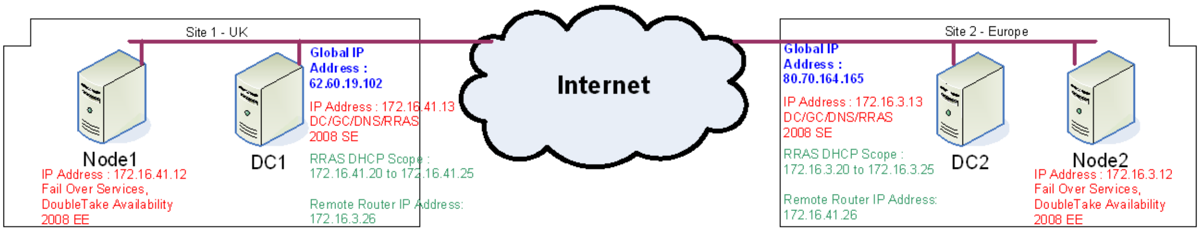
Expanding AD Domain Services into the cloud and across multiple sites

How to establish inter-site link via Windows 2008 Routing and Remote Access and expand AD into the cloud

This guide provides an introduction to the process for connecting two sites (with different subnets) via Windows 2008 Routing and Remote Access feature, so that an additional Domain Controller (DC) can be deployed at the site. It does not provide details on Active Directory design, or detailed instructions for deploying the DC, but does document the steps taken to establish networking links between two sites, which will be sufficient for the deployment to take place. Caution: This document should not be treated as a fully validated or documented solution, but as an aid in your design and validation process for connecting your existing domain to your cloud environment.

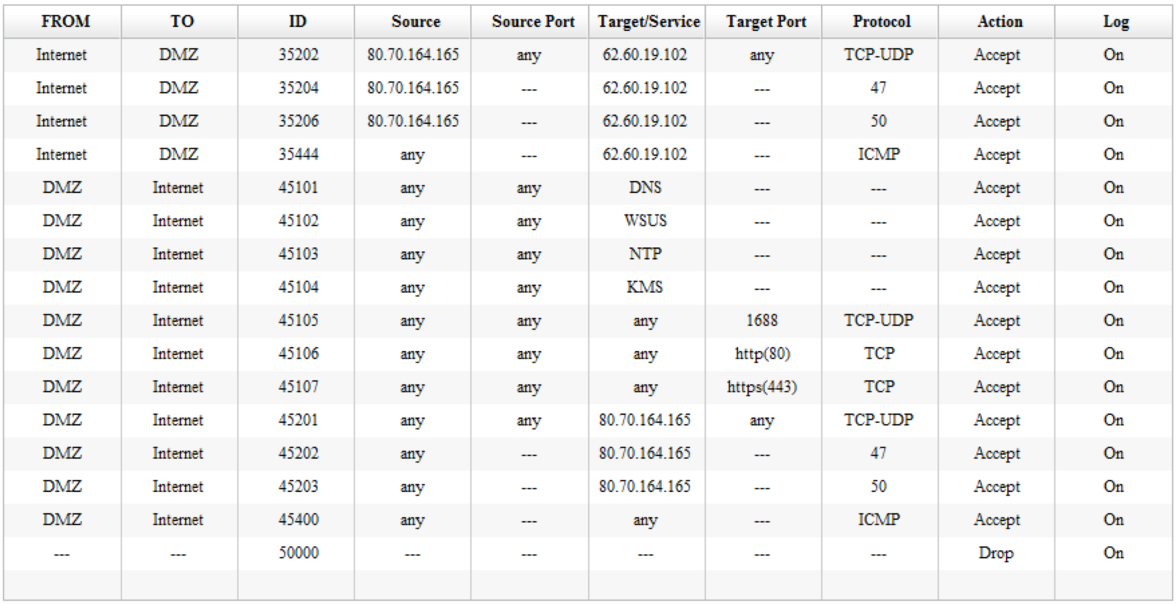
The diagram below shows an example scenario and summaries the Services and IP addresses used when preparing this document:


Site 1 - UK
Node1
IP Address : 172.16.41.12
Fail Over Services,
DoubleTake Availability
2008 EE
DC1
Global IP Address : 62.60.19.102
IP Address : 172.16.41.13
DC/GC/DNS/RRAS
2008 SE
RRAS DHCP Scope : 172.16.41.20 to 172.16.41.25
Remote Router IP Address: 172.16.3.26
Internet
Site 2 - Europe
Global IP Address : 80.70.164.165
IP Address : 172.16.3.13
DC/GC/DNS/RRAS
2008 SE
RRAS DHCP Scope : 172.16.3.20 to 172.16.3.25
Remote Router IP Address: 172.16.41.26
DC2
Node2
IP Address : 172.16.3.12
Fail Over Services,
DoubleTake Availability
2008 EE

In order to connect two remote sites over the Internet, the ‘Routing and Remote Access’ role needs to be added to a server within each site. This could be a separate server if required but this guide assumes that the server that will act as the Domain Controller, will also perform this role.

Before beginning, AD should be installed or pre exist within one of the sites. The site can then be connected using the following instructions, with additional domain controllers deployed at the secondary site.

