Foundry Security Best Practices

Deploying MAC Authentication with Microsoft Internet Authentication Service (RADIUS)

Table of Contents

Deploying IAS for dynamic VLAN assignment

1.1 Windows 2003 Server Configuration

In order to configure a Windows 2003 Server to act as an Internet Authentication Service (IAS), or RADIUS, server the service must be installed as described in the preceding section. Once that is completed you are ready to begin the setup of IAS. The basic structure of RADIUS services consists of three components: RADIUS Clients, the RADIUS server and remote users. In order to understand how these services interoperate, it is important to remember that the IAS server is the authentication server and the Foundry networking equipment is the RADIUS client. The MAC address based authentication attempt is "proxied" by the Foundry router or switch. The IAS server has no knowledge of where the users are physically or logically located in the your network environment. The benefit to this configuration is the ability to authenticate devices without any client or supplicant dependencies.

1.2 Installing the IAS Service

In order to install the service, navigate to the "Add or Remove Programs" applet in the control panel of the Windows 2003 server on which you wish to install the service. From the "Windows Components" Select the Internet Authentication Service and click OK. This will install the needed files and start the service. A reboot of the server is not required.

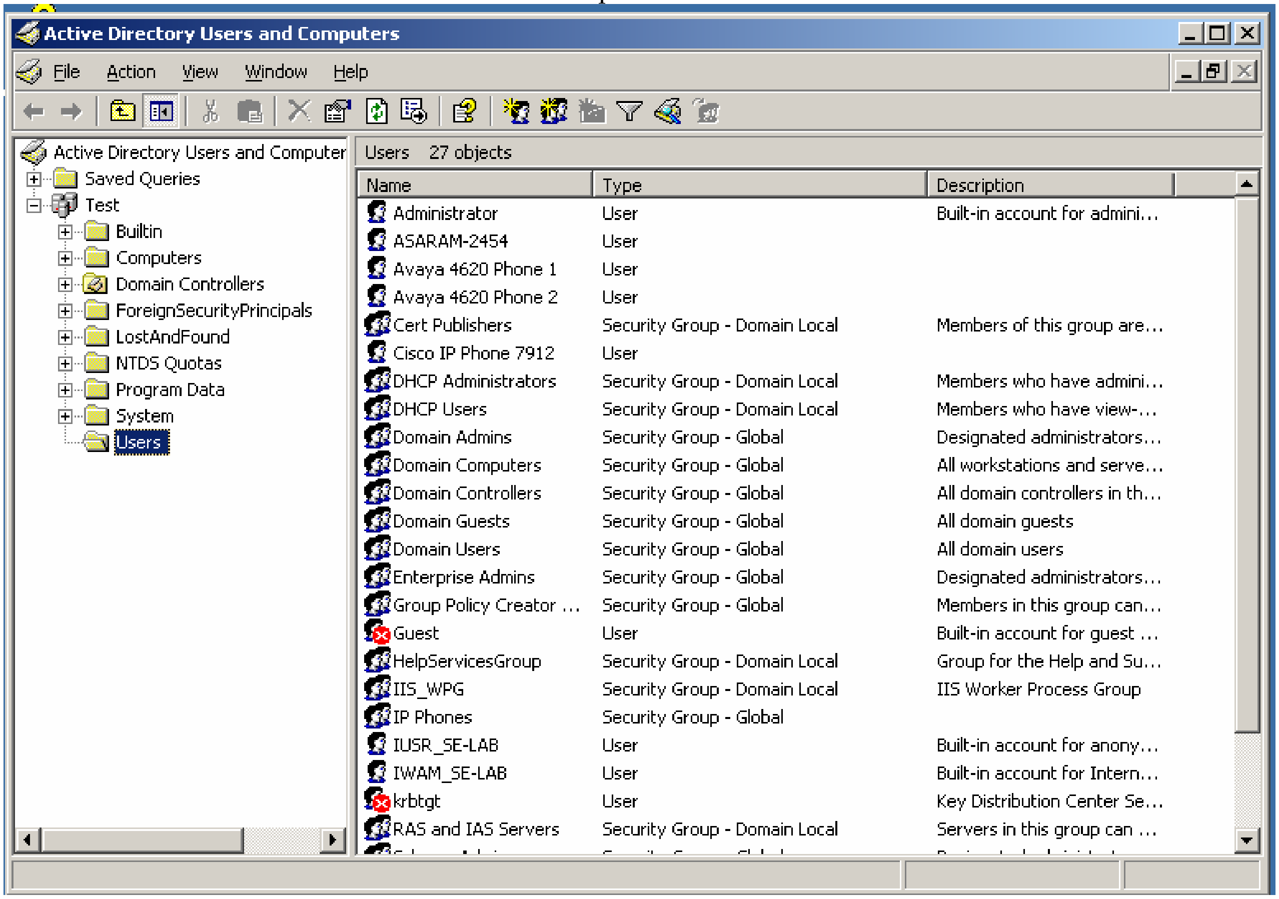
1.3 Overview of MAC based authentication and dynamic VLAN assignment.

Before configuring the IAS service you must first add users to the Active Directory. Even though it's referred to as "users" in this document these are actually machines that get authenticated by the radius server. Because these are machines, and not interactive end users, security polices such as password aging, and password complexity rules must be disabled for these accounts. The users (machines) are identified and authenticated using their physical address or Media Access Control (MAC) address. During this authentication process the actual end user is not involved, and is unaware of the authentication process. Depending on the organization security policy the end user will logon to the network and access resources based on credentials that are different from what is configured in the Active Directory for MAC authentication. If the machine successfully authenticated with the Radius server (This means an active account in the Active Directory) based on its MAC address the switch port is configured for the appropriate VLAN dynamically and is enabled for that machine to pass traffic to the network. If the machines MAC address is not present in the Active Directory or if the account is disabled, the machine is denied from the switch port, and is not allowed to pass traffic to the network. Optionally if the machines MAC address is not present in the Active Directory or if the account is disabled, the switch can be configured to place the machine in a restricted VLAN for limited connectivity.

1.4 Adding a user (machine) to the Active Directory.

You can add any type of machine, that you trust and know, that has a MAC address to the Active Directory as a user. For examples; IP Phones, Uninterrupted Power Supplies, Video Cameras, Laptops, Desktops, etc, etc. all have MAC addresses.
Following is and example of adding a trusted Laptop computer.

1. Open up the Microsoft Management Console (MMC) for Active Directory Users and Computers.
2. Select users from the containers in the left pane.

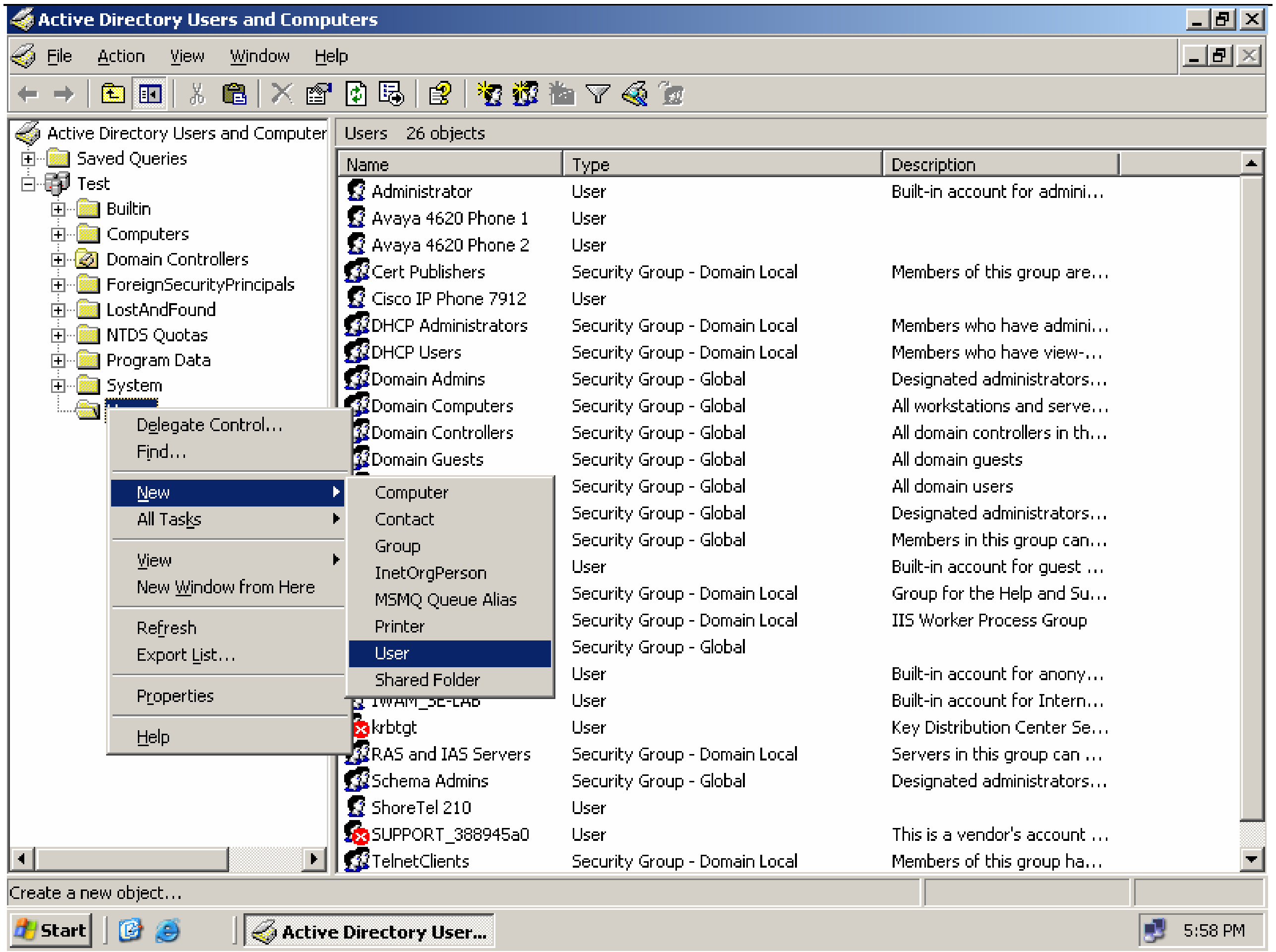


- Active Directory Users and Computer
  - Saved Queries
  - Test
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - LostAndFound
    - NTDS Quotas
    - Program Data
    - System
    - Users

Users 27 objects

Name	Type	Description
Administrator	User	Built-in account for admini...
ASARAM-2454	User	
Avaya 4620 Phone 1	User	
Avaya 4620 Phone 2	User	
Cert Publishers	Security Group - Domain Local	Members of this group are...
Cisco IP Phone 7912	User	
DHCP Administrators	Security Group - Domain Local	Members who have admini...
DHCP Users	Security Group - Domain Local	Members who have view-...
Domain Admins	Security Group - Global	Designated administrators...
Domain Computers	Security Group - Global	All workstations and serve...
Domain Controllers	Security Group - Global	All domain controllers in th...
Domain Guests	Security Group - Global	All domain guests
Domain Users	Security Group - Global	All domain users
Enterprise Admins	Security Group - Global	Designated administrators...
Group Policy Creator ...	Security Group - Global	Members in this group can...
Guest	User	Built-in account for guest ...
HelpServicesGroup	Security Group - Domain Local	Group for the Help and Su...
IIS_WPG	Security Group - Domain Local	IIS Worker Process Group
IP Phones	Security Group - Global	
IUSR_SE-LAB	User	Built-in account for anony...
IWAM_SE-LAB	User	Built-in account for Intern...
krbtgt	User	Key Distribution Center Se...
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can ...

3. Right click to add a new user.

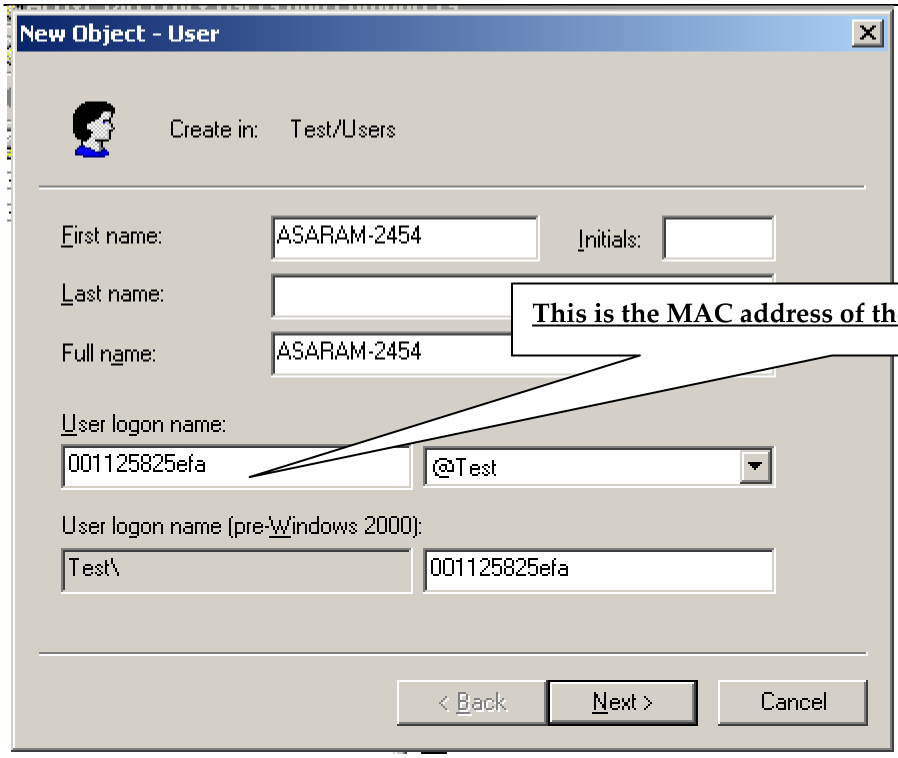


Users 26 objects

Name	Type	Description
Administrator	User	Built-in account for admini...
Avaya 4620 Phone 1	User	
Avaya 4620 Phone 2	User	
Cert Publishers	Security Group - Domain Local	Members of this group are...
Cisco IP Phone 7912	User	
DHCP Administrators	Security Group - Domain Local	Members who have admini...
DHCP Users	Security Group - Domain Local	Members who have view-...
Domain Admins	Security Group - Global	Designated administrators...
Domain Computers	Security Group - Global	All workstations and serve...
Domain Controllers	Security Group - Global	All domain controllers in th...
Domain Guests	Security Group - Global	All domain guests
	Security Group - Global	All domain users
	Security Group - Global	Designated administrators...
	Security Group - Global	Members in this group can...
	User	Built-in account for guest ...
	Security Group - Domain Local	Group for the Help and Su...
	Security Group - Domain Local	IIS Worker Process Group
	Security Group - Global	
	User	Built-in account for anony...
IWAM_SE-LAB	User	Built-in account for Intern...
krbtgt	User	Key Distribution Center Se...
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can ...
Schema Admins	Security Group - Global	Designated administrators...
ShoreTel 210	User	
SUPPORT_388945a0	User	This is a vendor's account ...
TelnetClients	Security Group - Domain Local	Members of this group ha...

Create a new object...

4. Type in the MAC address of the machine that you wish to add to the Active Directory.



New Object - User

Create in: Test/Users

First name: ASARAM-2454

Initials:

Last name:

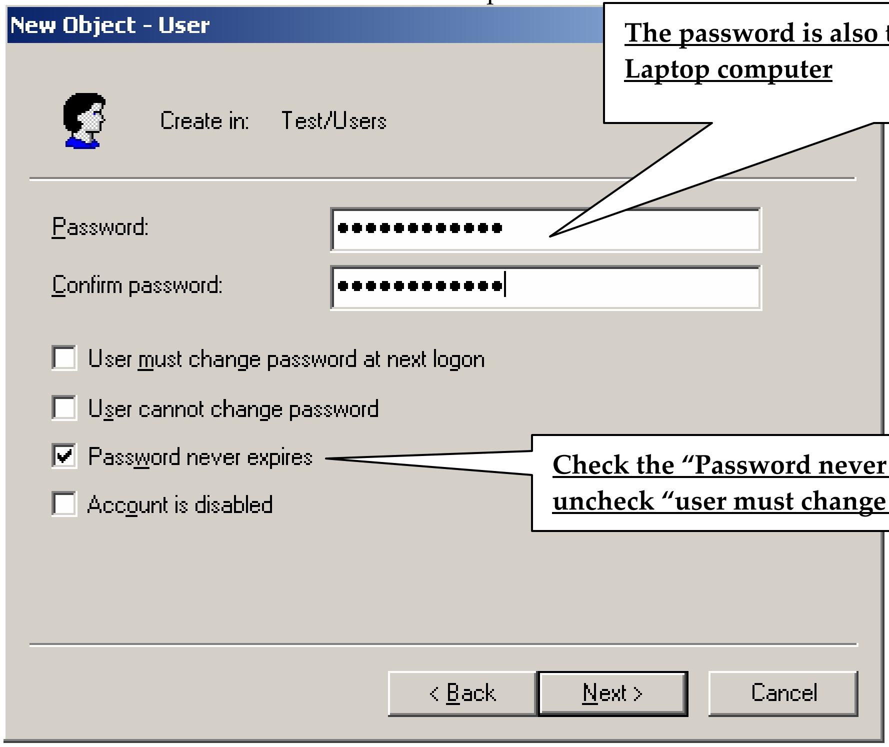
Full name: ASARAM-2454

User logon name: 001125825efa @Test

User logon name (pre-Windows 2000): Test\ 001125825efa

This is the MAC address of the Laptop computer

5. Click next and enter the account password



New Object - User

Create in: Test/Users

Password: ●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●

□ User must change password at next logon

□ User cannot change password

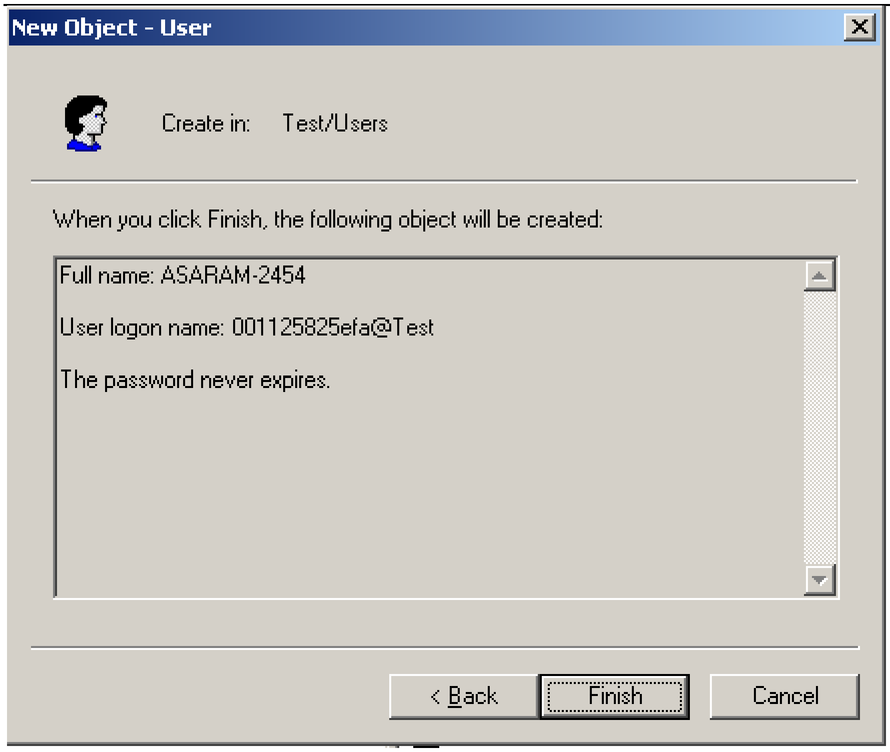
☑ Password never expires

□ Account is disabled

The password is also the MAC address of the Laptop computer

Check the "Password never expires box; and uncheck "user must change password at next

6. Click next after you have completed entering the password, and click finish on the next screen.



Create in: Test/Users

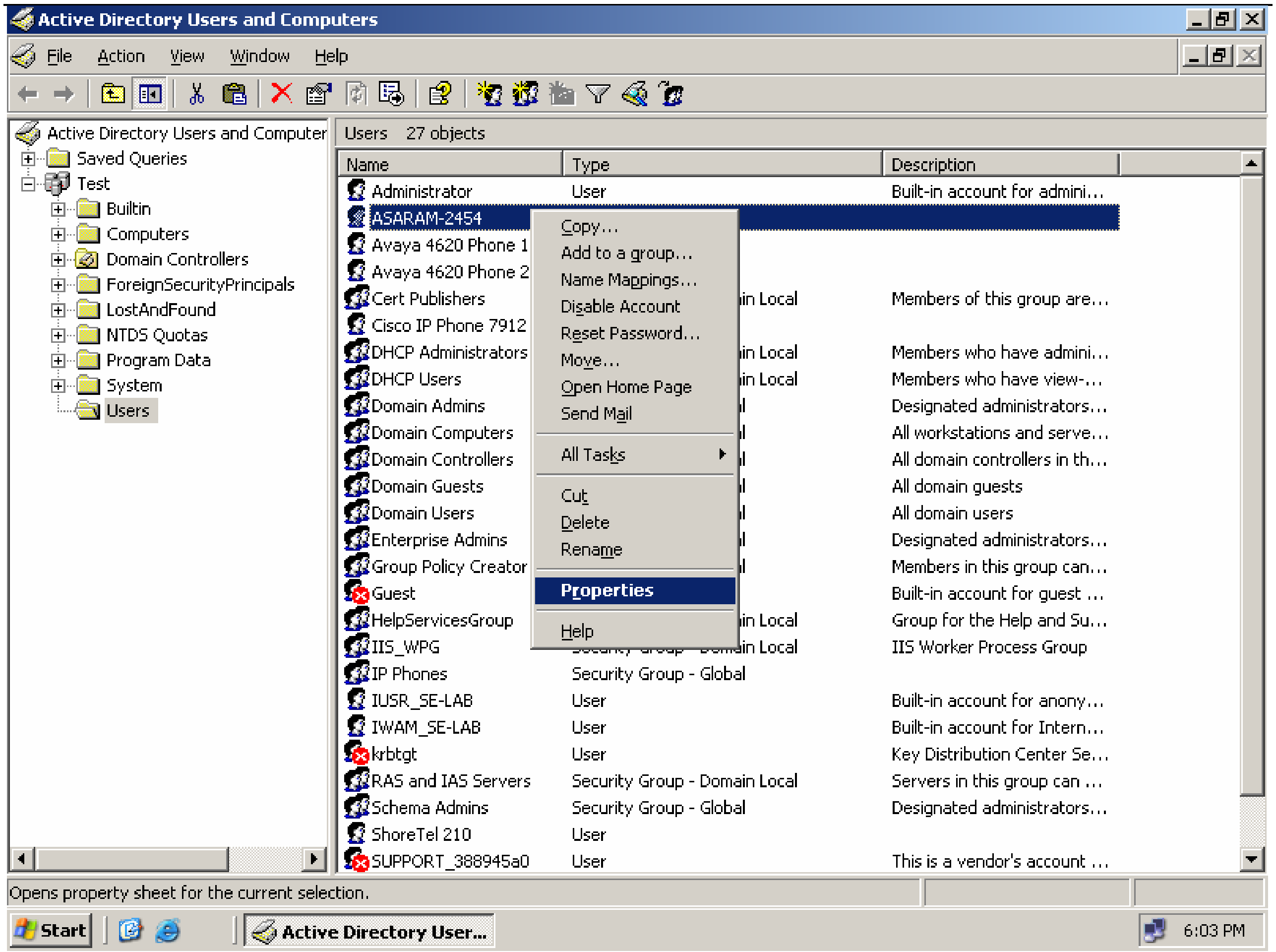
When you click Finish, the following object will be created:

Full name: ASARAM-2454

User logon name: 001125825efa@Test

The password never expires.

