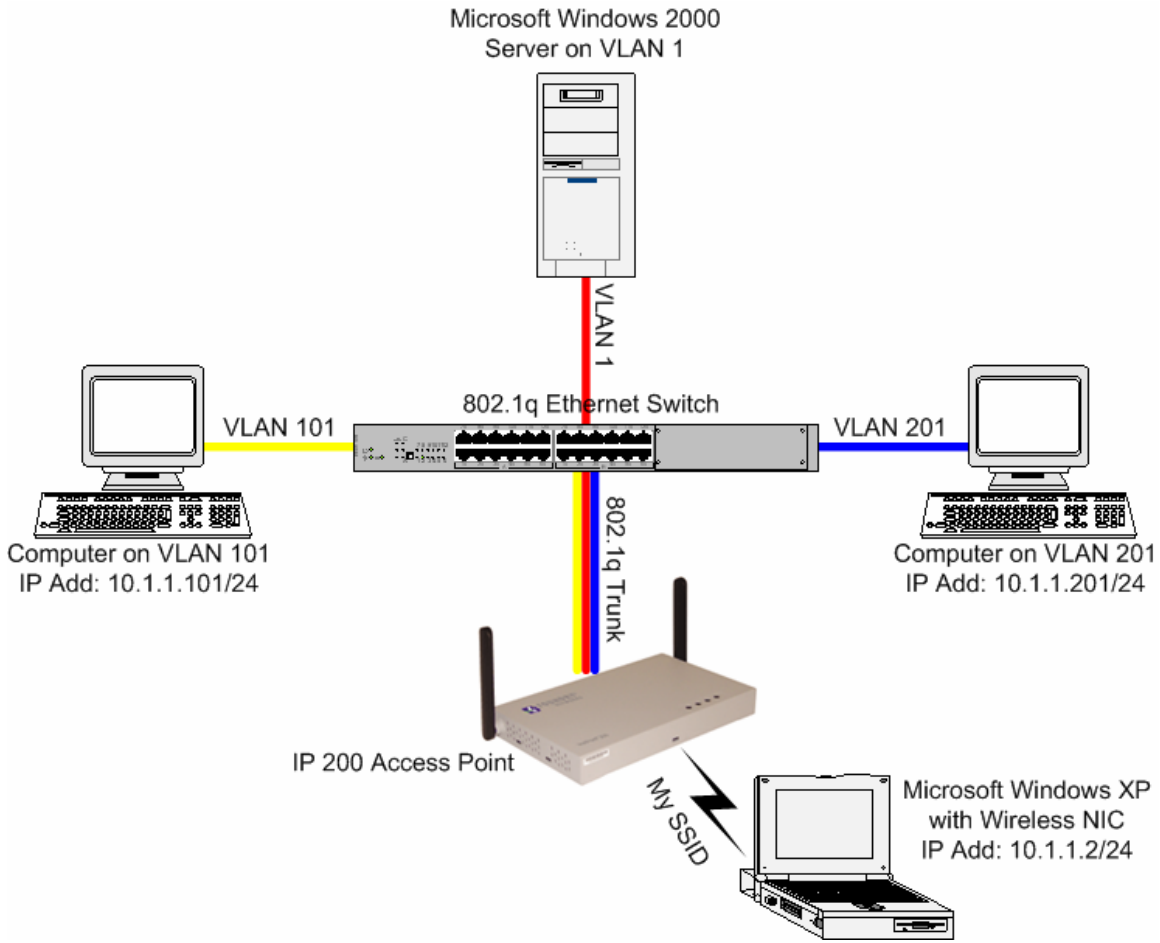


Figure 1 – Physical Network Configuration

NOTE: This installation guide does not include instructions on how to configure the 802.1q Ethernet switch or the two computers on VLAN 101 and VLAN 201.



IronPoint 200 Configuration

The IP 200 access point must be using firmware version 01.2.12.00Tw8 (or newer). The IP 200 must have been already configured using the IP 200 Installation Guide: WPA 802.1x PEAP with Microsoft IAS.

The IP 200 can be configured from either the CLI or from the Web Interface. If you prefer configuring the IP 200 from the Web Interface, you can skip the following section **Configuring from the CLI** and go to the next section **Configuring from the Web Interface**.

Configuring from the CLI

From the CLI, go to the configure context. Enter the following commands:

```
Foundry AP(config)#management-vlanid 1
```

```
Foundry AP(config)#vlan enable
```

```
Foundry AP(config)#end
```

```
Foundry AP#reset board
```

```
Reboot system now? <y/n>: y
```

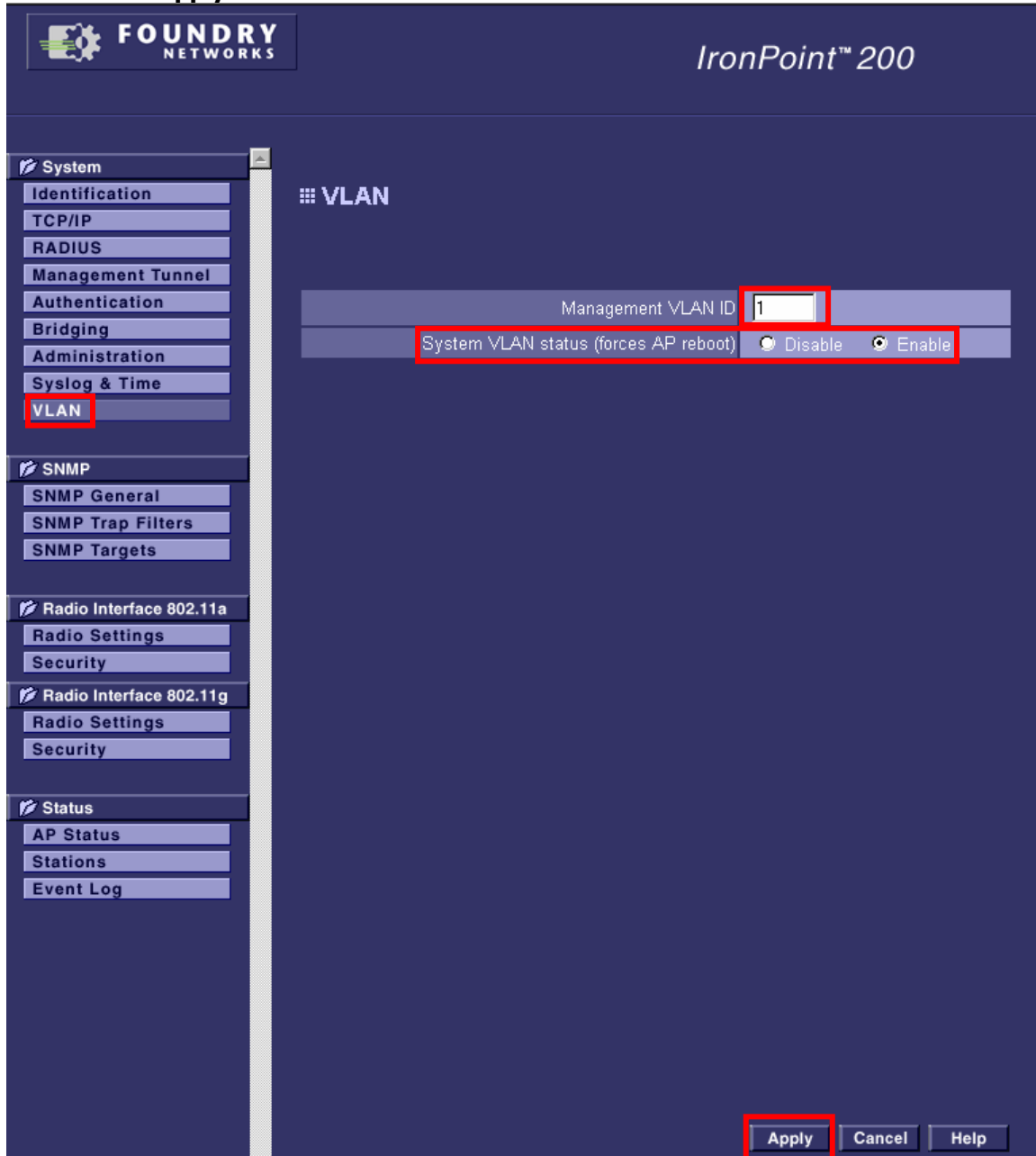
The IP 200 will reboot. Go to the next section: **Windows 2000 Server Configuration**.



Configuring from the Web Interface

If you have configured the IP 200 using the previous section **Configuring from the CLI**, you do not need to configure the IP 200 using the Web Interface and you can go to the next section: **Windows 2000 Server Configuration**.

Go to the **VLAN** menu. For **Management VLAN ID**, enter **1**. For **System VLAN status**, select **Enable**. Click **Apply**.



The IP 200 will reboot. Go to the next section: **Windows 2000 Server Configuration**.



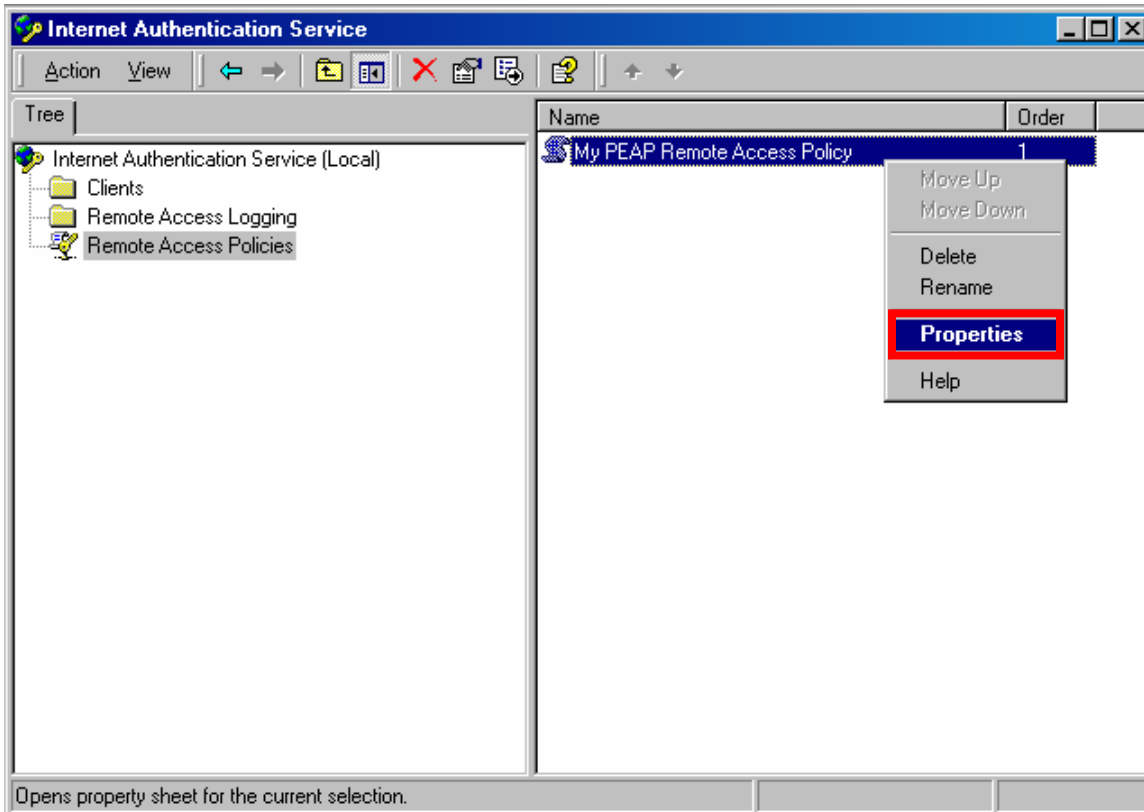
Windows 2000 Server Configuration

The Windows 2000 Server (or Advanced Server) must have Service Pack 4 and have already been configured using the *IP 200 Installation Guide: WPA 802.1x PEAP with Microsoft IAS*.

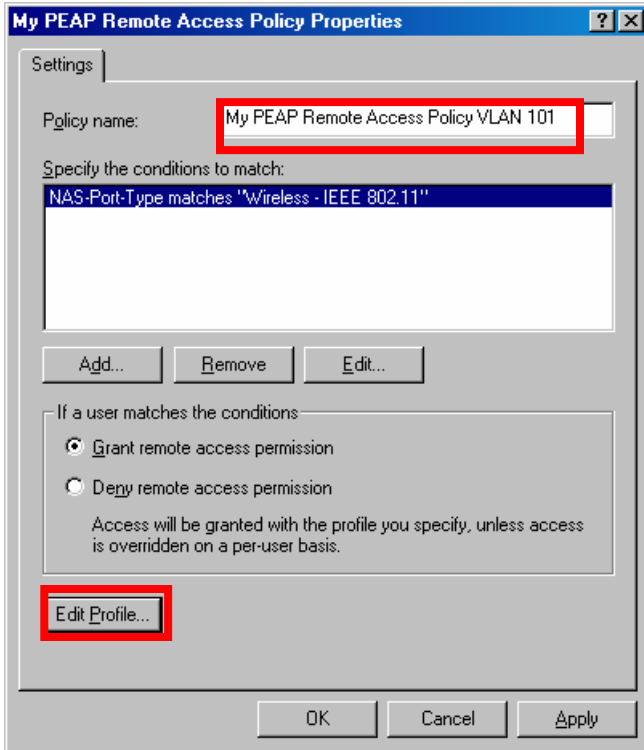
In this section we are going to configure the Windows 2000 Server to return RADIUS attributes so the IP 200 can tag the authenticating client's frames with the appropriate 802.1q VLAN tag. First you will configure a Remote Access Policy so that authenticating clients will be tagged for VLAN 101. Next, you will configure a Remote Access Policy for VLAN 201.

Configuring a Remote Access Policy for VLAN 101

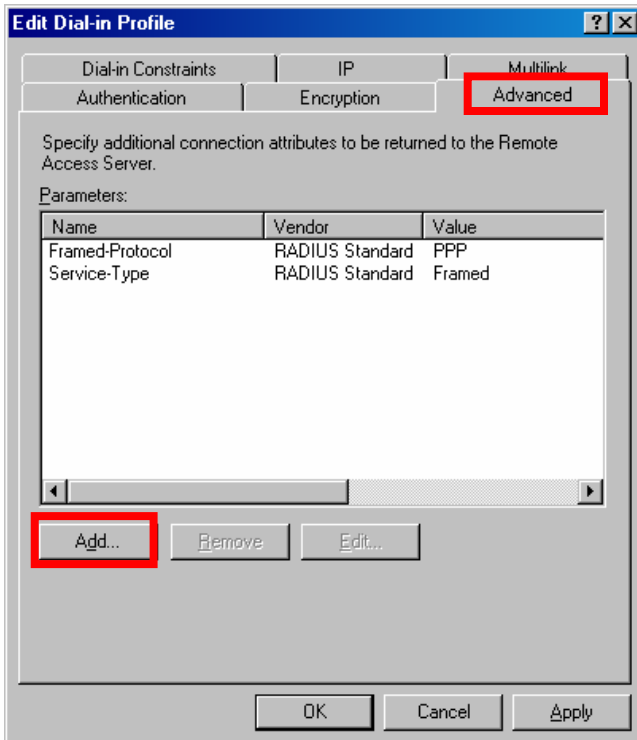
From **Internet Authentication Service**, right click on the **Remote Access Policy** that you've created from the WPA 802.1x PEAP with Microsoft installation guide. Select **Properties**.



Rename the **Policy name** to identify it as the VLAN 101 configuration. Click Edit **Profile...** .



Select the **Advanced** tab. Click **Add...** .

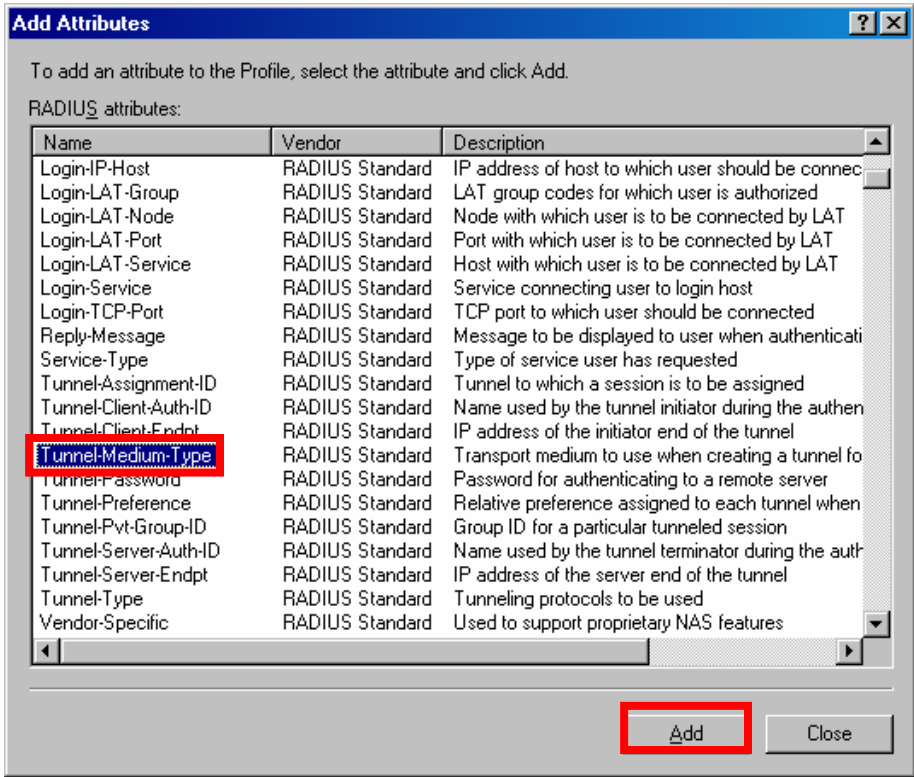


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

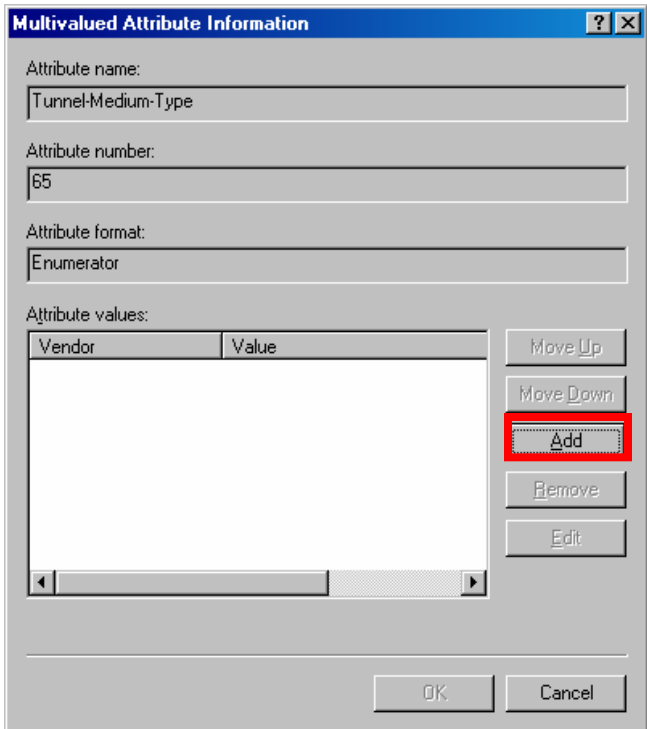
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Select **Tunnel-Medium-Type**. Click **Add**.



Click **Add**.





Select **802 (including all 802 media plus Ethernet canonical format)**. Click **OK**.

The screenshot shows the 'Enumerable Attribute Information' dialog box. The 'Attribute name' field contains 'Tunnel-Medium-Type', 'Attribute number' is '65', and 'Attribute format' is 'Enumerator'. The 'Attribute value' dropdown menu is open, showing the selected option: '802 (includes all 802 media plus Ethernet canonical format)'. The 'OK' button is highlighted with a red box.

Click **OK**.

The screenshot shows the 'Multivalued Attribute Information' dialog box. The 'Attribute name' field contains 'Tunnel-Medium-Type', 'Attribute number' is '65', and 'Attribute format' is 'Enumerator'. The 'Attribute values' table contains one entry:

Vendor	Value
RADIUS Standard	802 (includes all 802 media plus E

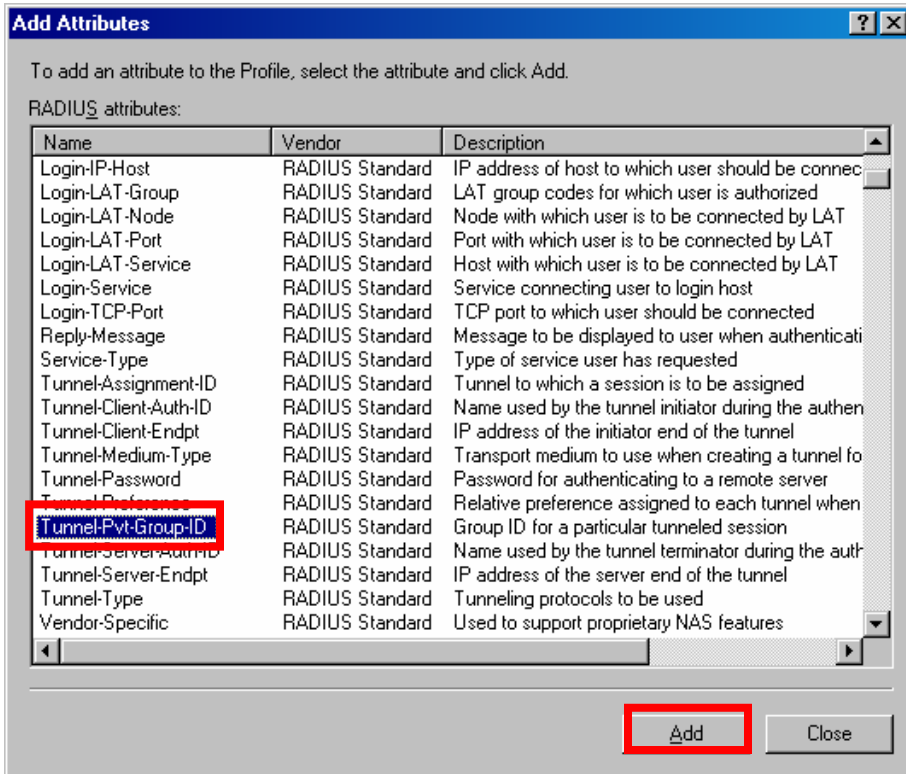
Buttons for 'Move Up', 'Move Down', 'Add', 'Remove', and 'Edit' are visible to the right of the table. The 'OK' button is highlighted with a red box.