Firewalls should also be configured between sites to allow all required communications. As AD and other applications could potentially communicate over many ports, it is recommended to open all TCP/UDP ports between sites, but specify the Global IP address in the rules for the allowed source/target IP addresses. Rules to allow Protocols 47, 50 both ways, between both sites, must also be specified.

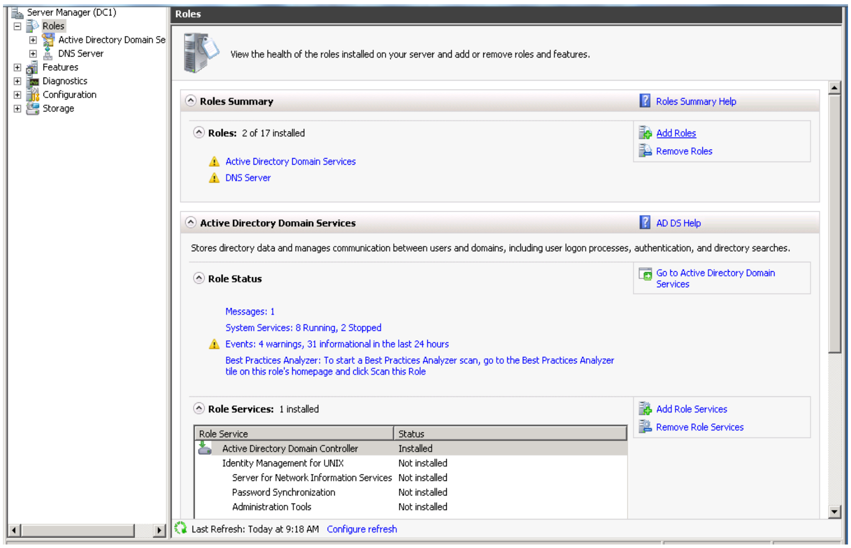


FROM	TO	ID	Source	Source Port	Target/Service	Target Port	Protocol	Action	Log
Internet	DMZ	35202	80.70.164.165	any	62.60.19.102	any	TCP-UDP	Accept	On
Internet	DMZ	35204	80.70.164.165	---	62.60.19.102	---	47	Accept	On
Internet	DMZ	35206	80.70.164.165	---	62.60.19.102	---	50	Accept	On
Internet	DMZ	35444	any	---	62.60.19.102	---	ICMP	Accept	On
DMZ	Internet	45101	any	any	DNS	---	---	Accept	On
DMZ	Internet	45102	any	any	WSUS	---	---	Accept	On
DMZ	Internet	45103	any	any	NTP	---	---	Accept	On
DMZ	Internet	45104	any	any	KMS	---	---	Accept	On
DMZ	Internet	45105	any	any	any	1688	TCP-UDP	Accept	On
DMZ	Internet	45106	any	any	any	http(80)	TCP	Accept	On
DMZ	Internet	45107	any	any	any	https(443)	TCP	Accept	On
DMZ	Internet	45201	any	any	80.70.164.165	any	TCP-UDP	Accept	On
DMZ	Internet	45202	any	---	80.70.164.165	---	47	Accept	On
DMZ	Internet	45203	any	---	80.70.164.165	---	50	Accept	On
DMZ	Internet	45400	any	---	any	---	ICMP	Accept	On
---	---	50000	---	---	---	---	---	Drop	On

Install RRAS Role

Repeat the following steps on each RRAS server (e.g. DC):

1. Open Server Manager
2. Expand ‘Server Manager | Roles’ and click ‘Add Roles’



View the health of the roles installed on your server and add or remove roles and features.

Roles Summary Roles Summary Help

Roles: 2 of 17 installed

- Active Directory Domain Services
- DNS Server

Add Roles
Remove Roles

Active Directory Domain Services AD DS Help

Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

Role Status

Go to Active Directory Domain Services

Messages: 1
System Services: 8 Running, 2 Stopped
Events: 4 warnings, 31 informational in the last 24 hours
Best Practices Analyzer: To start a Best Practices Analyzer scan, go to the Best Practices Analyzer tile on this role's homepage and click Scan this Role

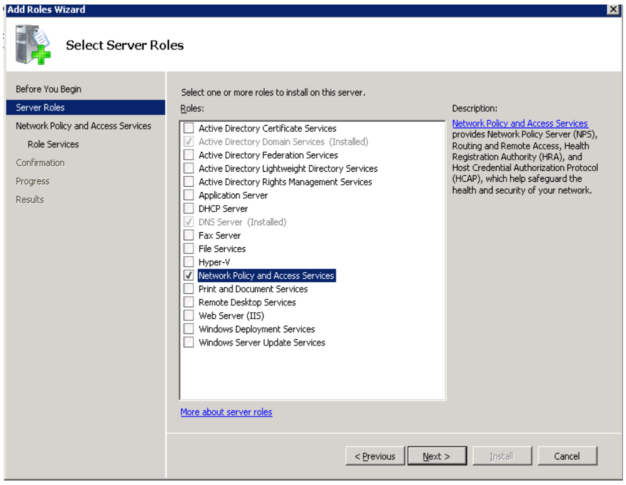
Role Services: 1 installed

Add Role Services
Remove Role Services

Role Service	Status
Active Directory Domain Controller	Installed
Identity Management for UNIX	Not installed
Server for Network Information Services	Not installed
Password Synchronization	Not installed
Administration Tools	Not installed

Last Refresh: Today at 9:18 AM Configure refresh

3. Tick 'Network Policy and Access Services' and click 'Next'



Select Server Roles

Select one or more roles to install on this server.

