Procedure

English

Setting Up the Kodak Magnus Computer to the Network

Part number 731-01022A-EN

graphics.kodak.com

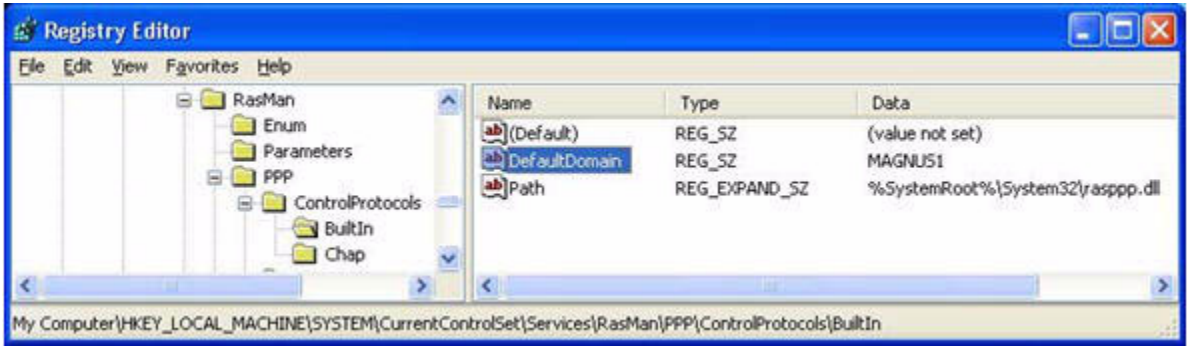
Kodak

Setting Up the Magnus 800 Computer to the Network

This section describes how to set up the *Magnus* 800 to the customer's local network.

Setting Up and Verifying the Computer's Name in the Registry

1. Find out the *Magnus* 800's computer name.
   - Right-click **My Computer** and select **Properties**.
   - Click the **Computer Name** tab.
   - The name of the computer appears in the **Full computer name** box. Disregard anything that appears after the first period.
     For example, if **MAGNUS1.kodak.com** appears in the **Full computer name** box, then the name of the computer is **MAGNUS1**.
2. From the **Registry Key** window, select **BuiltIn** (**HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Services** > **RasMan** > **PPP** > **ControlProtocols** > **BuiltIn**).
3. Amend the value of the **DefaultDomain** to that of the computer name.



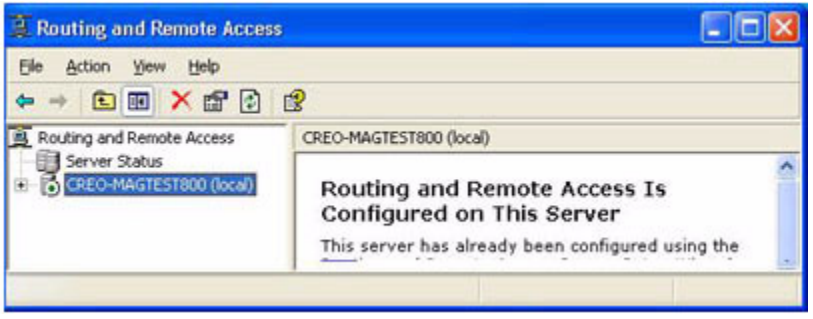
Changing the RRAS Address Pool for MCE and Dialup

Obtain three consecutive, non-occupied IP addresses belonging to the customer's network—for example, 10.70.4.100, 10.70.4.101, and 10.70.4.102.

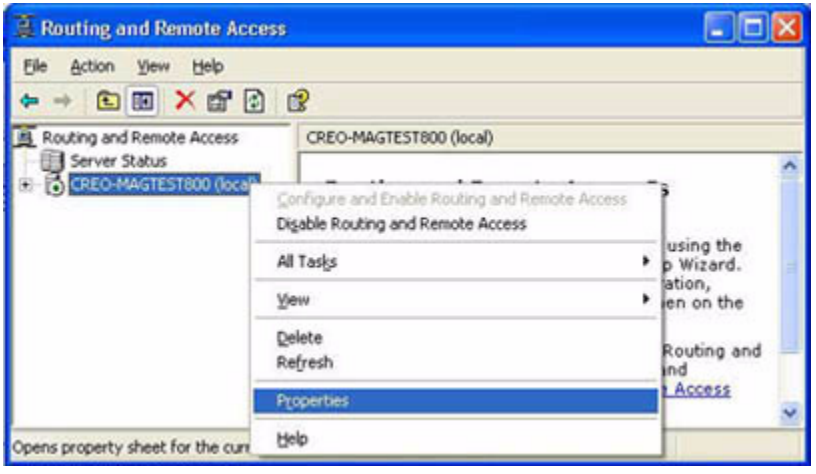
Note: Throughout this procedure, the above IP addresses are used for example purposes only.