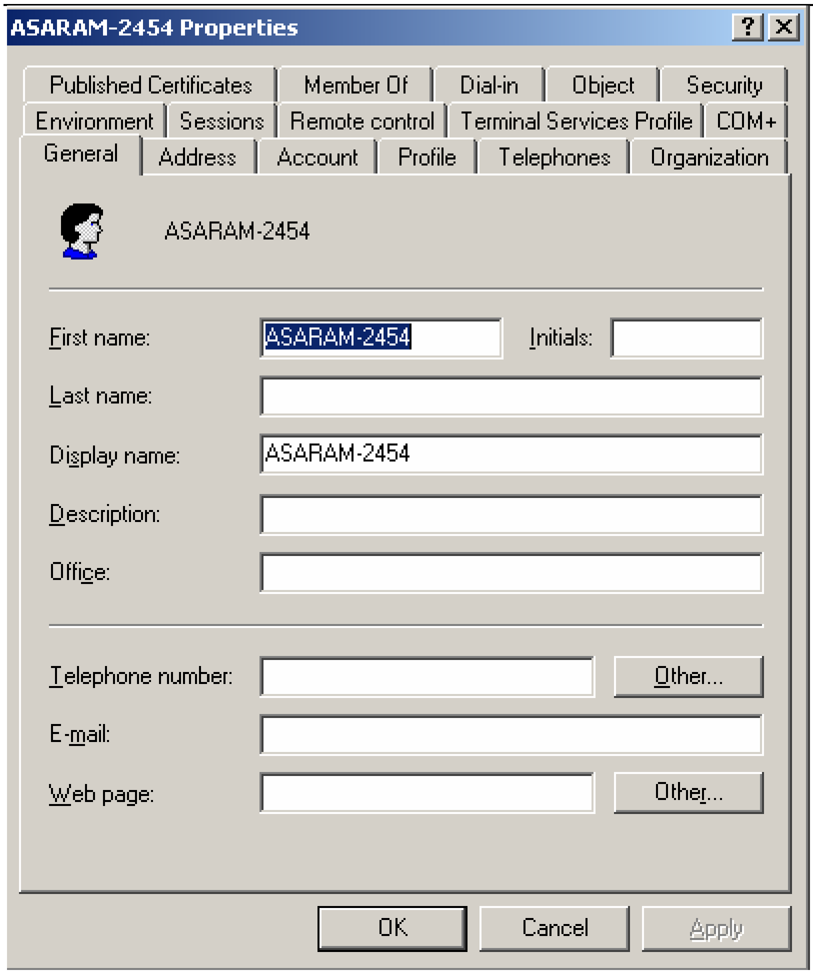
7. Additional configuration is required to complete the user account information. Highlight the Active Directory account that you just created and right click to select account properties.



Name	Type	Description
Administrator	User	Built-in account for admini...
ASARAM-2454		
Avaya 4620 Phone 1		
Avaya 4620 Phone 2		
Cert Publishers	in Local	Members of this group are...
Cisco IP Phone 7912		
DHCP Administrators	in Local	Members who have admini...
DHCP Users	in Local	Members who have view-...
Domain Admins	l	Designated administrators...
Domain Computers	l	All workstations and serve...
Domain Controllers	l	All domain controllers in th...
Domain Guests	l	All domain guests
Domain Users	l	All domain users
Enterprise Admins	l	Designated administrators...
Group Policy Creator	l	Members in this group can...
Guest		Built-in account for guest ...
HelpServicesGroup	in Local	Group for the Help and Su...
IIS_WPG	in Local	IIS Worker Process Group
IP Phones	Security Group - Global	
IUSR_SE-LAB	User	Built-in account for anony...
IWAM_SE-LAB	User	Built-in account for Intern...
krbtgt	User	Key Distribution Center Se...
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can ...
Schema Admins	Security Group - Global	Designated administrators...
ShoreTel 210	User	
SUPPORT_388945a0	User	This is a vendor's account ...

Opens property sheet for the current selection.

8. The following screen will appear



ASARAM-2454 Properties

ASARAM-2454

First name: ASARAM-2454

Initials:

Last name:

Display name: ASARAM-2454

Description:

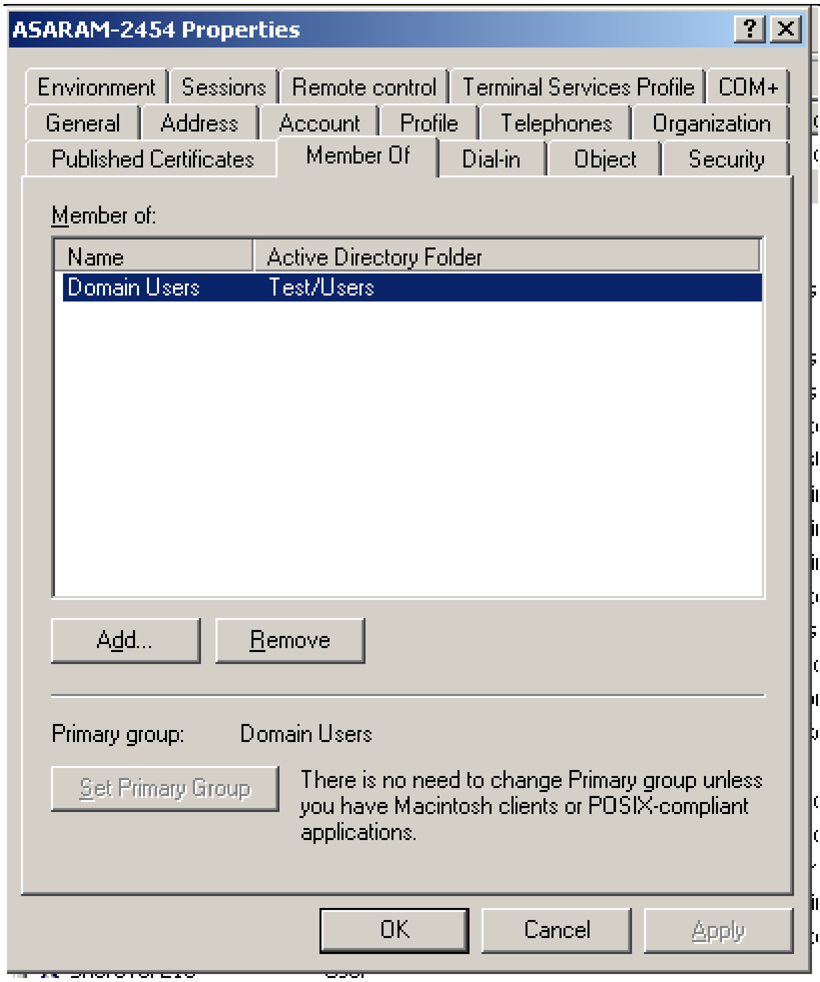
Office:

Telephone number:

E-mail:

Web page:

9. Select the "member of" tab and click on Add.



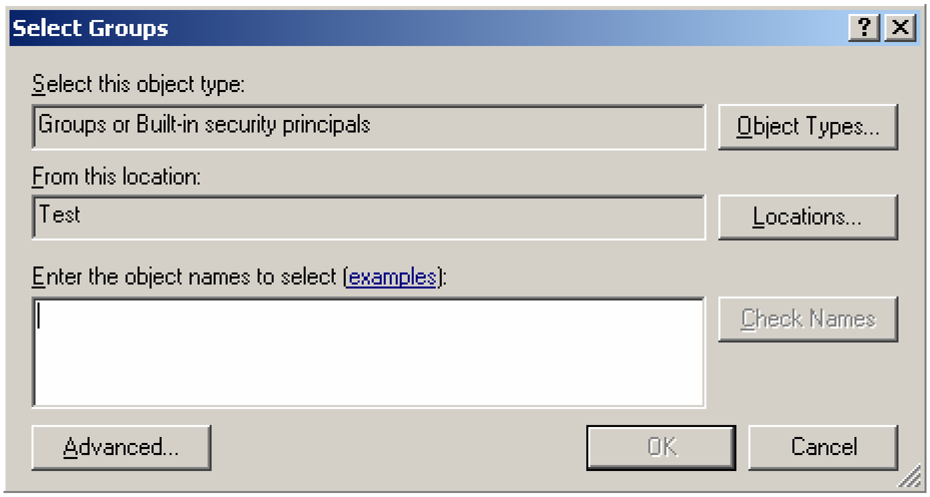
Member of:

Name	Active Directory Folder
Domain Users	Test/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

10. Click on Advance on the next screen.

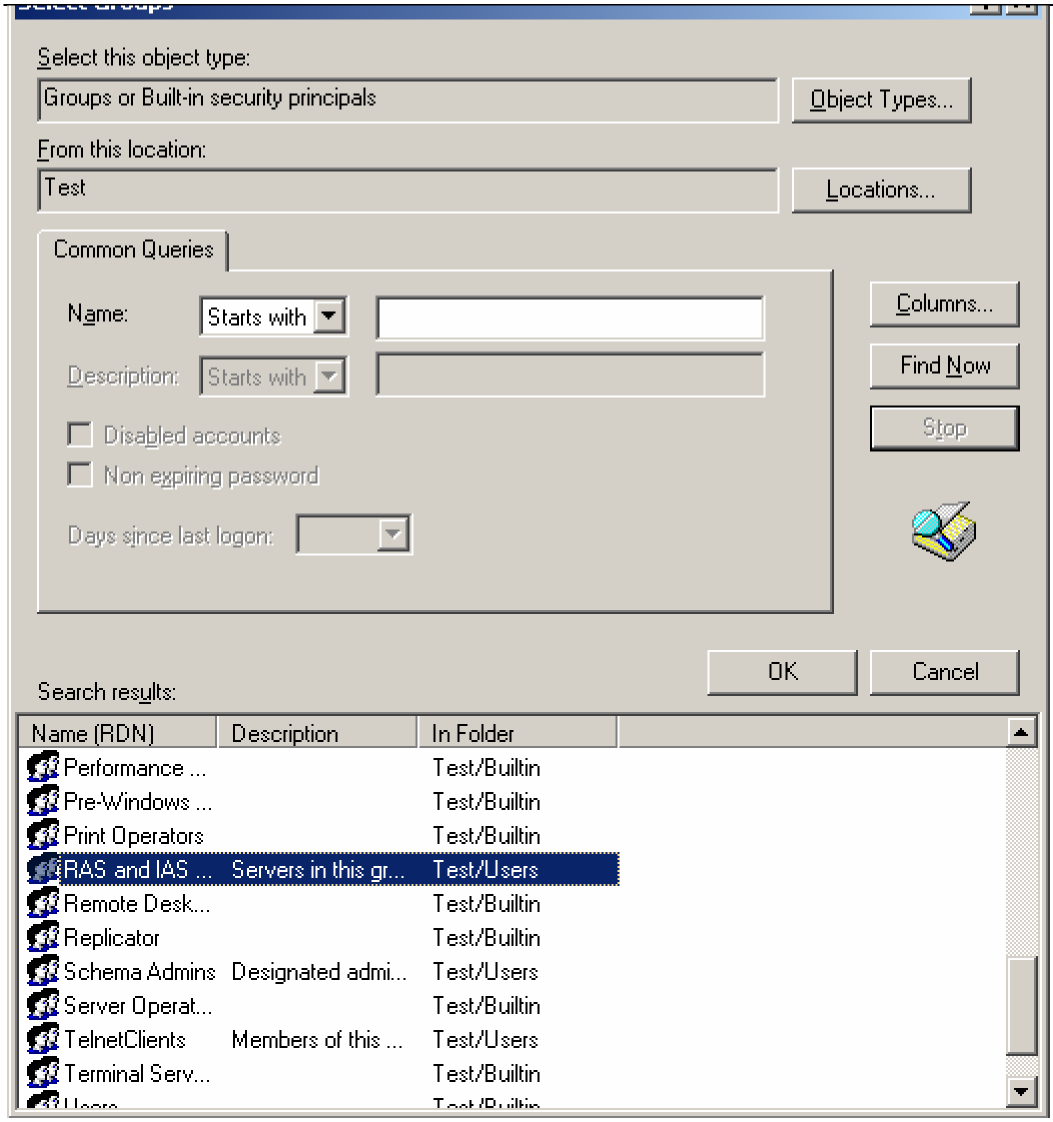


Select this object type: Groups or Built-in security principals

From this location: Test

Enter the object names to select (examples):

11. Then click on find now, and select RAS and IAS ….



Select this object type: Groups or Built-in security principals

From this location: Test

Name: Starts with

Description: Starts with

☐ Disabled accounts

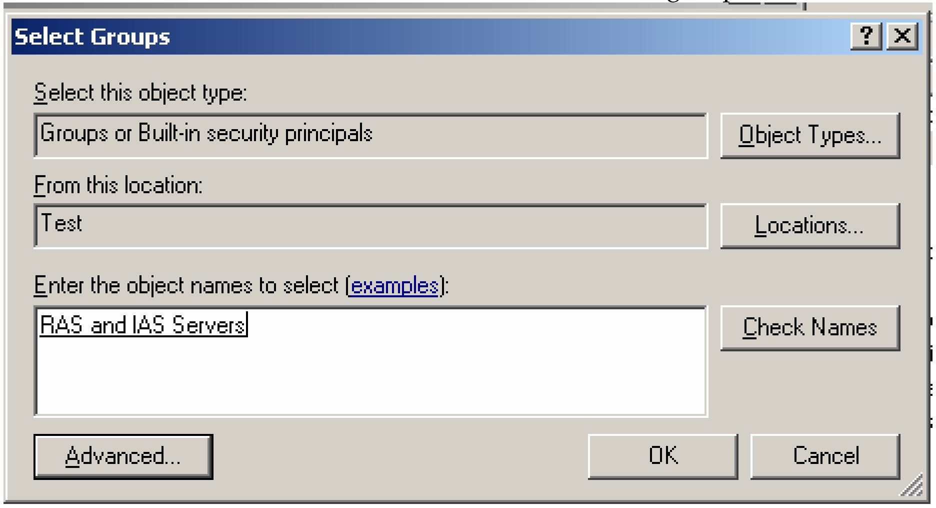
☐ Non expiring password

Days since last logon:

Search results:

Name (RDN)	Description	In Folder
Performance ...		Test/Builtin
Pre-Windows ...		Test/Builtin
Print Operators		Test/Builtin
RAS and IAS ...	Servers in this gr...	Test/Users
Remote Desk...		Test/Builtin
Replicator		Test/Builtin
Schema Admins	Designated admi...	Test/Users
Server Operat...		Test/Builtin
TelnetClients	Members of this ...	Test/Users
Terminal Serv...		Test/Builtin
Users		Test/Builtin

12. Make sure RAS and IAS Servers is added to the groups and click on Ok.

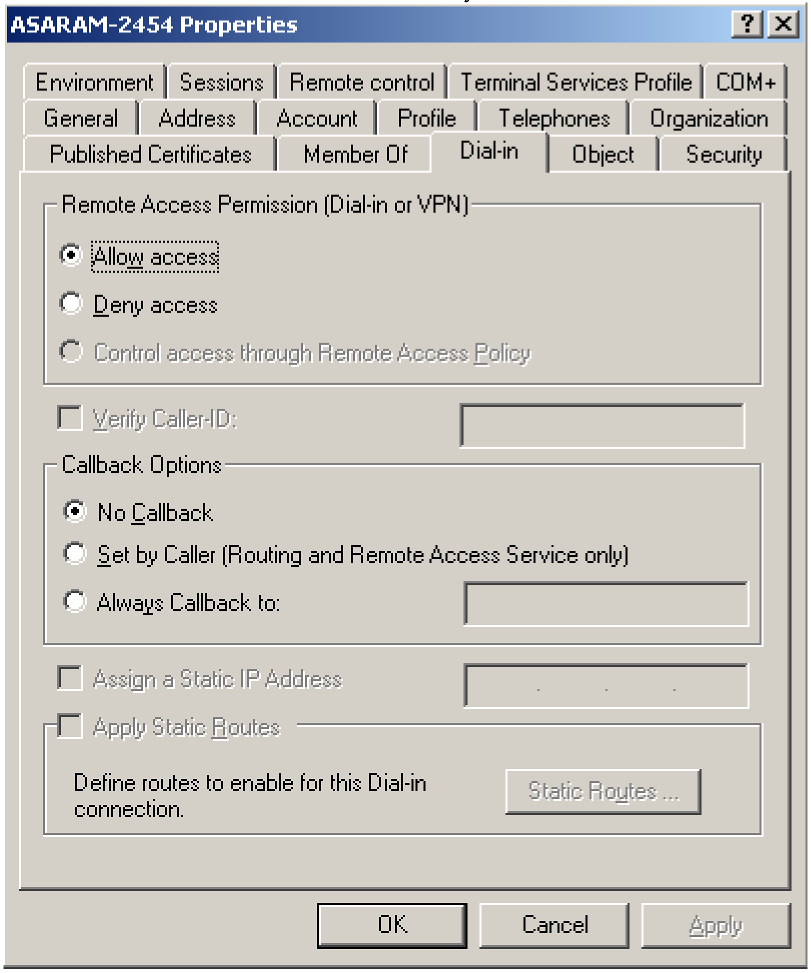


Select this object type: Groups or Built-in security principals

From this location: Test

Enter the object names to select (examples): RAS and IAS Servers

13. Now click on the Dial in tab and check Allow access. This will complete the account information for this trusted Laptop. Continue these steps for all other trusted devices that you want to create accounts in the Active Directory.



Remote Access Permission (Dial-in or VPN)

● Allow access

○ Deny access

○ Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

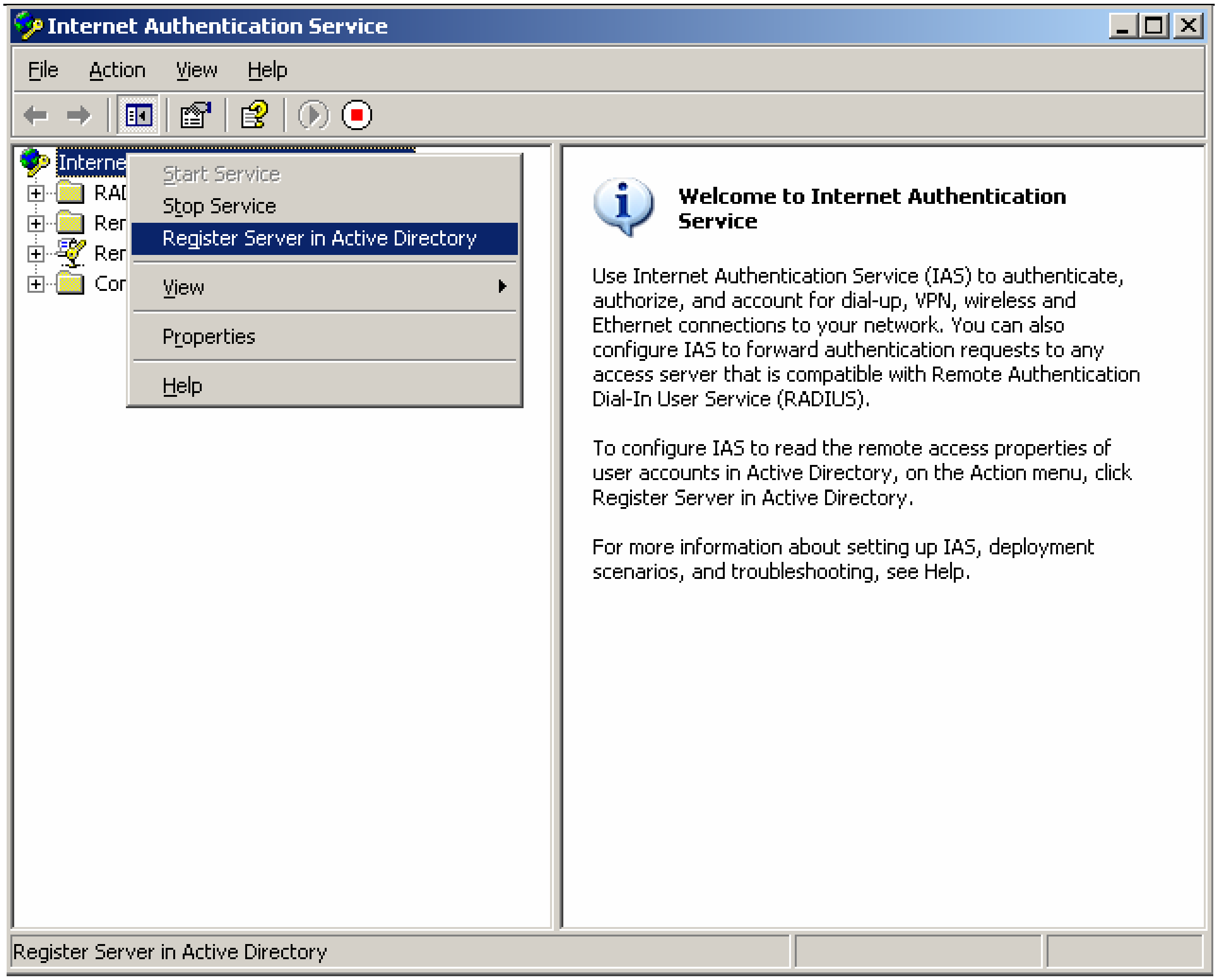
□ Assign a Static IP Address

□ Apply Static Routes

Define routes to enable for this Dial-in connection.

1.5 *Configuring IAS*

1. Open up the Microsoft Management Console (MMC) for the IAS service and connect to the server.
2. Register the IAS service with the Active Directory to authorize accounts that are defined in the Active Directory. Right click on Internet Authentication Service container on the left pane and select Register Server in Active Directory.



Welcome to Internet Authentication Service

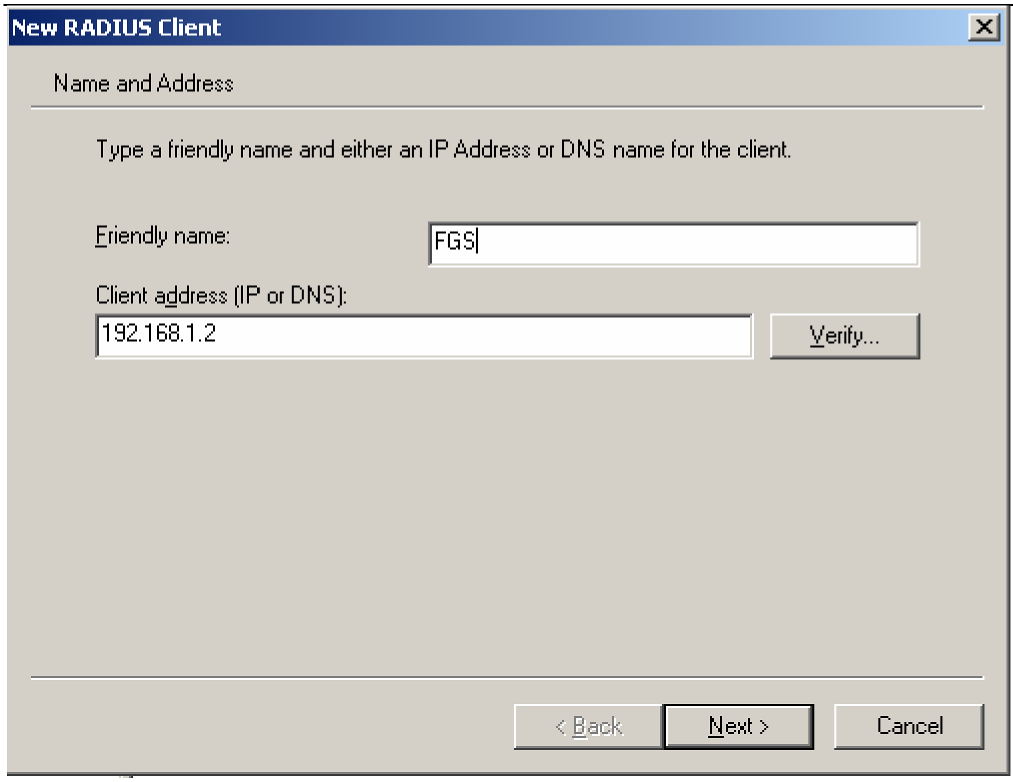
Use Internet Authentication Service (IAS) to authenticate, authorize, and account for dial-up, VPN, wireless and Ethernet connections to your network. You can also configure IAS to forward authentication requests to any access server that is compatible with Remote Authentication Dial-In User Service (RADIUS).

To configure IAS to read the remote access properties of user accounts in Active Directory, on the Action menu, click Register Server in Active Directory.

For more information about setting up IAS, deployment scenarios, and troubleshooting, see Help.

Register Server in Active Directory

3. Next right click on the Radius Client and create a new radius client. Enter the hostname and the IP address of the radius client, and click next. The IP address you enter here is the management IP address of the Foundry switch.