Roles:

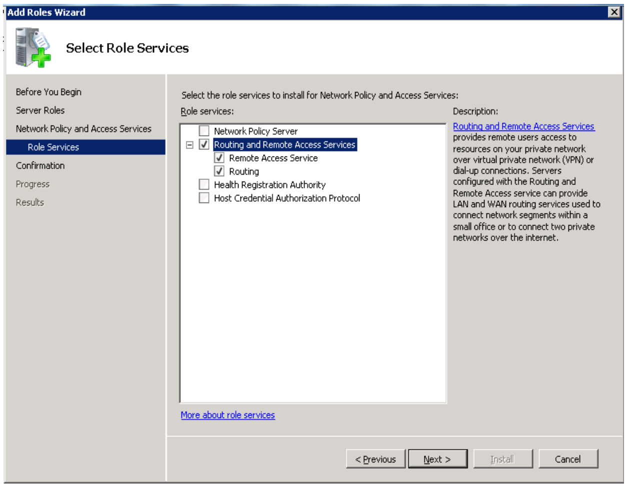
- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- ☑ DNS Server (Installed)
- □ Fax Server
- □ File Services
- □ Hyper-V
- ☑ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Desktop Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

More about server roles

Description:

Network Policy and Access Services provides Network Policy Server (NPS), Routing and Remote Access, Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP), which help safeguard the health and security of your network.

4. On the following screen, click 'Next'
5. Tick 'Routing and Remote Access Services' including the two sub options and click 'Next'.



Select Role Services

Select the role services to install for Network Policy and Access Services:

Role services:

- □ Network Policy Server
- ☑ Routing and Remote Access Services
  - ☑ Remote Access Service
  - ☑ Routing
- □ Health Registration Authority
- □ Host Credential Authorization Protocol

More about role services

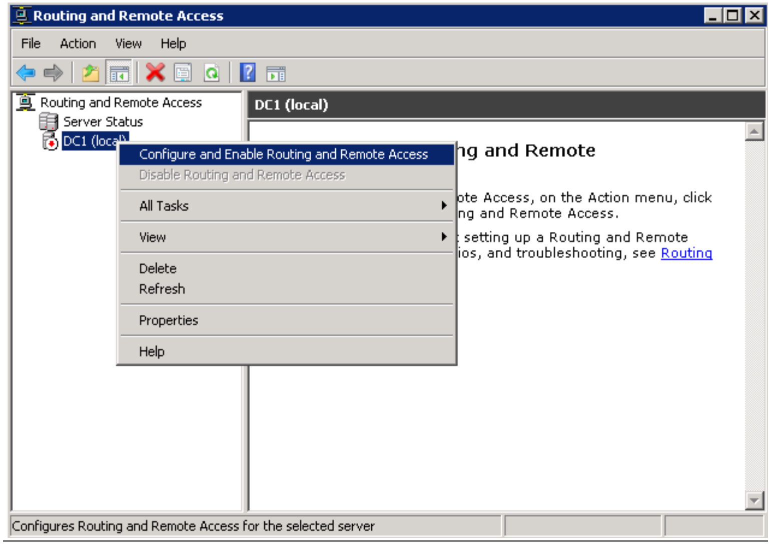
Description:

Routing and Remote Access Services provides remote users access to resources on your private network over virtual private network (VPN) or dial-up connections. Servers configured with the Routing and Remote Access service can provide LAN and WAN routing services used to connect network segments within a small office or to connect two private networks over the internet.

6. Click 'Install' on next screen
7. When complete, click 'Close'.

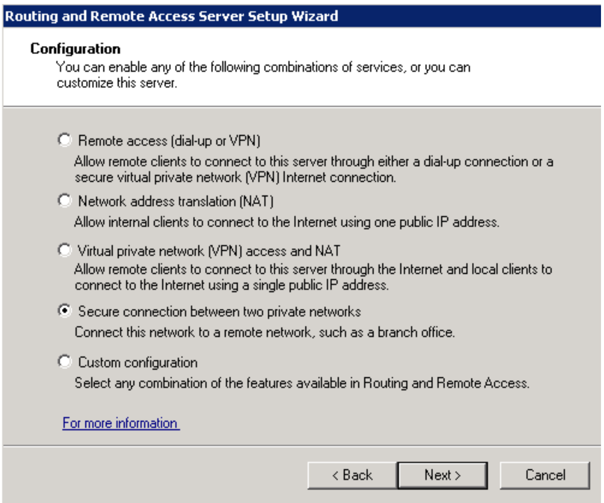
Configure 'Secure Connection between two private networks'

1. Select 'Start | Administrative Tools | Routing and Remote Access'
2. Right click on server name and select 'Configure and Enable Routing and Remote Access'


Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
DC1 (local)
DC1 (local)
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
All Tasks
View
Delete
Refresh
Properties
Help
ng and Remote
ote Access, on the Action menu, click
ng and Remote Access.
setting up a Routing and Remote
ios, and troubleshooting, see Routing

Configures Routing and Remote Access for the selected server

3. On the resulting wizard 'Welcome Screen' click 'Next'
4. Select 'Secure connection between two private networks' and click 'Next'



Configuration

You can enable any of the following combinations of services, or you can customize this server.

○ Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.

○ Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.

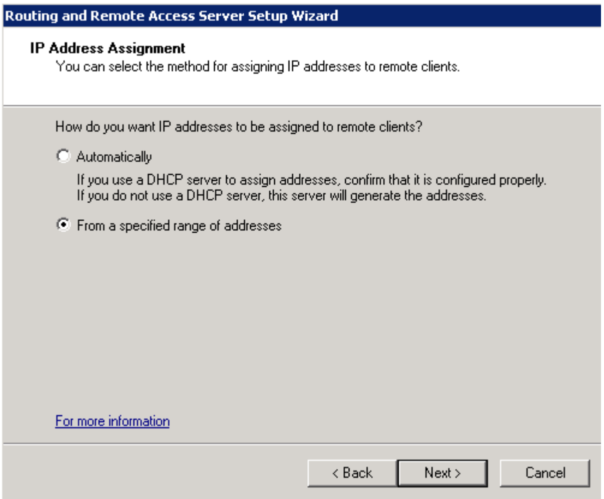
○ Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.

● Secure connection between two private networks
Connect this network to a remote network, such as a branch office.

○ Custom configuration
Select any combination of the features available in Routing and Remote Access.

For more information

5. Accept the default option of 'Yes' to used Demand –dial connection and click 'Next'



IP Address Assignment

You can select the method for assigning IP addresses to remote clients.

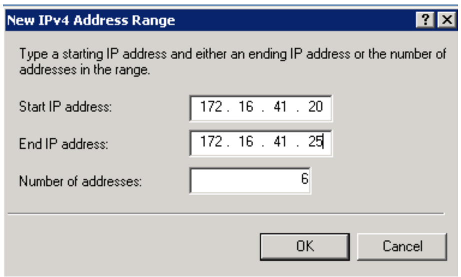
How do you want IP addresses to be assigned to remote clients?

○ Automatically
If you use a DHCP server to assign addresses, confirm that it is configured properly. If you do not use a DHCP server, this server will generate the addresses.

● From a specified range of addresses

For more information

6. On IP Address Assignment Screen, select 'From a specified range of addresses' radio button and click 'Next'
7. On 'Address Range Assignment' screen click 'New'
8. Enter an IP address in the range of the local subnet, but far away enough from the range to be allocated to DHCP (if performing this on a FGCP VM). Then click 'Ok', 'Next' and 'Finish'



New IPv4 Address Range

Type a starting IP address and either an ending IP address or the number of addresses in the range.

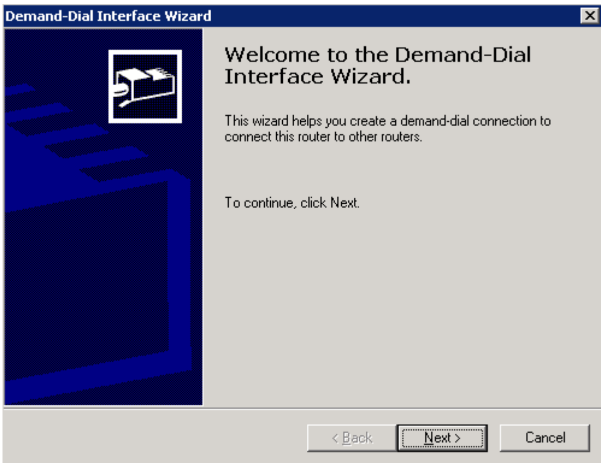
Start IP address: 172 . 16 . 41 . 20

End IP address: 172 . 16 . 41 . 25

Number of addresses: 6

Next, the Demand-Dial Interface Wizard automatically appears

1. Click 'Next' on the Welcome Screen



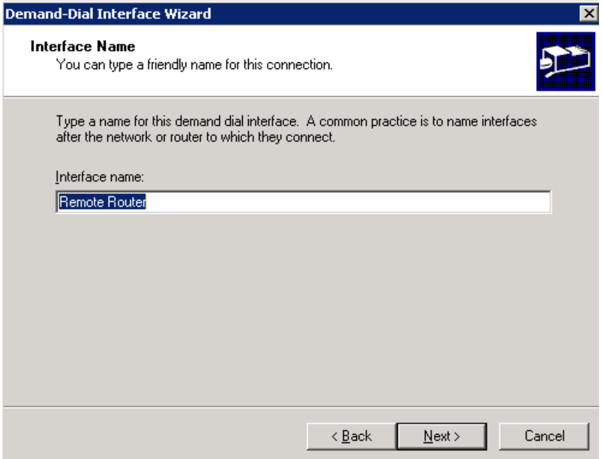
Demand-Dial Interface Wizard

Welcome to the Demand-Dial Interface Wizard.