Specifying the Static Address Pool in the RRAS

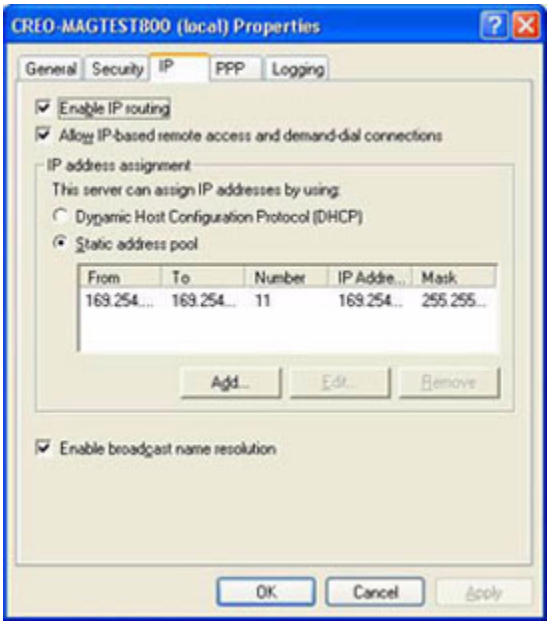
1. From the **Start** menu, select **Programs** > **Administrative Tools** > **Routing and Remote Access** to open the Routing and Remote Access dialog box.



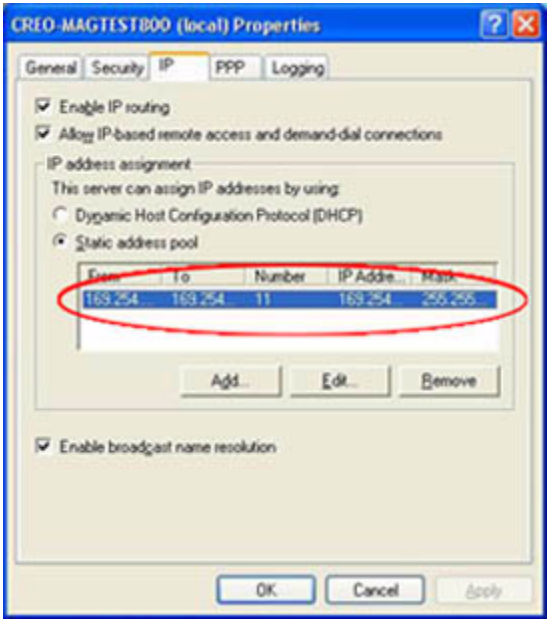
2. Right-click **Computer-Name (local)** and select **Properties**.



3. In the Properties dialog box, click the **IP** tab.



4. Click the IP addresses: (169.254.255.100 - 169.254.255.110.), and click **Edit**.



The Edit Address Range dialog box appears.



- Change the **Start IP address** to the first of the three consecutive IP addresses obtained from the customer, for example, 10.70.4.100
- Change the **End IP Address** to the last of the three consecutive IP addresses obtained from the customer, for example, 10.70.4.102
- Click **OK.**



- Click **OK** to close the Properties dialog box.

Modifying the Host File

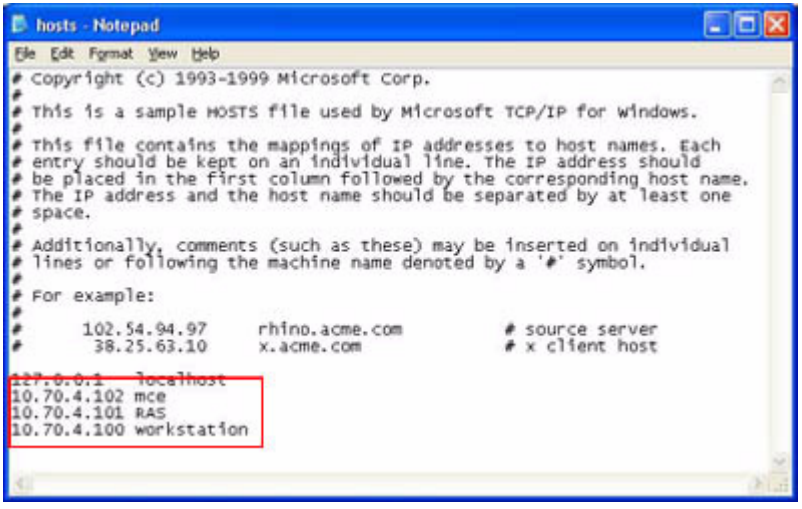
1. In *Microsoft Windows* Explorer, open the **etc** folder (**C:\Windows\System32\drivers\etc**) and locate the **hosts** file.
2. Use Notepad to open and edit the **hosts** file.