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

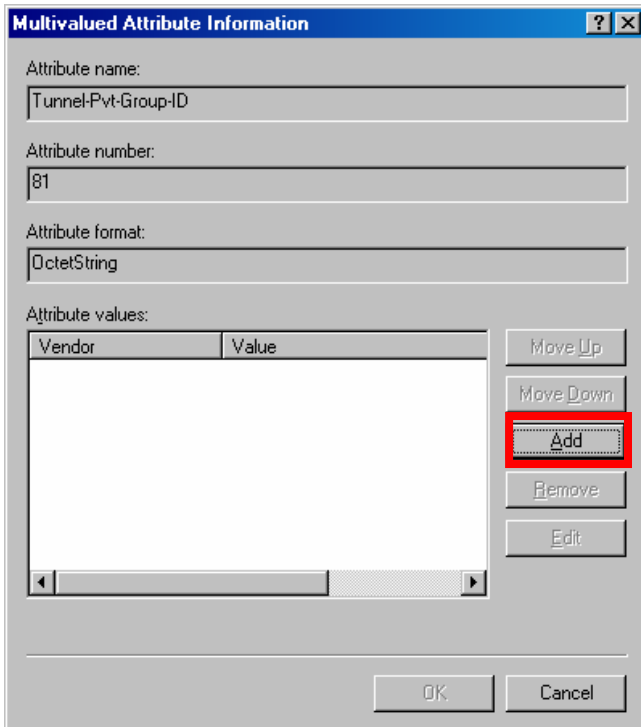
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Click **Finish**.



Click **OK**.



WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Set **Enter the attribute value in:** to **String**. Enter **101**. Click **OK**.

The dialog box 'Attribute Information' contains the following fields and controls:

- Attribute name: Tunnel-Pvt-Group-ID
- Attribute number: 81
- Attribute format: OctetString
- Enter the attribute value in: String Hexadecimal
- Value field: 101
- Buttons: OK, Cancel

Click **OK**.

The dialog box 'Multivalued Attribute Information' contains the following fields and controls:

- Attribute name: Tunnel-Pvt-Group-ID
- Attribute number: 81
- Attribute format: OctetString
- Attribute values table:

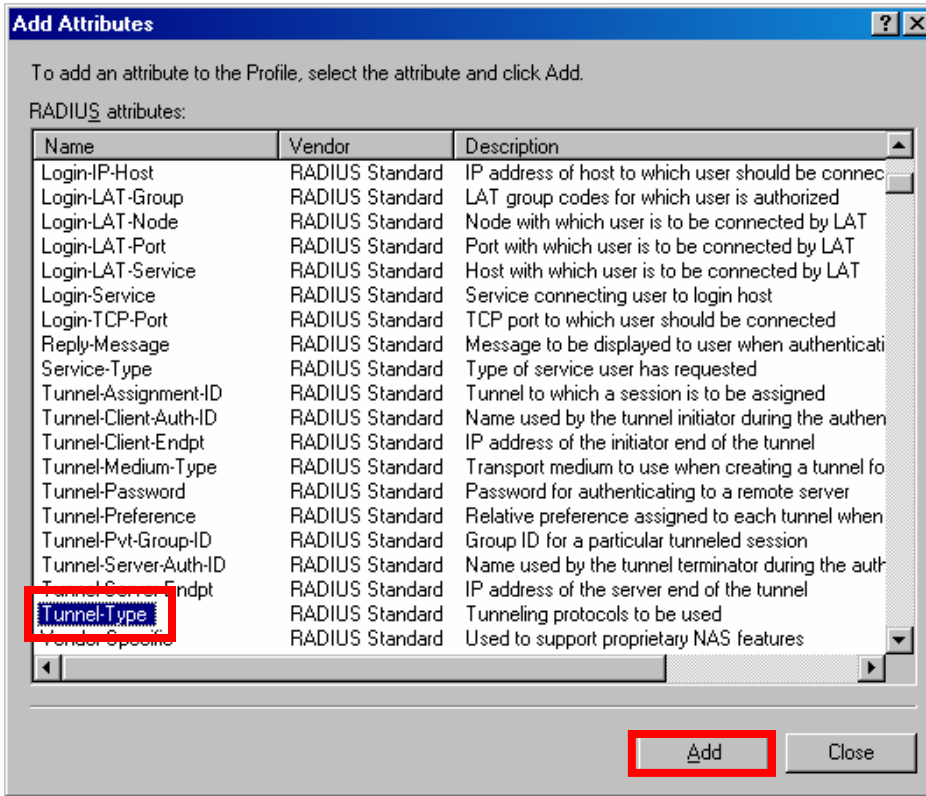
Vendor	Value
RADIUS Standard	101
- Buttons: Move Up, Move Down, Add, Remove, Edit, OK, Cancel

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

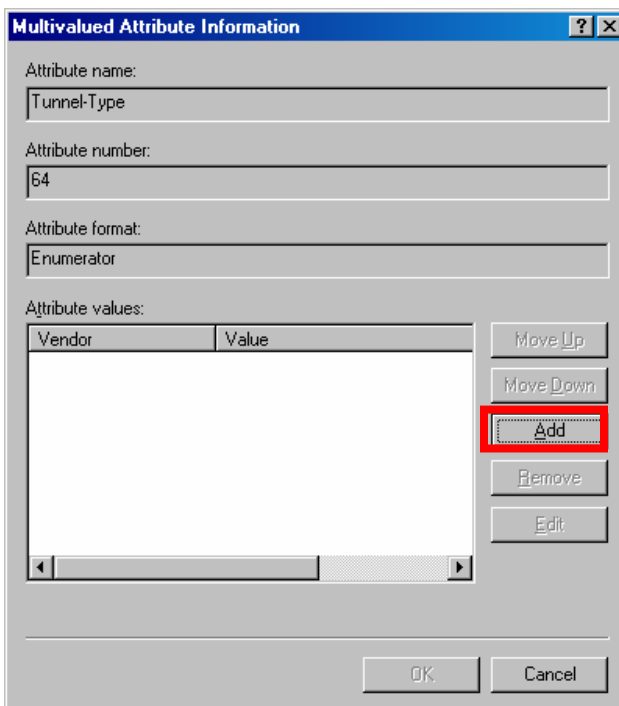
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Select **Tunnel-Type**. Click **Add**.



Click **Add**.



WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Select **Virtual LANs (VLAN)**. Click **OK**.

The dialog box 'Enumerable Attribute Information' has the following fields:

- Attribute name: Tunnel-Type
- Attribute number: 64
- Attribute format: Enumerator
- Attribute value: Virtual LANs (VLAN) (highlighted with a red box)

Buttons: OK (highlighted with a red box), Cancel

Click **OK**.

The dialog box 'Multivalued Attribute Information' has the following fields:

- Attribute name: Tunnel-Type
- Attribute number: 64
- Attribute format: Enumerator
- Attribute values:

Vendor	Value
RADIUS Standard	Virtual LANs (VLAN)

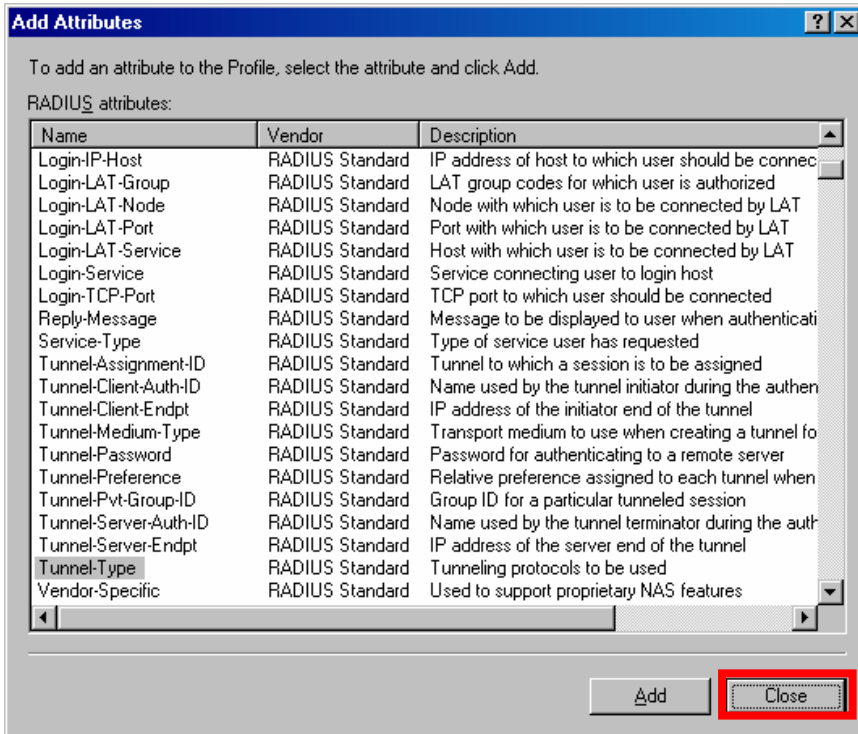
Buttons: Move Up, Move Down, Add, Remove, Edit, OK (highlighted with a red box), Cancel

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

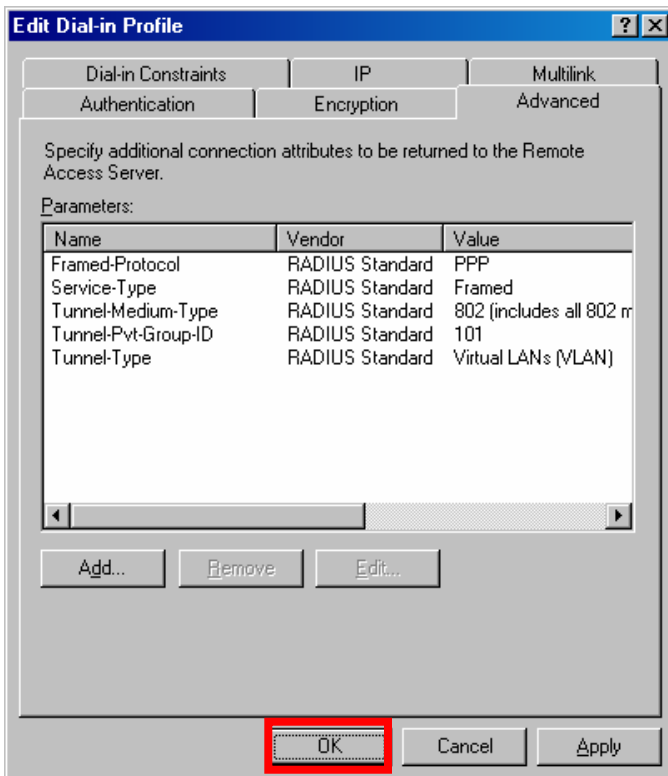
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Click **Close**.



Click **OK**

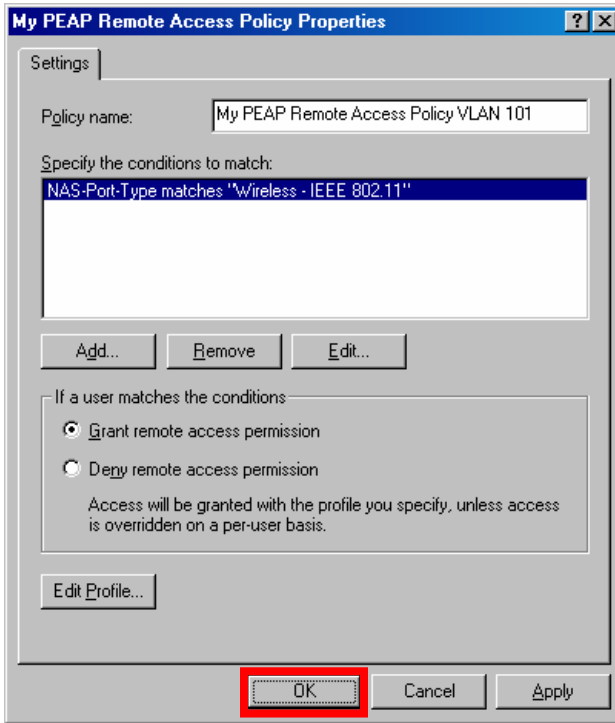


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

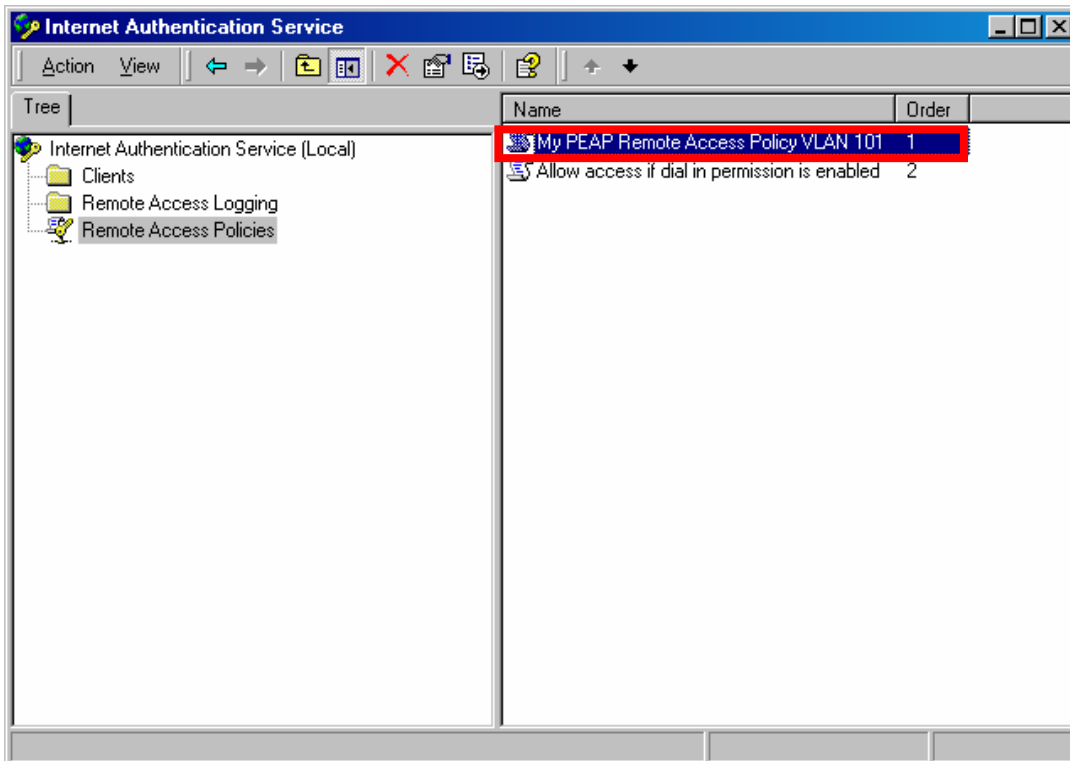
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Click **OK**.



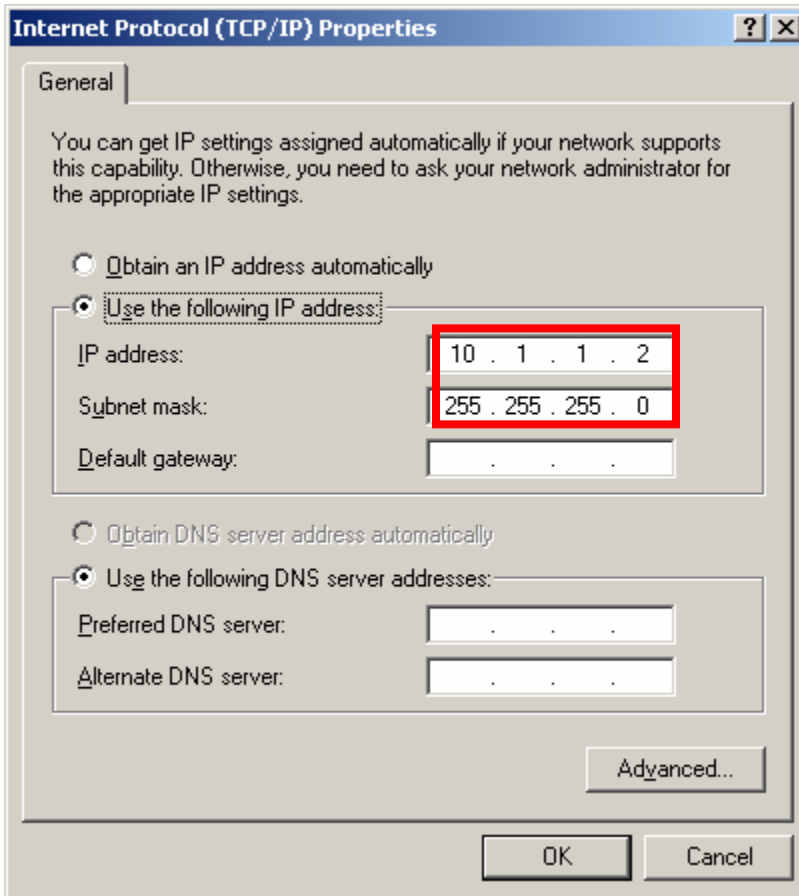
Check that your Remote Access Policy is Order 1. Use the **Move Up** and **Move Down** arrows to move it to Order 1 if necessary.



Testing the Configuration for VLAN 101

Test the configuration with the Windows XP computer. The Windows XP computer must have been already configured using the *IP 200 Installation Guide: WPA 802.1x PEAP with Microsoft IAS*.

First change the **IP address** of the wireless NIC on the Windows XP computer to **10.1.1.2/24**.

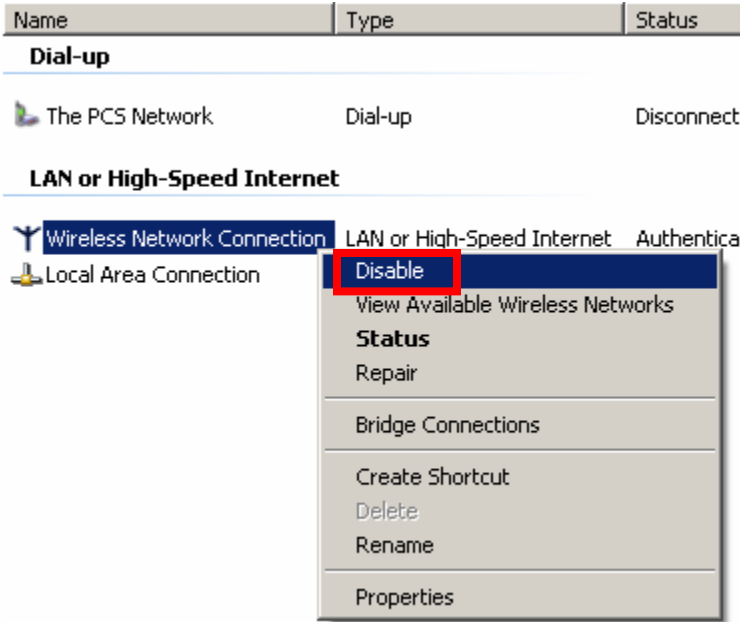


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

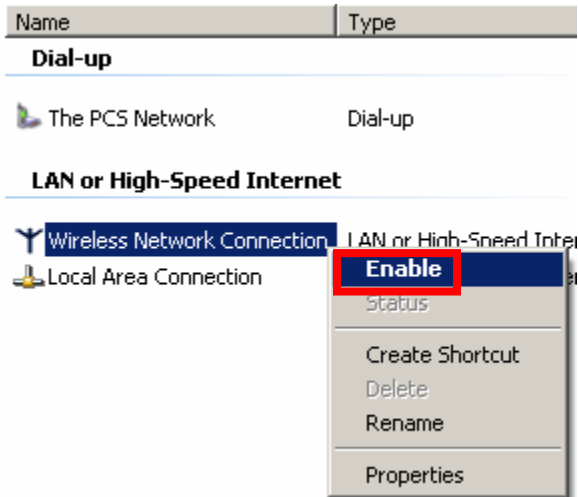
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



From **Network Connections**, right click on the wireless NIC. Select **Disable**



When the status of the NIC is disabled, right click on the wireless NIC again and select **Enable**.



This will force the XP computer to re-authenticate to the wireless LAN and receive the RADIUS attributes from the Remote Access Policy for VLAN 101.



Open a command prompt window and enter **ping 10.1.1.101**. Check that the pings are successful.

```
C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

U:\>ping 10.1.1.101

Pinging 10.1.1.101 with 32 bytes of data:

Reply from 10.1.1.101: bytes=32 time=7ms TTL=128
Reply from 10.1.1.101: bytes=32 time=10ms TTL=128
Reply from 10.1.1.101: bytes=32 time=11ms TTL=128
Reply from 10.1.1.101: bytes=32 time=8ms TTL=128

Ping statistics for 10.1.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 11ms, Average = 9ms

U:\>
```

Enter **ping 10.1.1.201**. Check that the pings are unsuccessful.

```
C:\WINDOWS\System32\cmd.exe

Pinging 10.1.1.101 with 32 bytes of data:

Reply from 10.1.1.101: bytes=32 time=7ms TTL=128
Reply from 10.1.1.101: bytes=32 time=10ms TTL=128
Reply from 10.1.1.101: bytes=32 time=11ms TTL=128
Reply from 10.1.1.101: bytes=32 time=8ms TTL=128

Ping statistics for 10.1.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 11ms, Average = 9ms

U:\>ping 10.1.1.201

Pinging 10.1.1.201 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.1.201:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

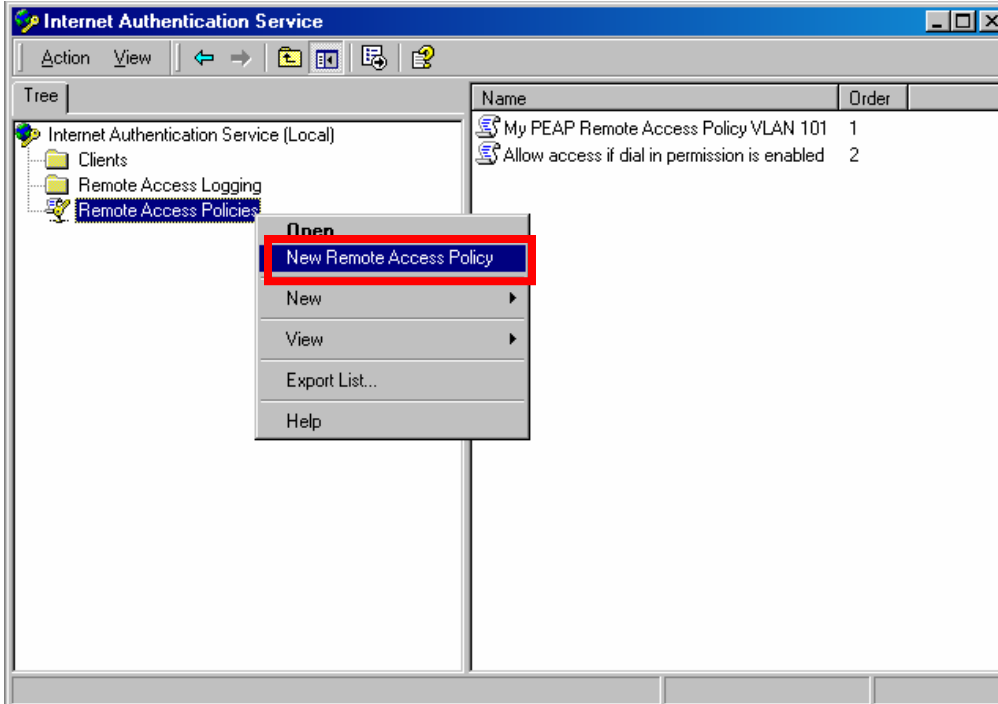
U:\>
```

This confirms that this Remote Access Policy is properly configured for VLAN 101.