This wizard helps you create a demand-dial connection to connect this router to other routers.

To continue, click Next.

2. On the Interface Name screen, accept the default of 'Remote Router' and click 'Next'. If you change this, make sure you use the same value on the configuration of the other site.



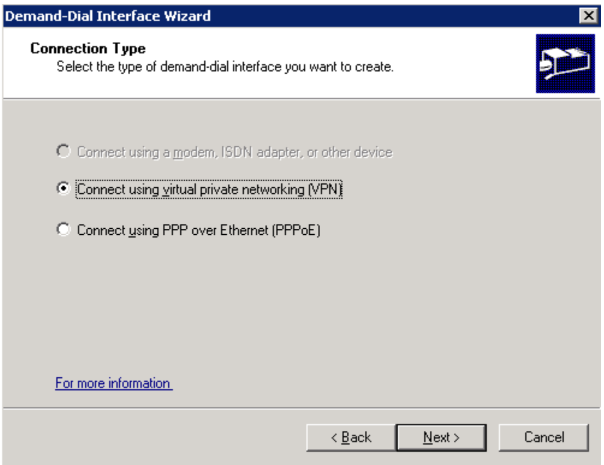
Demand-Dial Interface Wizard

Interface Name
You can type a friendly name for this connection.

Type a name for this demand dial interface. A common practice is to name interfaces after the network or router to which they connect.

Interface name: Remote Router

3. Accept the default option of VPN on Connection Type screen and click 'Next'



Demand-Dial Interface Wizard

Connection Type
Select the type of demand-dial interface you want to create.

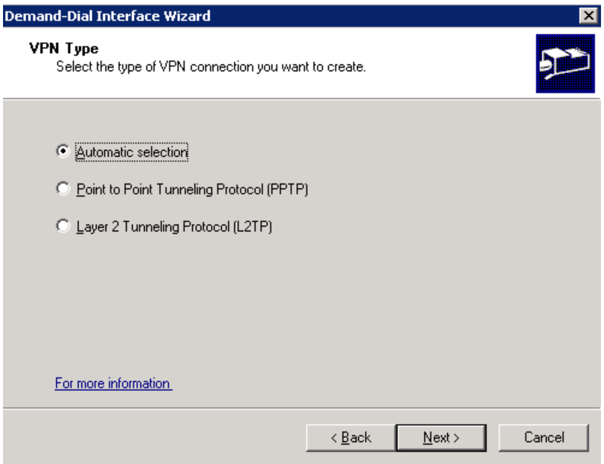
○ Connect using a modem, ISDN adapter, or other device

● Connect using virtual private networking (VPN)

○ Connect using PPP over Ethernet (PPPoE)

For more information

4. Accept default VPN Type of 'Automatic Selection' and click 'Next'



Demand-Dial Interface Wizard

VPN Type
Select the type of VPN connection you want to create.

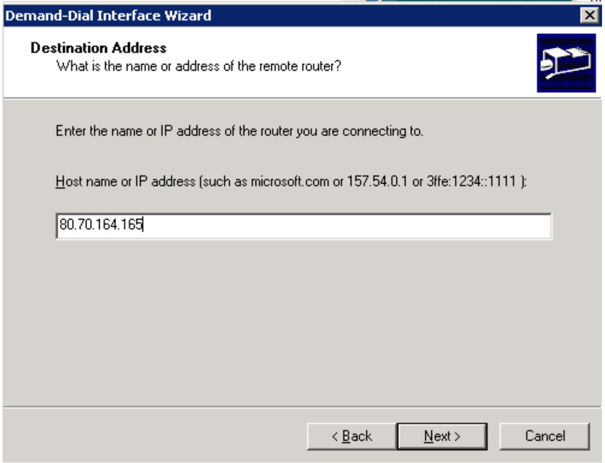
● Automatic selection

○ Point to Point Tunneling Protocol (PPTP)

○ Layer 2 Tunneling Protocol (L2TP)

For more information

5. Enter the Destination Global IP Address of the RRAS server at the second site and click ‘Next’



Demand-Dial Interface Wizard

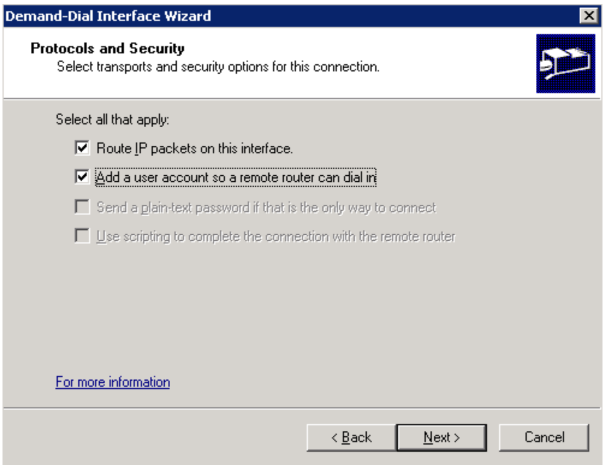
Destination Address
What is the name or address of the remote router?