Important: Do not use any other program except Notepad to open and edit the **hosts** file.

3. Amend the last three lines of the **hosts** file:

```
10.70.4.102 mce
10.70.4.101 RAS
10.70.4.100 workstation
```

Note: The above IP addresses are used for example purpose only. Use the IP addresses obtained from the customer.



4. Save and close the **hosts** file.

Setting up the MCE IP Address

1. Use the third of the three consecutive IP addresses obtained from the customer, for example, 10.70.4.102.
2. Use the Service Shell Client to configure the firmware on the MCE. Set the value for **IPAddress** by typing the following diagnostic monitor command:

```
set net IPAddress "10.70.4.102"
```

Important: If the communication fails to start, reset the case-sensitive password in the TMCE with the following command:

```
net newpassword 1 Creo1Spot
```

3. Type `set net` at the MCE diagnostic monitor.
   The following information appears on the monitor:

```
OTMCE>> set net
PRM net parameters:
Group Parameter    Active          Default   Units
net   IPAddress    "10.70.4.102" ""
net   NetMask      ""            ""
net   Gateway      ""            ""
net   AccountName  "MCEDvice"    ""
*** Command Complete
```

4. Reset the MCE device:
   `OTMCE>> reset`

5. Test the TCP/IP connection:
   Open a DOS command window and type `ping MCE`
   The following ping information should appear on the monitor:

```
Pinging MCE [10.70.4.102] with 32 bytes of data:

Reply from 10.70.4.102: bytes=32 time=31ms TTL=225
Reply from 10.70.4.102: bytes=32 time=31ms TTL=225
Reply from 10.70.4.102: bytes=32 time=31ms TTL=225

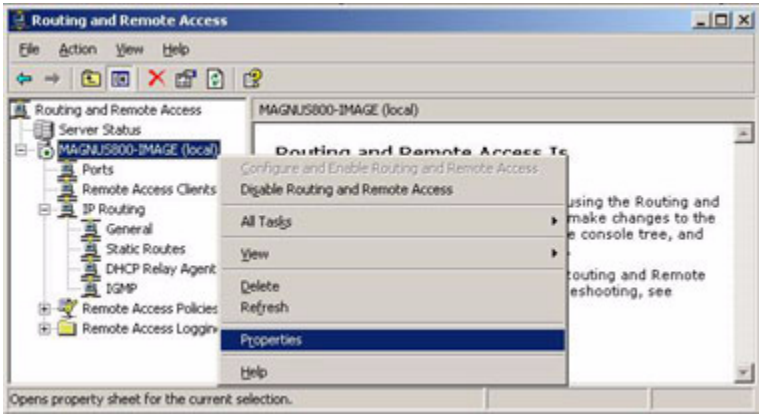
Ping statistics for 10.70.4.102:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip time in milliseconds:
Minimum = 16ms, Maximum = 31ms, Average = 23ms
```

Adding the Magnus 800 Computer to the Customer Domain

The *Magnus* 800 computer is configured by default under a *workgroup*.

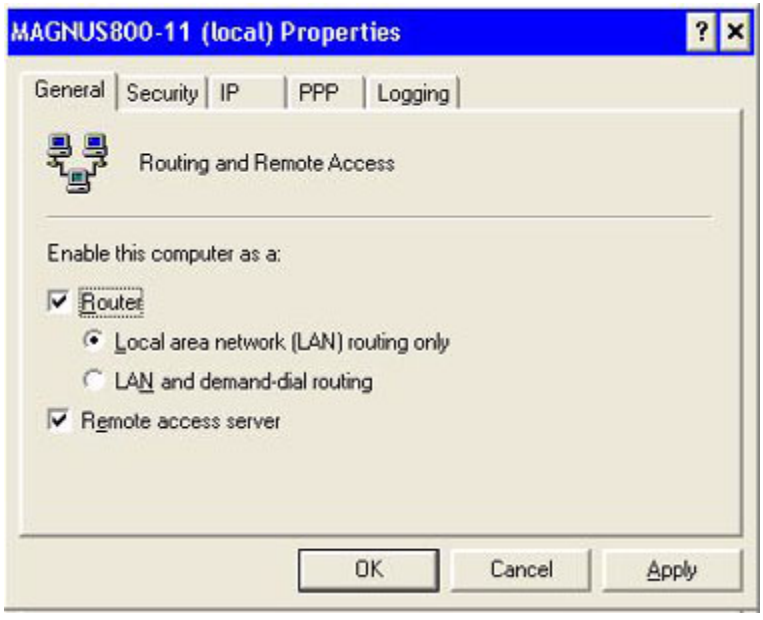
Note: When the *Magnus* is added to the customer's domain during installation, some of the RRAS settings may be missing. Verify that the PRAS settings are correct.