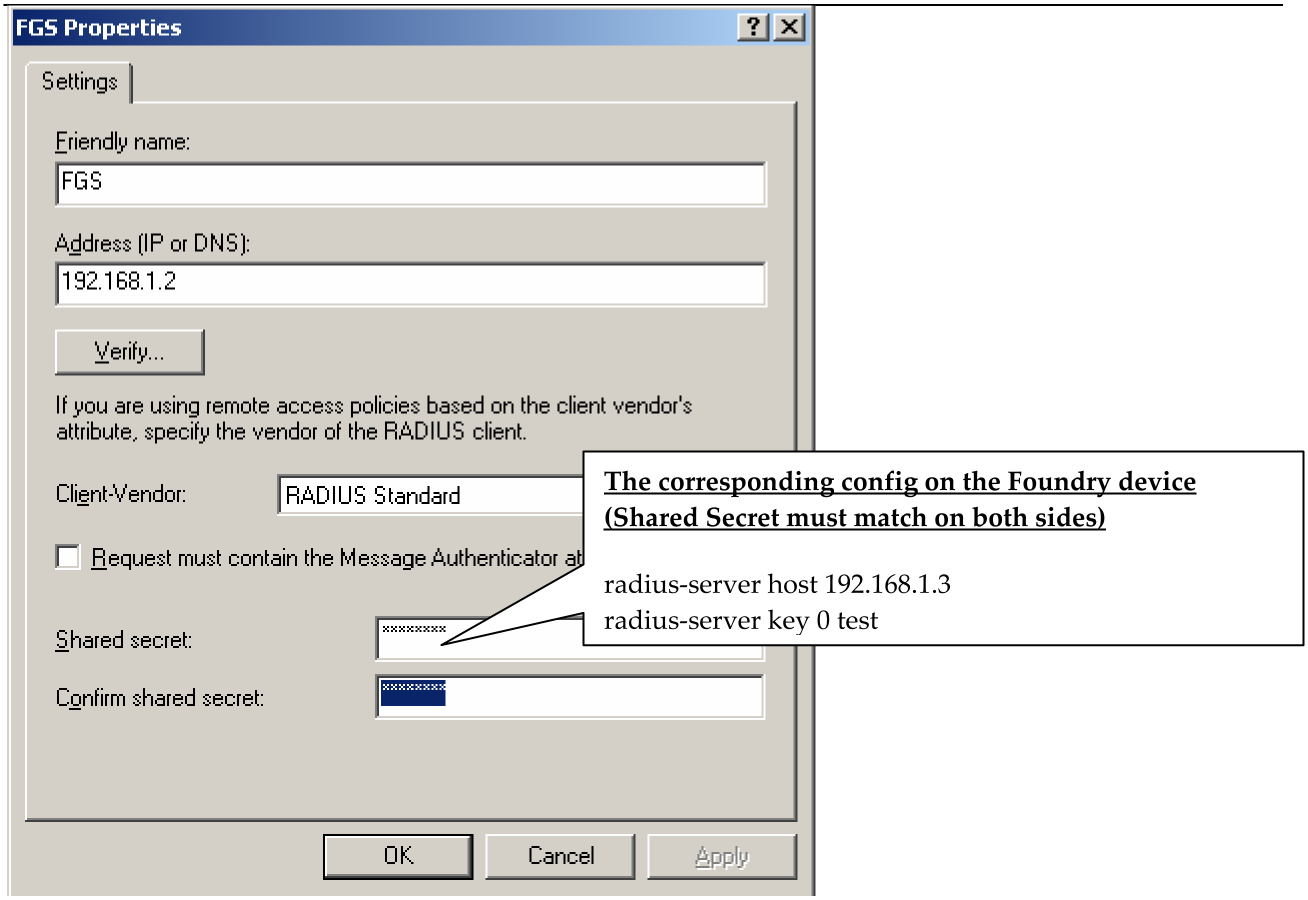


Type a friendly name and either an IP Address or DNS name for the client.

Friendly name: FGS

Client address (IP or DNS): 192.168.1.2

4. Enter the shared secret that will be used to authenticate the RADIUS client (Foundry Devices) to the IAS server.



FGS Properties

Friendly name: FGS

Address (IP or DNS): 192.168.1.2

If you are using remote access policies based on the client vendor's attribute, specify the vendor of the RADIUS client.

Client-Vendor: RADIUS Standard

☐ Request must contain the Message Authenticator at

Shared secret: ********

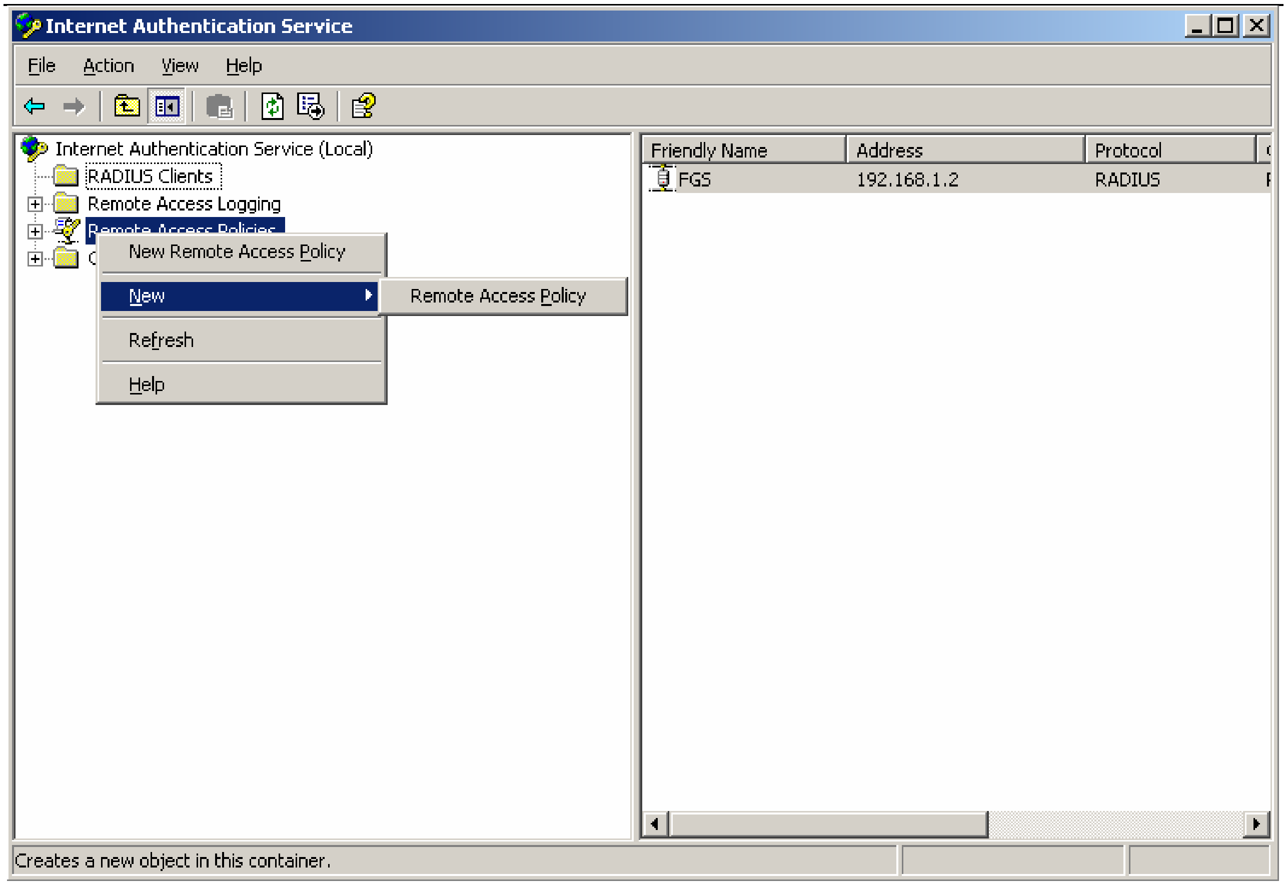
Confirm shared secret: ********

The corresponding config on the Foundry device (Shared Secret must match on both sides)

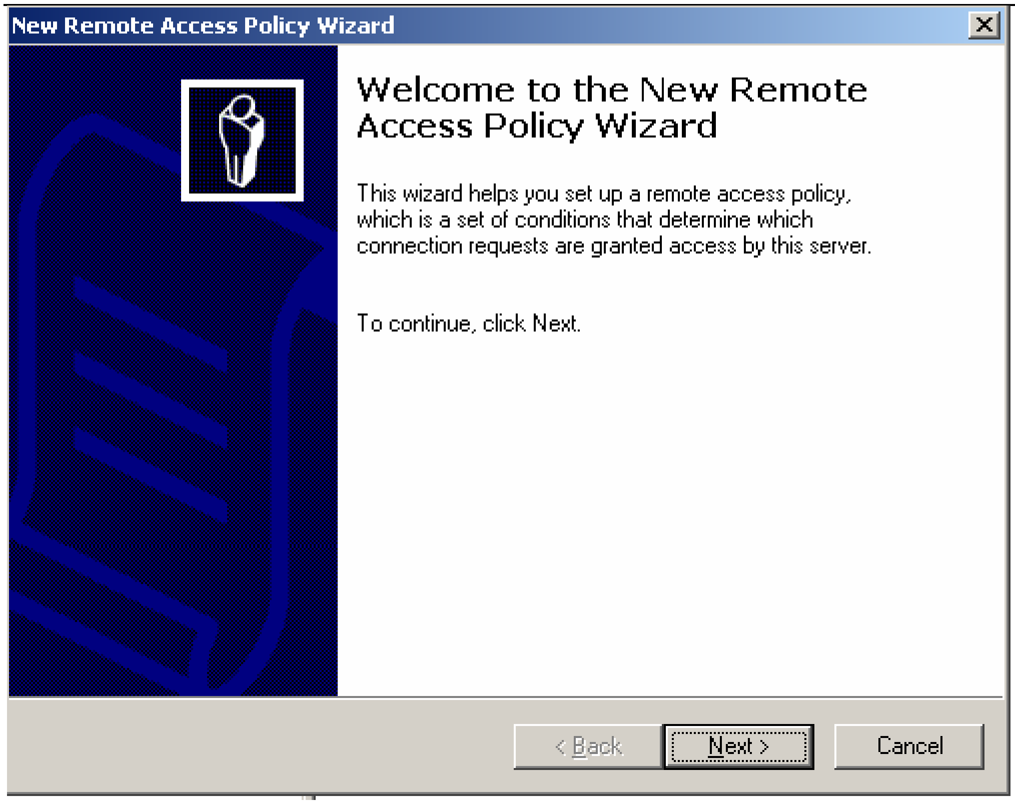
```
radius-server host 192.168.1.3
radius-server key 0 test
```

SETTING UP MAC BASED AUTHENTICATION POLICY FOR USERS (MACHINES)

5. Right-click on the Remote Access Policies container in the left pane of the MMC and select New Remote Access Policy.



6. A wizard will guide you through the configuration, click next.



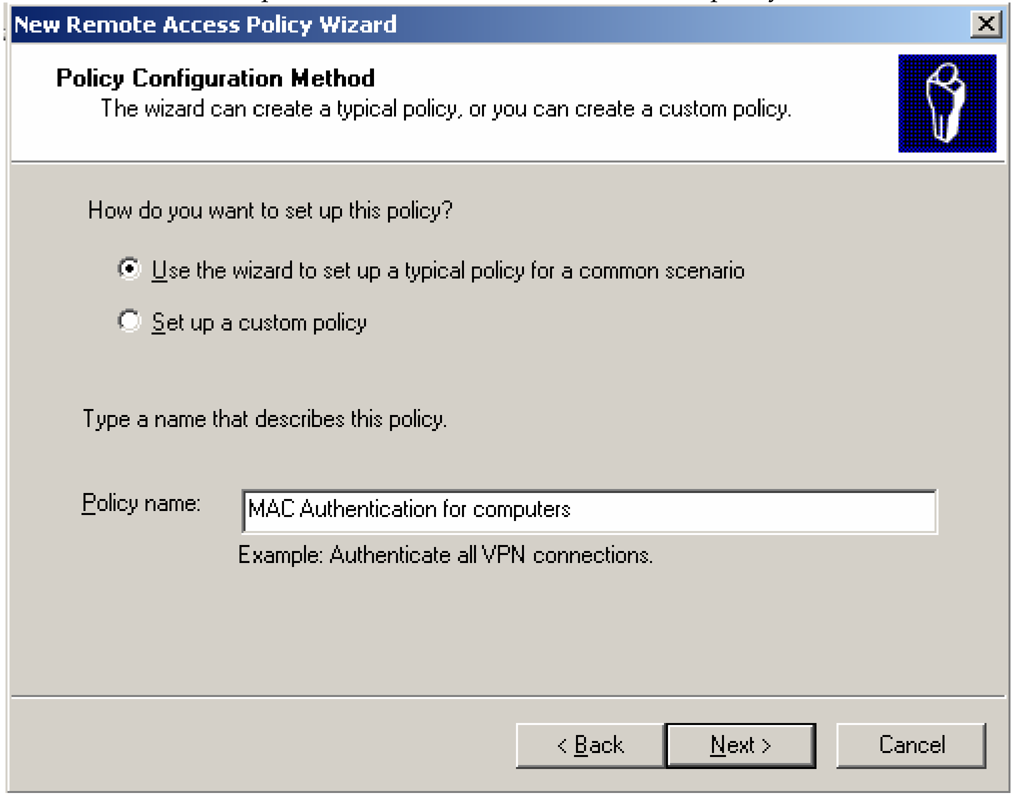
New Remote Access Policy Wizard

Welcome to the New Remote Access Policy Wizard

This wizard helps you set up a remote access policy, which is a set of conditions that determine which connection requests are granted access by this server.

To continue, click Next.

7. Enter a descriptive name for the new remote access policy and click next.



New Remote Access Policy Wizard

Policy Configuration Method

The wizard can create a typical policy, or you can create a custom policy.

How do you want to set up this policy?

● Use the wizard to set up a typical policy for a common scenario

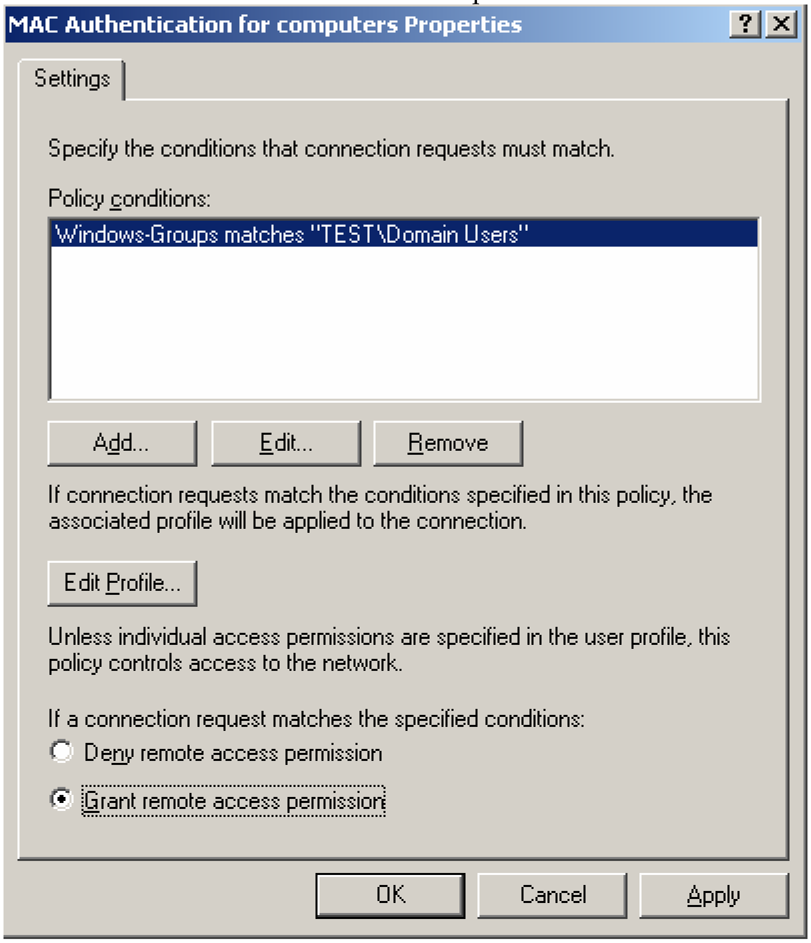
○ Set up a custom policy

Type a name that describes this policy.

Policy name: MAC Authentication for computers

Example: Authenticate all VPN connections.

8. Condition for connection request to the remote access policy is defined next, the default Windows Group is already selected as a matching condition. You can add more or remove Active Directory Groups by clicking on the Add or Remove button. Click on grant access permission when conditions are match. Click on Edit profile.



MAC Authentication for computers Properties

Settings

Specify the conditions that connection requests must match.

Policy conditions:

Windows-Groups matches "TEST\Domain Users"

If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.

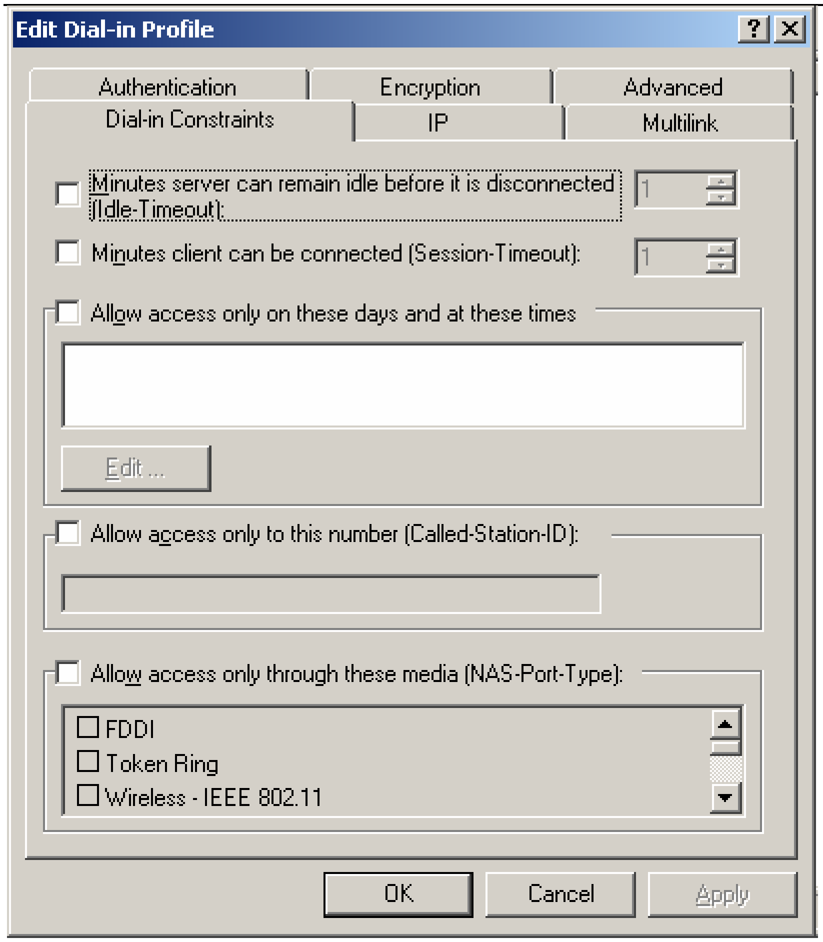
Unless individual access permissions are specified in the user profile, this policy controls access to the network.

If a connection request matches the specified conditions:

○ Deny remote access permission

● Grant remote access permission

9. When you click on Edit Profile the following tab filled pane will appear, click on the authentication tab.



□ Minutes server can remain idle before it is disconnected (Idle-Timeout): 1

□ Minutes client can be connected (Session-Timeout): 1

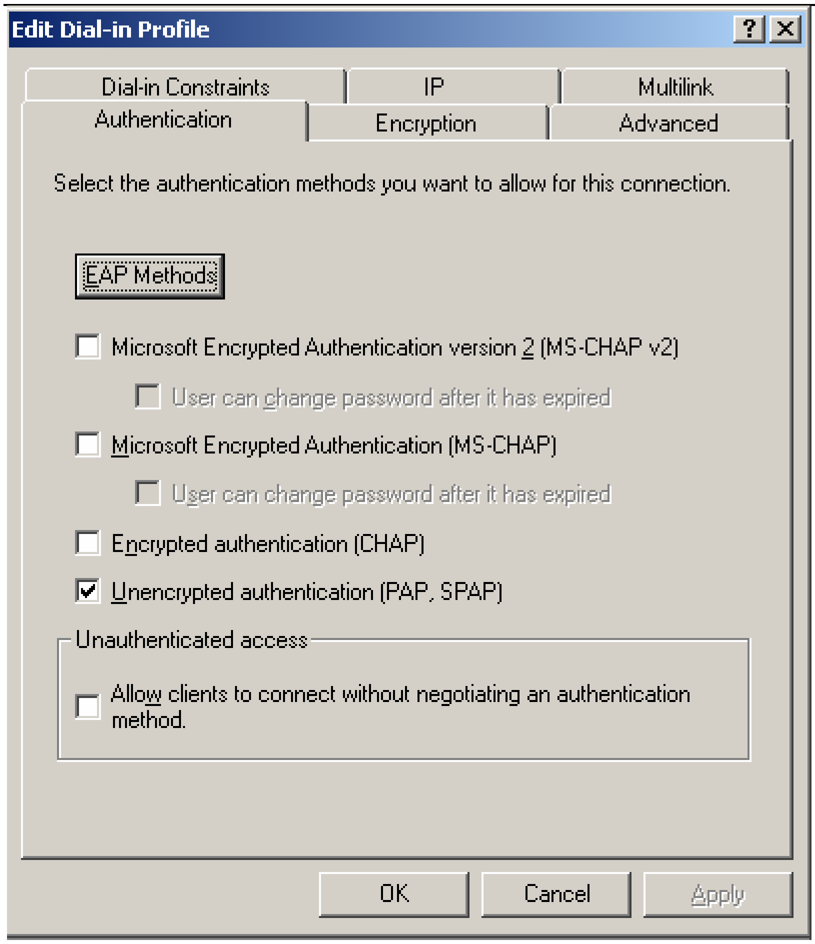
□ Allow access only on these days and at these times

□ Allow access only to this number (Called-Station-ID):

□ Allow access only through these media (NAS-Port-Type):

- □ FDDI
- □ Token Ring
- □ Wireless - IEEE 802.11

10. Select only unencrypted authentication



Edit Dial-in Profile

Select the authentication methods you want to allow for this connection.

□ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

□ User can change password after it has expired

□ Microsoft Encrypted Authentication (MS-CHAP)

□ User can change password after it has expired

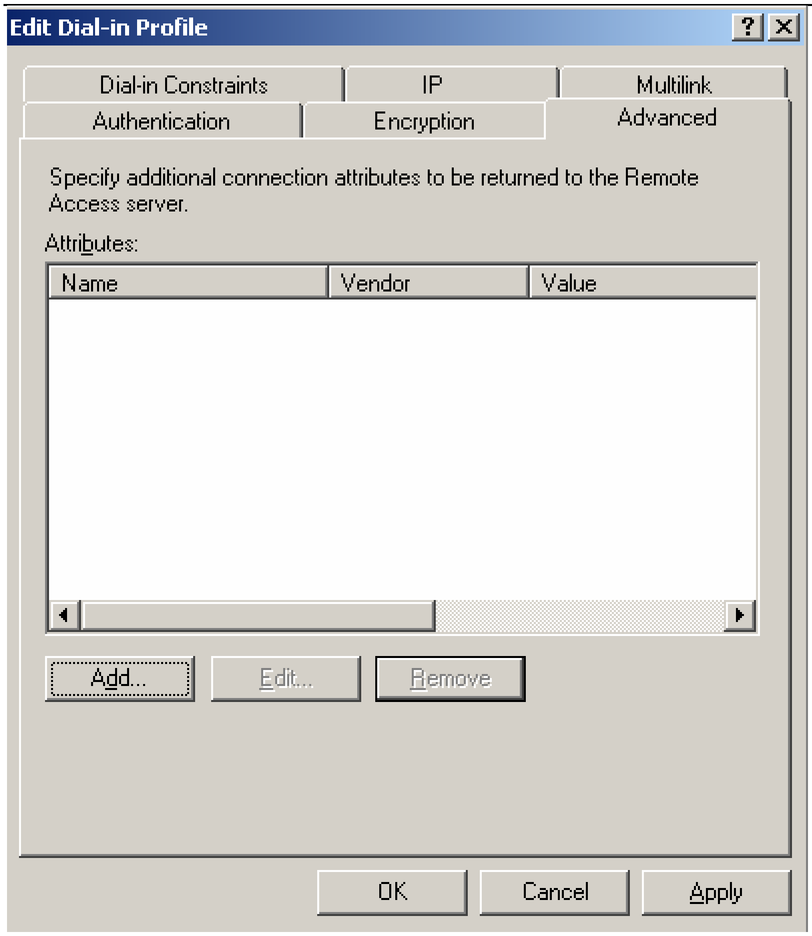
□ Encrypted authentication (CHAP)

☑ Unencrypted authentication (PAP, SPAP)

Unauthenticated access

□ Allow clients to connect without negotiating an authentication method.