Enter the name or IP address of the router you are connecting to.

Host name or IP address (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111):

80.70.164.165

6. Ensure both ‘Route IP Packets…’ and ‘Add a user account…’ boxes are ticked and click ‘Next’



Demand-Dial Interface Wizard

Protocols and Security
Select transports and security options for this connection.

Select all that apply:

☑ Route IP packets on this interface.

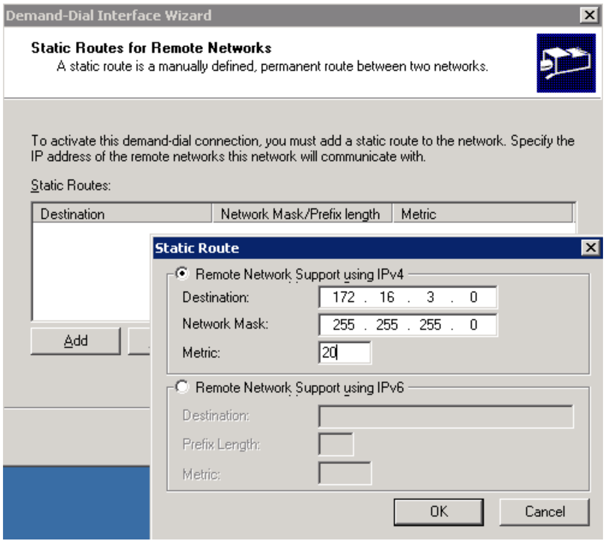
☑ Add a user account so a remote router can dial in

☐ Send a plain-text password if that is the only way to connect

☐ Use scripting to complete the connection with the remote router

For more information

7. On ‘Static Routes for Remote Network’ screen, click ‘Add’



Demand-Dial Interface Wizard

Static Routes for Remote Networks
A static route is a manually defined, permanent route between two networks.

To activate this demand-dial connection, you must add a static route to the network. Specify the IP address of the remote networks this network will communicate with.

Static Routes:

Destination	Network Mask/Prefix length	Metric

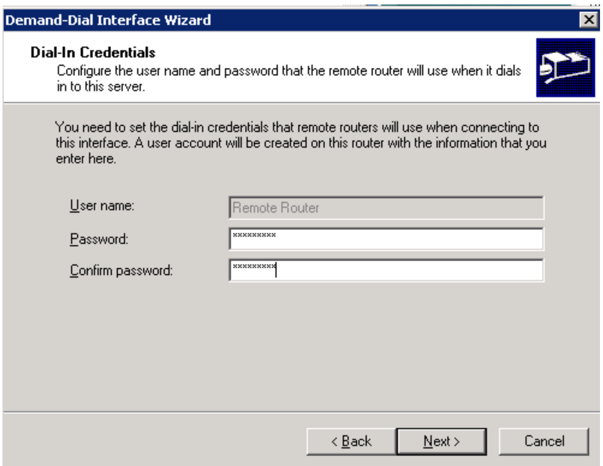
Static Route

● Remote Network Support using IPv4
Destination: 172 . 16 . 3 . 0
Network Mask: 255 . 255 . 255 . 0
Metric: 20

○ Remote Network Support using IPv6
Destination:
Prefix Length:
Metric:

Specify the subnet of the destination site, and a Metric value e.g. 20, click 'OK' and then 'Next'

8. Enter a password for the dial-in credentials and click 'Next'. Note the same password should be used when configuring this on both sites.



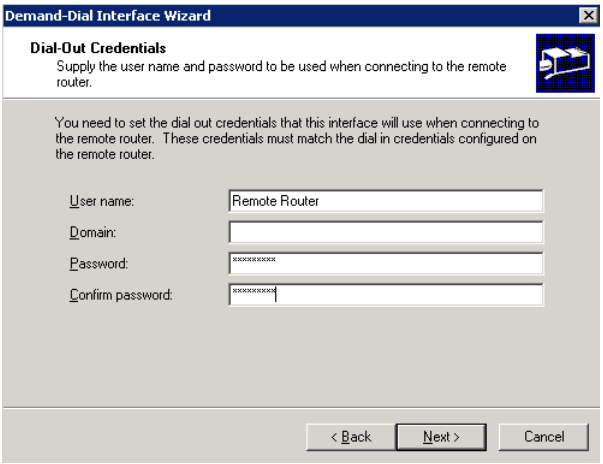
Demand-Dial Interface Wizard

Dial-In Credentials
Configure the user name and password that the remote router will use when it dials in to this server.

You need to set the dial-in credentials that remote routers will use when connecting to this interface. A user account will be created on this router with the information that you enter here.

User name: Remote Router
Password: *********
Confirm password: *********

9. For Dial-Out Credentials, use the same account and password as for the dial-in credentials. (Recommend using first letter capitals as per default account)



Demand-Dial Interface Wizard

Dial-Out Credentials
Supply the user name and password to be used when connecting to the remote router.

You need to set the dial out credentials that this interface will use when connecting to the remote router. These credentials must match the dial in credentials configured on the remote router.