1. From the **Start** menu, select **Programs** > **Administrative Tools** > **Routing and Remote Access.**
2. Right-click **Computer-Name** (local), and select **Properties.**

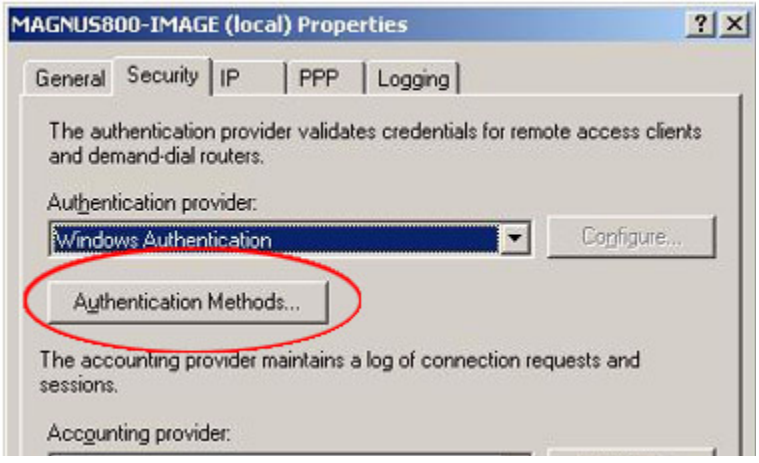


3. In the Properties dialog box, click the **General** tab.

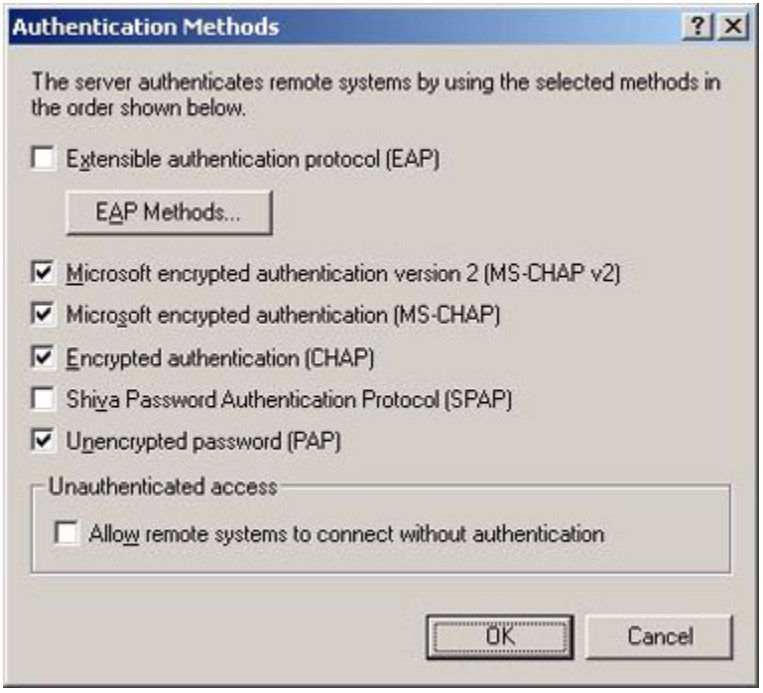
4. If required, select the **Router** check box, click **Local area network (LAN) routing only**, and select the **Remote access server** check box.