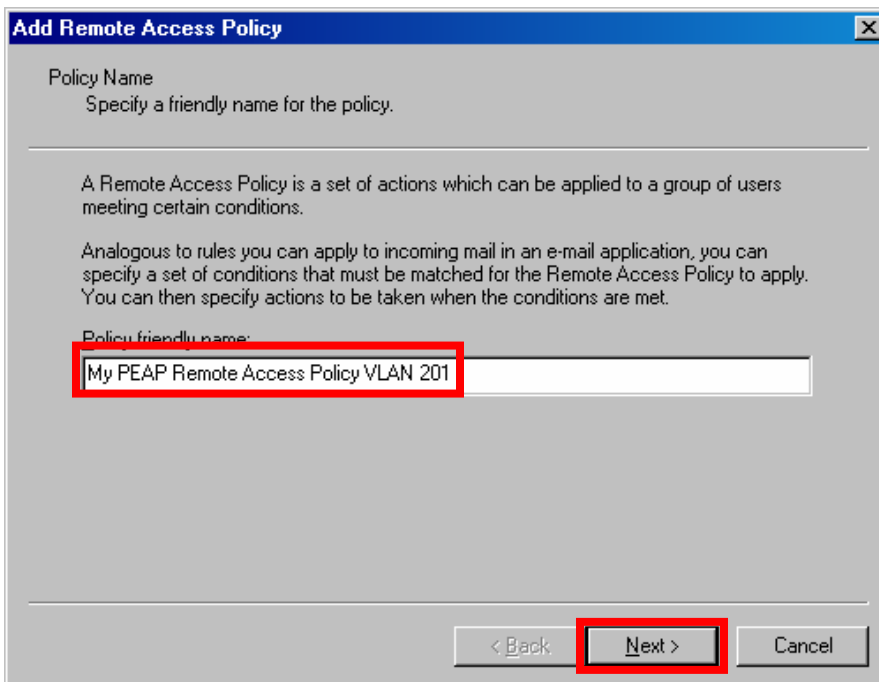


Configuring a Remote Access Policy for VLAN 201

From **Internet Authentication Service**, right click on the **Remote Access**. Select **New Remote Access Policy**.



Enter a **Policy friendly name** and identify it as the VLAN 201 configuration. Click **Next**.

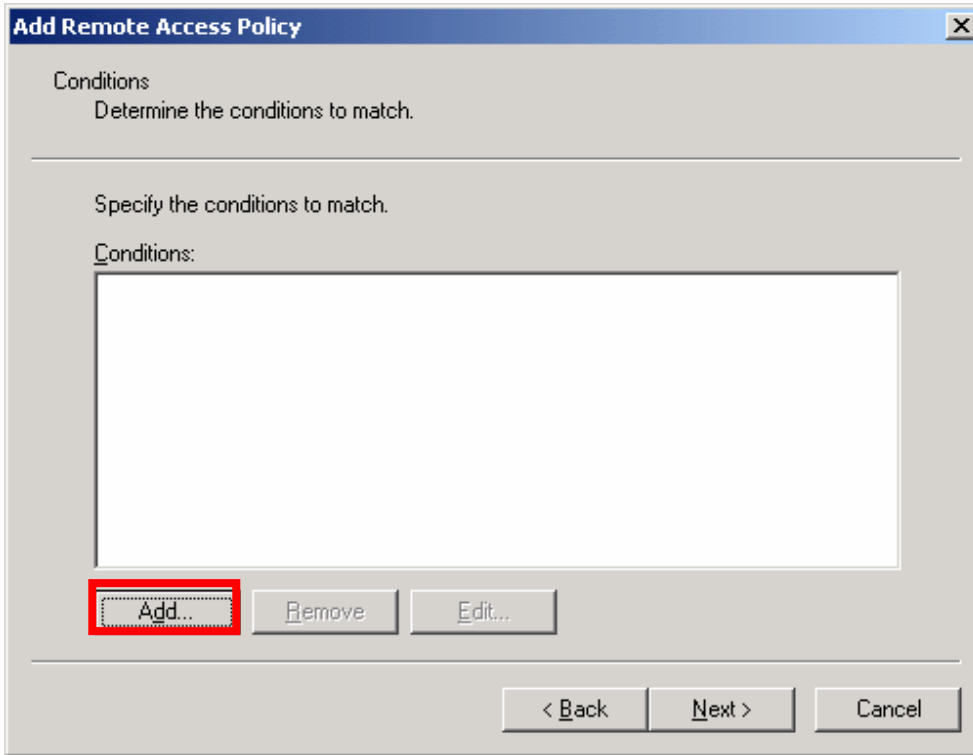


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

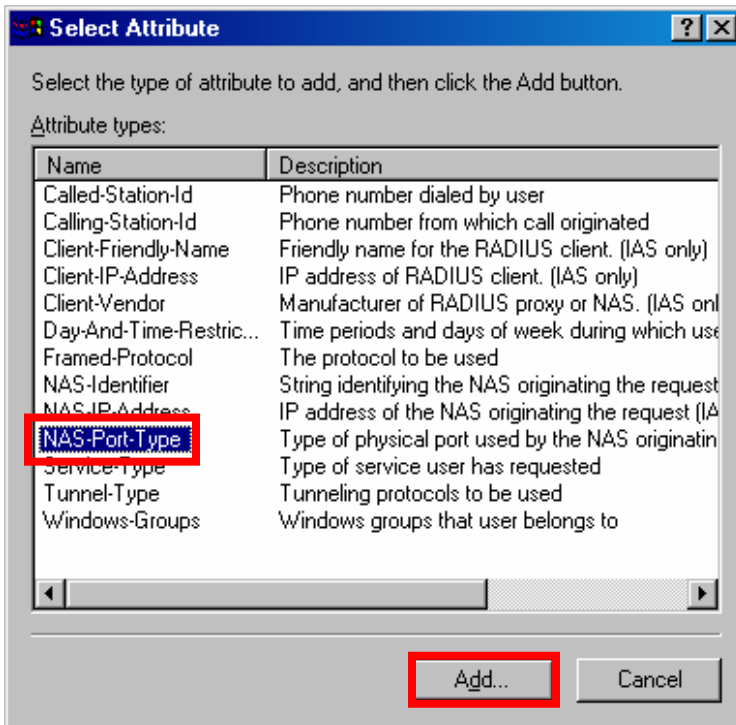
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Click **Add**.



Select **Attribute type NAS-Port-Type**. Click **Add...**

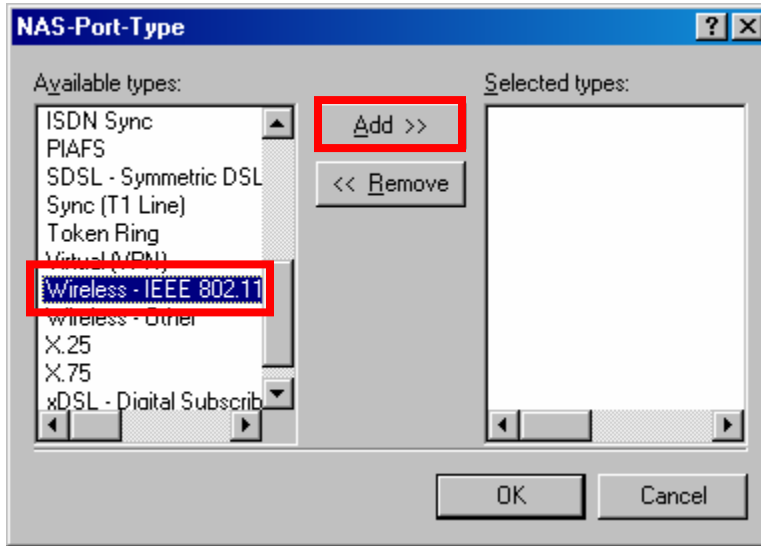


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

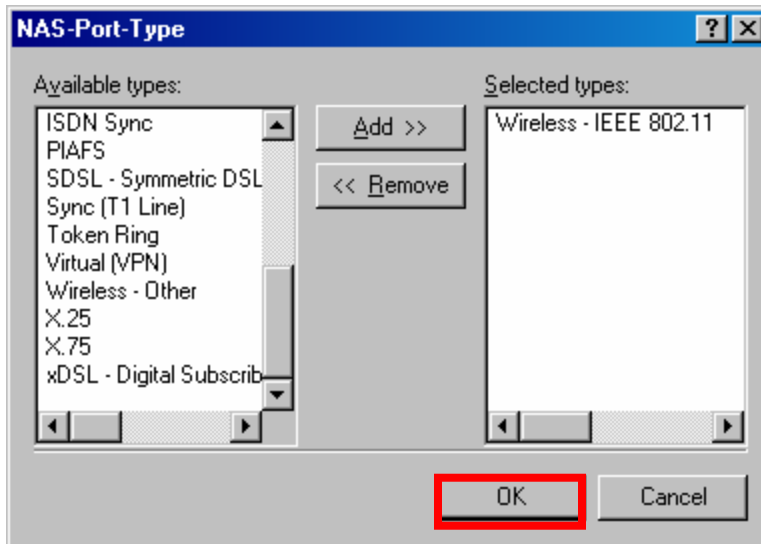
802.1X DYNAMIC VLANS WITH MICROSOFT IAS



Select **Wireless IEEE 802.11**. Click **Add >>**.



Click **OK**.



WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Click **Next >**.

The screenshot shows the 'Add Remote Access Policy' dialog box with the 'Conditions' tab selected. The text 'Determine the conditions to match.' is at the top. Below it, a list of conditions is shown with 'NAS-Port-Type matches "Wireless - IEEE 802.11"' selected. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.

Select **Grant remote access permission**. Click **Next >**.

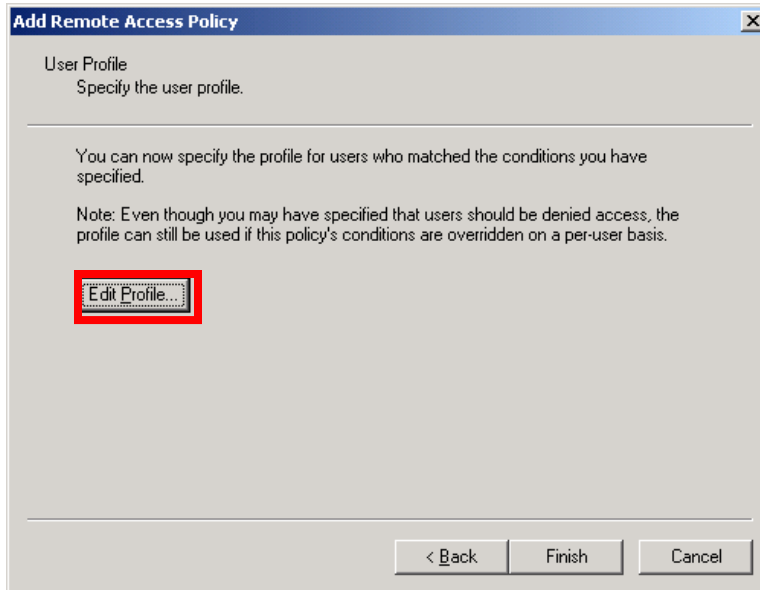
The screenshot shows the 'Add Remote Access Policy' dialog box with the 'Permissions' tab selected. The text 'Determine whether to grant or deny remote access permission.' is at the top. Below it, there is explanatory text: 'You can use a Remote Access Policy either to grant certain access privileges to a group of users, or to act as a filter and deny access privileges to a group of users.' Underneath, it says 'If a user matches the specified conditions:' followed by two radio button options: 'Grant remote access permission' (which is selected and highlighted with a red box) and 'Deny remote access permission'. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

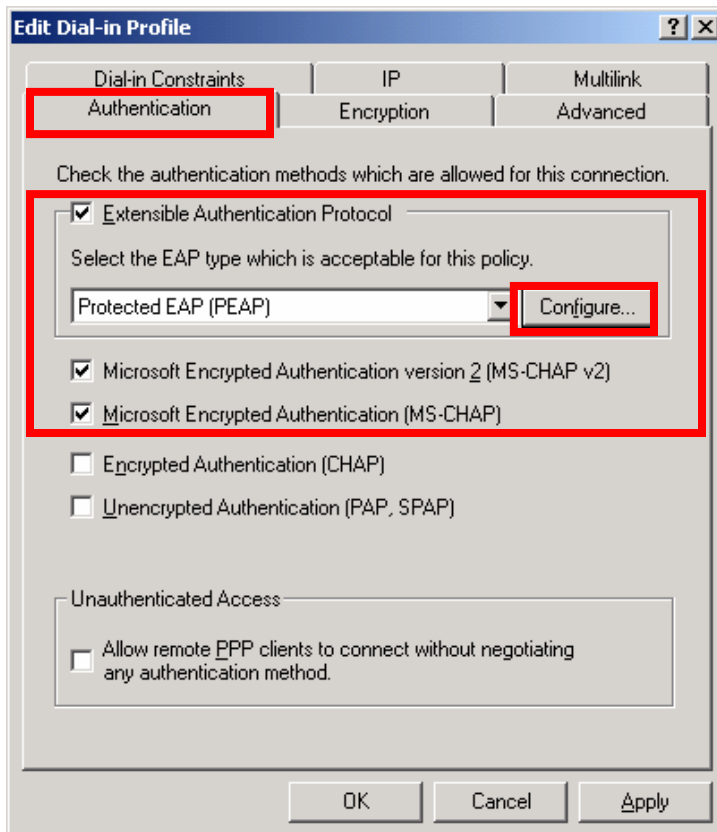
802.1X DYNAMIC VLANs WITH MICROSOFT IAS

**FOUNDRY**[®]
NETWORKS

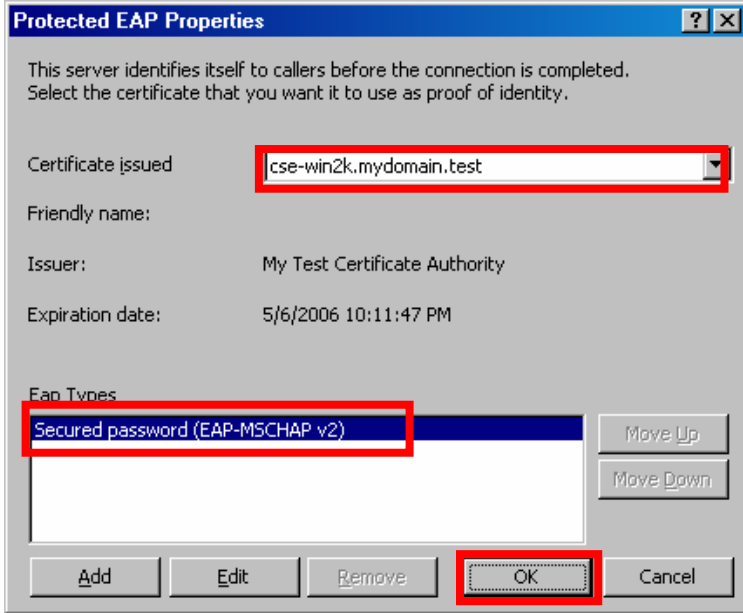
Click **Edit Profile ...** .



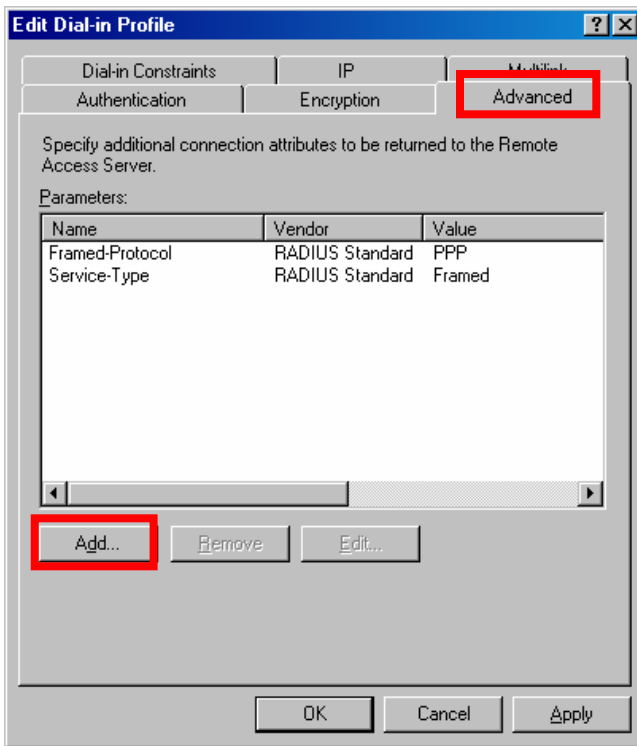
Click on the **Authentication** tab. Check **Extensible Authentication Protocol** and select **Protected EAP (PEAP)** from the drop down box. Check **Microsoft Encrypted Authentication version 2 (MS-CHAP v2)** and **Microsoft Encrypted Authentication (MS-CHAP)**. Click **Configure ...** .



If there is more than one selection available for **Certificate issued**, select the certificate whose **Issuer** is the same CA name that you enter in the **Installing Certification Authority** section. From the **Eap Types** box, select **Secured password (EAP-MSCHAP v2)** and click **Move Up** so that it is at the top of the list. Click **OK**.



Select the **Advanced** tab. Click **Add...** .

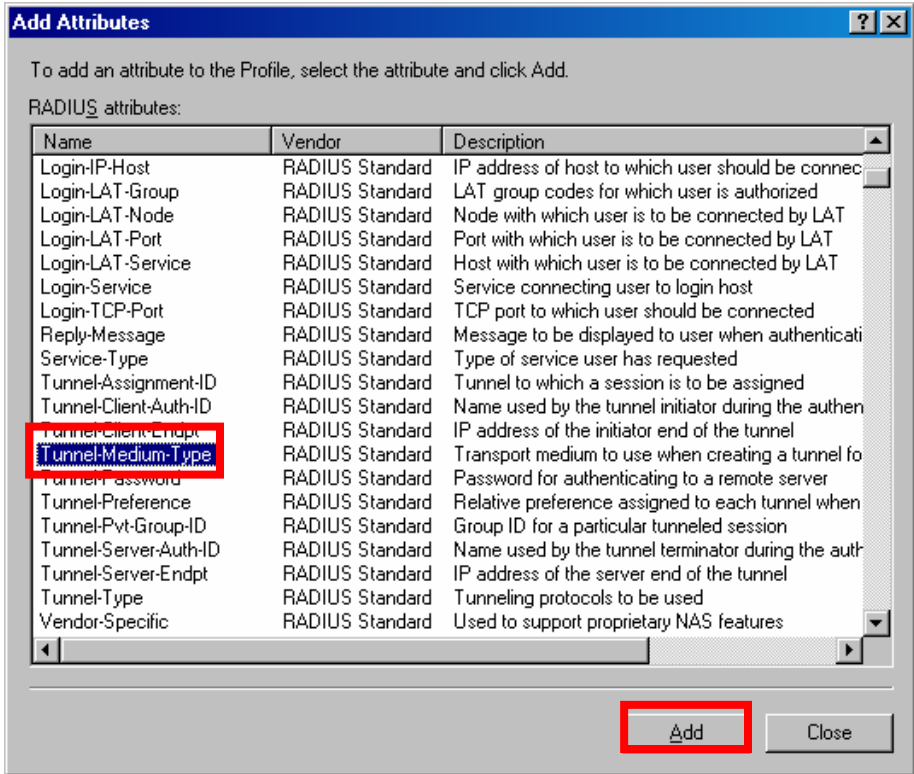


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

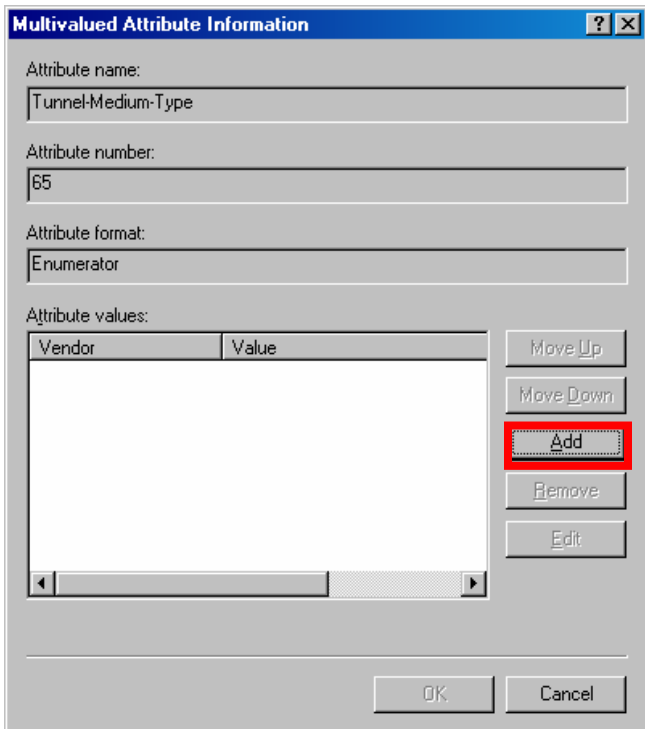
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Select **Tunnel-Medium-Type**. Click **Add**.



Click **Add**.





Select **802 (including all 802 media plus Ethernet canonical format)**. Click **OK**.

Enumerable Attribute Information [?] [X]

Attribute name:
Tunnel-Medium-Type

Attribute number:
65

Attribute format:
Enumerator

Attribute value:
802 (includes all 802 media plus Ethernet canonical format)

[OK] [Cancel]

Click **OK**.

Multivalued Attribute Information [?] [X]

Attribute name:
Tunnel-Medium-Type

Attribute number:
65

Attribute format:
Enumerator

Attribute values:

Vendor	Value
RADIUS Standard	802 (includes all 802 media plus E...