11. Click on the advanced tab, and add additional attributes.



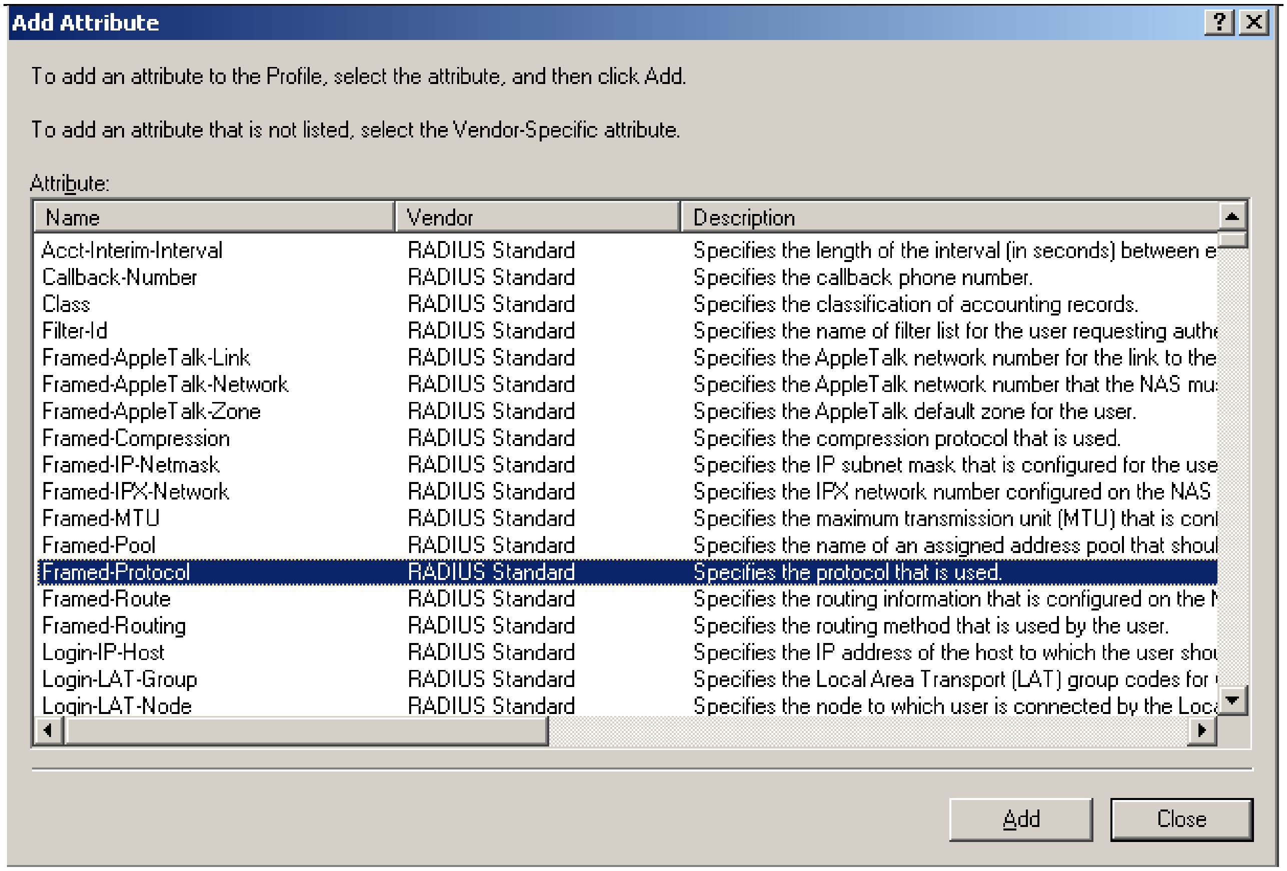
Edit Dial-in Profile

Specify additional connection attributes to be returned to the Remote Access server.

Attributes:

Name	Vendor	Value

12. Click on Framed Protocol on the next screen and click on add.



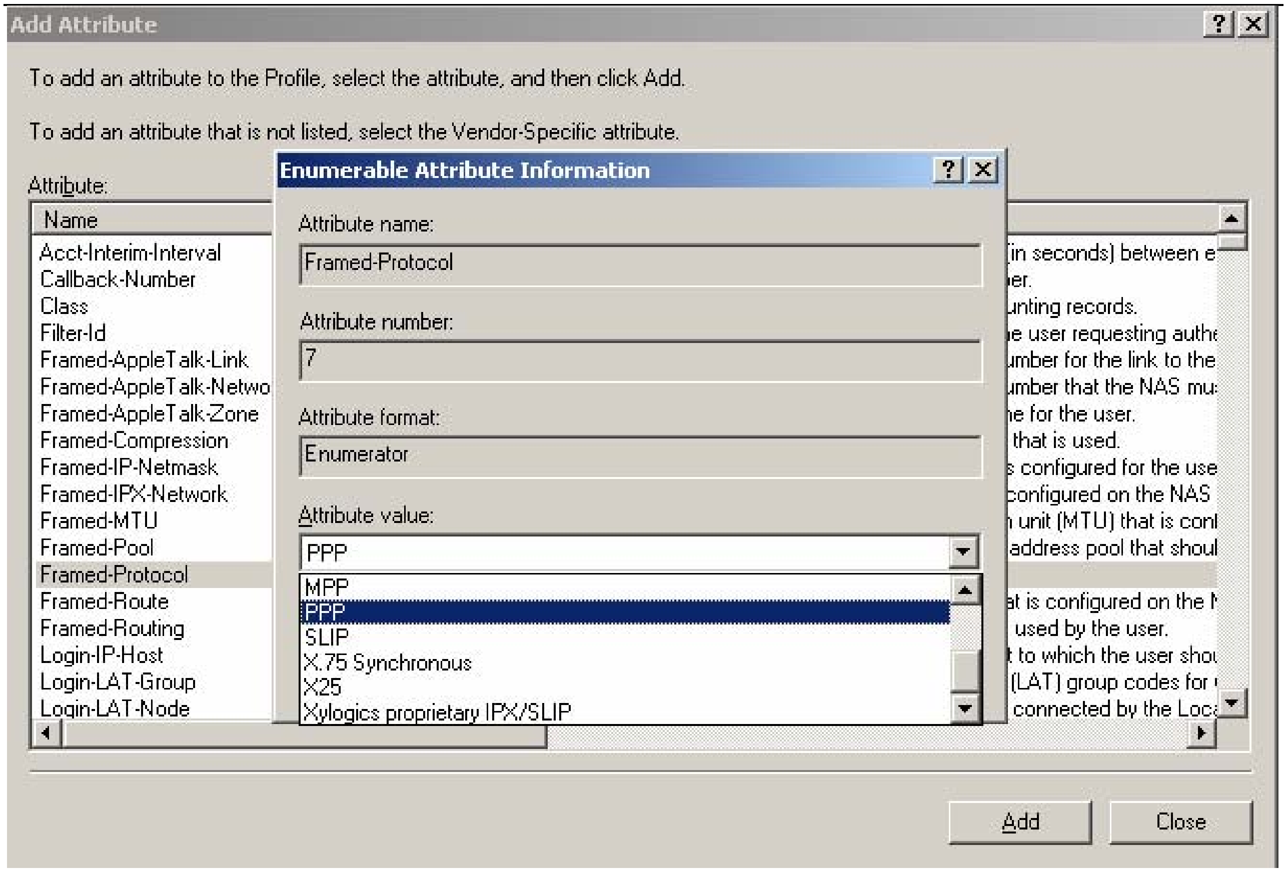
To add an attribute to the Profile, select the attribute, and then click Add.

To add an attribute that is not listed, select the Vendor-Specific attribute.

Attribute:

Name	Vendor	Description
Acct-Interim-Interval	RADIUS Standard	Specifies the length of the interval (in seconds) between e
Callback-Number	RADIUS Standard	Specifies the callback phone number.
Class	RADIUS Standard	Specifies the classification of accounting records.
Filter-Id	RADIUS Standard	Specifies the name of filter list for the user requesting authe
Framed-AppleTalk-Link	RADIUS Standard	Specifies the AppleTalk network number for the link to the
Framed-AppleTalk-Network	RADIUS Standard	Specifies the AppleTalk network number that the NAS mu:
Framed-AppleTalk-Zone	RADIUS Standard	Specifies the AppleTalk default zone for the user.
Framed-Compression	RADIUS Standard	Specifies the compression protocol that is used.
Framed-IP-Netmask	RADIUS Standard	Specifies the IP subnet mask that is configured for the use
Framed-IPX-Network	RADIUS Standard	Specifies the IPX network number configured on the NAS
Framed-MTU	RADIUS Standard	Specifies the maximum transmission unit (MTU) that is conl
Framed-Pool	RADIUS Standard	Specifies the name of an assigned address pool that shoul
Framed-Protocol	RADIUS Standard	Specifies the protocol that is used.
Framed-Route	RADIUS Standard	Specifies the routing information that is configured on the N
Framed-Routing	RADIUS Standard	Specifies the routing method that is used by the user.
Login-IP-Host	RADIUS Standard	Specifies the IP address of the host to which the user shou
Login-LAT-Group	RADIUS Standard	Specifies the Local Area Transport (LAT) group codes for (
Login-LAT-Node	RADIUS Standard	Specifies the node to which user is connected by the Loca

13. Select PPP as the enumerable attribute on the next screen.



Add Attribute

To add an attribute to the Profile, select the attribute, and then click Add.

To add an attribute that is not listed, select the Vendor-Specific attribute.

Enumerable Attribute Information

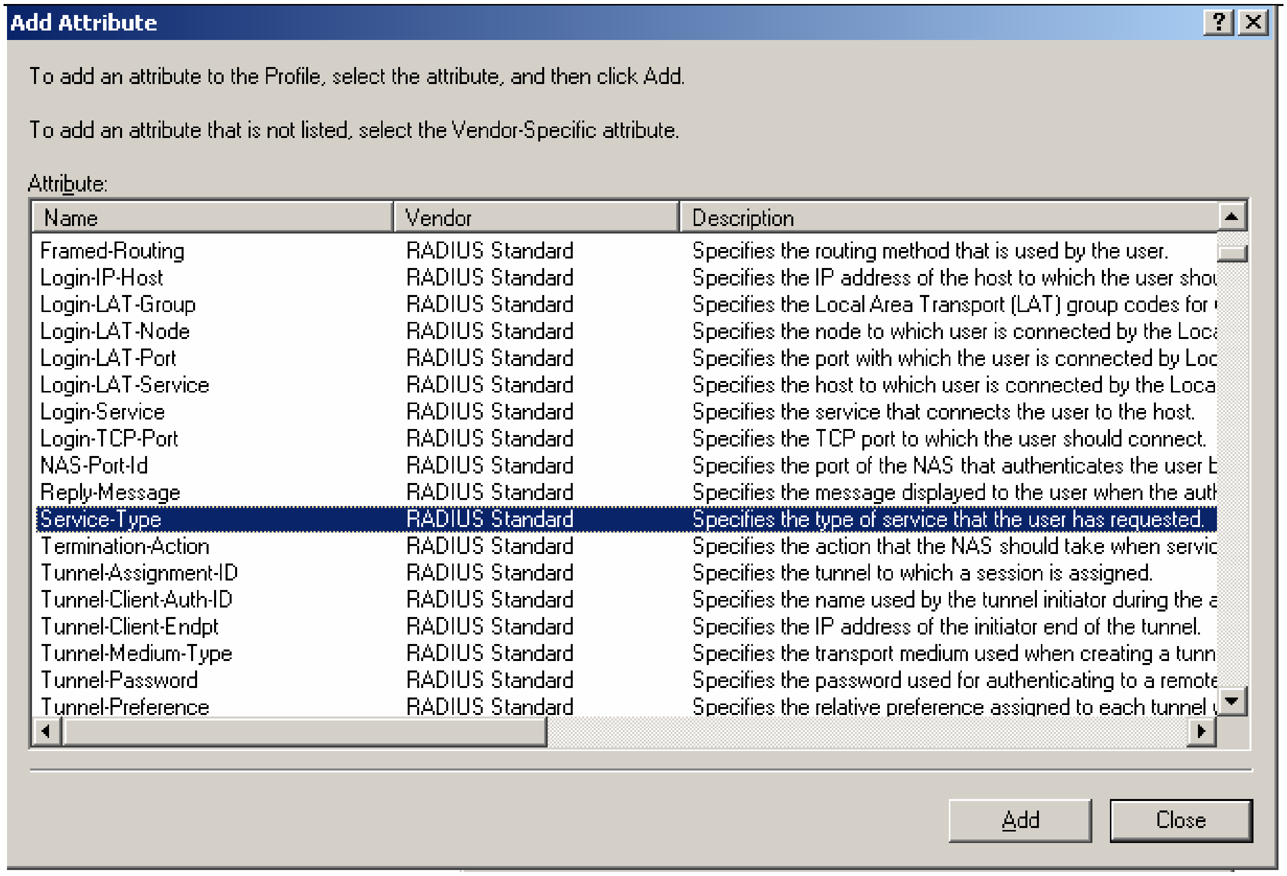
Attribute name: Framed-Protocol

Attribute number: 7

Attribute format: Enumerator

Attribute value: PPP

14. Add the second attribute. Click on add and select Service Type as the attribute, and click on add.



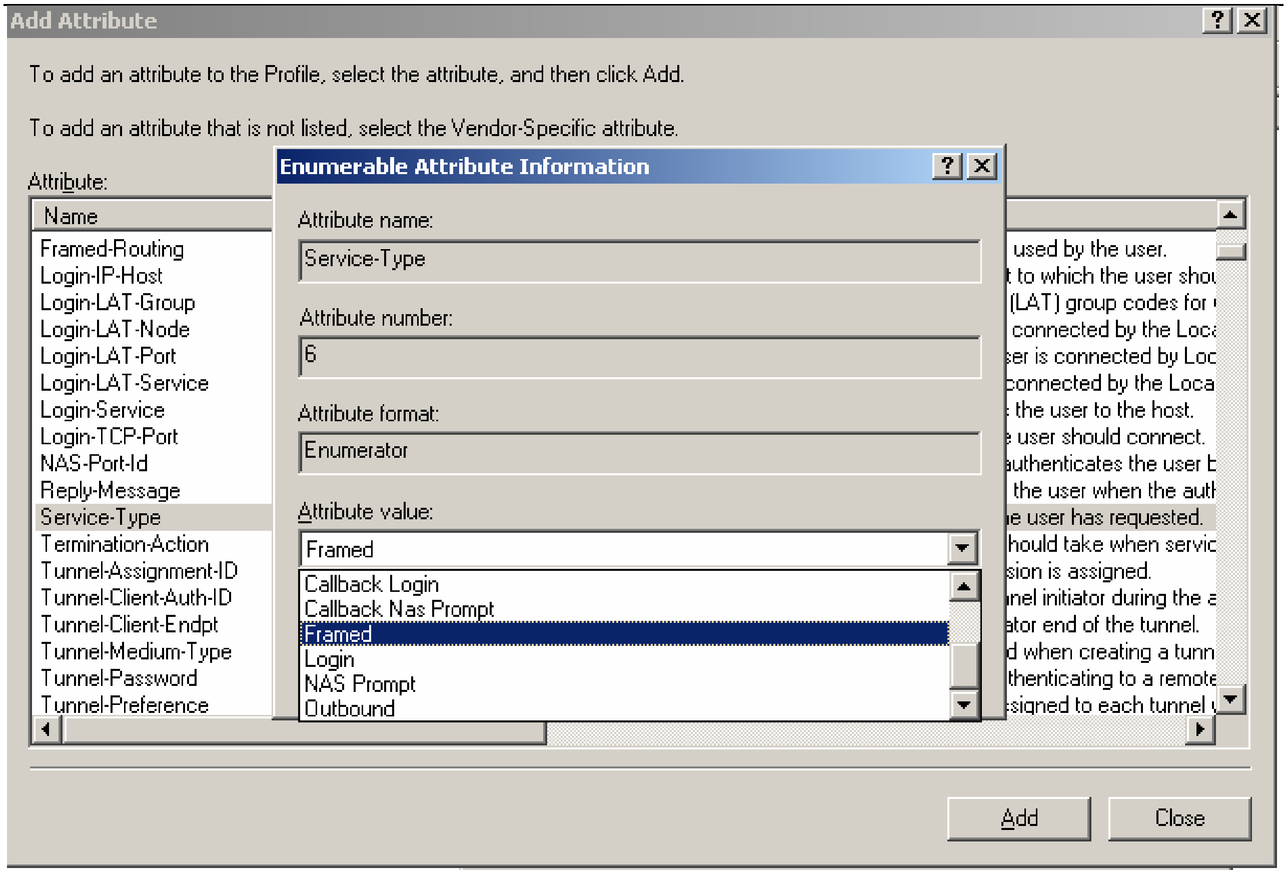
To add an attribute to the Profile, select the attribute, and then click Add.

To add an attribute that is not listed, select the Vendor-Specific attribute.

Attribute:

Name	Vendor	Description
Framed-Routing	RADIUS Standard	Specifies the routing method that is used by the user.
Login-IP-Host	RADIUS Standard	Specifies the IP address of the host to which the user shou
Login-LAT-Group	RADIUS Standard	Specifies the Local Area Transport (LAT) group codes for
Login-LAT-Node	RADIUS Standard	Specifies the node to which user is connected by the Loca
Login-LAT-Port	RADIUS Standard	Specifies the port with which the user is connected by Loc
Login-LAT-Service	RADIUS Standard	Specifies the host to which user is connected by the Loca
Login-Service	RADIUS Standard	Specifies the service that connects the user to the host.
Login-TCP-Port	RADIUS Standard	Specifies the TCP port to which the user should connect.
NAS-Port-Id	RADIUS Standard	Specifies the port of the NAS that authenticates the user b
Reply-Message	RADIUS Standard	Specifies the message displayed to the user when the auth
Service-Type	RADIUS Standard	Specifies the type of service that the user has requested.
Termination-Action	RADIUS Standard	Specifies the action that the NAS should take when servic
Tunnel-Assignment-ID	RADIUS Standard	Specifies the tunnel to which a session is assigned.
Tunnel-Client-Auth-ID	RADIUS Standard	Specifies the name used by the tunnel initiator during the a
Tunnel-Client-Endpt	RADIUS Standard	Specifies the IP address of the initiator end of the tunnel.
Tunnel-Medium-Type	RADIUS Standard	Specifies the transport medium used when creating a tunn
Tunnel-Password	RADIUS Standard	Specifies the password used for authenticating to a remote
Tunnel-Preference	RADIUS Standard	Specifies the relative preference assigned to each tunnel v

15. Select Framed as the enumerable attribute on the next screen and click on Add.



Add Attribute

To add an attribute to the Profile, select the attribute, and then click Add.

To add an attribute that is not listed, select the Vendor-Specific attribute.

Attribute:

Name	
Framed-Routing	used by the user.
Login-IP-Host	t to which the user shou
Login-LAT-Group	(LAT) group codes for
Login-LAT-Node	connected by the Loca
Login-LAT-Port	ser is connected by Loc
Login-LAT-Service	connected by the Loca
Login-Service	the user to the host.
Login-TCP-Port	e user should connect.
NAS-Port-Id	authenticates the user b
Reply-Message	the user when the auth
Service-Type	ne user has requested.
Termination-Action	hould take when servic
Tunnel-Assignment-ID	sion is assigned.
Tunnel-Client-Auth-ID	nel initiator during the a
Tunnel-Client-Endpt	ator end of the tunnel.
Tunnel-Medium-Type	d when creating a tunn
Tunnel-Password	thenticating to a remote
Tunnel-Preference	signed to each tunnel

Enumerable Attribute Information

Attribute name: Service-Type

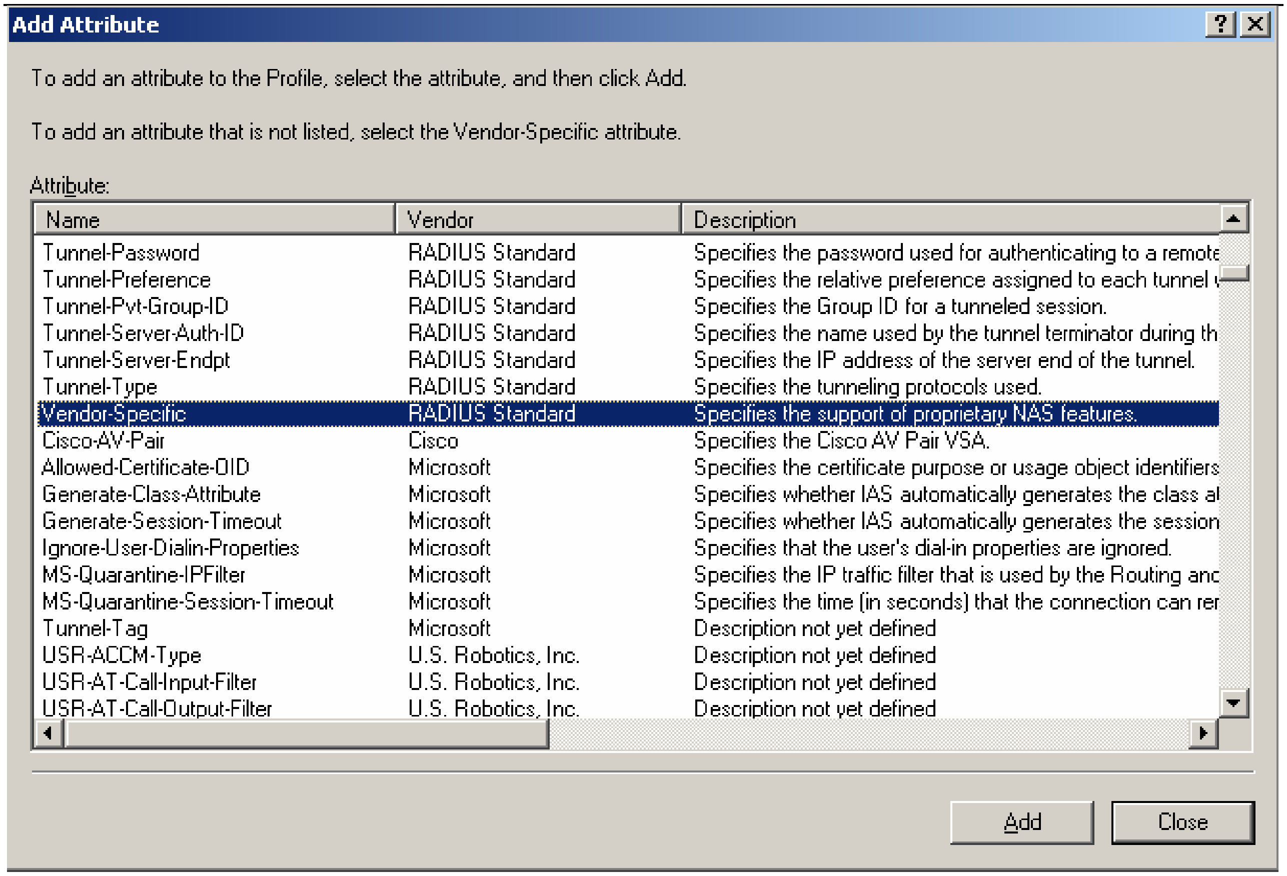
Attribute number: 6

Attribute format: Enumerator

Attribute value: Framed

Callback Login
Callback Nas Prompt
Framed
Login
NAS Prompt
Outbound

16. Add the third attribute by clicking on Add and select vendor specific attributes, and click add.



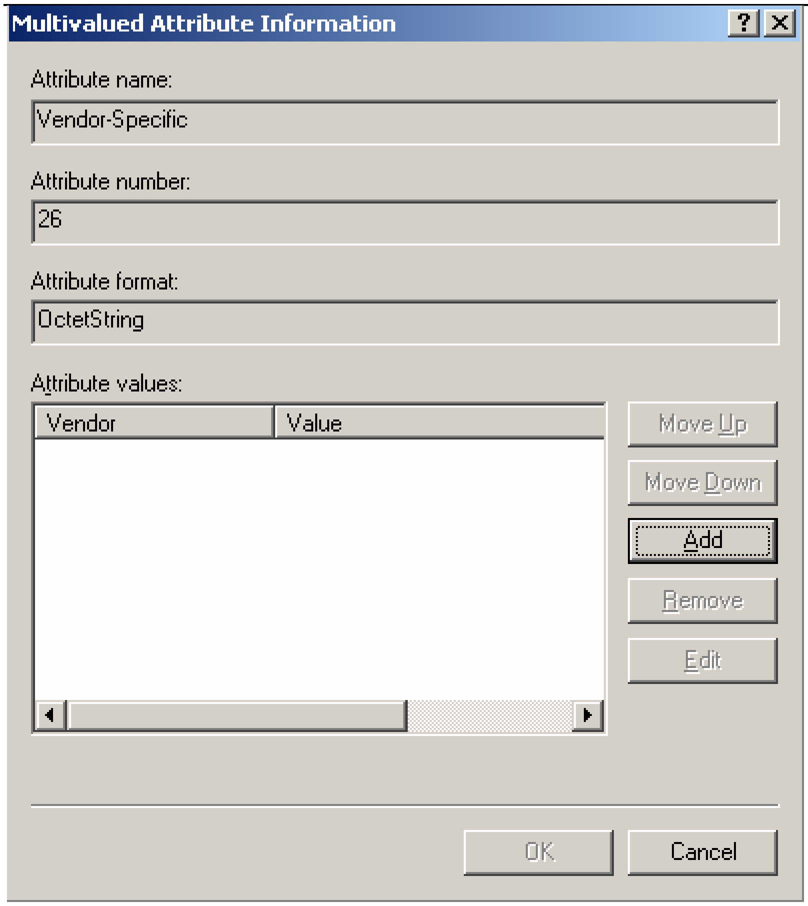
To add an attribute to the Profile, select the attribute, and then click Add.