5. In the Properties dialog box, click the **Security** tab.
6. Click **Authentication Methods.**

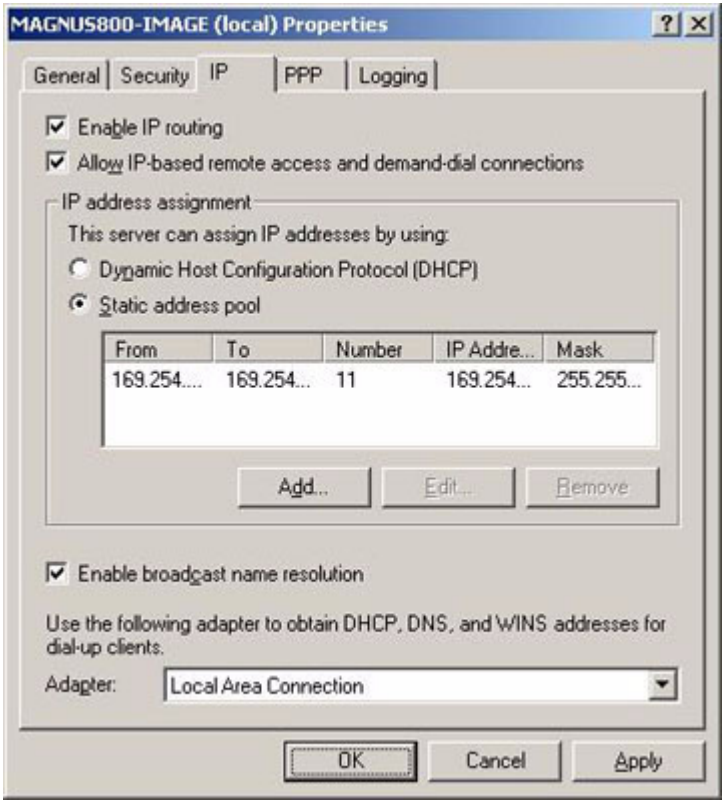


7. In the Authentication Methods dialog box, perform the following actions:
   - Clear the **EAP** check box.
   - Select the **MS-CHAP v2** check box.
   - Select the **MS-CHAP** check box.
   - Select the **CHAP** check box.
   - Select the **SPAP** check box.
   - Select the **PAP** check box.
   - Clear the **Allow remote systems to connect without authentication** check box.
   - Click **OK**.



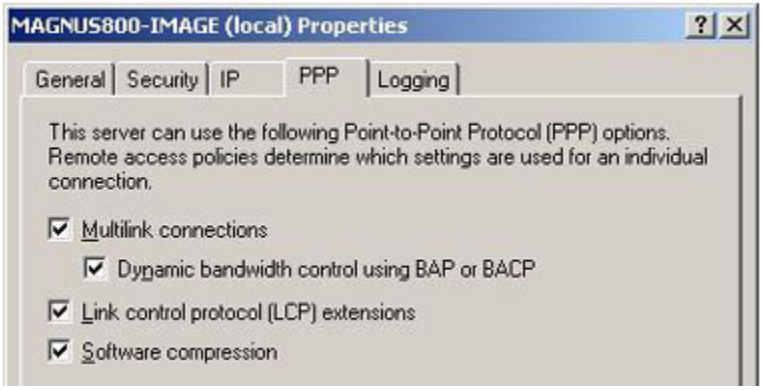
8. In the Properties dialog box, click the **IP** tab.

9. In the IP dialog box, perform the following actions:
   - Select the **Enable IP routing** check box.
   - Select the **Allow IP-based remote access and demand-dial connections** check box.
   - Click **Static address pool**.
   - Select the **Enable broadcast name resolution** check box.

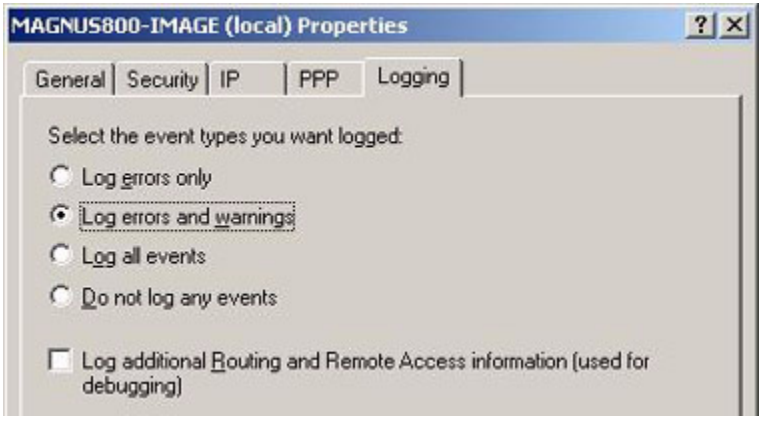


10. In the Properties dialog box, click the **PPP** tab.

11. Select all the check boxes.



12. In the Properties dialog box, click the **Logging** tab.
13. If required, select the **Log errors and warnings** check box, and click **OK**.