Move Up
Move Down
Add
Remove
Edit

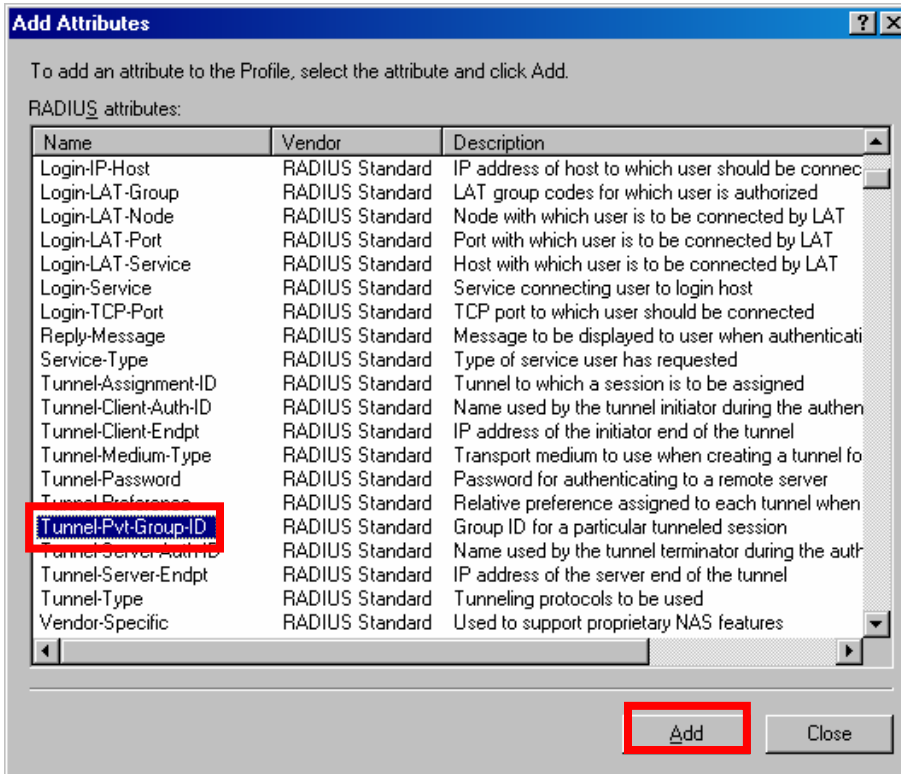
[OK] [Cancel]

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

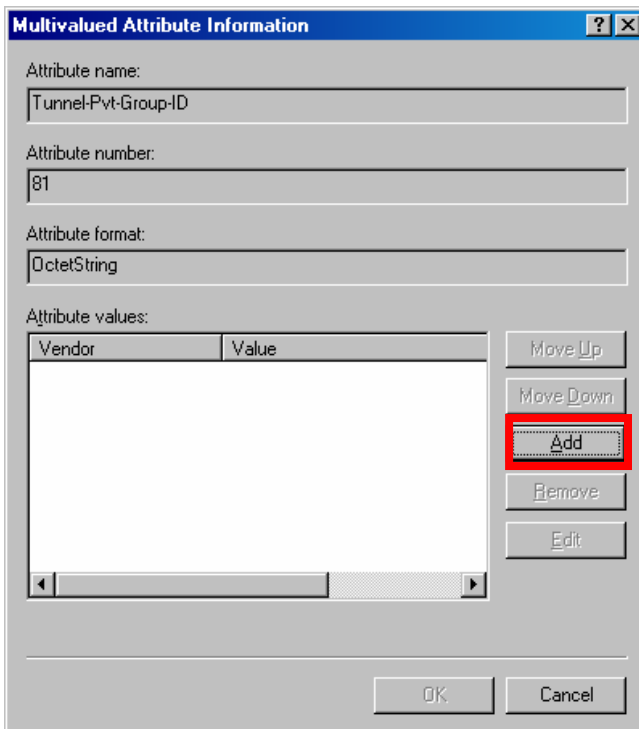
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Click **Tunnel Pvt-Group-ID**. Click **Add**.



Click **Add**.



WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Set **Enter the attribute value in:** to **String**. Enter **102**. Click **OK**.

The dialog box 'Attribute Information' has the following fields and controls:

- Attribute name: Tunnel-Pvt-Group-ID
- Attribute number: 81
- Attribute format: OctetString
- Enter the attribute value in: String Hexadecimal
- Value field: 201
- Buttons: OK, Cancel

Click **OK**.

The dialog box 'Multivalued Attribute Information' has the following fields and controls:

- Attribute name: Tunnel-Pvt-Group-ID
- Attribute number: 81
- Attribute format: OctetString
- Attribute values table:

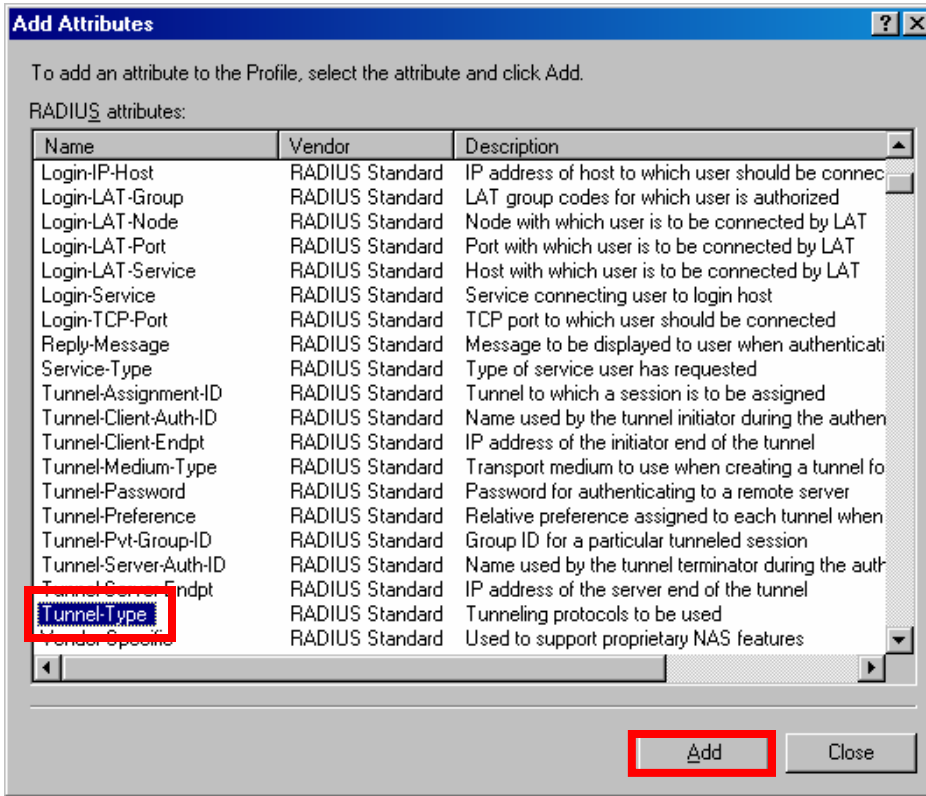
Vendor	Value
RADIUS Standard	201
- Buttons: Move Up, Move Down, Add, Remove, Edit, OK, Cancel

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

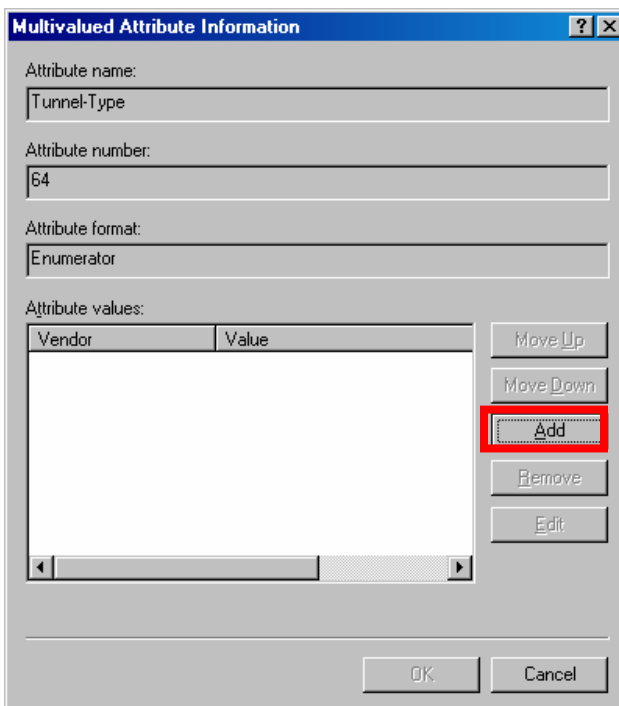
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Select **Tunnel-Type**. Click **Add**.



Click **Add**.



WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Select **Virtual LANs (VLAN)**. Click **OK**.

The dialog box 'Enumerable Attribute Information' has the following fields:

- Attribute name: Tunnel-Type
- Attribute number: 64
- Attribute format: Enumerator
- Attribute value: Virtual LANs (VLAN) (highlighted with a red box)

Buttons: OK (highlighted with a red box), Cancel

Click **OK**.

The dialog box 'Multivalued Attribute Information' has the following fields:

- Attribute name: Tunnel-Type
- Attribute number: 64
- Attribute format: Enumerator
- Attribute values:

Vendor	Value
RADIUS Standard	Virtual LANs (VLAN)

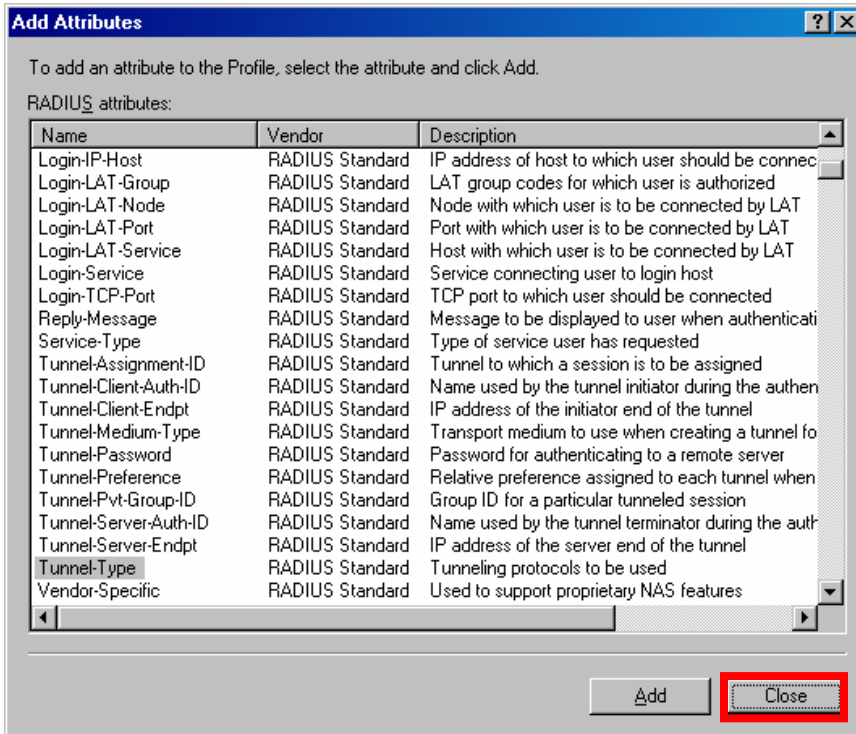
Buttons: Move Up, Move Down, Add, Remove, Edit, OK (highlighted with a red box), Cancel

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

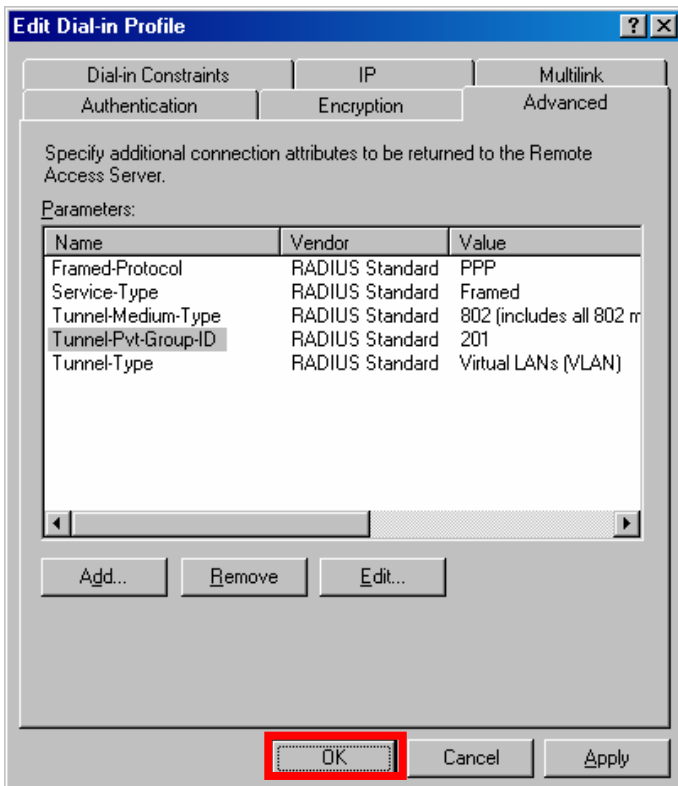
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Click **Close**.



Click **OK**

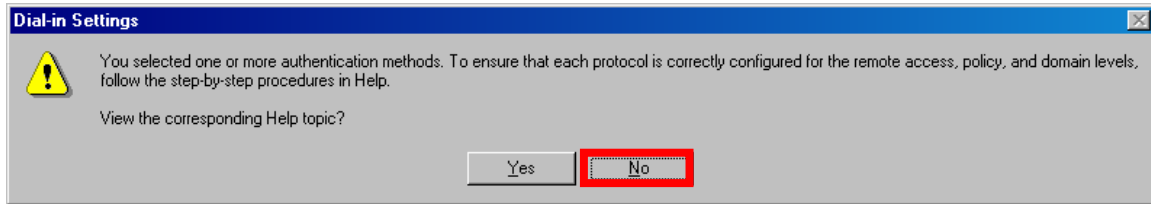


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

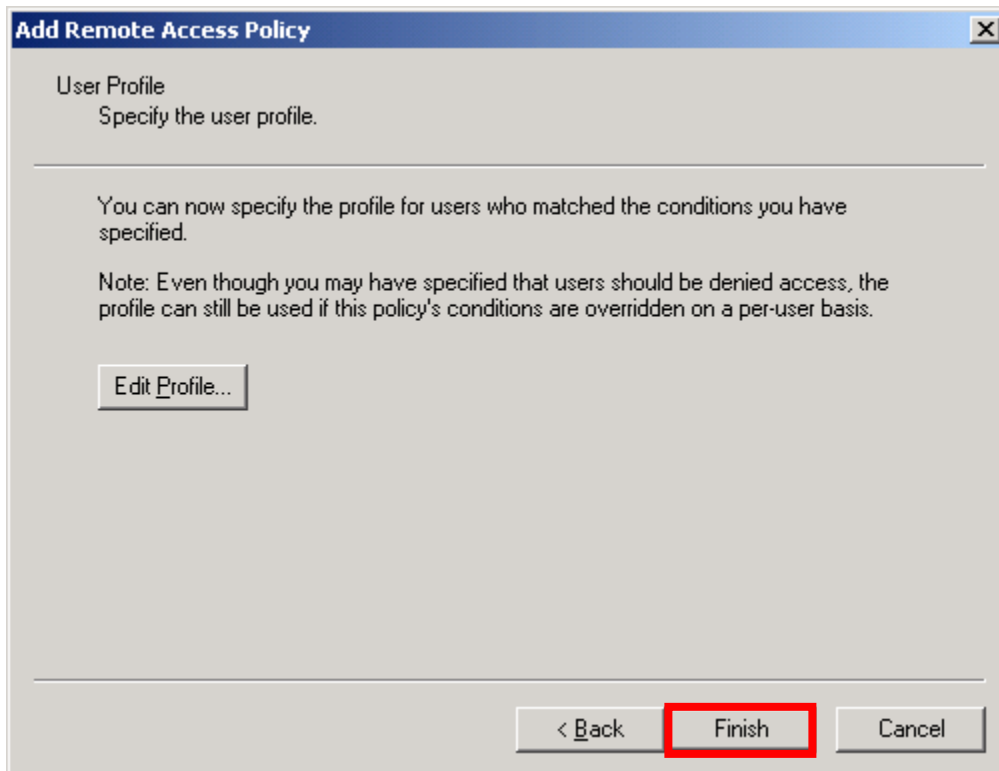
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



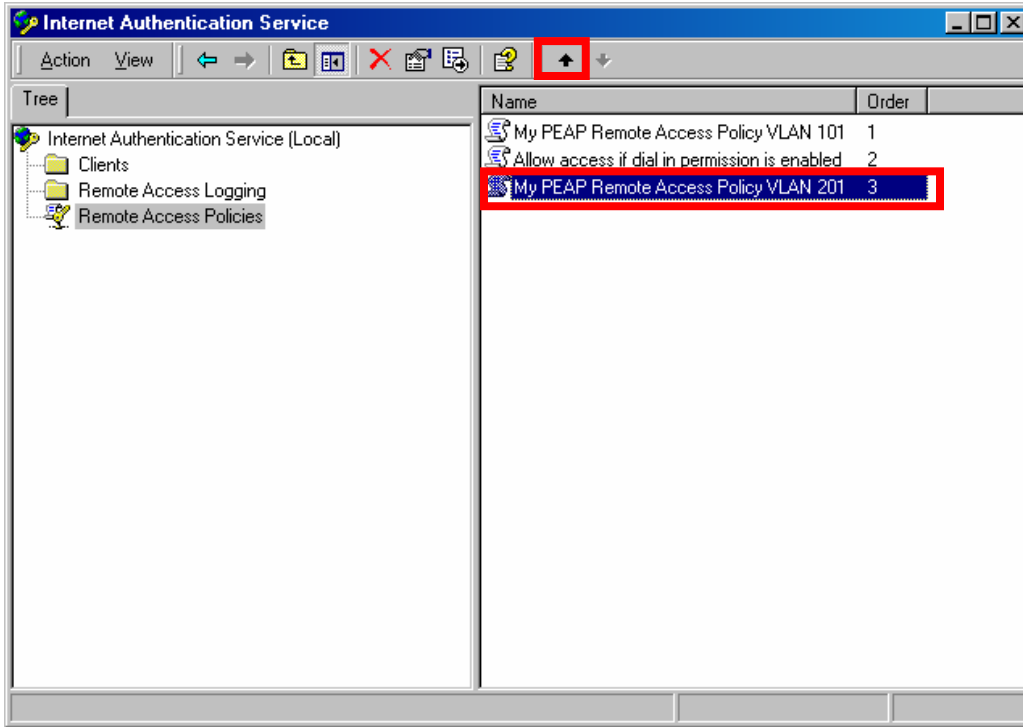
You may see this warning. Click **No**.



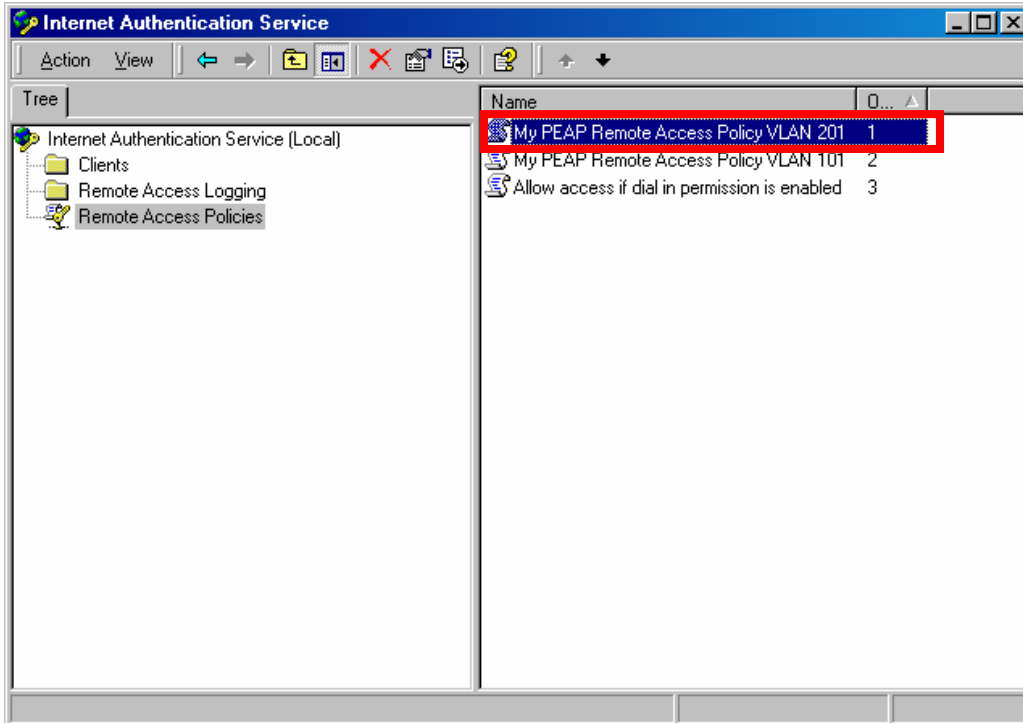
Click **Finish**.



Select the Remote Access Policy you've just created and click on the **Move Up** button until it is at Order 1.

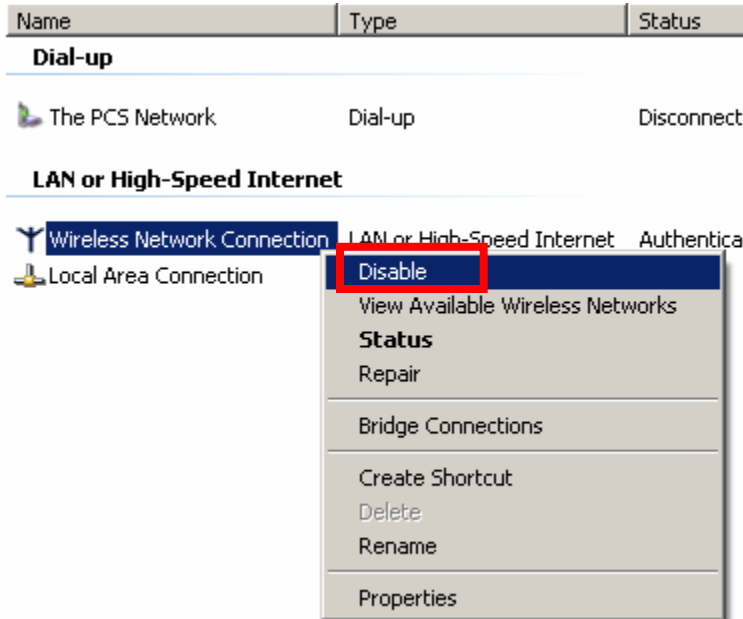


Ensure that this Remote Access Policy as at Order 1.

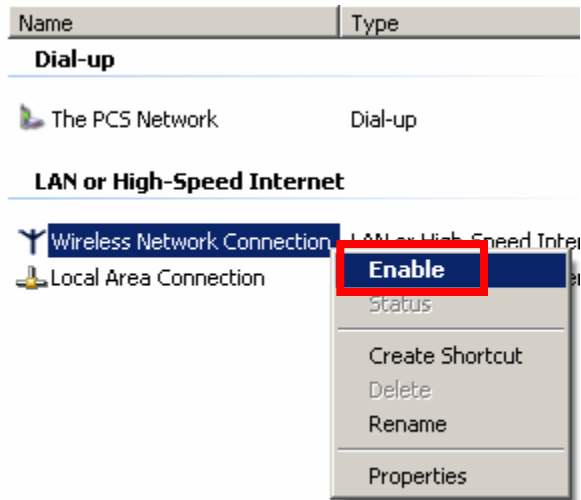


Testing the Configuration for VLAN 201

Test the configuration with the Windows XP computer. From Network Connections, right click on the wireless NIC. Select **Disable**



When the status of the NIC is disabled, right click on the wireless NIC again and select **Enable**.