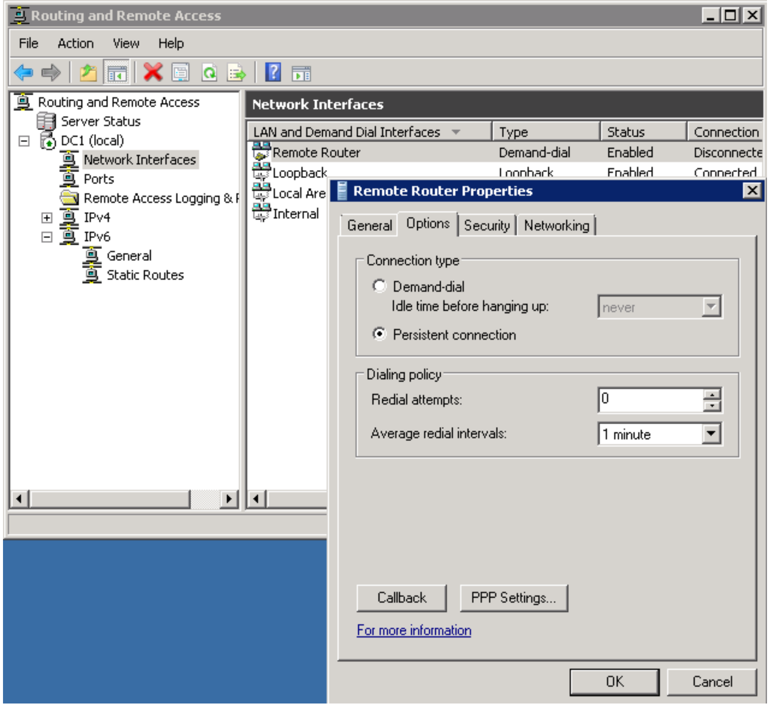
User name: Remote Router
Domain:
Password: *********
Confirm password: *********

Click 'Next' and then 'Finish'

When a demand dial connection is setup between two 2008 RRAS servers each server receives an address from the pool of available addresses located on the server it is connecting to. By default though, both servers will not be able to PING or as the RRAS server needs a host route adding to its local routing table.

1. Within 'Routing and Remote Access', expand 'Routing and Remote Access | <ServerName> | Network Interface'.

2. Right click on 'Remote Router' and select properties.
3. On the Options tab, select 'Persistent Connection



LAN and Demand Dial Interfaces	Type	Status	Connection
Remote Router	Demand-dial	Enabled	Disconnecte
Loopback	Loopback	Enabled	Connected
Local Are			
Internal			

Remote Router Properties

General | Options | Security | Networking

Connection type

○ Demand-dial

Idle time before hanging up: never

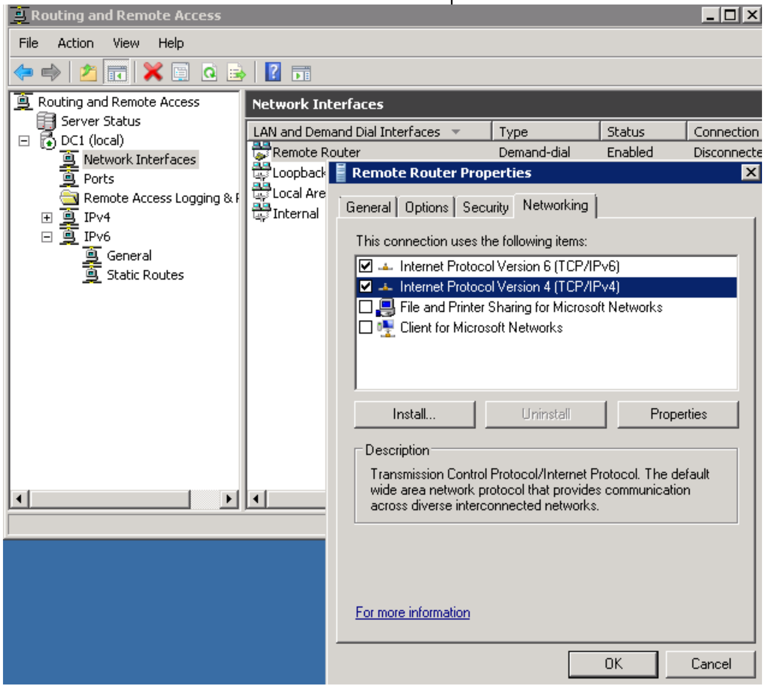
● Persistent connection

Dialing policy

Redial attempts: 0

Average redial intervals: 1 minute

4. Select the 'Networking' tab, then 'Internet Protocol Version4…' and click 'Properties'.



LAN and Demand Dial Interfaces	Type	Status	Connection
Remote Router	Demand-dial	Enabled	Disconnecte
Loopback			
Local Are			
Internal			