14. Close the Routing and Remote Access dialog box.

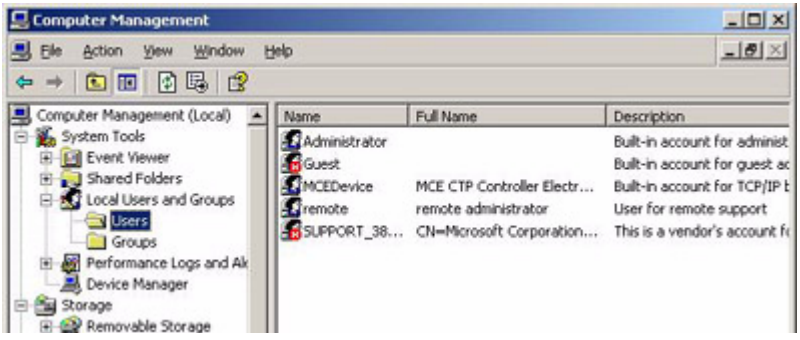
Setting the Magnus 800 Computer as a PPTP Server (Optional)

There are two steps involved in this procedure:

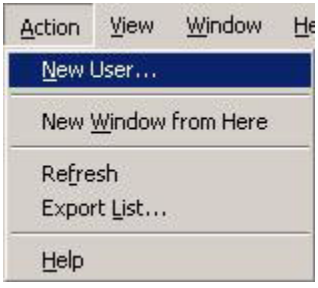
- Defining a PPP user
- Enabling PPTP under RRAS

Defining a PPP User

1. From the **Start** menu, select **Programs** > **Administrative Tools** > **Computer Management.**
2. From the **Computer Management (local)** tree, click **Local Users and Groups**, and then click **Users.**



3. From the **Action** menu, select **New User.**

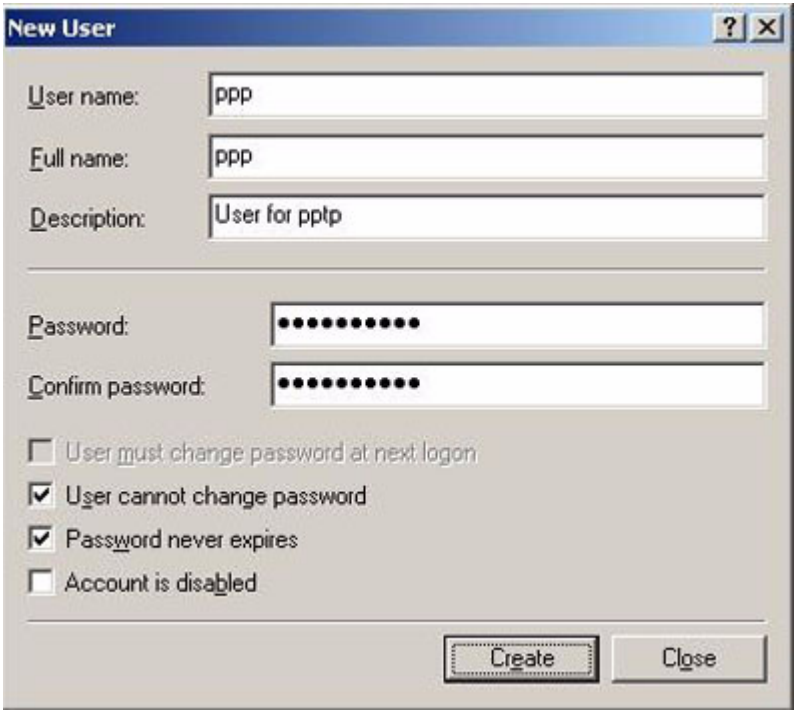


4. In the New User dialog box, perform the following actions:
   - In the **User name** box, type `ppp`
   - In the **Full name** box, type `ppp`
   - In the **Description** box, type `User for pptp`
   - In both the **Password** and **Confirm password** boxes, type a unique password.