To add an attribute that is not listed, select the Vendor-Specific attribute.

Attribute:

Name	Vendor	Description
Tunnel-Password	RADIUS Standard	Specifies the password used for authenticating to a remote
Tunnel-Preference	RADIUS Standard	Specifies the relative preference assigned to each tunnel v
Tunnel-Pvt-Group-ID	RADIUS Standard	Specifies the Group ID for a tunneled session.
Tunnel-Server-Auth-ID	RADIUS Standard	Specifies the name used by the tunnel terminator during th
Tunnel-Server-Endpt	RADIUS Standard	Specifies the IP address of the server end of the tunnel.
Tunnel-Type	RADIUS Standard	Specifies the tunneling protocols used.
Vendor-Specific	RADIUS Standard	Specifies the support of proprietary NAS features.
Cisco-AV-Pair	Cisco	Specifies the Cisco AV Pair VSA.
Allowed-Certificate-OID	Microsoft	Specifies the certificate purpose or usage object identifiers
Generate-Class-Attribute	Microsoft	Specifies whether IAS automatically generates the class at
Generate-Session-Timeout	Microsoft	Specifies whether IAS automatically generates the session
Ignore-User-Dialin-Properties	Microsoft	Specifies that the user's dial-in properties are ignored.
MS-Quarantine-IPFilter	Microsoft	Specifies the IP traffic filter that is used by the Routing anc
MS-Quarantine-Session-Timeout	Microsoft	Specifies the time (in seconds) that the connection can rer
Tunnel-Tag	Microsoft	Description not yet defined
USR-ACCM-Type	U.S. Robotics, Inc.	Description not yet defined
USR-AT-Call-Input-Filter	U.S. Robotics, Inc.	Description not yet defined
USR-AT-Call-Output-Filter	U.S. Robotics, Inc.	Description not yet defined

17. On the multivalued attribute information window click on add.



Multivalued Attribute Information

Attribute name:
Vendor-Specific

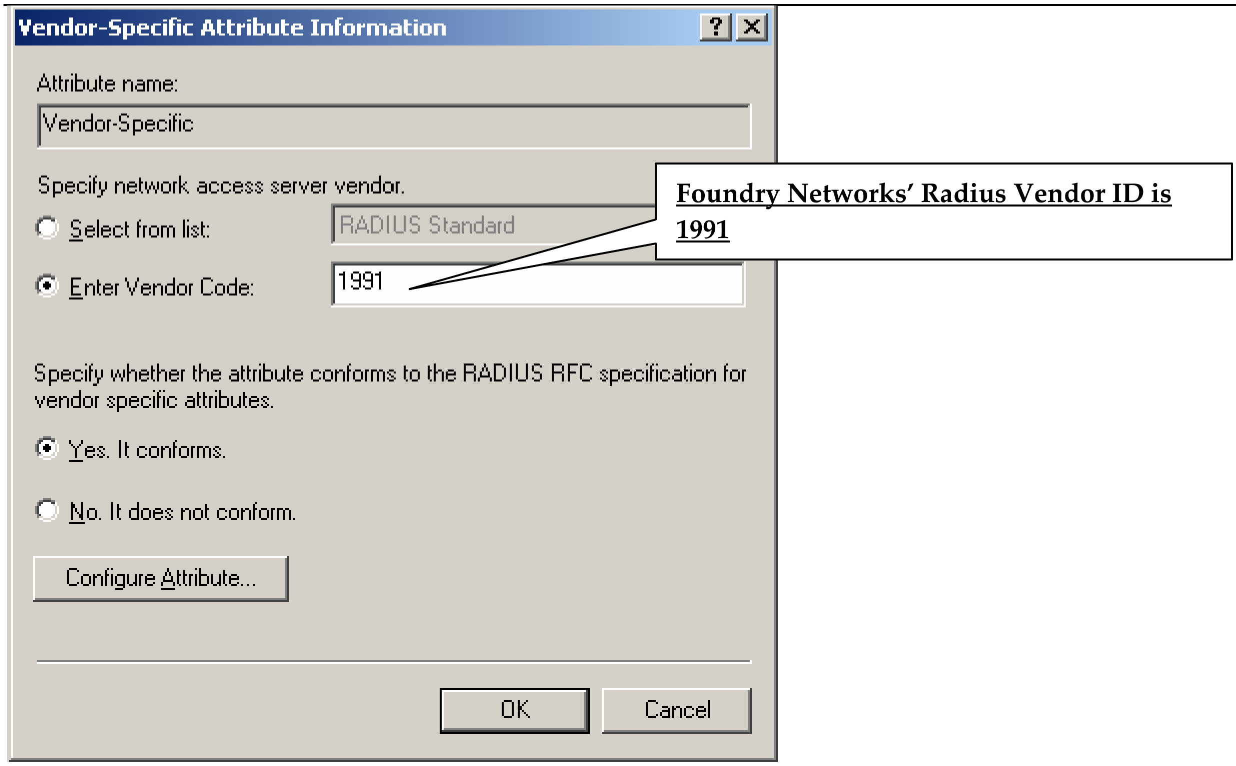
Attribute number:
26

Attribute format:
OctetString

Attribute values:

Vendor	Value

18. A vendor specific attribute window will appear enter the Foundry Vendor ID, click on yes it confirms, and configure attribute to proceed.



Vendor-Specific Attribute Information

Attribute name: Vendor-Specific

Specify network access server vendor.

○ Select from list: RADIUS Standard

● Enter Vendor Code: 1991

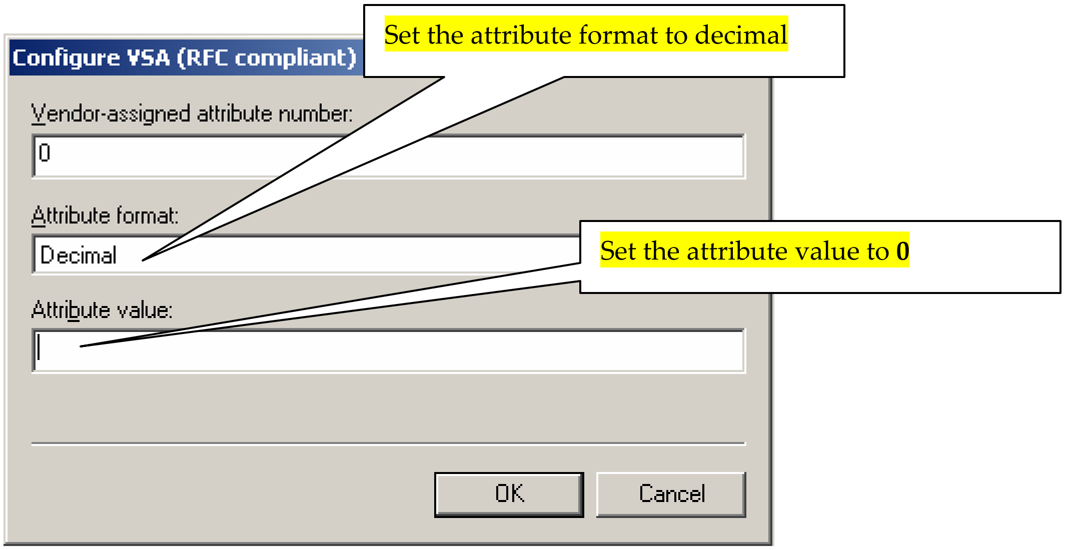
Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

● Yes. It conforms.

○ No. It does not conform.

Foundry Networks' Radius Vendor ID is 1991

19. On the next pane enter Foundry specific attributes.



Configure VSA (RFC compliant)

Vendor-assigned attribute number: 0

Attribute format: Decimal

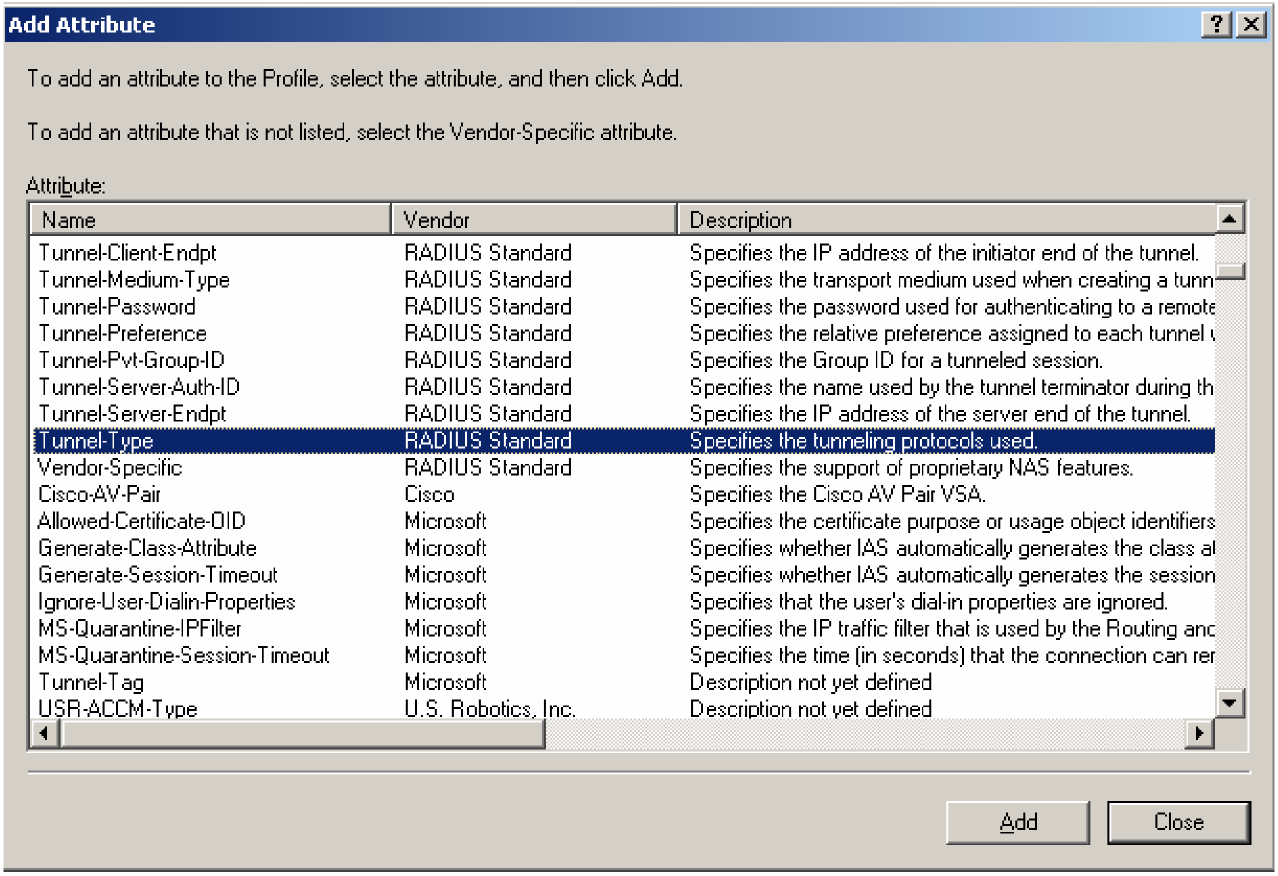
Attribute value:

Set the attribute format to decimal

Set the attribute value to **0**

20. To dynamically place the switch port as an untagged in to a VLAN associated with a MAC address you must select two more attributes (Attribute number 64 and 81). They are:
    a. Attribute number 64 is named Tunnel-Type (Value = Virtual LANs)
    b. Attribute number 81 is named Tunnel-Pvt-Group-Id (Value = "the VLAN number or the name")

21. Click on add to add an attribute and select Tunnel-Type attribute (attribute number 64), and click add.



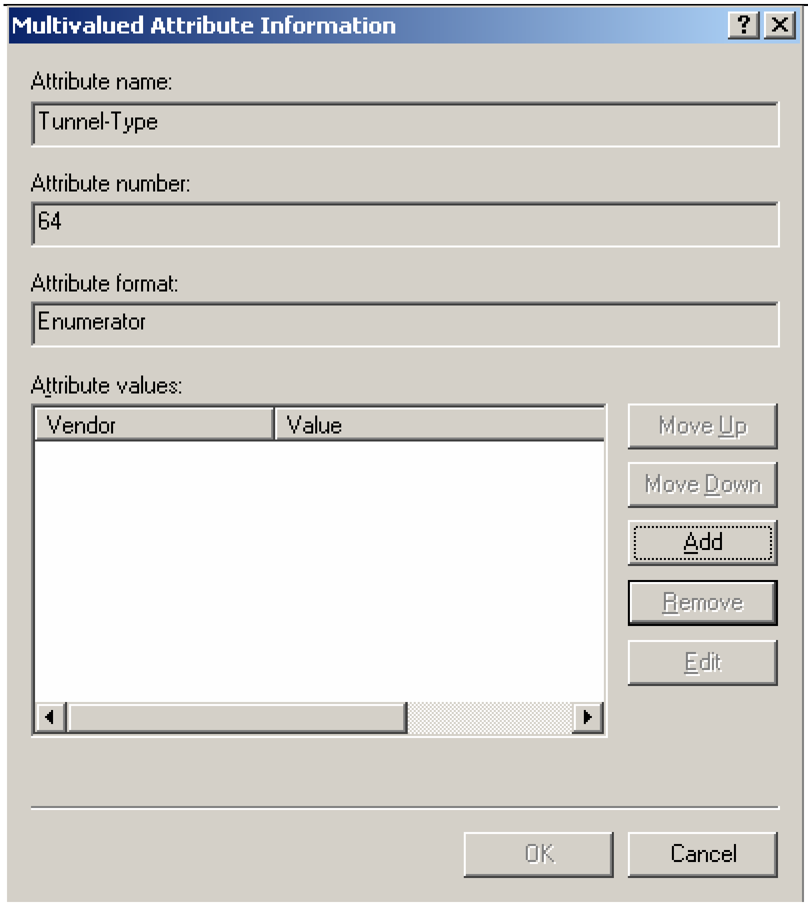
To add an attribute to the Profile, select the attribute, and then click Add.

To add an attribute that is not listed, select the Vendor-Specific attribute.

Attribute:

Name	Vendor	Description
Tunnel-Client-Endpt	RADIUS Standard	Specifies the IP address of the initiator end of the tunnel.
Tunnel-Medium-Type	RADIUS Standard	Specifies the transport medium used when creating a tunn
Tunnel-Password	RADIUS Standard	Specifies the password used for authenticating to a remote
Tunnel-Preference	RADIUS Standard	Specifies the relative preference assigned to each tunnel \
Tunnel-Pvt-Group-ID	RADIUS Standard	Specifies the Group ID for a tunneled session.
Tunnel-Server-Auth-ID	RADIUS Standard	Specifies the name used by the tunnel terminator during th
Tunnel-Server-Endpt	RADIUS Standard	Specifies the IP address of the server end of the tunnel.
Tunnel-Type	RADIUS Standard	Specifies the tunneling protocols used.
Vendor-Specific	RADIUS Standard	Specifies the support of proprietary NAS features.
Cisco-AV-Pair	Cisco	Specifies the Cisco AV Pair VSA.
Allowed-Certificate-OID	Microsoft	Specifies the certificate purpose or usage object identifiers
Generate-Class-Attribute	Microsoft	Specifies whether IAS automatically generates the class at
Generate-Session-Timeout	Microsoft	Specifies whether IAS automatically generates the session
Ignore-User-Dialin-Properties	Microsoft	Specifies that the user's dial-in properties are ignored.
MS-Quarantine-IPFilter	Microsoft	Specifies the IP traffic filter that is used by the Routing anc
MS-Quarantine-Session-Timeout	Microsoft	Specifies the time (in seconds) that the connection can rer
Tunnel-Tag	Microsoft	Description not yet defined
USR-ACCM-Type	U.S. Robotics, Inc.	Description not yet defined

22. Click add in the multivalued attribute screen.



Multivalued Attribute Information

Attribute name: Tunnel-Type

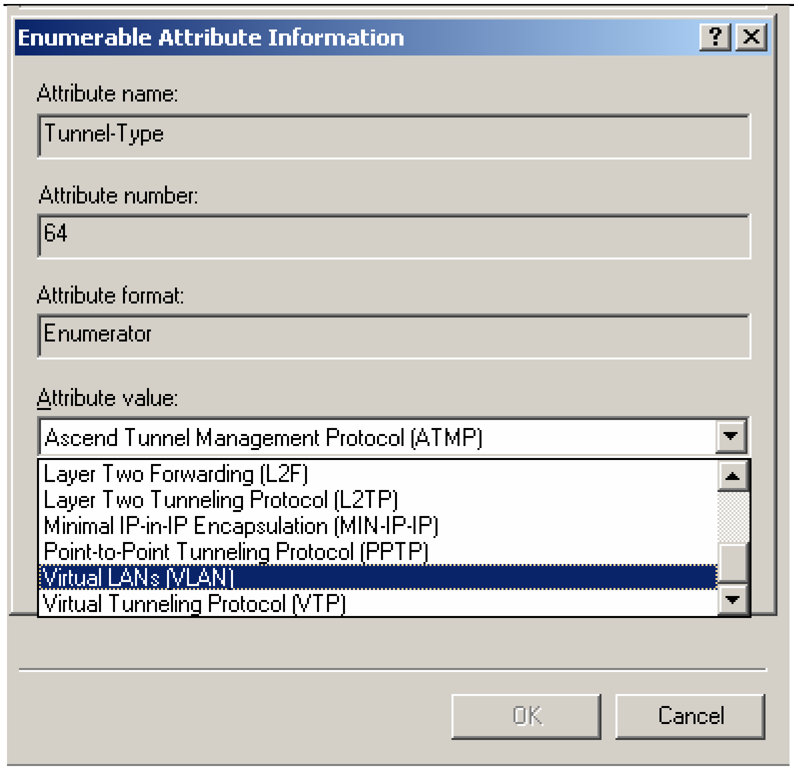
Attribute number: 64

Attribute format: Enumerator

Attribute values:

Vendor	Value

23. Select Virtual LANs on the enumerated value pane, and click ok.



Enumerable Attribute Information

Attribute name:
Tunnel-Type

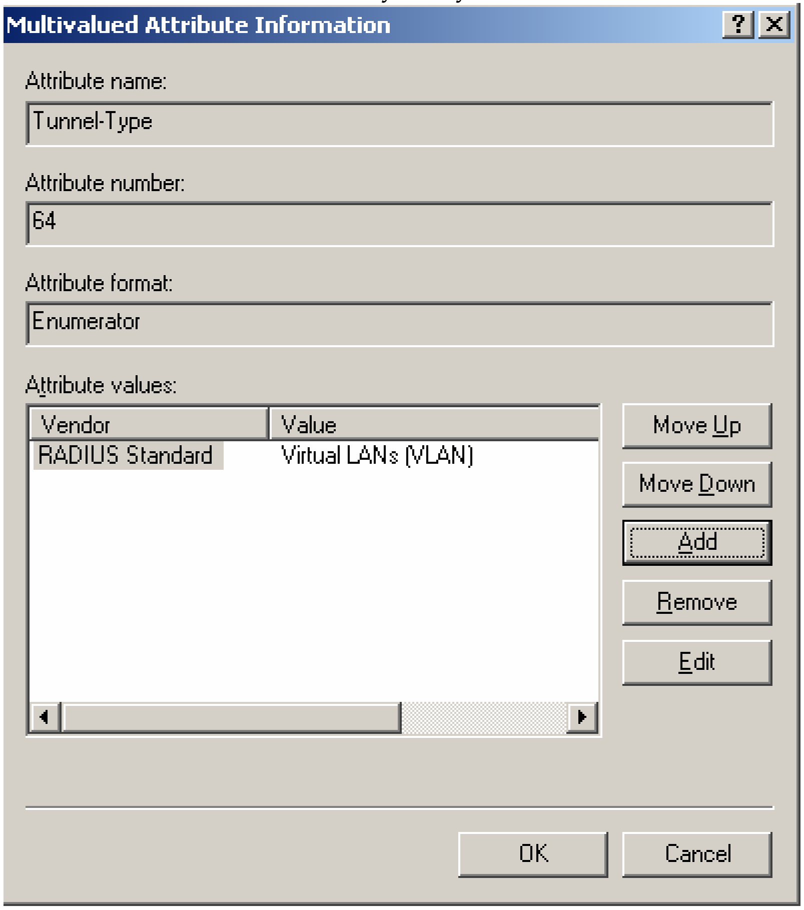
Attribute number:
64

Attribute format:
Enumerator

Attribute value:
Ascend Tunnel Management Protocol (ATMP)

Layer Two Forwarding (L2F)
Layer Two Tunneling Protocol (L2TP)
Minimal IP-in-IP Encapsulation (MIN-IP-IP)
Point-to-Point Tunneling Protocol (PPTP)
Virtual LANs (VLAN)
Virtual Tunneling Protocol (VTP)

24. On the next screen verify that you have selected the Virtual LANs attribute, and click ok.



Multivalued Attribute Information

Attribute name: Tunnel-Type

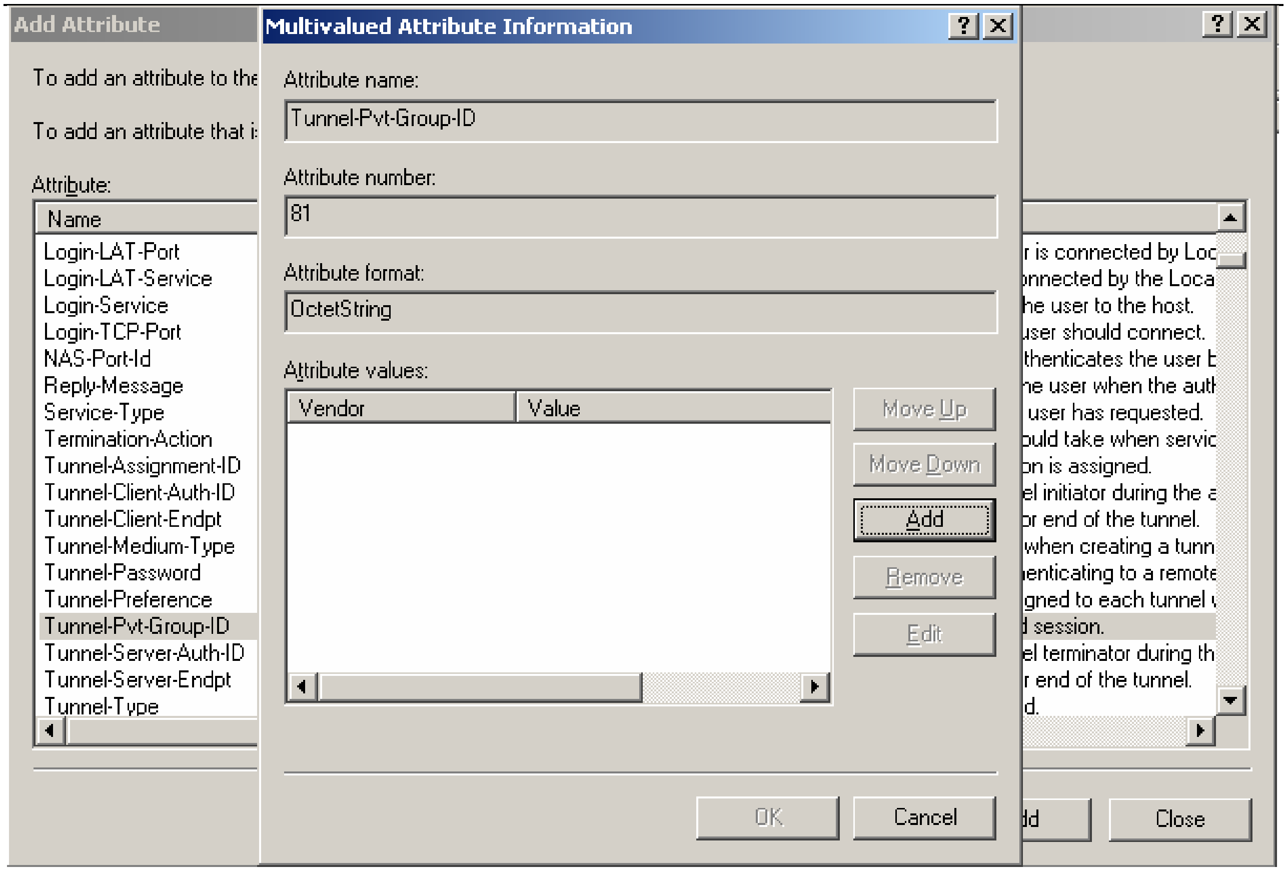
Attribute number: 64

Attribute format: Enumerator

Attribute values:

Vendor	Value
RADIUS Standard	Virtual LANs (VLAN)

25. To add the VLAN ID associated with the MAC address click on add to add an attribute and select Tunnel-Pvt-Group-Id (attribute number 81), and click on add on the next screen.