This will force the XP computer to re-authenticate to the wireless LAN and receive the RADIUS attributes from the Remote Access Policy for VLAN 201.



Open a command prompt window and enter **ping 10.1.1.201**. Check that the pings are successful.

```
C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
U:\>ping 10.1.1.201
Pinging 10.1.1.201 with 32 bytes of data:
Reply from 10.1.1.201: bytes=32 time=2ms TTL=128
Reply from 10.1.1.201: bytes=32 time=4ms TTL=128
Reply from 10.1.1.201: bytes=32 time=2ms TTL=128
Reply from 10.1.1.201: bytes=32 time=3ms TTL=128
Ping statistics for 10.1.1.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 2ms
U:\>
```

Enter **ping 10.1.1.101**. Check that the pings are unsuccessful.

```
C:\WINDOWS\System32\cmd.exe
Pinging 10.1.1.201 with 32 bytes of data:
Reply from 10.1.1.201: bytes=32 time=2ms TTL=128
Reply from 10.1.1.201: bytes=32 time=4ms TTL=128
Reply from 10.1.1.201: bytes=32 time=2ms TTL=128
Reply from 10.1.1.201: bytes=32 time=3ms TTL=128
Ping statistics for 10.1.1.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 2ms
U:\>ping 10.1.1.101
Pinging 10.1.1.101 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.1.1.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
U:\>
```

This confirms that this Remote Access Policy is properly configured for VLAN 201.

So now, we have two Remote Access Policies: one that will tag wireless clients for VLAN 101 and another that will tag wireless clients for VLAN 201.

In the next section, you will be configuring the Windows 2000 Server to select which Remote Access Policy to use depending on the authentication credentials entered by the wireless client.



Configuring Active Directory User Groups

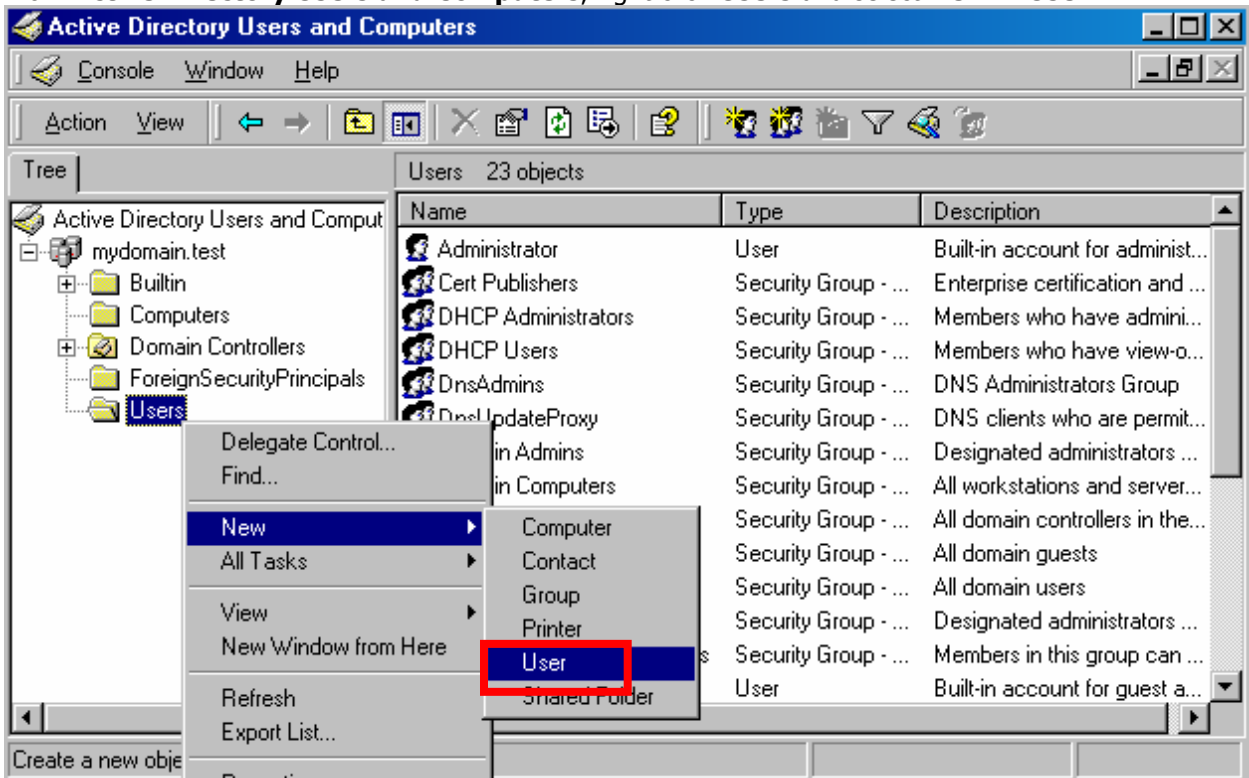
Using the physical network configuration from Figure 1, let's create an example of how Dynamic VLANs can be used with Microsoft IAS. Let's say we make the following network policies:

- VLAN 1: For network management only. No wireless LAN clients permitted.
- VLAN 101: For wireless "Guest" users only.
- VLAN 201: For wireless "Test" users only.

In this section, you will configure the Windows 2000 Server Active Directory and IAS such that all wireless "Guest" users will be a member of VLAN 101 and all wireless "Test" users will be a member of VLAN 201.

In Active Directory, you are going to create a "Guest" user and assign it to group "Domain Guests". Then, you are going to take the existing "Test" user and assign it to the group "Domain Admins".

From **Active Directory Users and Computers**, right click **Users** and select **New > User**.





Enter a **First name**, **Last name** and **User logon name** for a "Guest" user. Click **Next >**.

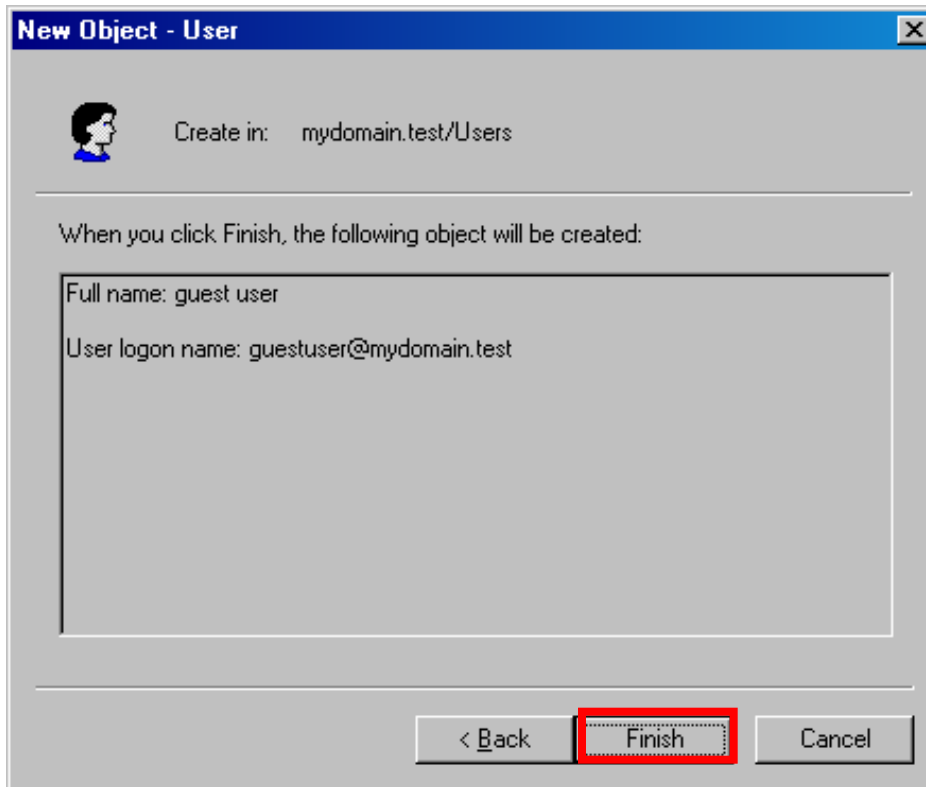
The screenshot shows the 'New Object - User' dialog box. The 'Create in' field is set to 'mydomain.test/Users'. The 'First name' field contains 'guest', the 'Last name' field contains 'user', and the 'Full name' field contains 'guest user'. The 'User logon name' field contains 'guestuser' and the domain dropdown is set to '@mydomain.test'. The 'User logon name (pre-Windows 2000)' field contains 'MYDOMAIN\guestuser'. The 'Next >' button is highlighted with a red box.

Enter a **Password** and **Confirm password** for the "Guest" user. Click **Next >**.

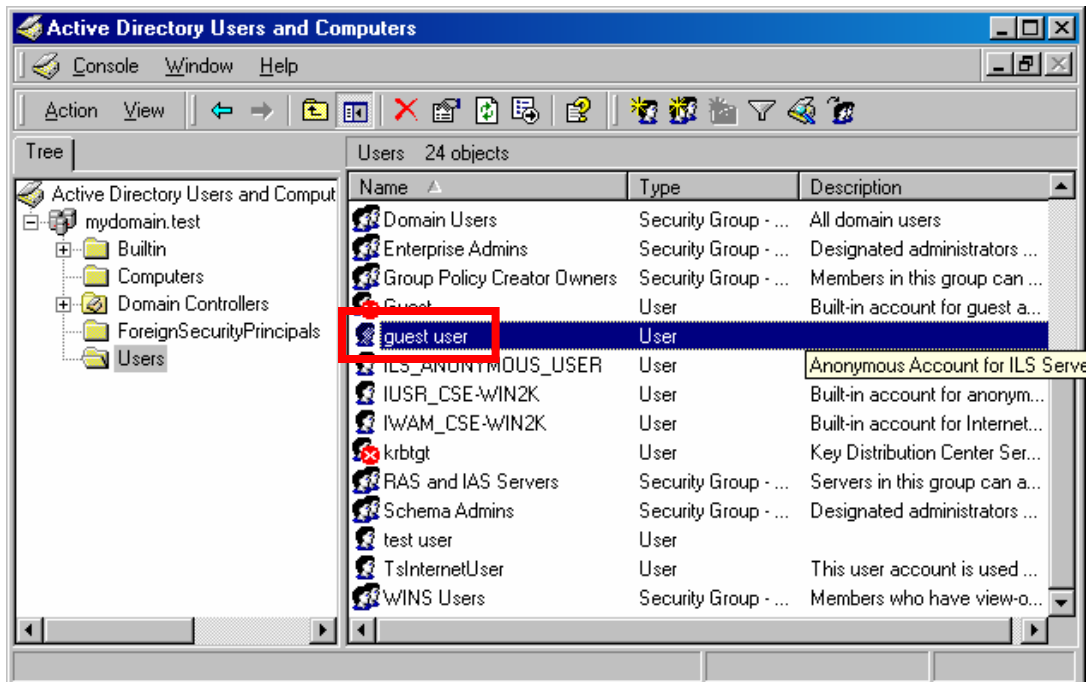
The screenshot shows the 'New Object - User' dialog box. The 'Create in' field is set to 'mydomain.test/Users'. The 'Password' and 'Confirm password' fields are both filled with '*****' and are highlighted with a red box. Below these fields are four unchecked checkboxes: 'User must change password at next logon', 'User cannot change password', 'Password never expires', and 'Account is disabled'. The 'Next >' button is highlighted with a red box.



Click **Finish**.



Double click the Active Directory "Guest" user you've just created.

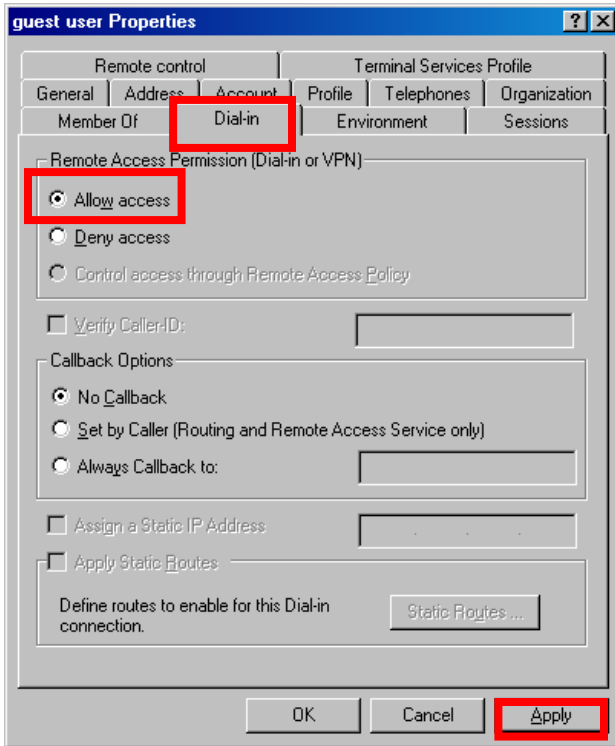


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

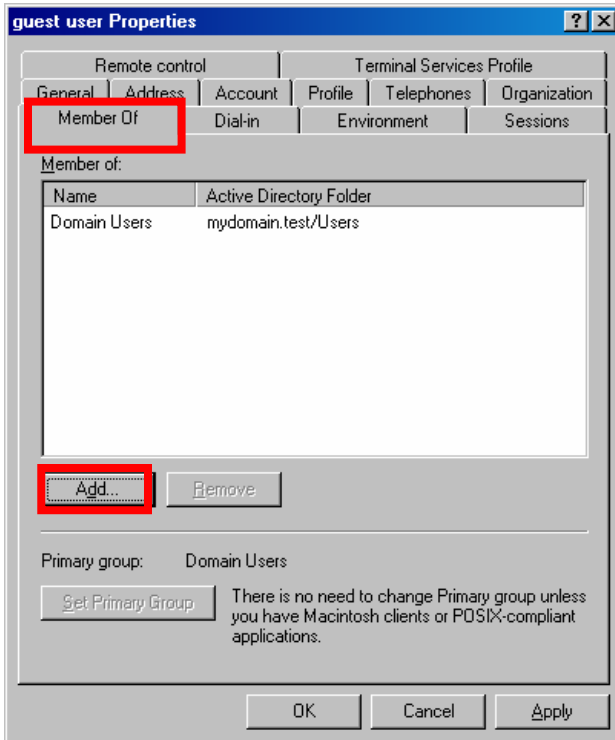
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Select the **Dial-in** tab. Select **Allow access**. Click **Apply**.



Select the **Member Of** tab. Click **Add...**

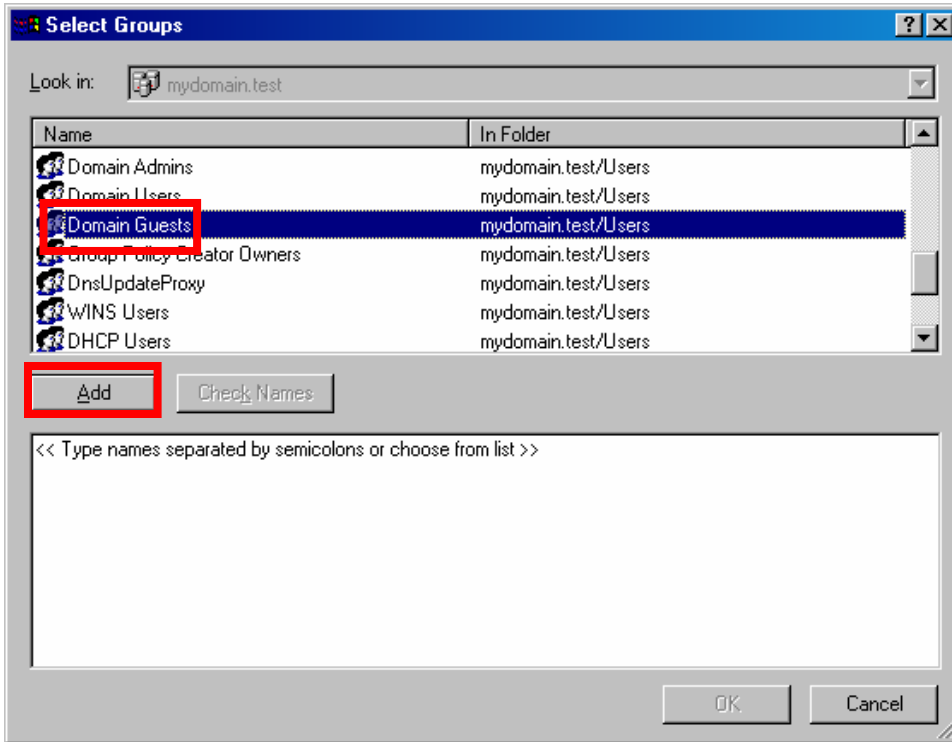


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

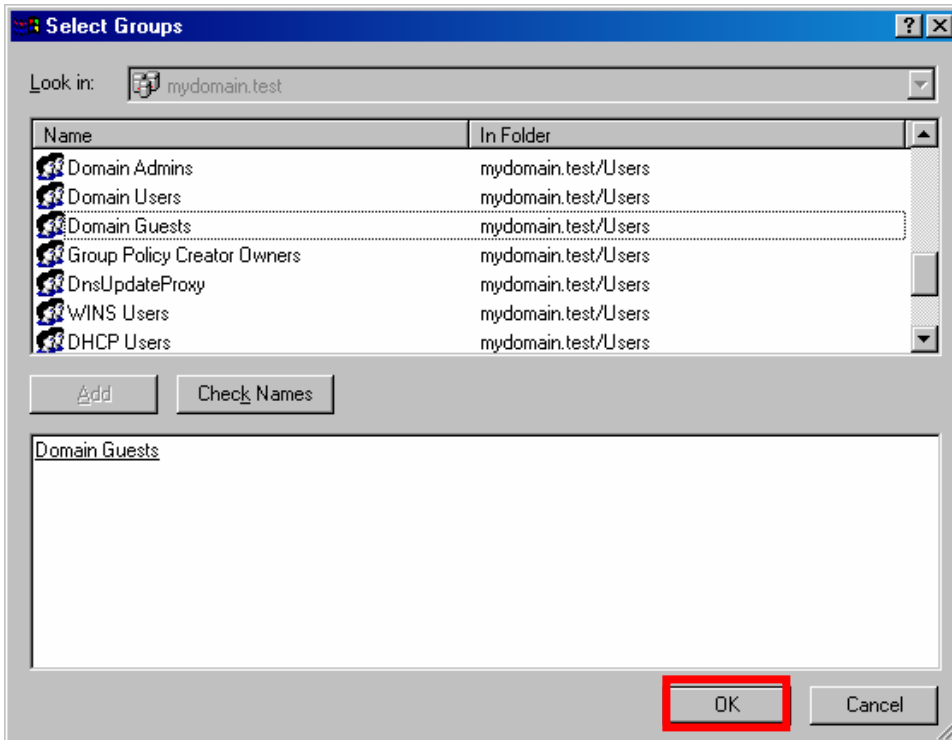
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Select the group **Domain Guest**. Click **Add**.



Click **OK**.

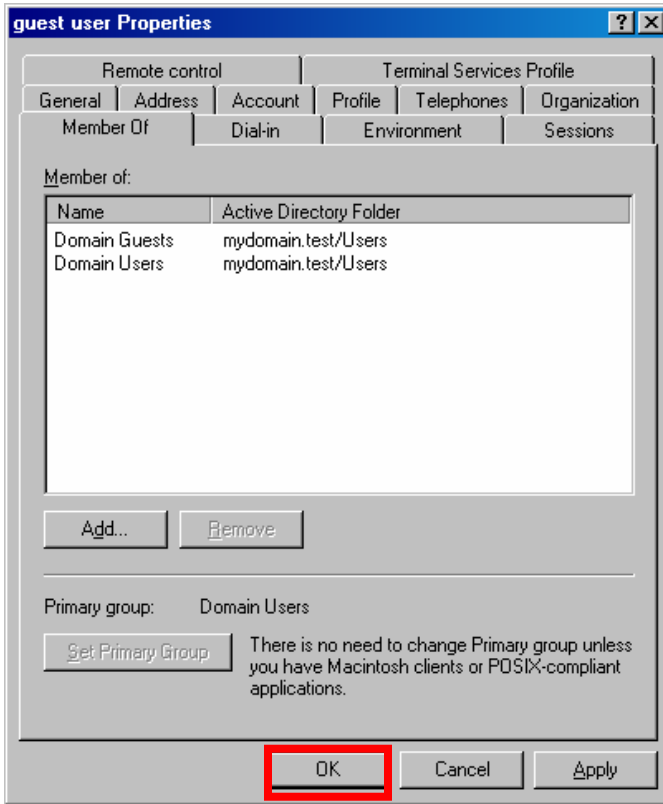


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

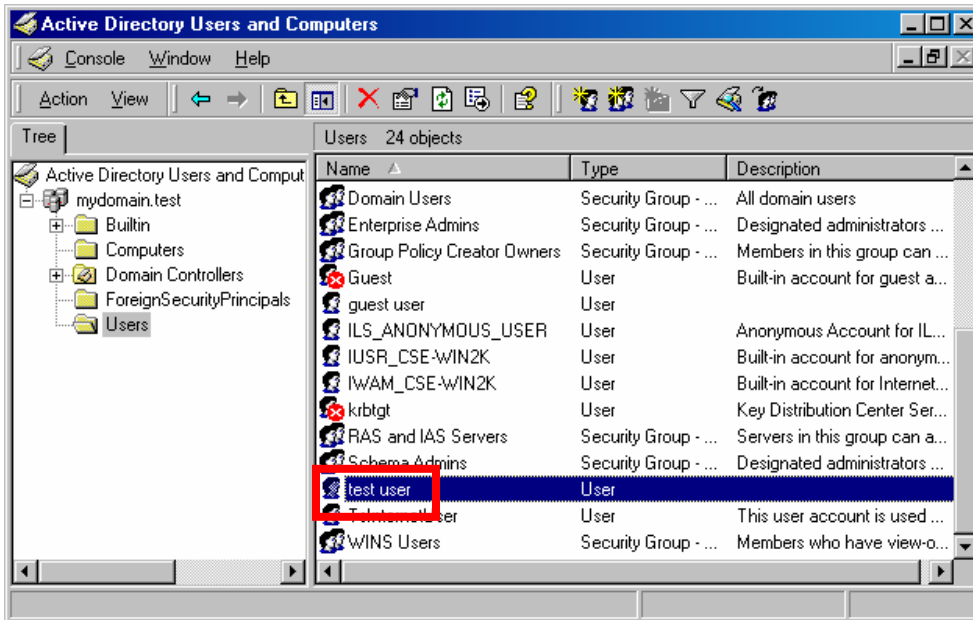
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Click **OK**.