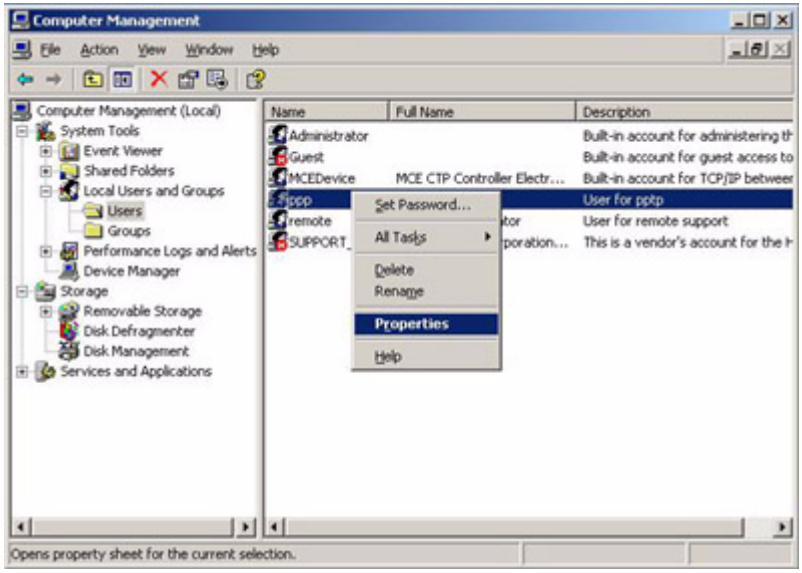
Important: Update the support center regarding the password information. The support center must know the password so that it can be used in the RSS settings.

   - Clear the **User must change password at next logon** check box.
   - Select the **User cannot change password** check box.
   - Select the **Password never expires** check box.
   - Clear the **Account is disabled** check bo.x



   - Click **Create**, and then click **Close**.

5. In the Computer Management window, right-click **ppp**, and select **Properties**.



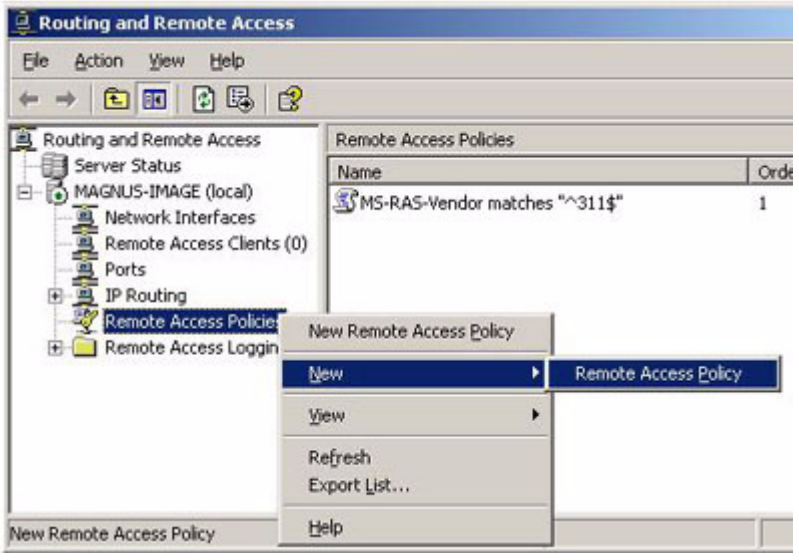
6. In the ppp Properties dialog box, click the **Dial-in** tab.
7. In the **Remote Access Permission** area, click **Allow access**.



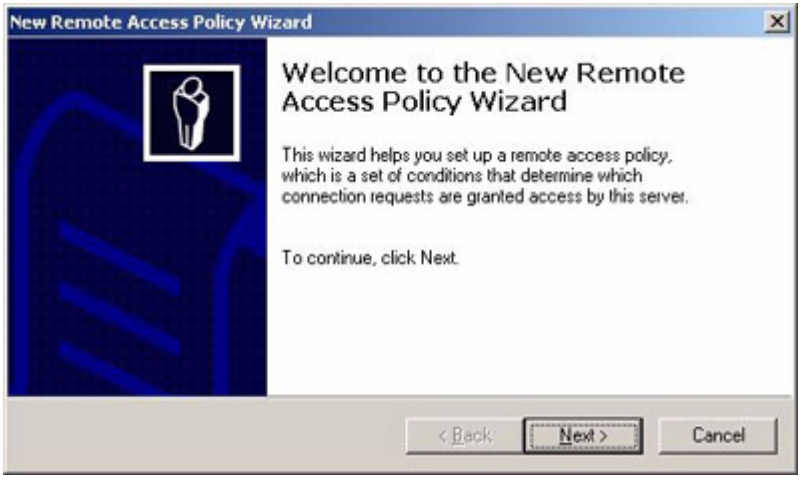
8. Click **OK** and close the Computer Management window.