Add Attribute

To add an attribute to the

To add an attribute that i

Attribute:

Name
Login-LAT-Port
Login-LAT-Service
Login-Service
Login-TCP-Port
NAS-Port-Id
Reply-Message
Service-Type
Termination-Action
Tunnel-Assignment-ID
Tunnel-Client-Auth-ID
Tunnel-Client-Endpt
Tunnel-Medium-Type
Tunnel-Password
Tunnel-Preference
Tunnel-Pvt-Group-ID
Tunnel-Server-Auth-ID
Tunnel-Server-Endpt
Tunnel-Type

Multivalued Attribute Information

Attribute name: Tunnel-Pvt-Group-ID

Attribute number: 81

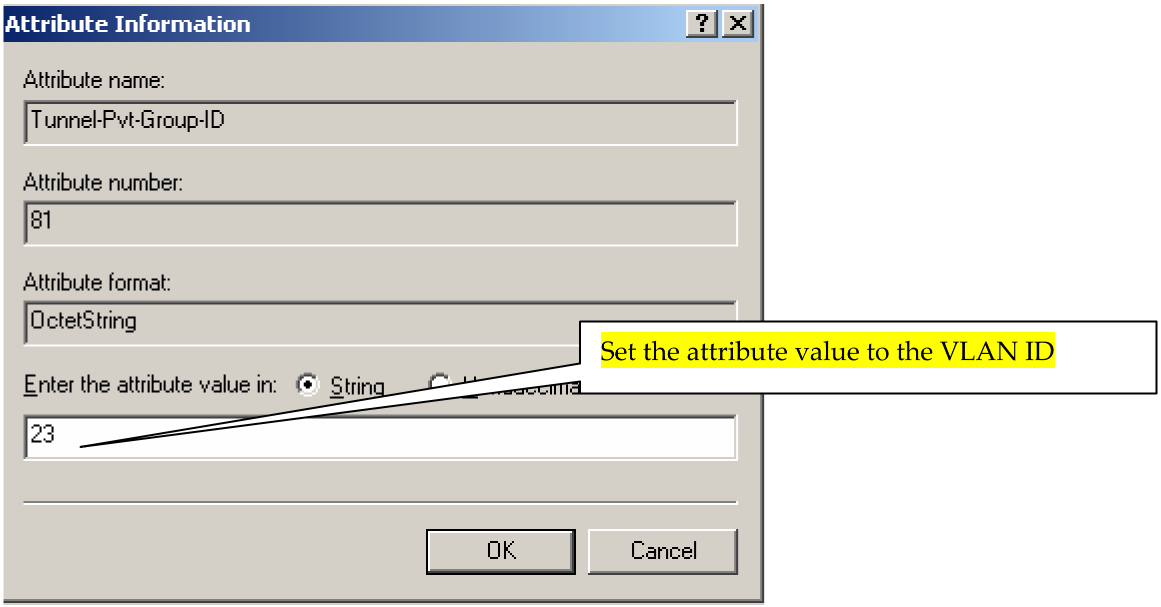
Attribute format: OctetString

Attribute values:

Vendor	Value

r is connected by Loc
onnected by the Loca
he user to the host.
user should connect.
thenticates the user b
he user when the auth
user has requested.
ould take when servic
on is assigned.
el initiator during the a
or end of the tunnel.
when creating a tunn
enticating to a remote
gned to each tunnel v
d session.
el terminator during th
r end of the tunnel.
d.

26. On the next screen define the VLAN associated with the MAC address



Attribute Information

Attribute name: Tunnel-Pvt-Group-ID

Attribute number: 81

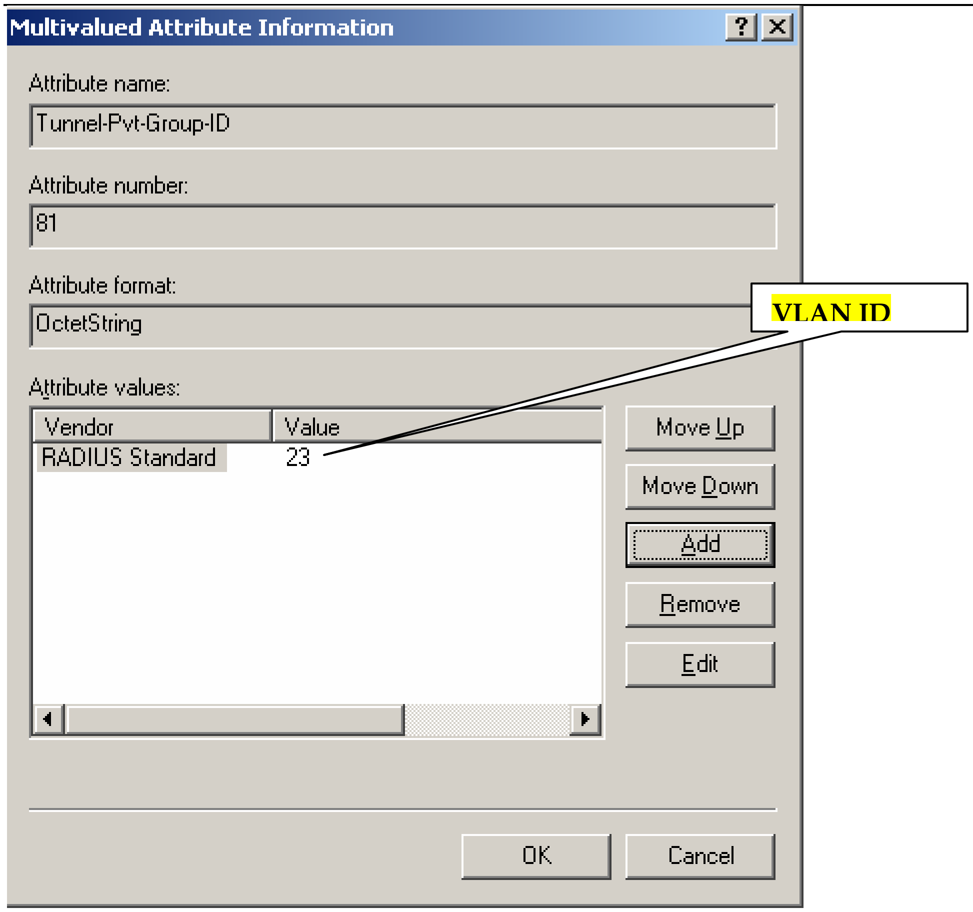
Attribute format: OctetString

Enter the attribute value in: ● String ○ Hexadecimal

23

Set the attribute value to the VLAN ID

27. Click ok to accept the VLAN ID value.



Attribute name: Tunnel-Pvt-Group-ID

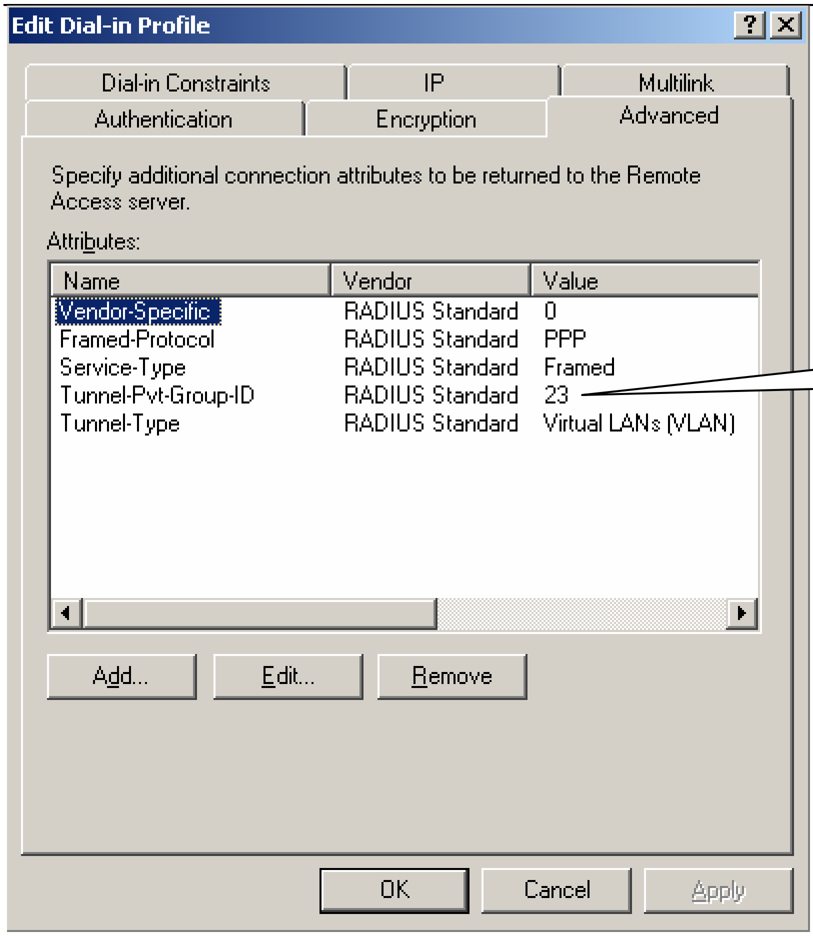
Attribute number: 81

Attribute format: OctetString

Attribute values:

Vendor	Value
RADIUS Standard	23

28. Review the remote access policy configuration to complete the profile and click ok.



Specify additional connection attributes to be returned to the Remote Access server.

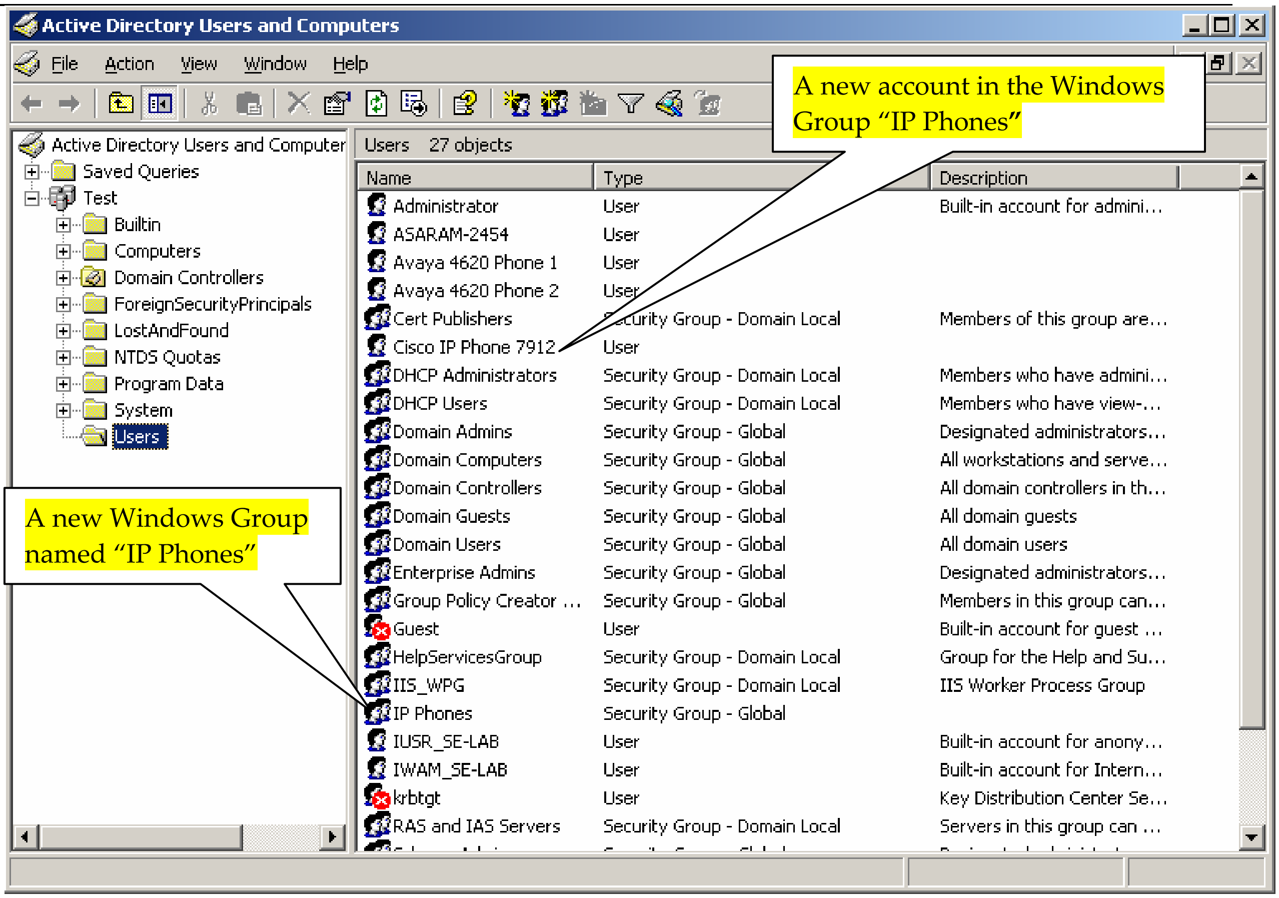
Attributes:

Name	Vendor	Value
Vendor-Specific	RADIUS Standard	0
Framed-Protocol	RADIUS Standard	PPP
Service-Type	RADIUS Standard	Framed
Tunnel-Pvt-Group-ID	RADIUS Standard	23
Tunnel-Type	RADIUS Standard	Virtual LANs (VLAN)

Devices matching this security policy are placed in to VLAN ID 23

29. Steps 5 through 27 creates a security policy named "MAC Authentication for computers", and sets it in the right hand container of Internet Authentication Services pane. This policy matches the following conditions:
    a. Users that are in the "Test\Domain" Windows group only.

    This policy also sends the following information to the Foundry switch.
    i. Attribute number 64 which specifies that user must belong to a Virtual LAN.
    ii. Attribute number 81 which identifies the unique VLAN ID for the user group.
30. In the above security policy access switch port will be placed in to the specified VLAN as an untagged port if the device is authenticated successfully.
31. In some instances, especially with IP Phones, the access switch port needs to be placed in to the specified radius VLAN, and must also be tagged with an IEEE 802.1Q VLAN ID, if the device is authenticated successfully. You will have to create a new security policy to accomplish this.
32. Before you create a new security policy you must create a new Windows group and accounts for devices that will be used as the matching condition for this new security policy.
33. Here is the Active directory configuration with a new windows group as a matching condition for the security policy named "MAC Authentication for IP Phones".



Active Directory Users and Computer
- Saved Queries
- Test
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - LostAndFound
  - NTDS Quotas
  - Program Data
  - System
  - Users

Users 27 objects

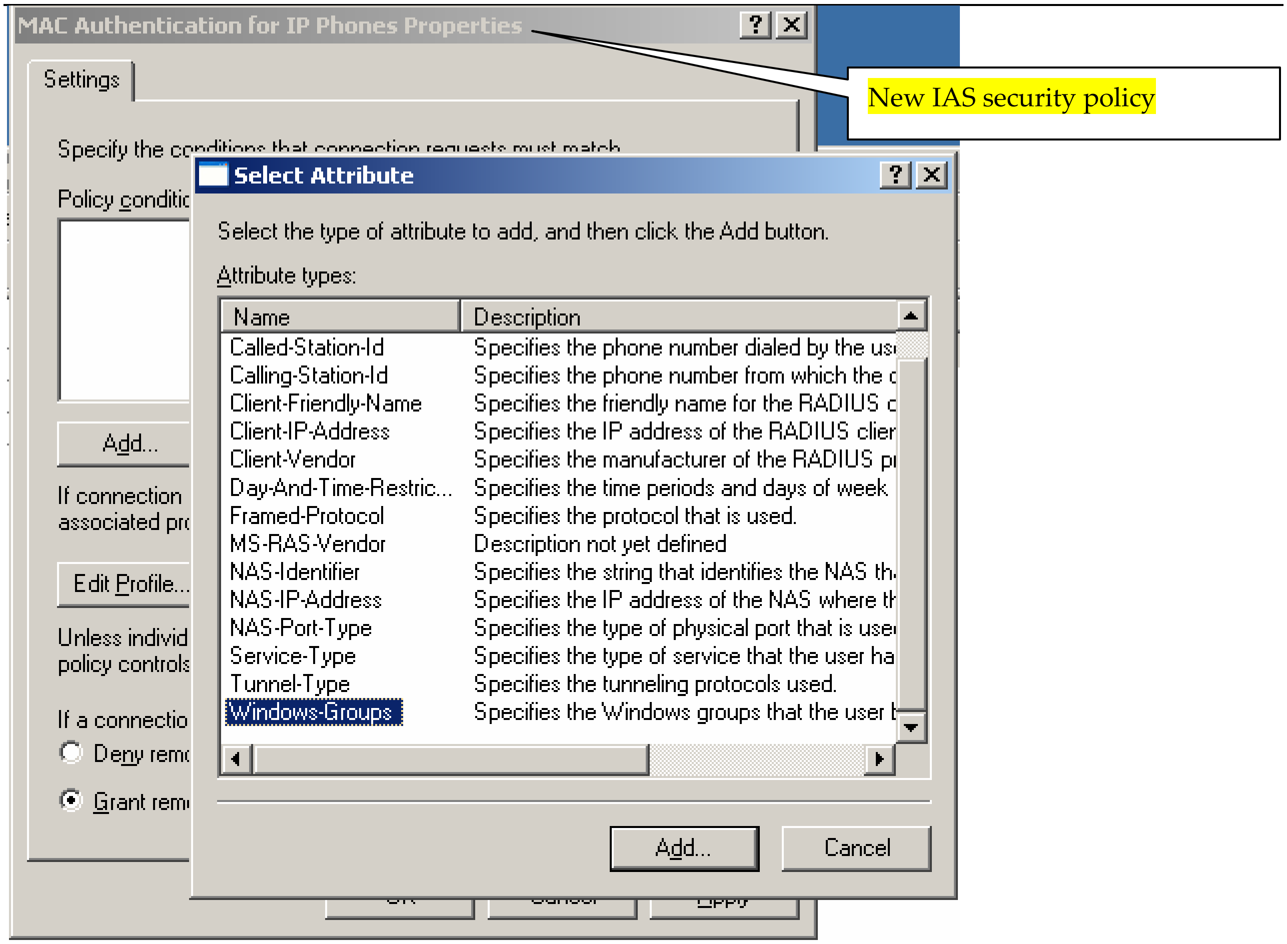
Name	Type	Description
Administrator	User	Built-in account for admini...
ASARAM-2454	User	
Avaya 4620 Phone 1	User	
Avaya 4620 Phone 2	User	
Cert Publishers	Security Group - Domain Local	Members of this group are...
Cisco IP Phone 7912	User	
DHCP Administrators	Security Group - Domain Local	Members who have admini...
DHCP Users	Security Group - Domain Local	Members who have view-...
Domain Admins	Security Group - Global	Designated administrators...
Domain Computers	Security Group - Global	All workstations and serve...
Domain Controllers	Security Group - Global	All domain controllers in th...
Domain Guests	Security Group - Global	All domain guests
Domain Users	Security Group - Global	All domain users
Enterprise Admins	Security Group - Global	Designated administrators...
Group Policy Creator ...	Security Group - Global	Members in this group can...
Guest	User	Built-in account for guest ...
HelpServicesGroup	Security Group - Domain Local	Group for the Help and Su...
IIS_WPG	Security Group - Domain Local	IIS Worker Process Group
IP Phones	Security Group - Global	
IUSR_SE-LAB	User	Built-in account for anony...
IWAM_SE-LAB	User	Built-in account for Intern...
krbtgt	User	Key Distribution Center Se...
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can ...

A new account in the Windows Group "IP Phones"

A new Windows Group named "IP Phones"

34. Repeat steps 5 through 7 in this section to create the new remote policy named "MAC Authentication for IP Phones".
35. Next you will be required to specify the condition that matches the new remote access policy, on this pane you must remove the pre populated default condition, and add the new Windows Group named "IP Phones".

DO NOT USE THE SAME WINDOWS GROUP FOR A NEW OR SUBSEQUENT SECURITY POLICY



New IAS security policy

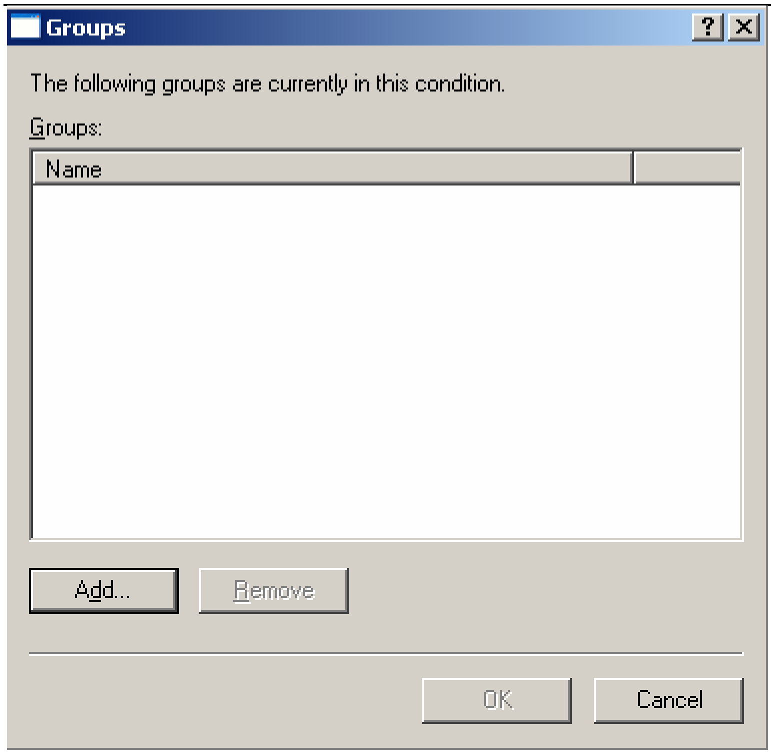
Select Attribute

Select the type of attribute to add, and then click the Add button.