Double click the Active Directory User that you created in the WPA 802.1x PEAP installation guide. This will be the "Test" user.

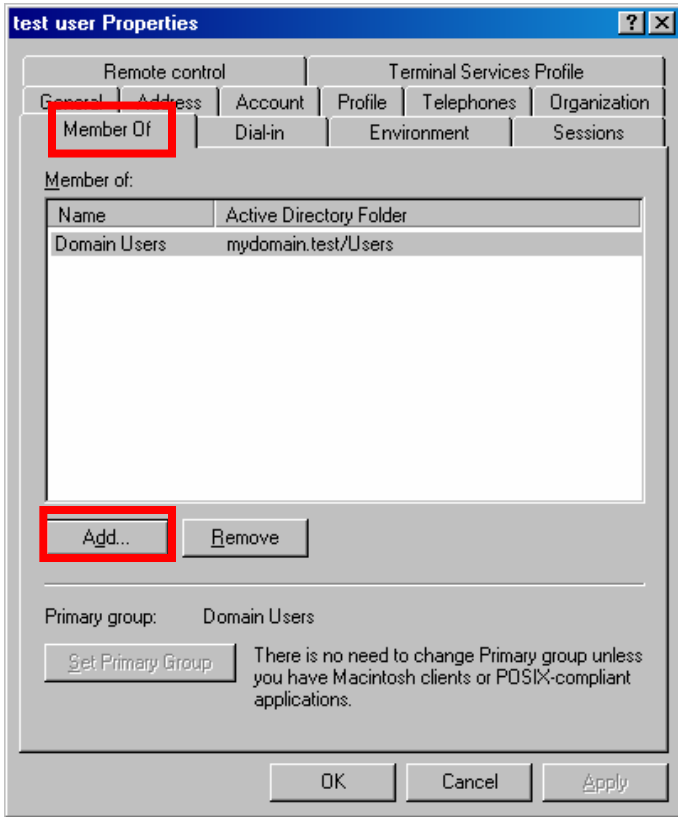


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

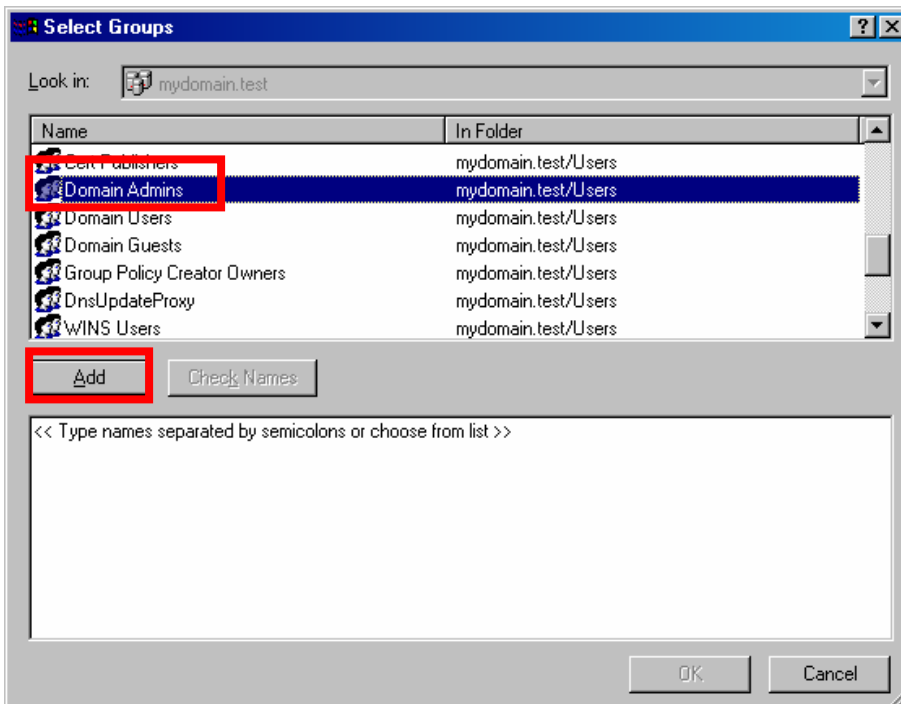
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Click on the **Member Of** tab. Click **Add**.



Select the group **Domain Admins**. Click **Add**.

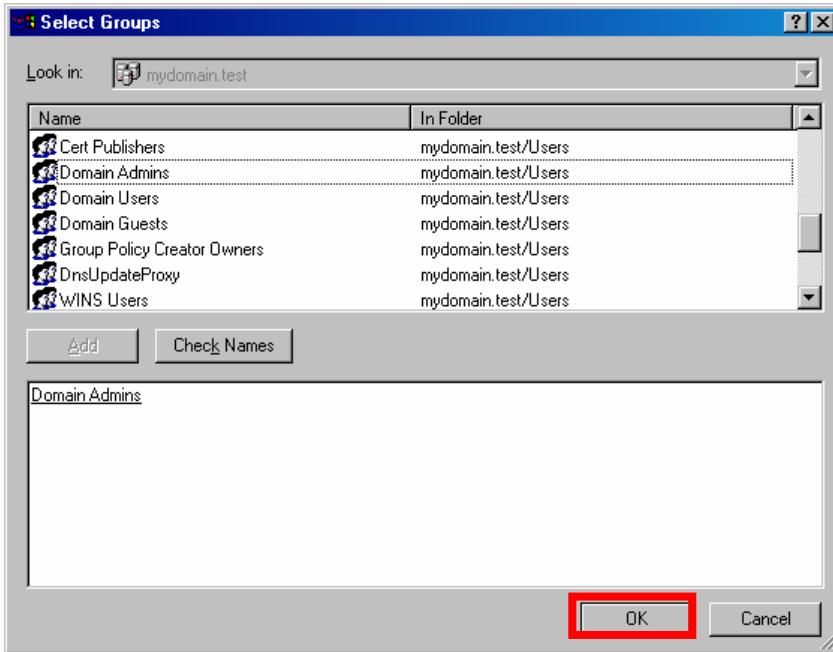


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

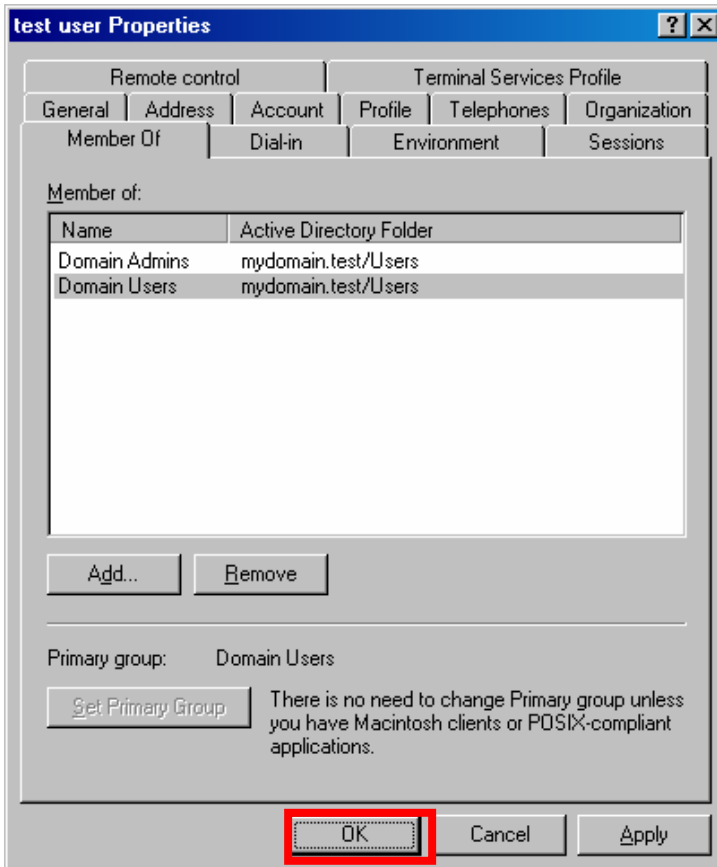
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Click **OK**.



Click **OK**.



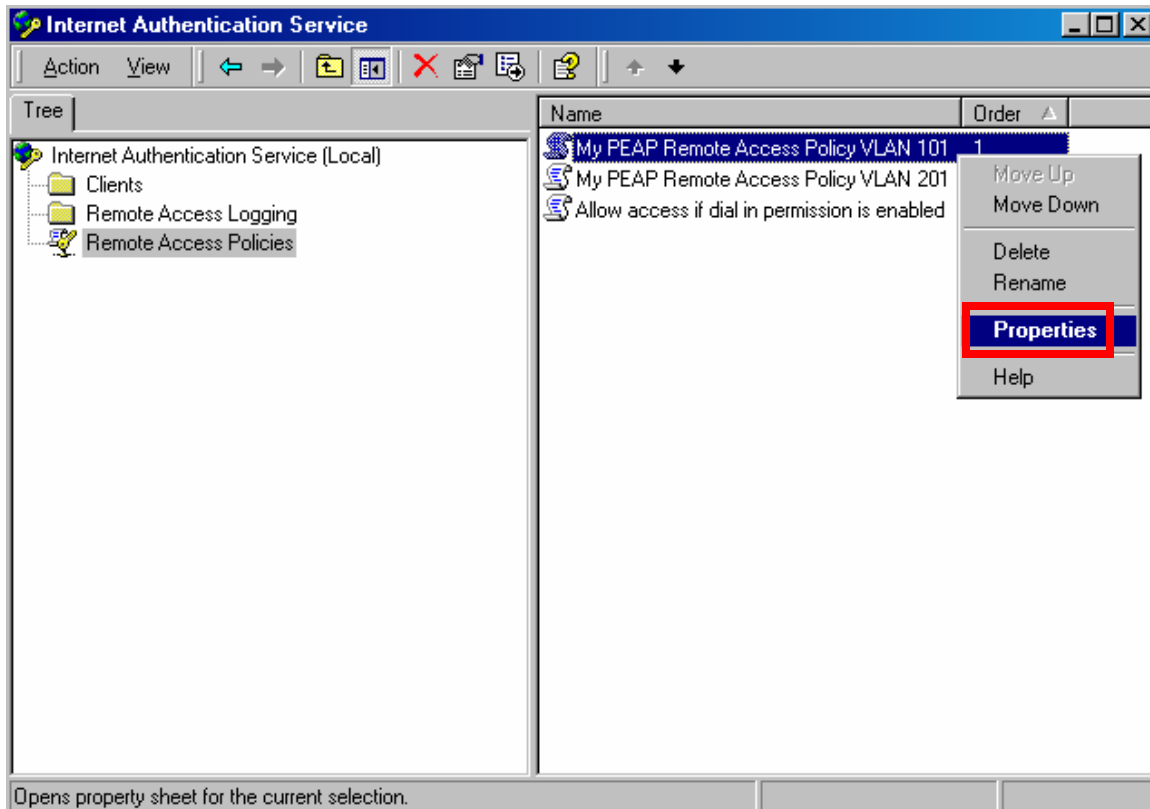
So now you have two users in Active Directory:

- "Guest" user assigned to the group "Domain Guests"
- "Test" user assigned to the group "Domain Admins"

Next, you are going to configure the Remote Access Policies in IAS to make all wireless "Guest" users a member of VLAN 101 and all wireless "Test" users a member of VLAN 201.

Configuring IAS

From **IAS**, right click on the Remote Access Policy for VLAN 101. Select **Properties**.

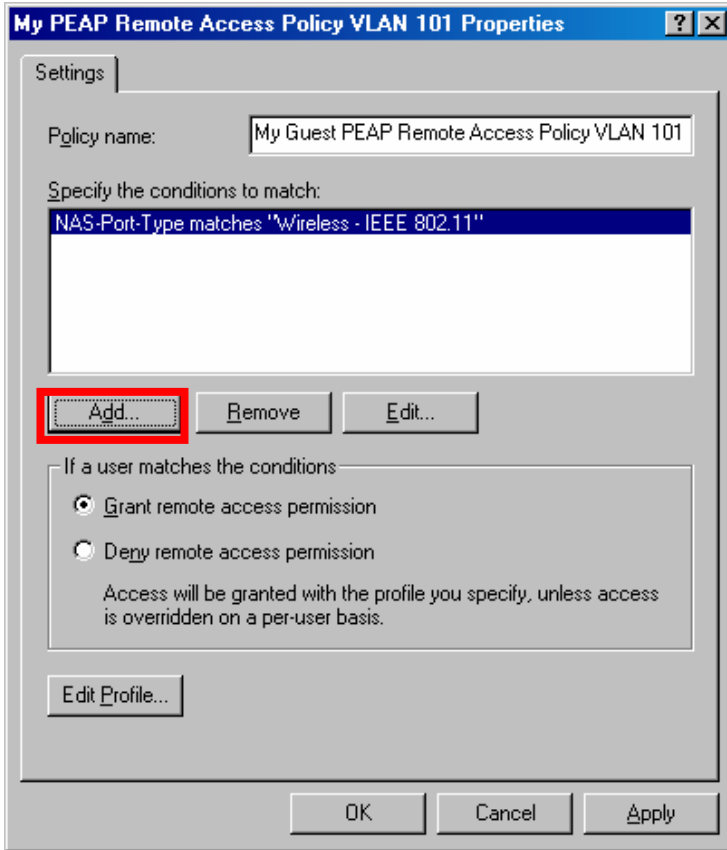


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

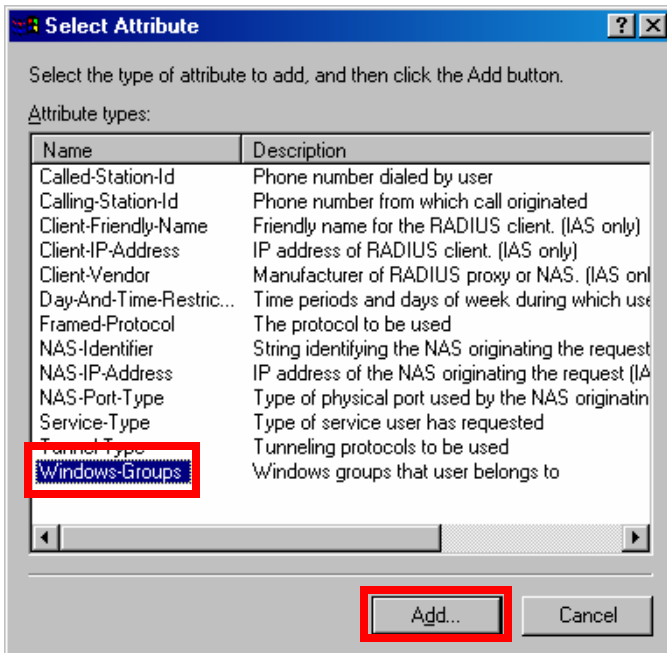
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Click **Add**.



Select **Windows-Group**. Click **Add...**



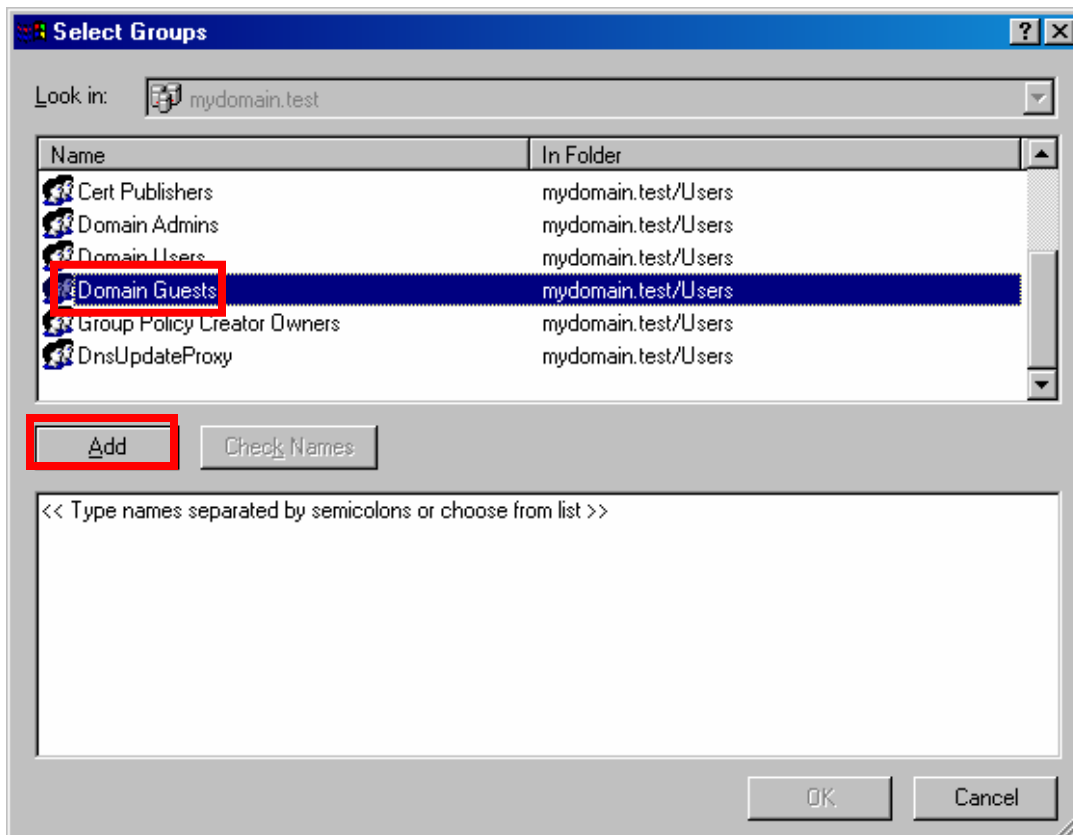
WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

802.1X DYNAMIC VLANS WITH MICROSOFT IAS

Click **Add...** .

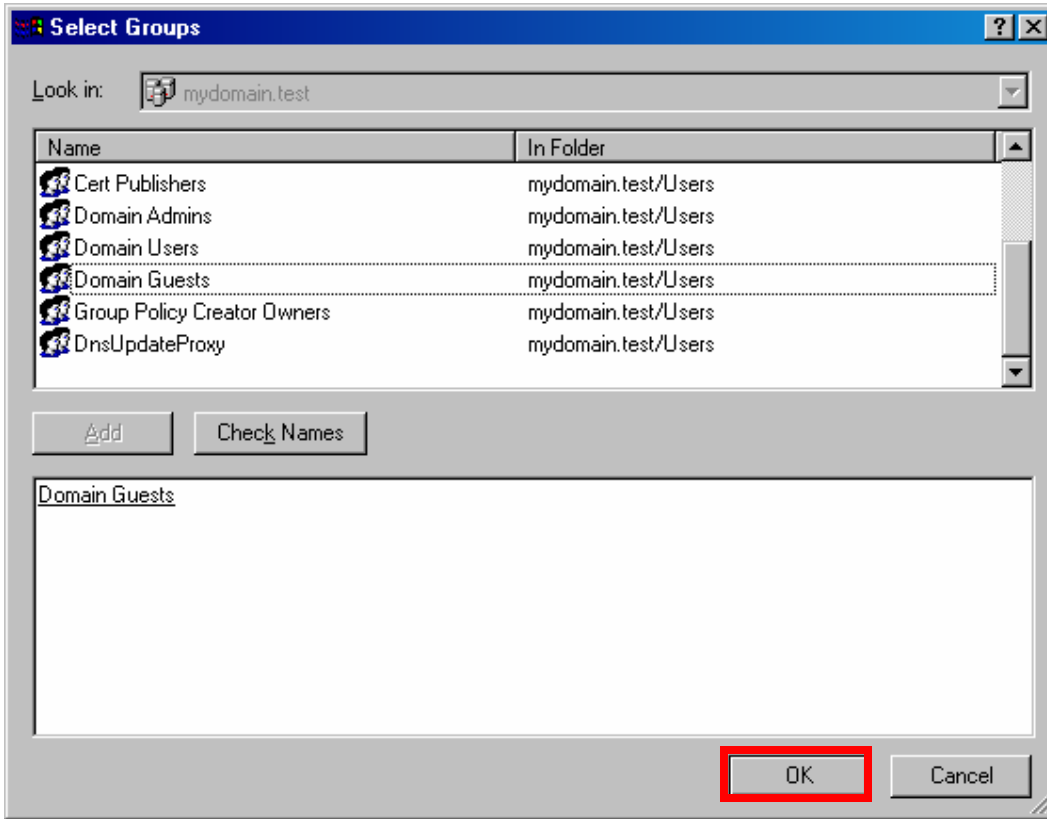


Select **Domain Guests**. Click **Add**.

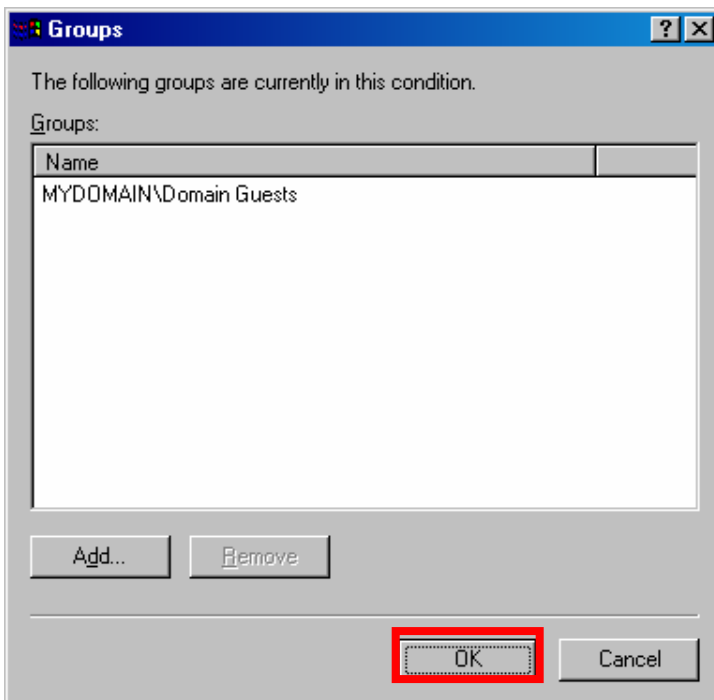




Click **OK**.



Click **OK**.