Enabling PPTP under RRAS

1. From the **Start** menu, select **Programs** > **Administrative Tools** > **Routing and Remote Access.**
2. Right-click **Remote Access Policies**, and from the **New** menu, select **Remote Access Policy.**



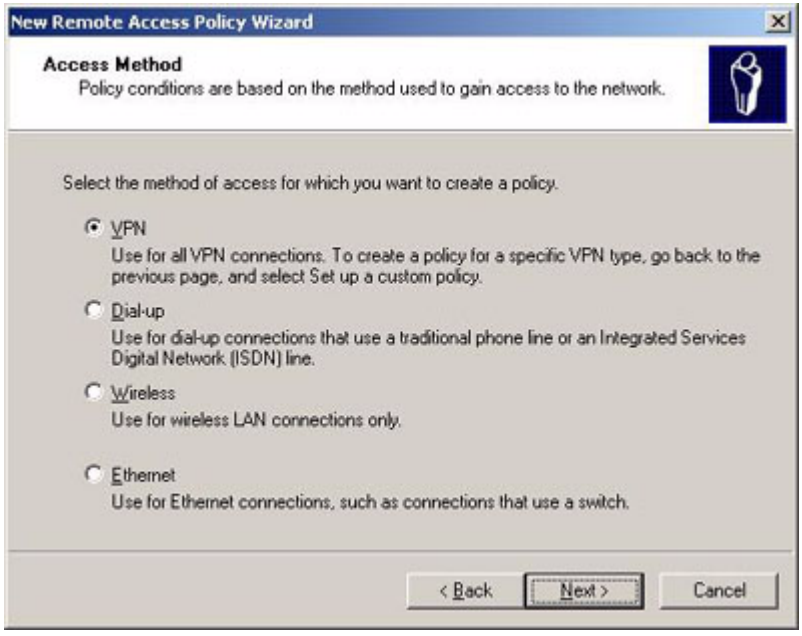
3. The New Remote Access Policy Wizard opens. Click **Next.**



4. In the Policy Configuration Method screen of the New Remote Access Policy Wizard, type `PPTP connection` in the **Policy name** box and click **Next**.



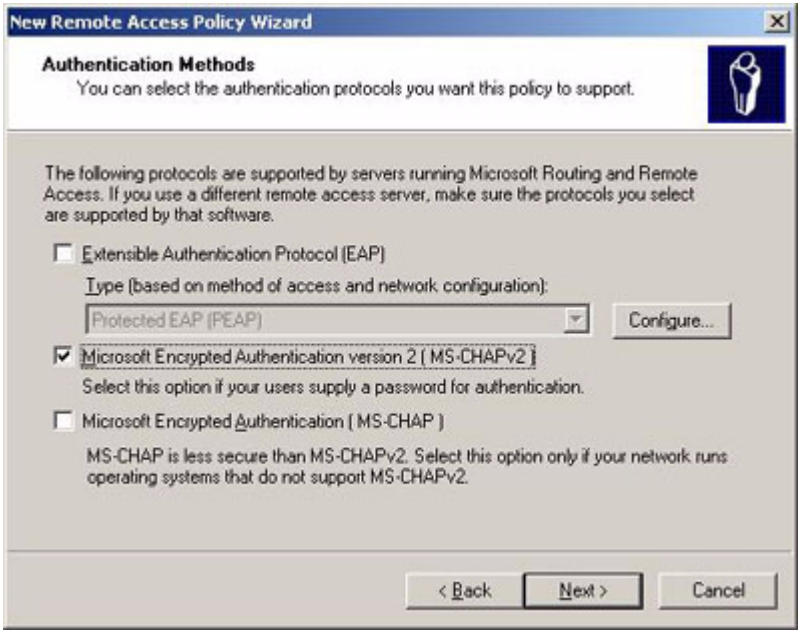
5. In the Access Method screen of the New Remote Access Policy Wizard, click **VPN**, and then click **Next**.



6. In the User or Group Access screen of the New Remote Access Policy Wizard, click **User**, and then click **Next.**



7. In the Authentication Methods screen of the New Remote Access Policy Wizard, select the **Microsoft Encrypted Authentication version 2** check box, clear all the remaining check boxes, and click **Next.**



8. In the Policy Encryption Level screen of the New Remote Access Policy Wizard, select the **Strongest encryption** check box, clear all the remaining check boxes, and click **Next**.



9. In the Completion screen, click **Finish.**