Attribute types:

Name	Description
Called-Station-Id	Specifies the phone number dialed by the us
Calling-Station-Id	Specifies the phone number from which the c
Client-Friendly-Name	Specifies the friendly name for the RADIUS c
Client-IP-Address	Specifies the IP address of the RADIUS clier
Client-Vendor	Specifies the manufacturer of the RADIUS pr
Day-And-Time-Restric...	Specifies the time periods and days of week
Framed-Protocol	Specifies the protocol that is used.
MS-RAS-Vendor	Description not yet defined
NAS-Identifier	Specifies the string that identifies the NAS th
NAS-IP-Address	Specifies the IP address of the NAS where th
NAS-Port-Type	Specifies the type of physical port that is use
Service-Type	Specifies the type of service that the user ha
Tunnel-Type	Specifies the tunneling protocols used.
Windows-Groups	Specifies the Windows groups that the user b

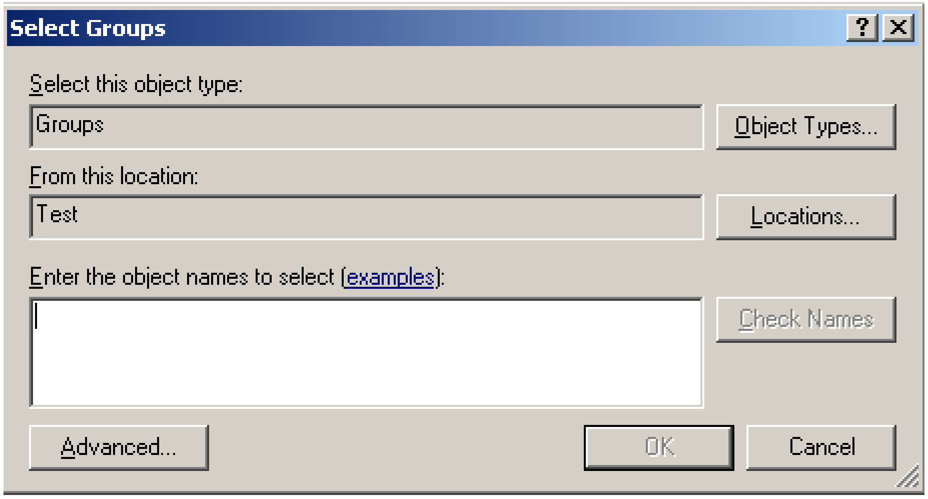
36. Click on add in the next group screen.


Groups

The following groups are currently in this condition.

Groups:

37. Click on advance on the next screen.

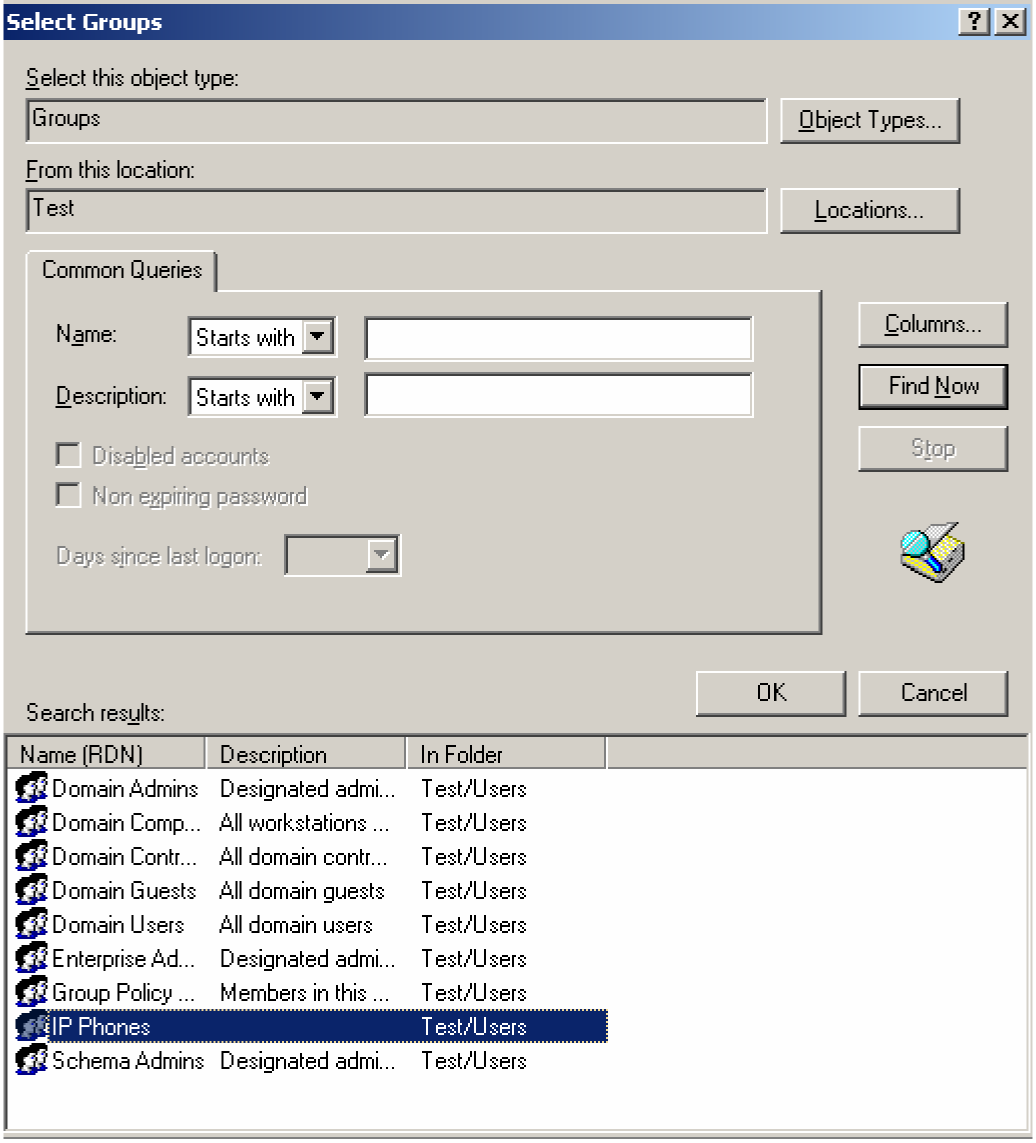

Select Groups

Select this object type: Groups

From this location: Test

Enter the object names to select (examples):

38. Click on find now and select the group named “IP Phones”.



Select this object type: Groups

From this location: Test

Name: Starts with

Description: Starts with

☐ Disabled accounts

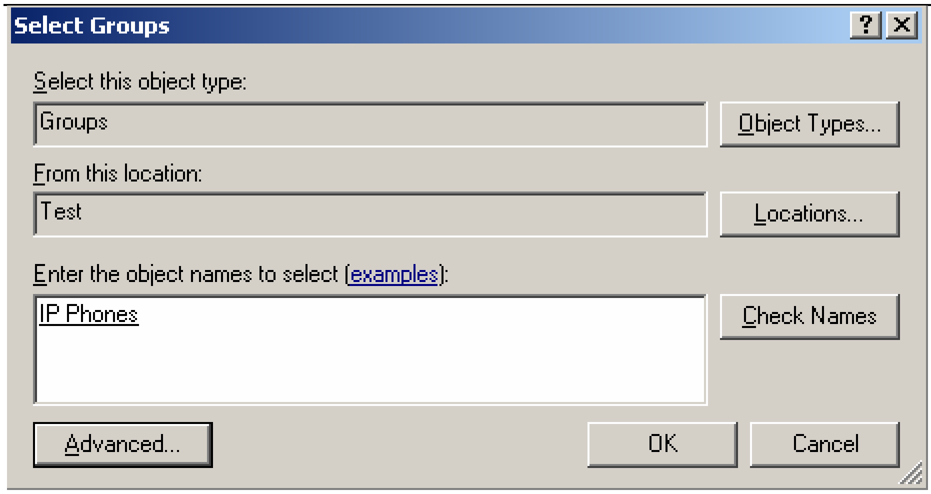
☐ Non expiring password

Days since last logon:

Search results:

Name (RDN)	Description	In Folder
Domain Admins	Designated admi...	Test/Users
Domain Comp...	All workstations ...	Test/Users
Domain Contr...	All domain contr...	Test/Users
Domain Guests	All domain guests	Test/Users
Domain Users	All domain users	Test/Users
Enterprise Ad...	Designated admi...	Test/Users
Group Policy ...	Members in this ...	Test/Users
IP Phones		Test/Users
Schema Admins	Designated admi...	Test/Users

39. Click ok on the next screen to accept the selection.

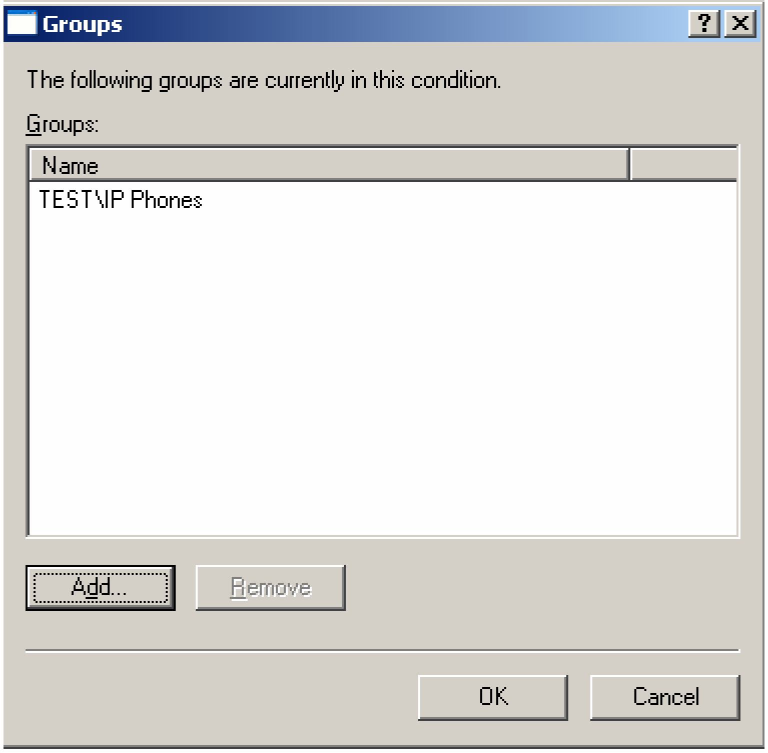


Select this object type:
Groups

From this location:
Test

Enter the object names to select (examples):
IP Phones

40. Click ok to on the next screen to complete the matching condition.

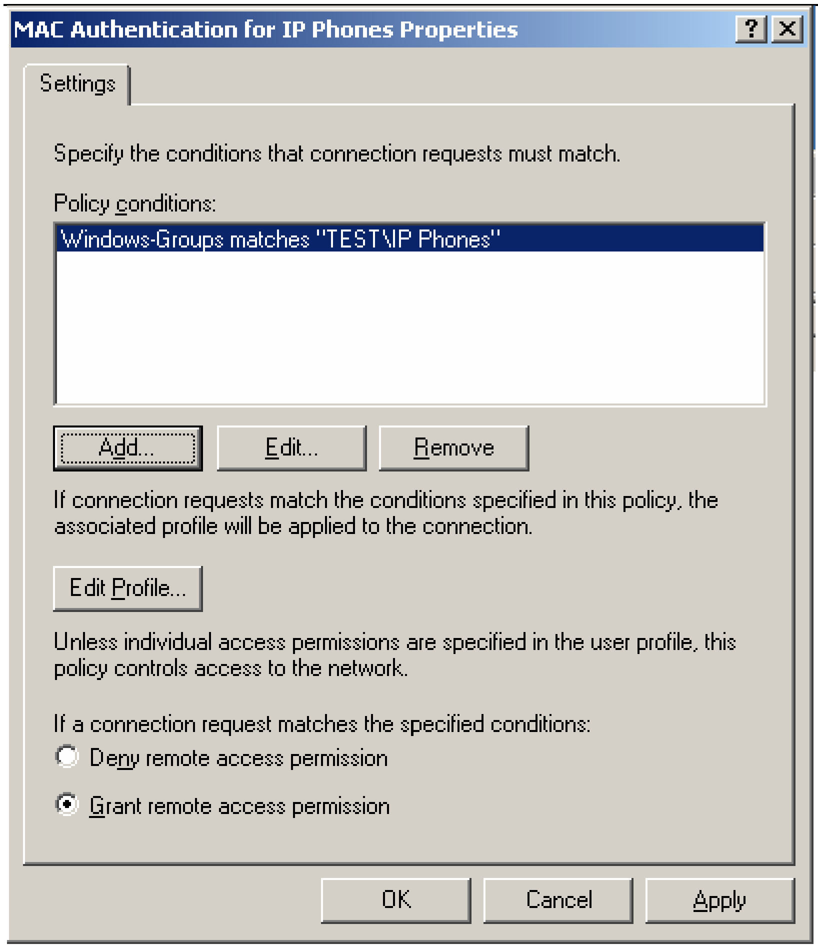


The following groups are currently in this condition.

Groups:

Name
TEST\IP Phones

41. Confirm that you have the correct matching condition for the remote access policy, and click ok.



Specify the conditions that connection requests must match.

Policy conditions:

Windows-Groups matches "TEST\IP Phones"

If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.

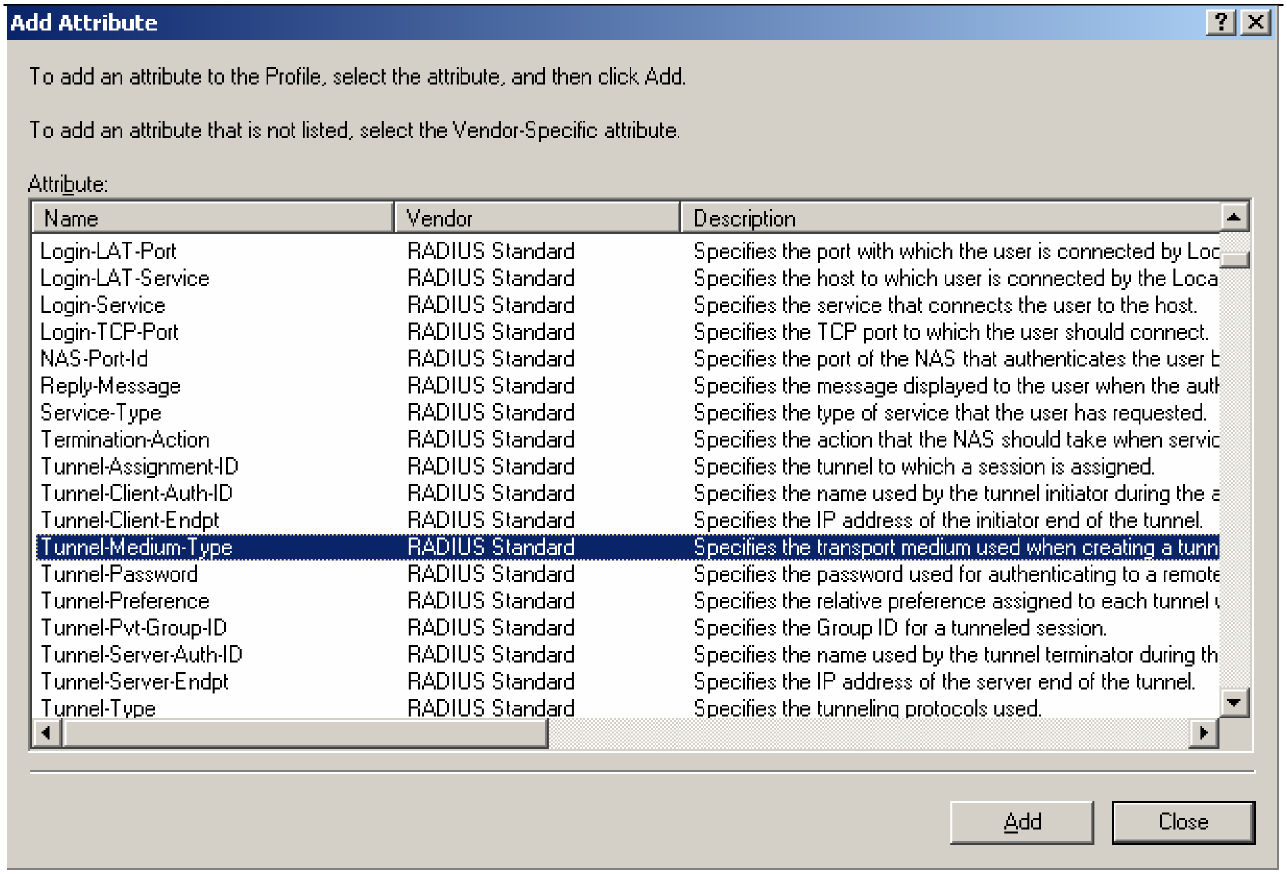
Unless individual access permissions are specified in the user profile, this policy controls access to the network.

If a connection request matches the specified conditions:

○ Deny remote access permission

● Grant remote access permission

42. Click on Edit Profile and repeat steps 9 through 27. Use the new tagged VLAN ID for attribute number 64.
43. You will need to add an additional attribute (attribute number 65) to tag the switch port with an IEEE 802.1Q VLAN ID. Click on add to add an attribute and select Tunnel-Medium-Type, and then click on add.



Add Attribute

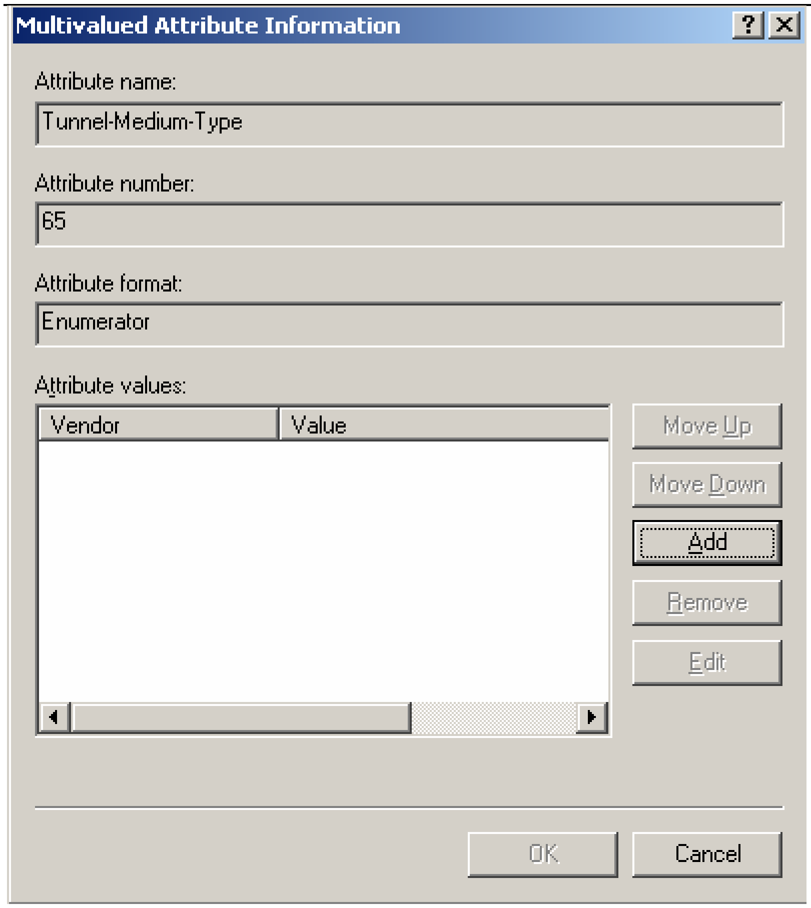
To add an attribute to the Profile, select the attribute, and then click Add.

To add an attribute that is not listed, select the Vendor-Specific attribute.

Attribute:

Name	Vendor	Description
Login-LAT-Port	RADIUS Standard	Specifies the port with which the user is connected by Loc
Login-LAT-Service	RADIUS Standard	Specifies the host to which user is connected by the Loca
Login-Service	RADIUS Standard	Specifies the service that connects the user to the host.
Login-TCP-Port	RADIUS Standard	Specifies the TCP port to which the user should connect.
NAS-Port-Id	RADIUS Standard	Specifies the port of the NAS that authenticates the user b
Reply-Message	RADIUS Standard	Specifies the message displayed to the user when the auth
Service-Type	RADIUS Standard	Specifies the type of service that the user has requested.
Termination-Action	RADIUS Standard	Specifies the action that the NAS should take when servic
Tunnel-Assignment-ID	RADIUS Standard	Specifies the tunnel to which a session is assigned.
Tunnel-Client-Auth-ID	RADIUS Standard	Specifies the name used by the tunnel initiator during the a
Tunnel-Client-Endpt	RADIUS Standard	Specifies the IP address of the initiator end of the tunnel.
Tunnel-Medium-Type	RADIUS Standard	Specifies the transport medium used when creating a tunn
Tunnel-Password	RADIUS Standard	Specifies the password used for authenticating to a remote
Tunnel-Preference	RADIUS Standard	Specifies the relative preference assigned to each tunnel v
Tunnel-Pvt-Group-ID	RADIUS Standard	Specifies the Group ID for a tunneled session.
Tunnel-Server-Auth-ID	RADIUS Standard	Specifies the name used by the tunnel terminator during th
Tunnel-Server-Endpt	RADIUS Standard	Specifies the IP address of the server end of the tunnel.
Tunnel-Type	RADIUS Standard	Specifies the tunneling protocols used.

44. From the Multivalued attribute pane click on add.



Multivalued Attribute Information

Attribute name: Tunnel-Medium-Type

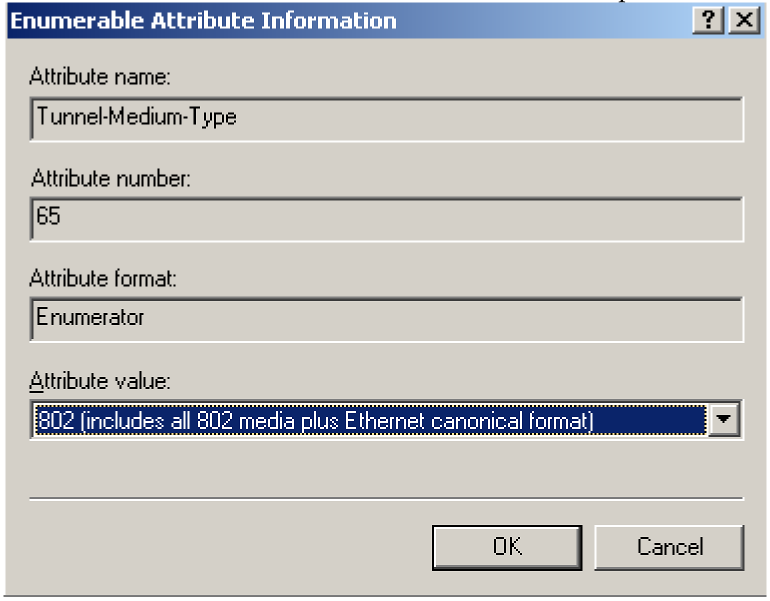
Attribute number: 65

Attribute format: Enumerator

Attribute values:

Vendor	Value

45. From the enumerated attribute information pane select 802 attribute value and click ok.



Enumerable Attribute Information

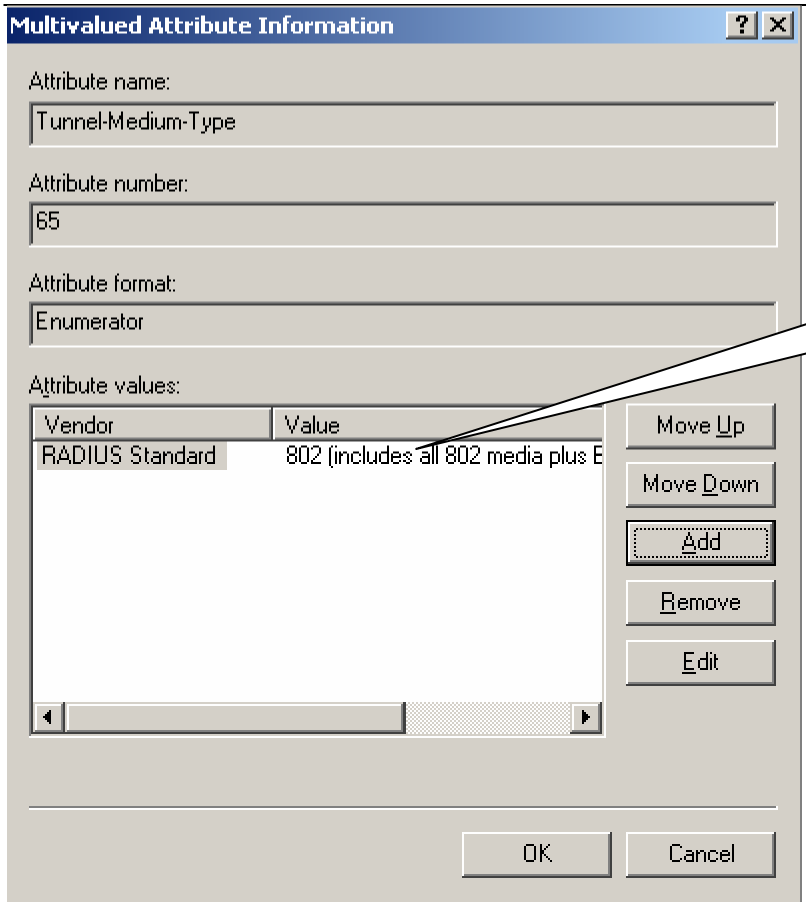
Attribute name: Tunnel-Medium-Type

Attribute number: 65

Attribute format: Enumerator

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

46. On the next pane verify the Attribute value, and click ok accept the value.



Multivalued Attribute Information

Attribute name: Tunnel-Medium-Type

Attribute number: 65

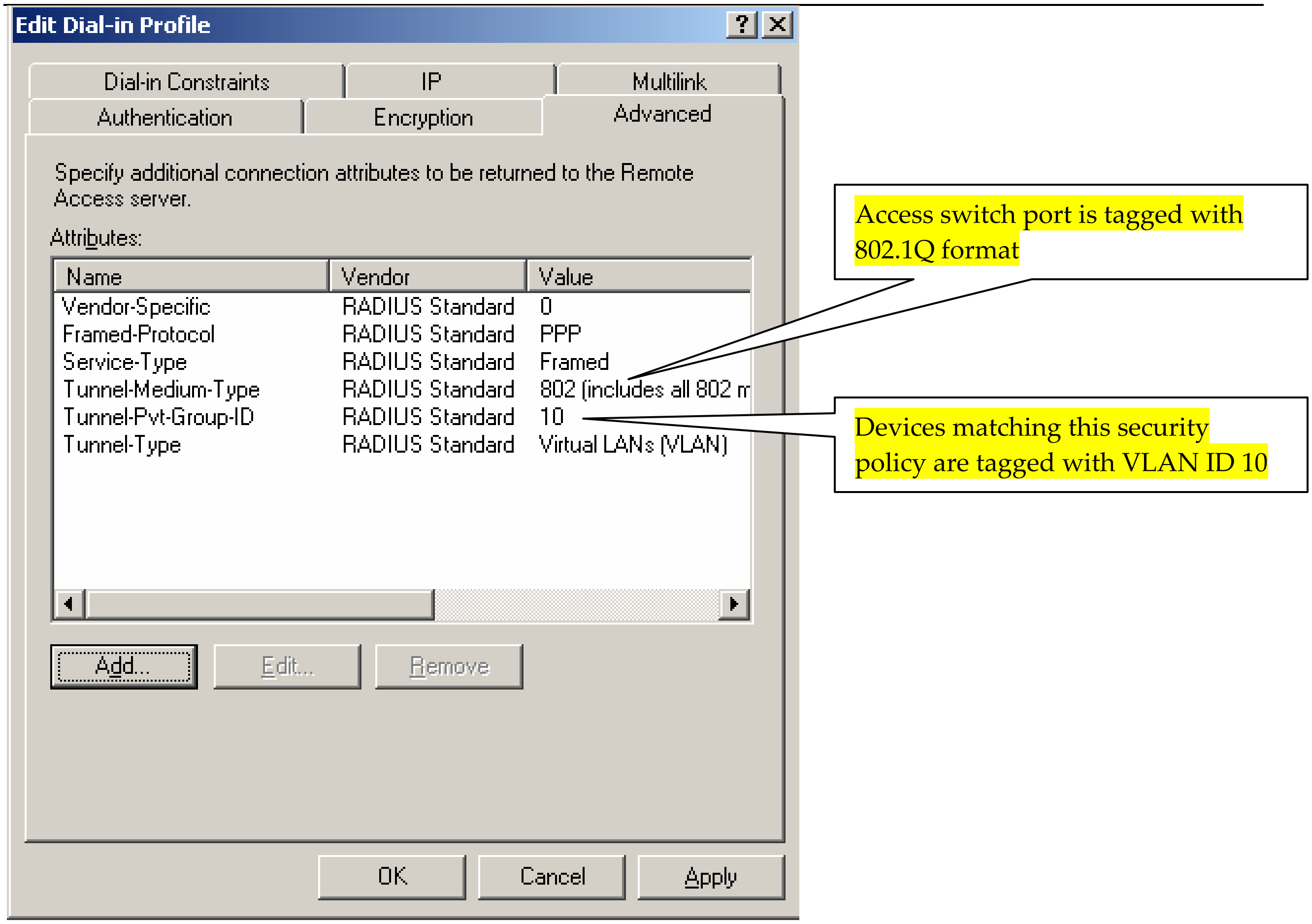
Attribute format: Enumerator

Attribute values:

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

Radius attribute number 65 must be set to 802 to tag access ports in the switch

47. Review the attributes for the new security policy named for “MAC Authentications for IP Phones”.



Specify additional connection attributes to be returned to the Remote Access server.

Attributes:

Name	Vendor	Value
Vendor-Specific	RADIUS Standard	0
Framed-Protocol	RADIUS Standard	PPP
Service-Type	RADIUS Standard	Framed
Tunnel-Medium-Type	RADIUS Standard	802 (includes all 802 m
Tunnel-Pvt-Group-ID	RADIUS Standard	10
Tunnel-Type	RADIUS Standard	Virtual LANs (VLAN)

Access switch port is tagged with 802.1Q format

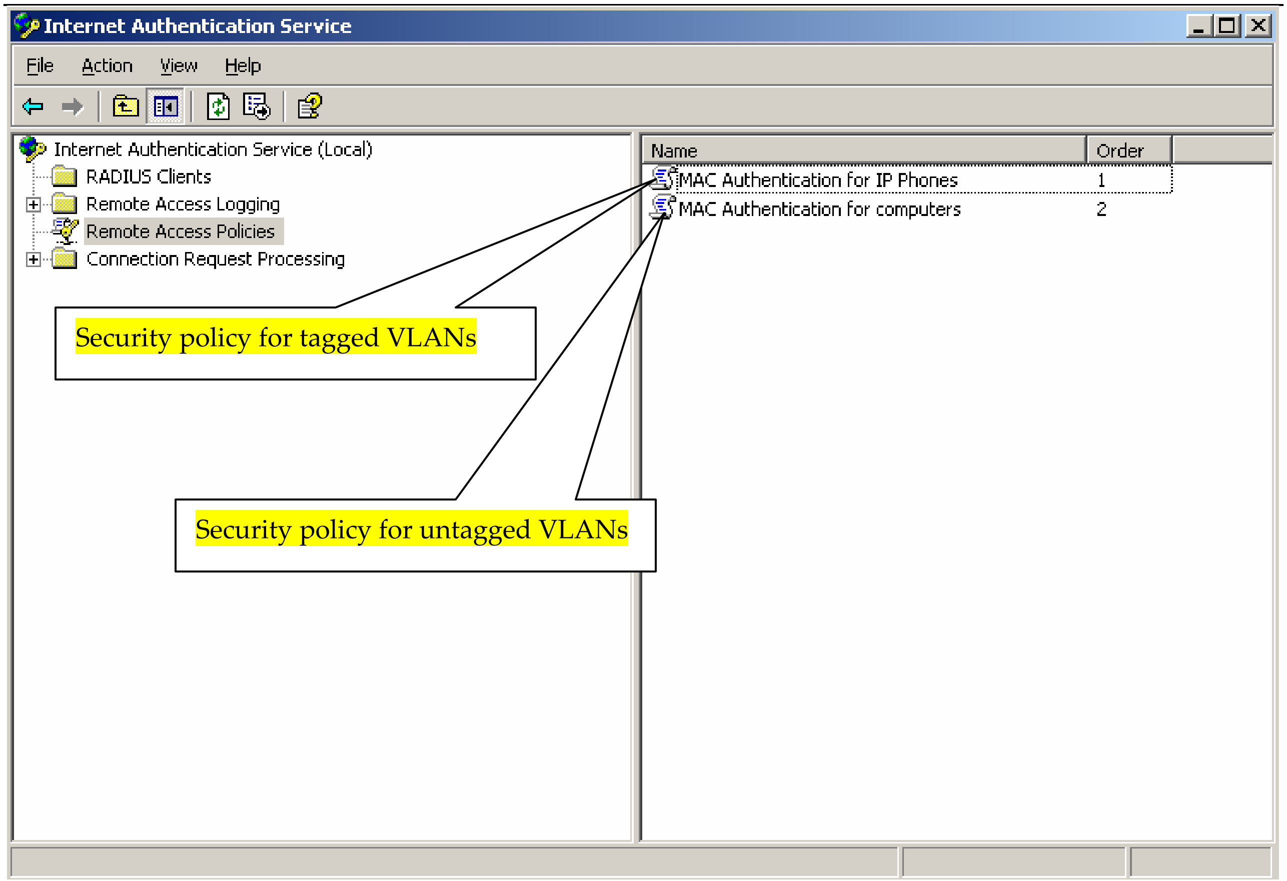
Devices matching this security policy are tagged with VLAN ID 10

48. Steps 34 through 47 creates a security policy named “MAC Authentication for IP Phones”, and sets it in the right hand container of Internet Authentication Services pane. This policy matches the following conditions:
    a. Users that are in the “Test\IP Phones” Windows group only.

    This policy also sends the following information to the Foundry switch.
    i. Attribute number 64 which specifies that user must belong to a Virtual LAN.
    ii. Attribute number 65 which specifies that user port must be tagged with the IEEE 802.1Q format.
    iii. Attribute number 81 which identifies the unique VLAN ID for the user group.

    .

49. You should now have two unique security policies that IAS uses to match and authenticate devices.

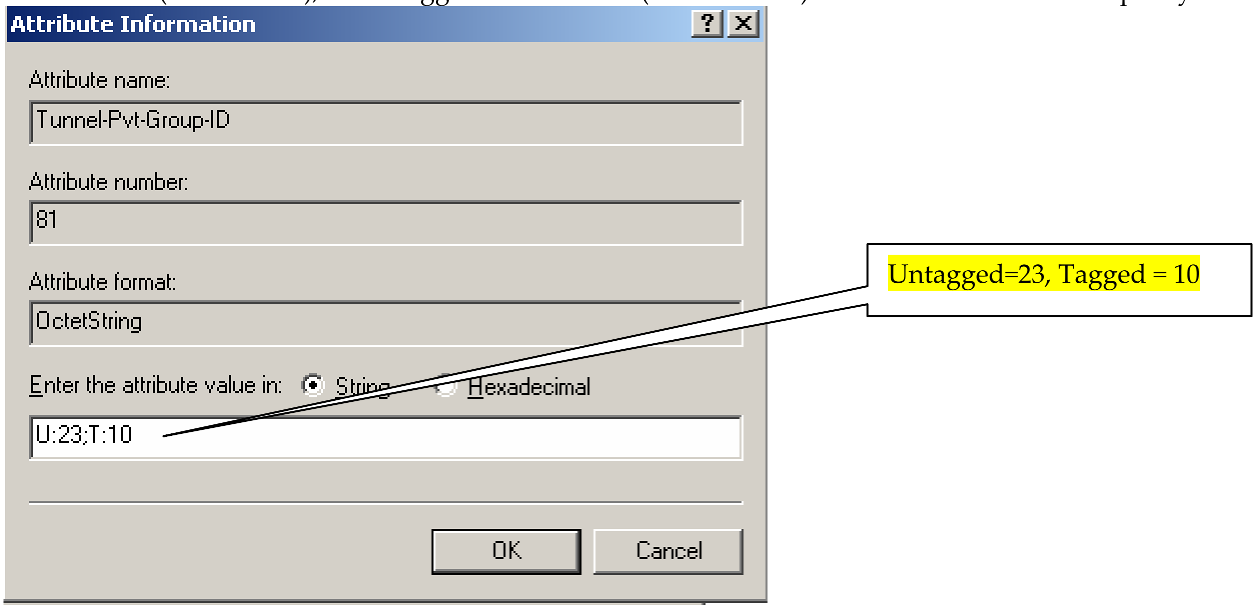

Internet Authentication Service
File
Action
View
Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing

Name	Order
MAC Authentication for IP Phones	1
MAC Authentication for computers	2

Security policy for tagged VLANs

Security policy for untagged VLANs

You can add a third remote access policy to handle cases where you need to have two VLANs, such as a Voice VLAN and a data VLAN (one with an IEEE 802.1Q tag, and one without a tag), assigned to the same switch port. You must enter the string "U:23;T:10" in the Attribute information field to assign an untagged VLAN ID 23 (data VLAN), and a tagged VLAN ID 10 (Voice VLAN) within the Remote access policy.



Attribute name:
Tunnel-Pvt-Group-ID

Attribute number:
81

Attribute format:
OctetString

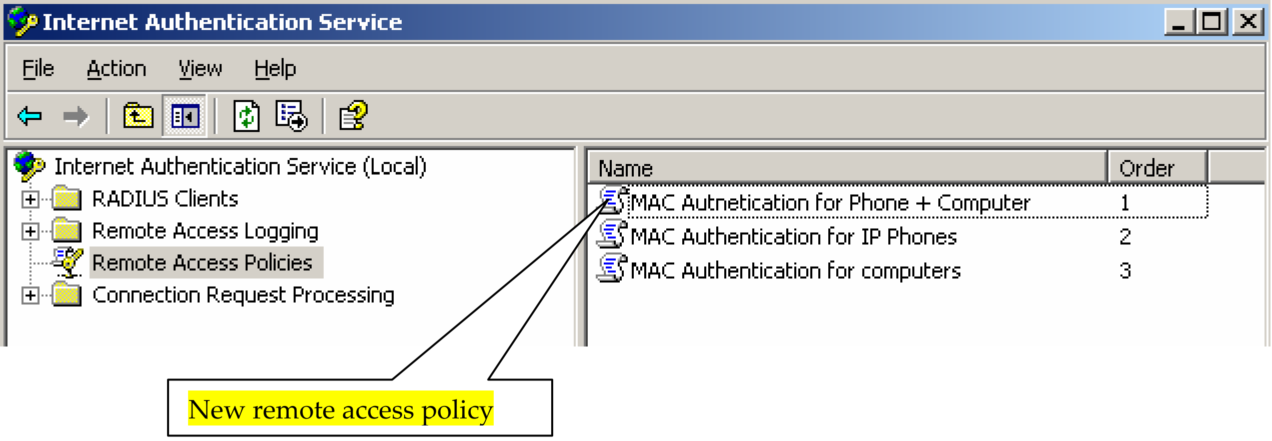
Enter the attribute value in: ● String ○ Hexadecimal

U:23;T:10

Untagged=23, Tagged = 10

Foundrv Security Best Practices

The remote access policy shown below is similar to the two polices that was created before, the only difference is that the Tunnel-Pvt-Group-ID field is modified to assign two VLAN IDs (one for the Voice VLAN and one for the data VLAN) upon successful authentication of MAC address of the IP Phone or the Computer.



Internet Authentication Service (Local)
- RADIUS Clients
- Remote Access Logging
- Remote Access Policies
- Connection Request Processing

Name	Order
MAC Autnetication for Phone + Computer	1
MAC Authentication for IP Phones	2
MAC Authentication for computers	3

New remote access policy

The key to the process that IAS uses to authenticate users is that it analyzes the RADIUS request against the available rules sequentially. The processing of these rules only continues until a match is found.

1.6 Setting up the Foundry Configurations (Switches and Routers)

1. The following command will enable MAC authentication globally (Required).

   ```
   mac-authentication enable
   ```

   The following command will enable mac authentication per interface (Required)

   ```
   interface ethernet [interface-number]
    mac-authentication enable
   ```

   The following command will assign the port to a dynamic MAC address based VLAN

   ```
   interface ethernet [interface-number]
    mac-authentication enable-dynamic-vlan
   ```

2. Setup the RADIUS server configuration on the equipment (Required).

   ```
   radius-server host [ip-address]
   radius-server key 0 [radius-secret]
   ```

3. Assign a IP address to the device (Required):

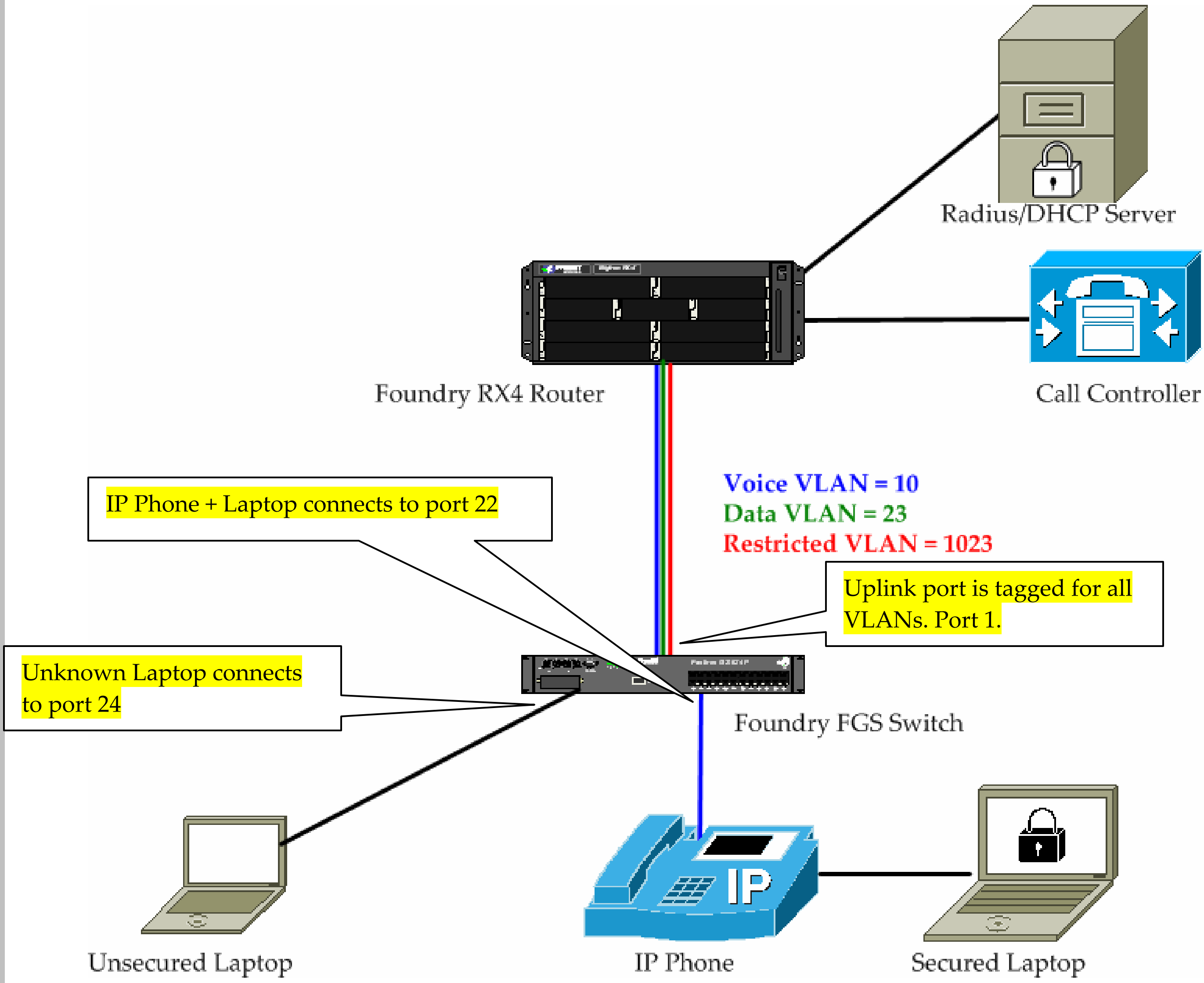
   ```
   ip address [ip-address] [netmask]
   ip default-gateway [ip-address]
   ```

Appendix A

a. Multidevice MAC authentication with restricted VLANs

The following example illustrates a configuration where an IP Phone and a laptop that is attached to the switch port of the IP Phone get authenticated via the radius server. The IP Phone is placed in to a Voice VLAN (VLAN 10), and the laptop computer is placed in to the data VLAN (VLAN 23).

Also an unknown Laptop computer that does not have an Active Directory account is placed in the restricted VLAN (VLAN 1023).



b. Switch configuration

```
FGS624P Switch#show run
Current configuration:
!
ver 02.4.00aT7e1
!
!
no global-stp
!
!
vlan 1 name DEFAULT-VLAN by port
 no spanning-tree
!
vlan 23 name data by port
 tagged ethe 1
 no spanning-tree
!
vlan 10 name voice by port
 tagged ethe 1 ethe 22
 no spanning-tree
!
vlan 1023 name restrict by port
 tagged ethe 1
 no spanning-tree
!
!
!
!
!
ip address 192.168.1.2 255.255.255.0
ip default-gateway 192.168.1.1
logging console
radius-server host 192.168.1.3
radius-server key 0 test
cdp run
fdp run
mac-authentication enable
mac-authentication save-dynamicvlan-to-config
mac-authentication auth-fail-vlan-id 1023

interface ethernet 13
 mac-authentication enable
!
interface ethernet 14
 mac-authentication enable
!
interface ethernet 15
 mac-authentication enable
!
interface ethernet 16
 mac-authentication enable
!
interface ethernet 17
```

```
 mac-authentication enable
!
interface ethernet 18
 mac-authentication enable
 inline power
!
interface ethernet 19
 mac-authentication enable
!
interface ethernet 20
 mac-authentication enable
!
interface ethernet 21
 mac-authentication enable
!
interface ethernet 22
 dual-mode
 mac-authentication enable
 mac-authentication enable-dynamic-vlan
 inline power
 voice-vlan 10
!
interface ethernet 23
 mac-authentication enable
 mac-authentication enable-dynamic-vlan
 inline power
!
interface ethernet 24
 mac-authentication enable
 mac-authentication enable-dynamic-vlan
 mac-authentication auth-fail-action restrict-vlan
 inline power
!
!
!
!
!
end
```

c. MAC Authentication Process.

```
FGS624P Switch#
SYSLOG: <14>Jan  1 00:00:00 192.168.1.2 System: Interface ethernet 22, state up

SYSLOG: <14>Jan  1 00:00:00 192.168.1.ated power of 15400 mwatts on port 22.
PoE: Power enabled on port 22.

SYSLOG: <14>Jan  1 00:00:00 192.168.1.2 System: PoE: Power enabled on port 22.

SYSLOG: <14>Jan  1 00:00:00 192.168.1.2 System: PoE: Power adjustment done:
decreased power by 9100 mwatts on port 22 .

SYSLOG: <13>Jan  1 00:00:00 192.168.1.2 MAC Authentication succeeded for
[000d.bcd8.2402 ] on port 22
```

IP Phone MAC address

```
SYSLOG: <13>Jan  1 00:00:00 192.168.1.2 MAC Authentication: port 22 default
vlan-id changes to 23

SYSLOG: <13>Jan  1 00:00:00 192.168.1.2 MAC Authentication succeeded for
[0011.2582.5efa ] on port 22
```

Laptop MAC address

```
SYSLOG: <13>Jan  1 00:00:00 192.168.1.2 MAC Authentication succeeded for
[000d.bcd8.2402 ] on port 22

SYSLOG: <14>Jan  1 00:00:00 192.168.1.2 System: Interface ethernet 24, state up

SYSLOG: <13>Jan  1 00:00:00 192.168.1.2 MAC Authentication: port 24 default
vlan-id changes to 1023

SYSLOG: <9>Jan  1 00:00:00 192.168.1.2 MAC Authentication failed for
[0004.0d27.c34e ] on port 24 (Invalid User)
```

Unknown MAC address

```
FGS624P Switch#show mac
Total active entries from all ports = 11
MAC-Address     Port         Type        Index       VLAN
0004.80a0.4000  1            Dynamic     16252       10
0004.0d05.c870  1            Dynamic     1484        10
0004.0d02.2a1c  1            Dynamic     4944        10
0004.0d92.44ae  1            Dynamic     14184       10
0004.0d02.44ae  1            Dynamic     4940        10
0004.0d4d.66d6  23           Dynamic     3084        10
0004.0d27.c34e  24           Dynamic     12592       1023
0014.2208.f455  1            Dynamic     1808        10
000d.bcd8.2402  22           Dynamic     3764        10
0011.2582.5efa  22           Dynamic     10976       23
0004.80a0.4000  1            Dynamic     15412       23

FGS624P Switch#show run

......................................
......................................

interface ethernet 22
 dual-mode  23
 mac-authentication enable
 mac-authentication enable-dynamic-vlan
 inline power
 voice-vlan 10

......................................
......................................
```

VLAN ID changed to 23