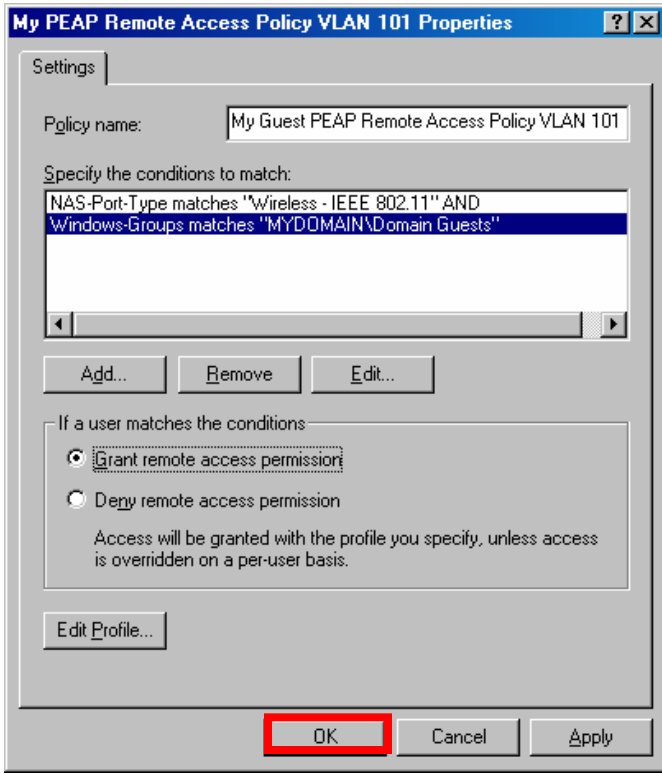


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

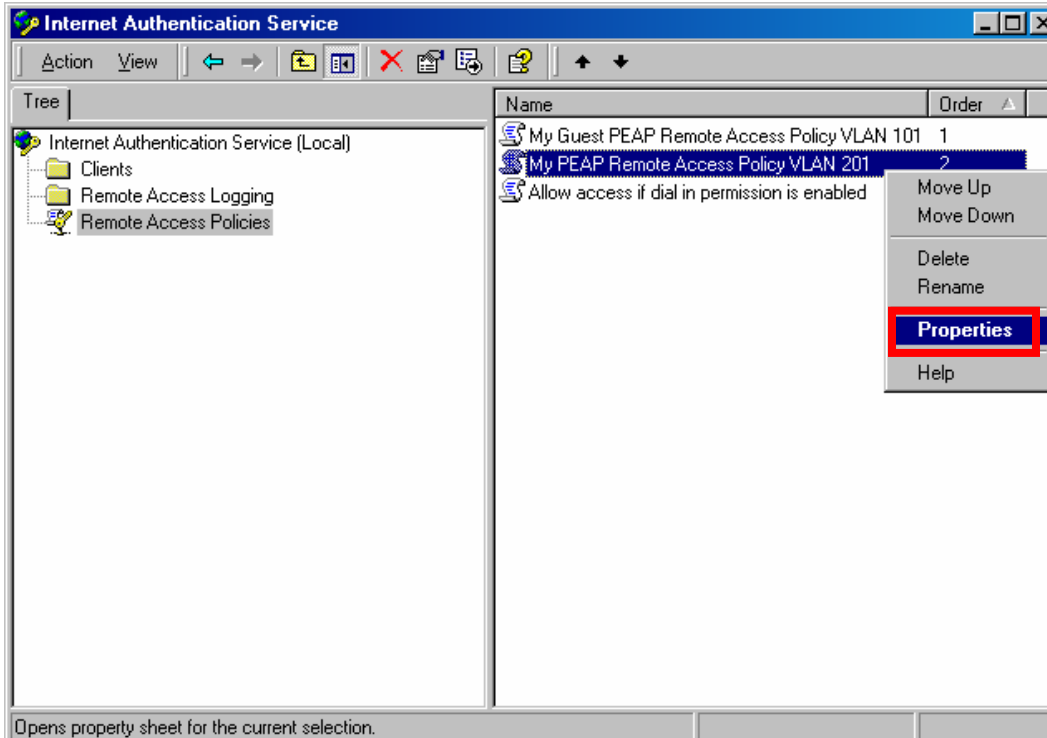
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Click **OK**.



Right click the Remote Access Policy for VLAN 201. Select **Properties**.

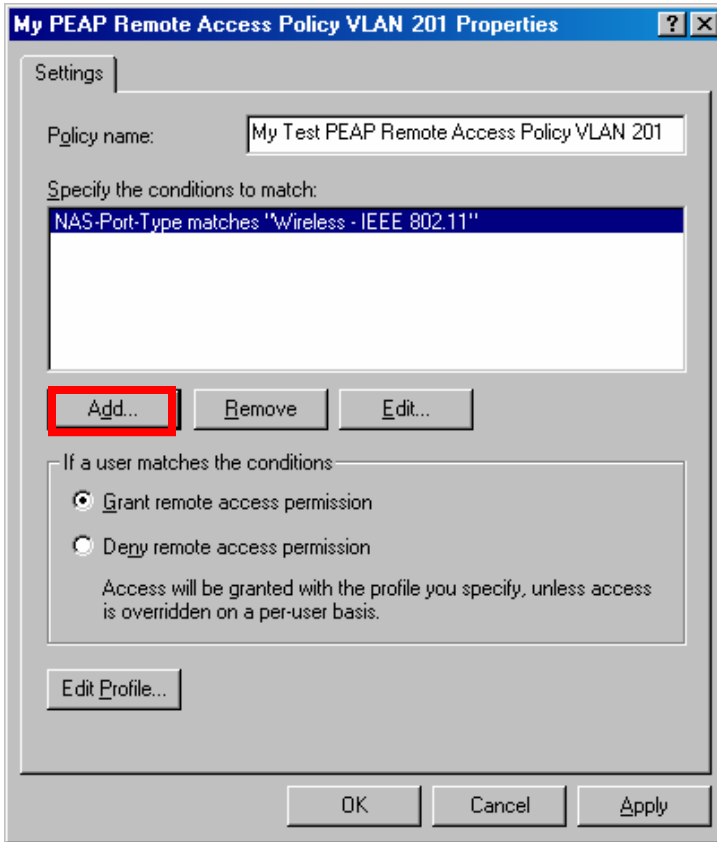


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

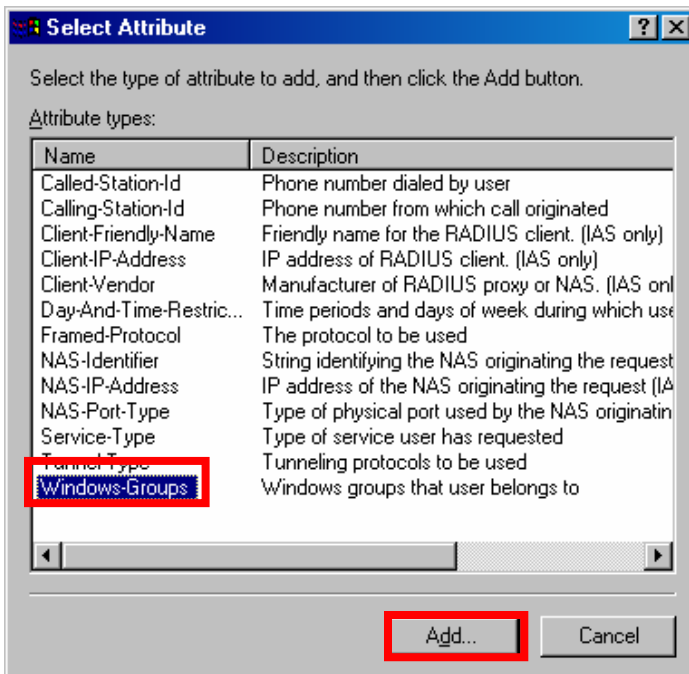
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Click **Add...** .



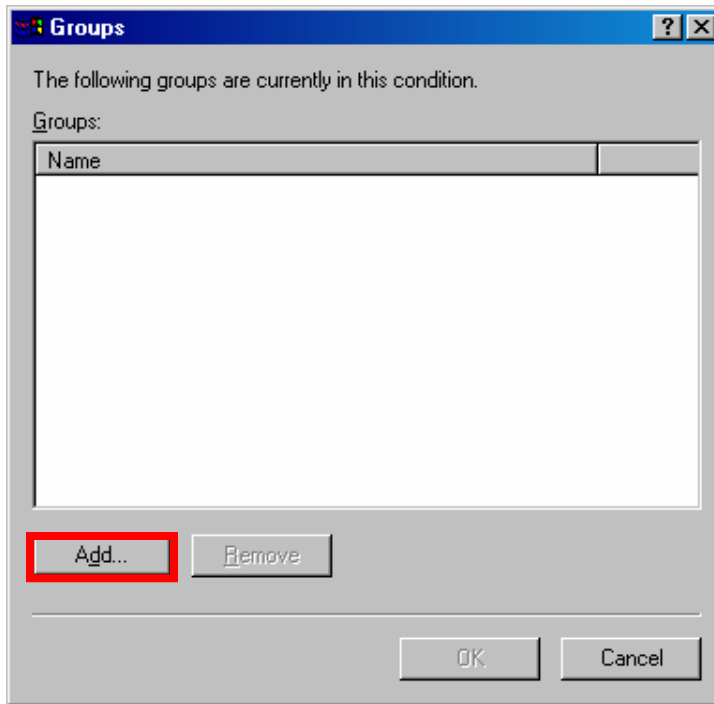
Select **Windows-Group**. Click **Add...** .



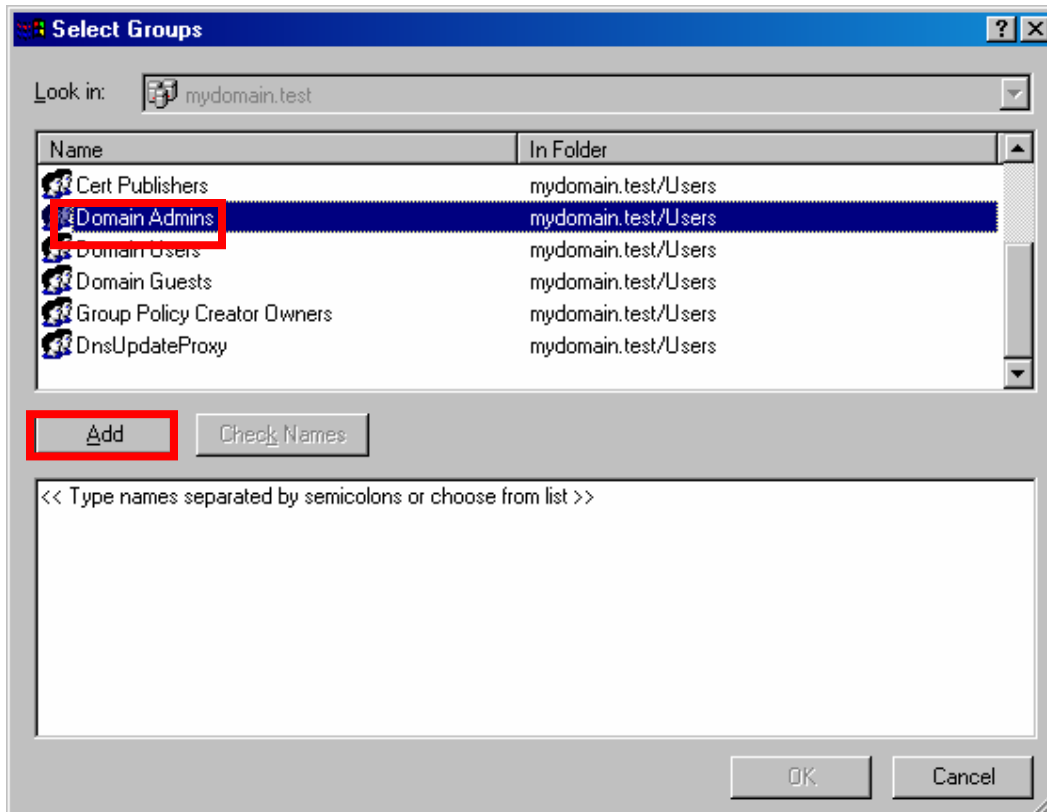
WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

802.1X DYNAMIC VLANS WITH MICROSOFT IAS

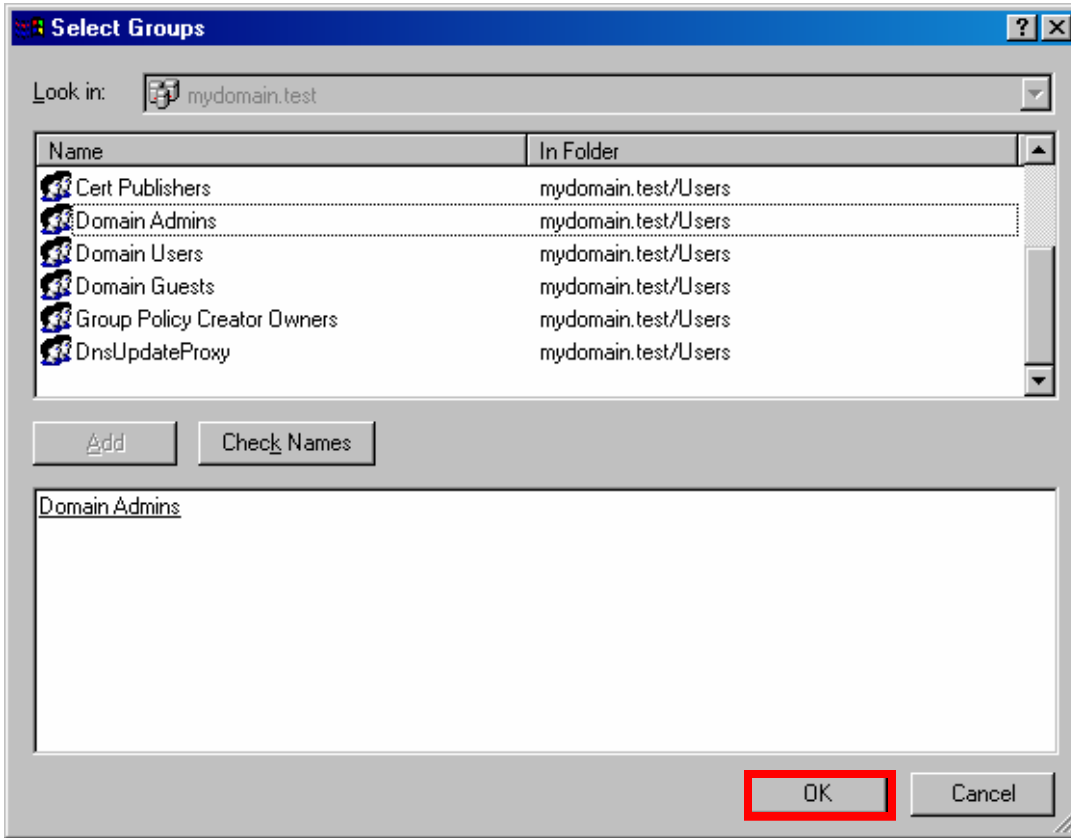
Click **Add...** .



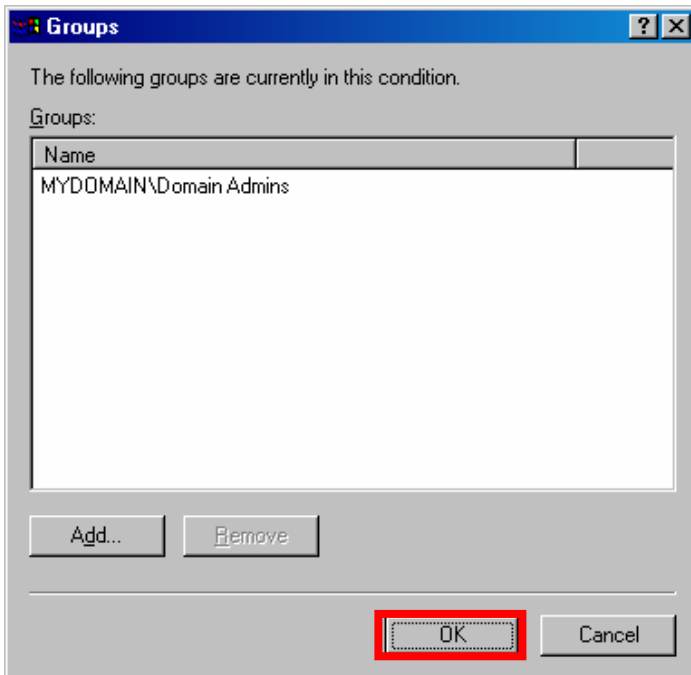
Select **Domain Admins**. Click **Add**.



Click **OK**.



Click **OK**.

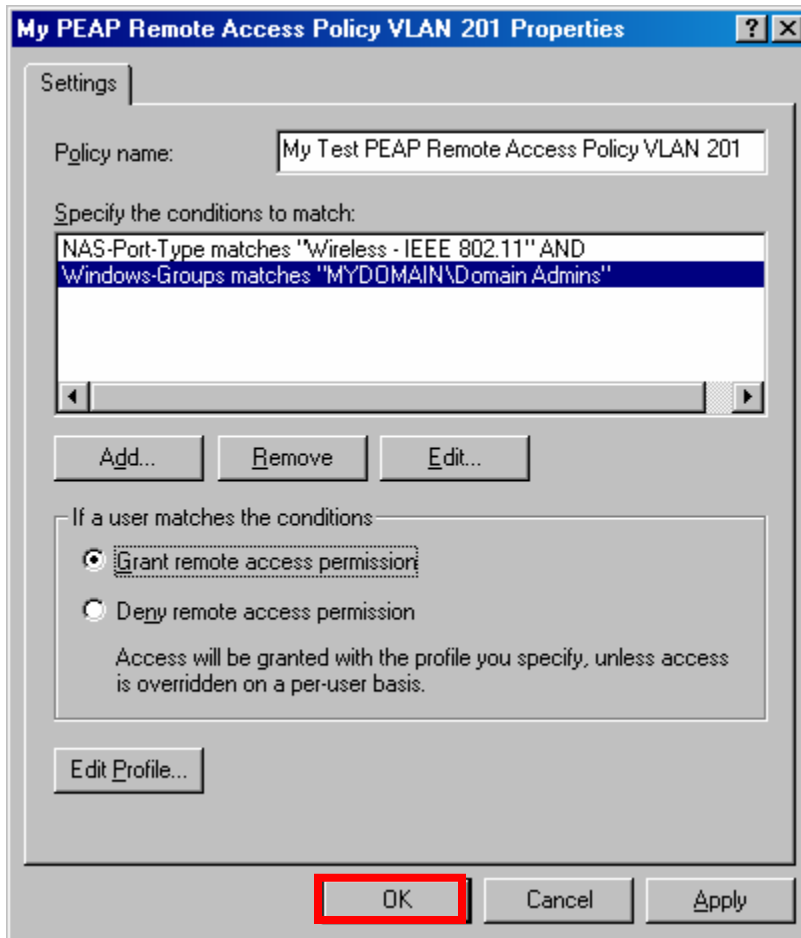


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

802.1X DYNAMIC VLANS WITH MICROSOFT IAS



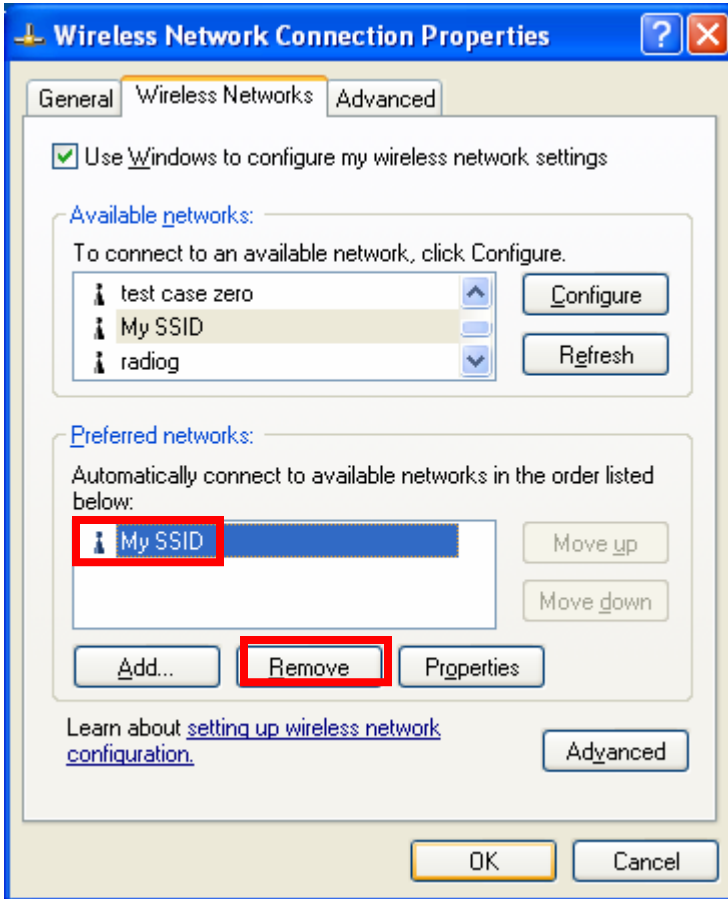
Click **OK**.



Now you are ready to test the Windows 2000 Server configuration using the Windows XP computer as the wireless client.

Testing the Configuration for "Guest" User on VLAN 101

From the Windows XP computer, open the properties for the wireless NIC. Select the **Wireless Networks** tab. Select the network (or SSID) configured on the IP 200 from **Preferred networks**. Click **Remove**.

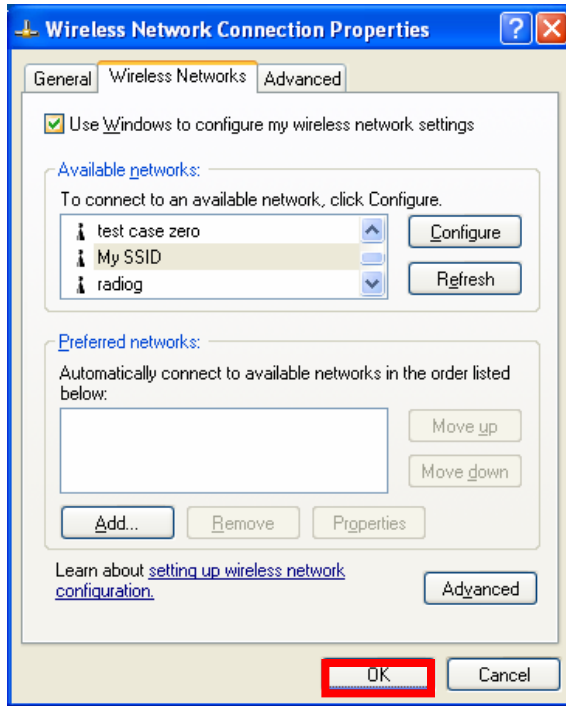


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

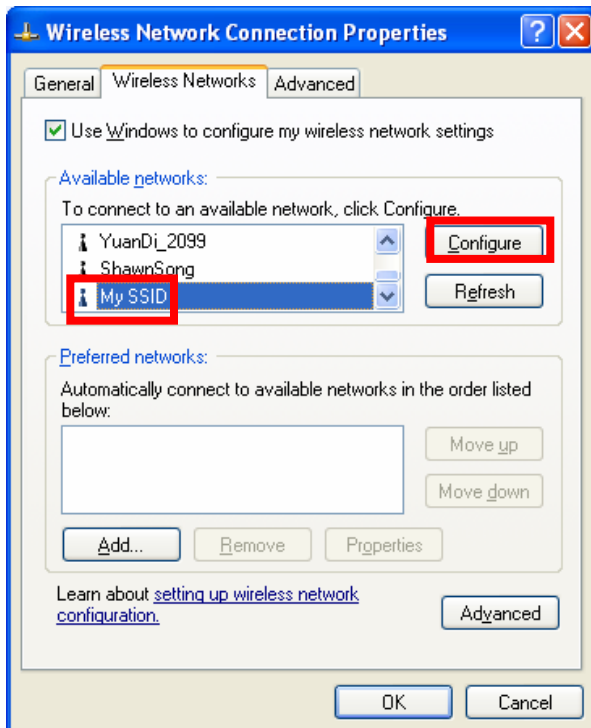
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Click **OK**.



Open the properties of the wireless NIC. Select the **Wireless Networks** tab. From **Available networks**, select the wireless network (SSID) that you configured on the IP 200 and click **Configure**.

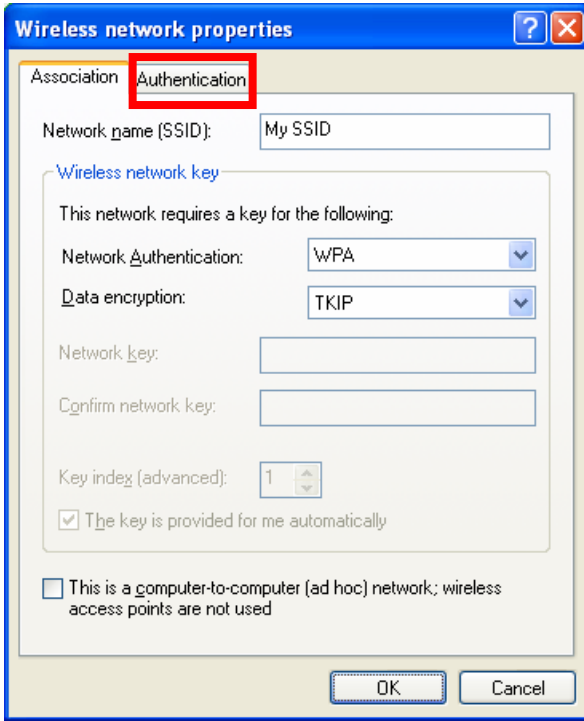


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

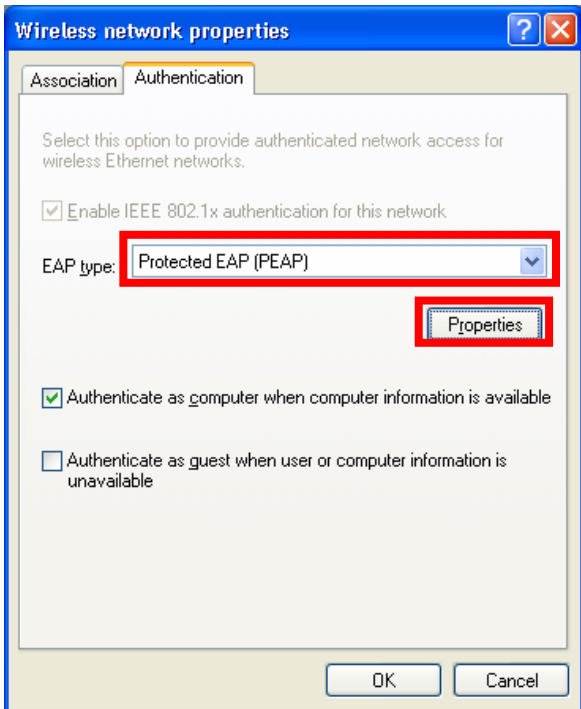
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Click on the **Authentication** tab.

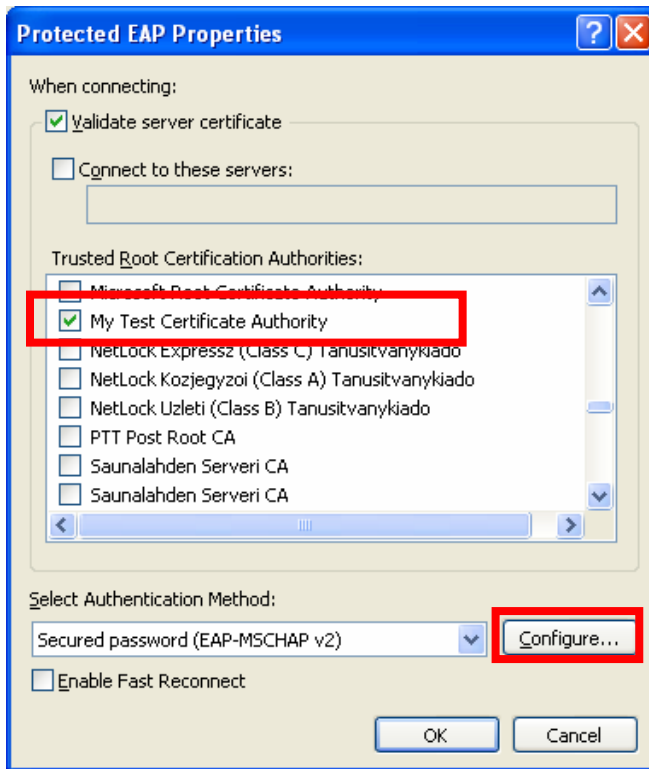


Select **Protected EAP (PEAP)** from the EAP type drop down box. Click **Properties**.

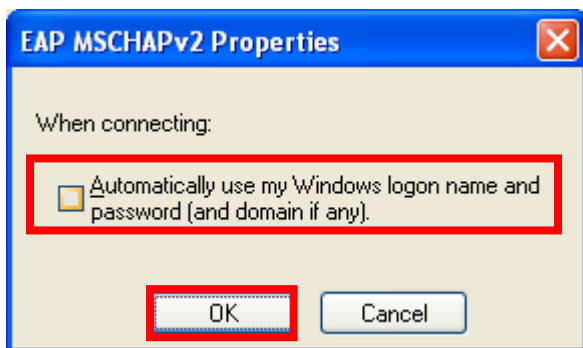




From **Trusted Root Certification Authorities**, check the certificate with the CA name that you entered in the Installing Certification Authority section. Click **Configure...** .



Uncheck **Automatically use my Windows logon name and password (and domain if any)**. Click **OK**.

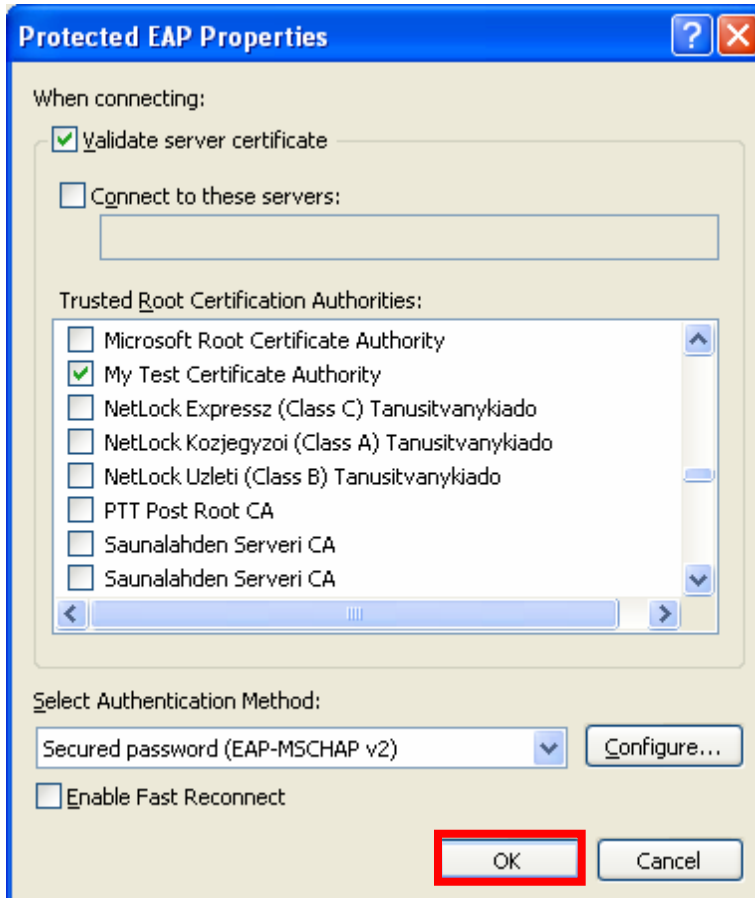


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Click **OK**.

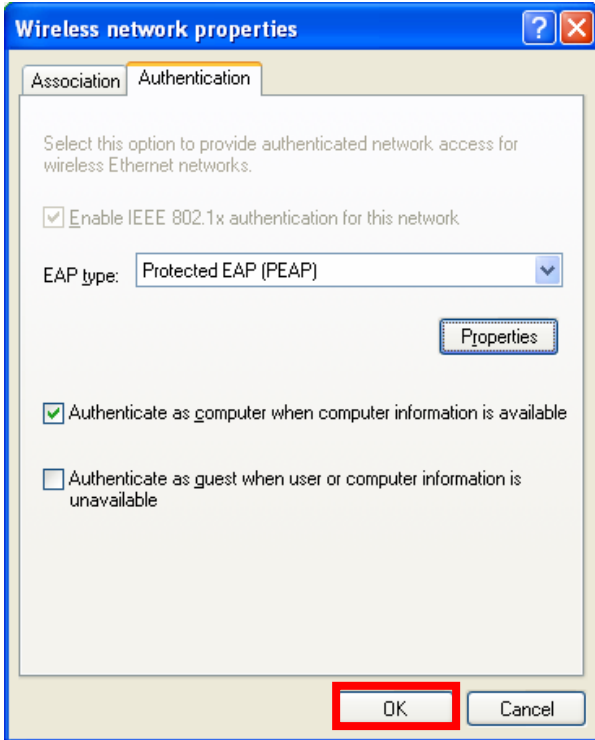


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

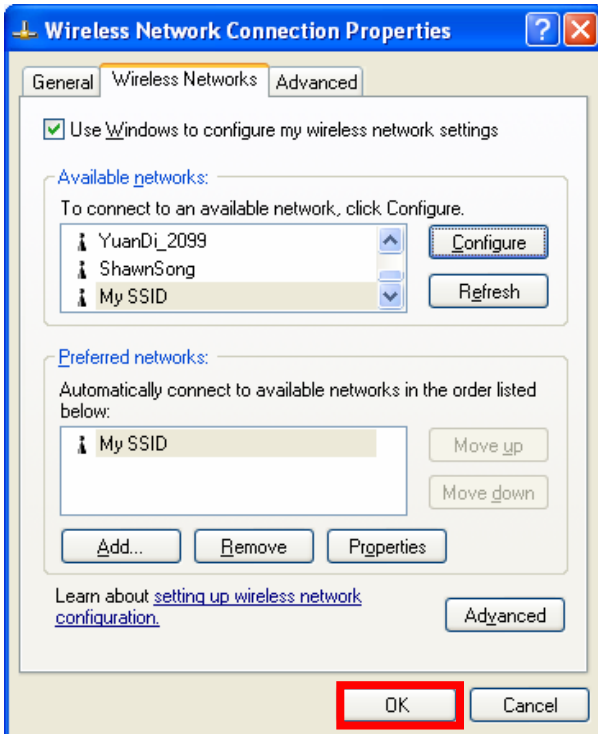
802.1X DYNAMIC VLANs WITH MICROSOFT IAS



Click **OK**.



Click **OK**.

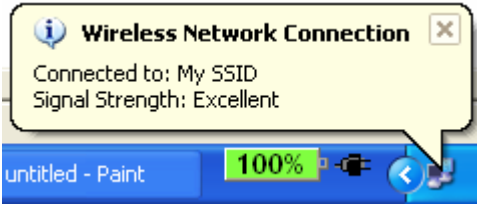


WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE

802.1X DYNAMIC VLANs WITH MICROSOFT IAS



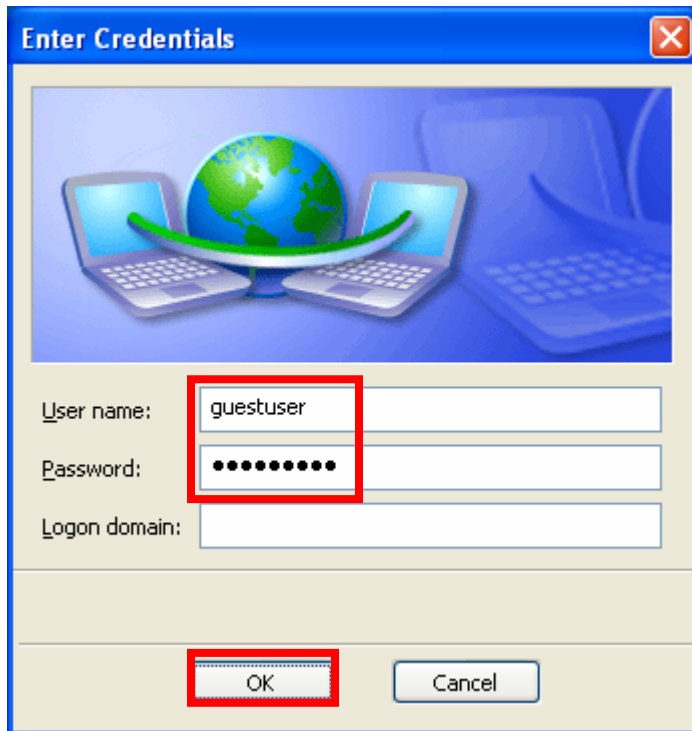
This information bubble will appear for the task tray icon for the wireless NIC.



Then, this information bubble will appear. Click on the information bubble.

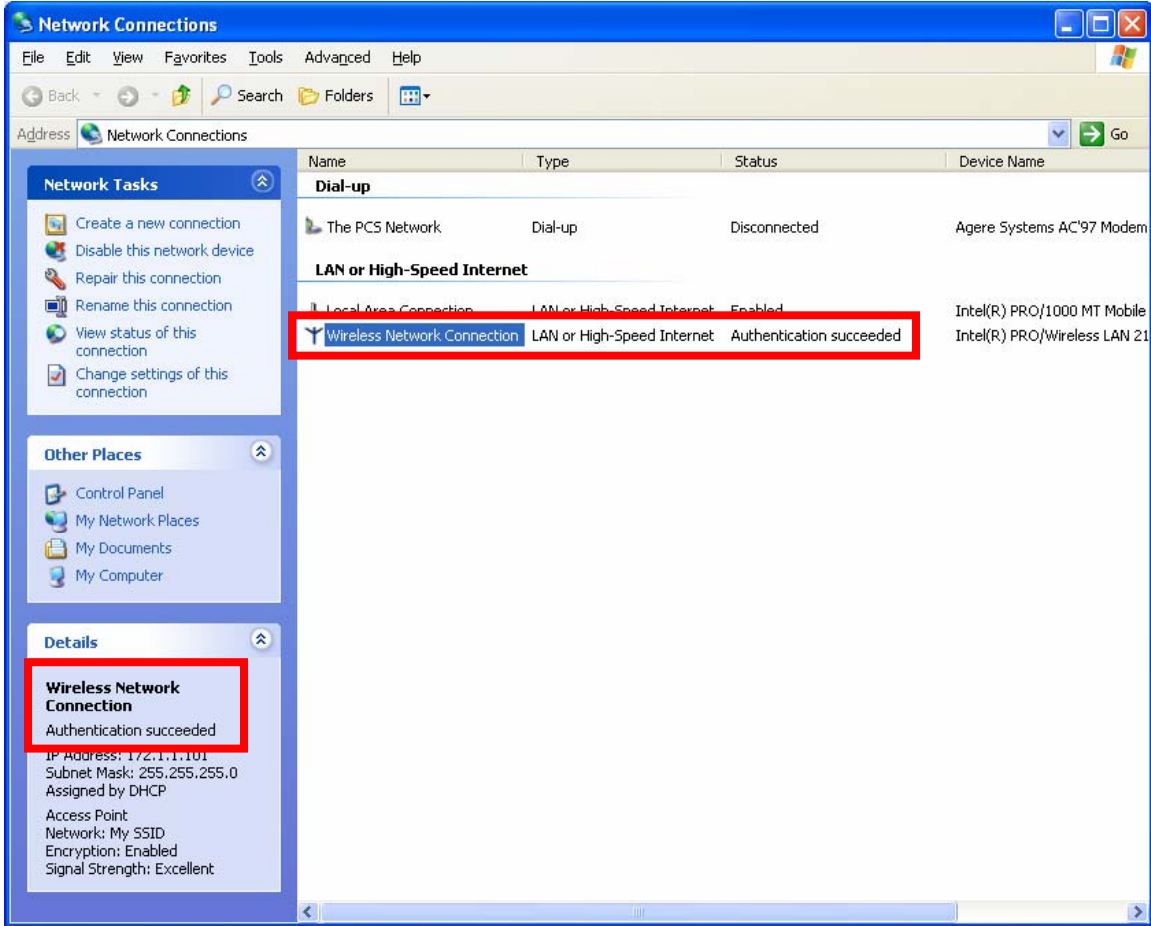


Enter the **User name** and **Password** for the "Guest" user you created in Active Directory. Click **OK**.





If the correct user name and password are entered the status of the wireless NIC will change to **Authentication succeeded**. The Windows XP computer is now connected to the IP 200 and is a member of VLAN 101.





Open a command prompt window and enter **ping 10.1.1.101**. Check that the pings are successful.

```
C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

U:\>ping 10.1.1.101

Pinging 10.1.1.101 with 32 bytes of data:

Reply from 10.1.1.101: bytes=32 time=7ms TTL=128
Reply from 10.1.1.101: bytes=32 time=10ms TTL=128
Reply from 10.1.1.101: bytes=32 time=11ms TTL=128
Reply from 10.1.1.101: bytes=32 time=8ms TTL=128

Ping statistics for 10.1.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 11ms, Average = 9ms

U:\>
```

Enter **ping 10.1.1.201**. Check that the pings are unsuccessful.

```
C:\WINDOWS\System32\cmd.exe

Pinging 10.1.1.101 with 32 bytes of data:

Reply from 10.1.1.101: bytes=32 time=7ms TTL=128
Reply from 10.1.1.101: bytes=32 time=10ms TTL=128
Reply from 10.1.1.101: bytes=32 time=11ms TTL=128
Reply from 10.1.1.101: bytes=32 time=8ms TTL=128

Ping statistics for 10.1.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 11ms, Average = 9ms

U:\>ping 10.1.1.201

Pinging 10.1.1.201 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.1.201:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

U:\>
```

This confirms that the Windows 2000 Server is properly configured for "Guest" users on VLAN 101.

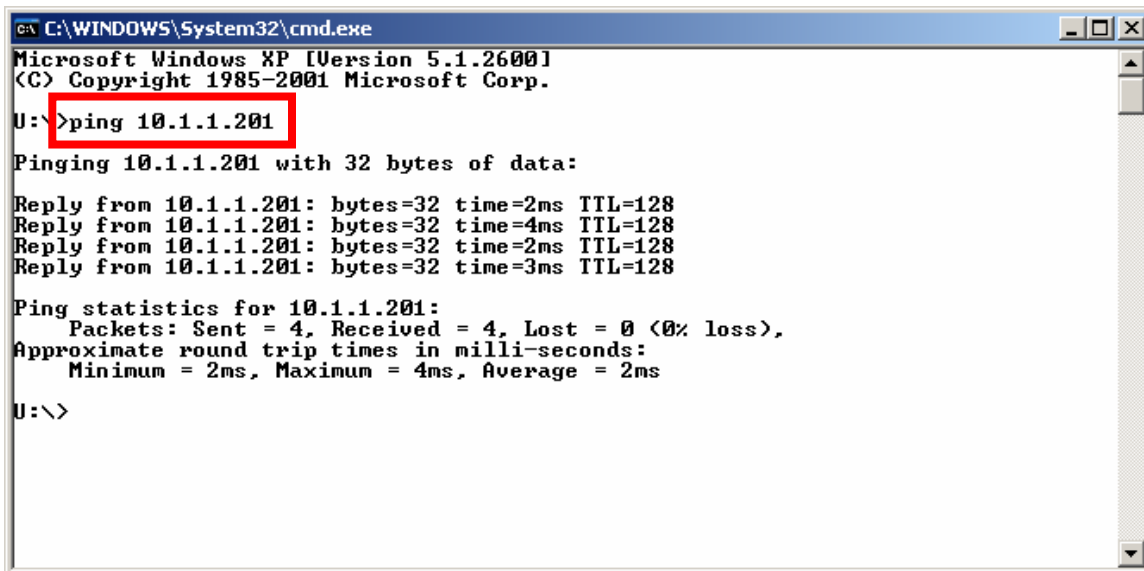


Testing the Configuration for "Test" User on VLAN 201

Repeat all of the instructions from the previous section, **Testing the Configuration for "Guest" Users on VLAN 101**, except enter the **User name** and **Password** for the "Test" user instead of the "Guest" user. Click **OK**.



Open a command prompt window and enter **ping 10.1.1.201**. Check that the pings are successful.





Enter **ping 10.1.1.101**. Check that the pings are unsuccessful.

```
C:\WINDOWS\System32\cmd.exe
Pinging 10.1.1.201 with 32 bytes of data:
Reply from 10.1.1.201: bytes=32 time=2ms TTL=128
Reply from 10.1.1.201: bytes=32 time=4ms TTL=128
Reply from 10.1.1.201: bytes=32 time=2ms TTL=128
Reply from 10.1.1.201: bytes=32 time=3ms TTL=128
Ping statistics for 10.1.1.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 2ms
U:\>ping 10.1.1.101
Pinging 10.1.1.101 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.1.1.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
U:\>
```

This confirms that the Windows 2000 Server is properly configured for "Test" users on VLAN 201.

WHITE PAPER: IRONPOINT 200 INSTALLATION GUIDE
802.1X DYNAMIC VLANS WITH MICROSOFT IAS



Foundry Networks, Inc.
Headquarters
2100 Gold Street
P.O. Box 649100
San Jose, CA 95164-9100

U.S. and Canada Toll-free: (888) TURBOLAN
Direct telephone: +1 408.586.1700
Fax: +1 408.586.1900
Email: info@foundrynet.com
Web: <http://www.foundrynet.com>

Foundry Networks, BigIron, EdgeIron, FastIron, NetIron, ServerIron, and the "Iron" family of marks are trademarks or registered trademarks of Foundry Networks, Inc. in the United States and other countries. All other trademarks are the properties of their respective owners.

©2004 Foundry Networks, Inc. All Rights Reserved.