Remote Router Properties

General | Options | Security | Networking

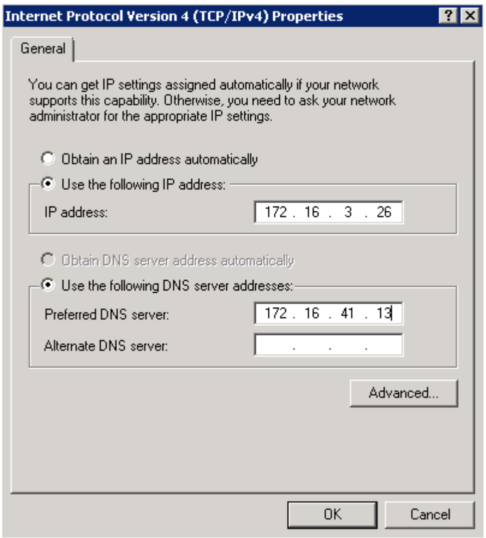
This connection uses the following items:

☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☐ File and Printer Sharing for Microsoft Networks
☐ Client for Microsoft Networks

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

5. Select 'Use the following IP address' and specify an IP address that is not in use from the other site. E.g. 172.16.3.26. This is required for this workaround to succeed.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 172 . 16 . 3 . 26

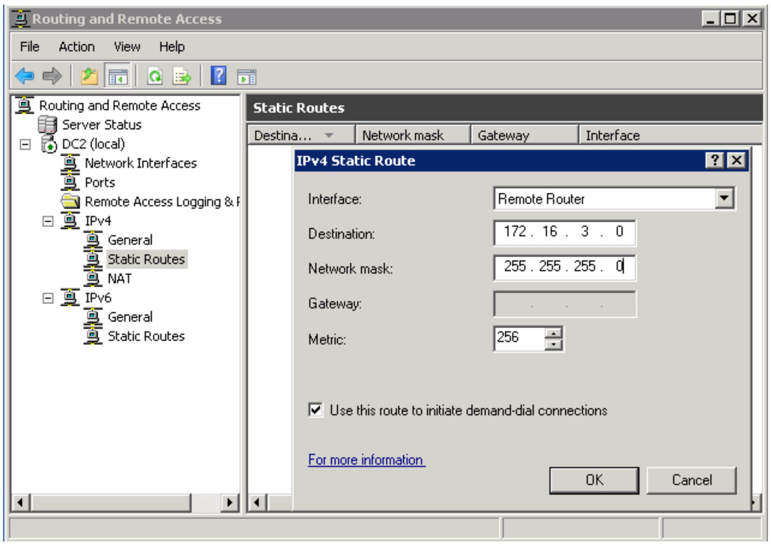
○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 172 . 16 . 41 . 13
Alternate DNS server: . . .

Also set the 'Preferred DNS server' to the IP address of the DC/DNS server in the local site. E.g. 172.16.41.13. Then click 'Ok', 'Ok'

Add Static IP Address

Perform the following on each RRAS Server:

1. Expand '<servername> | IPv4 ' and right click on 'Static Router' and select 'New Static Route'
2. Under Interface, select 'Remote Router' and specify the subnet of the target site and network mask.



IPv4 Static Route

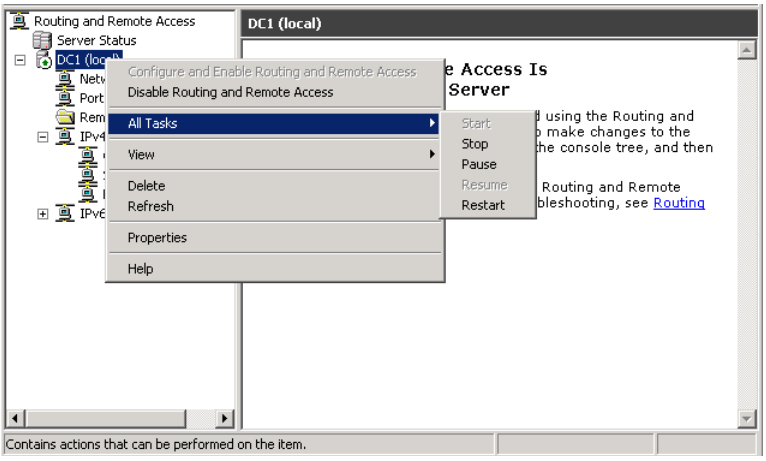
Interface: Remote Router
Destination: 172 . 16 . 3 . 0
Network mask: 255 . 255 . 255 . 0
Gateway: . . .
Metric: 256

☑ Use this route to initiate demand-dial connections

3. Click 'Ok' to complete

Restart RRAS

1. Right click on <ServerName>, select 'All tasks | Restart'



Configure Network Routing on RRAS Servers

Routing needs to be configured between both RRAS servers to be able to communicate and also on all other servers/clients at each site, to redirect traffic for the other subnet to the RRAS server.
On each RRAS server, open a command prompt with administrative permissions and enter the following commands.

Route Add -p <Static IP of target RRAS Server> address of mask 255.255.255.255 <Static IP of source RRAS Server>

Route Add -p <Static IP of source RRAS Server> address of mask 255.255.255.255 <Static IP of target RRAS Server>

e.g.
Route Add -p 172.16.3.26 mask 255.255.255.255 172.16.41.26
Route Add -p 172.16.41.26 mask 255.255.255.255 172.16.3.26

Configure Network Routing on other Servers to use RRAS

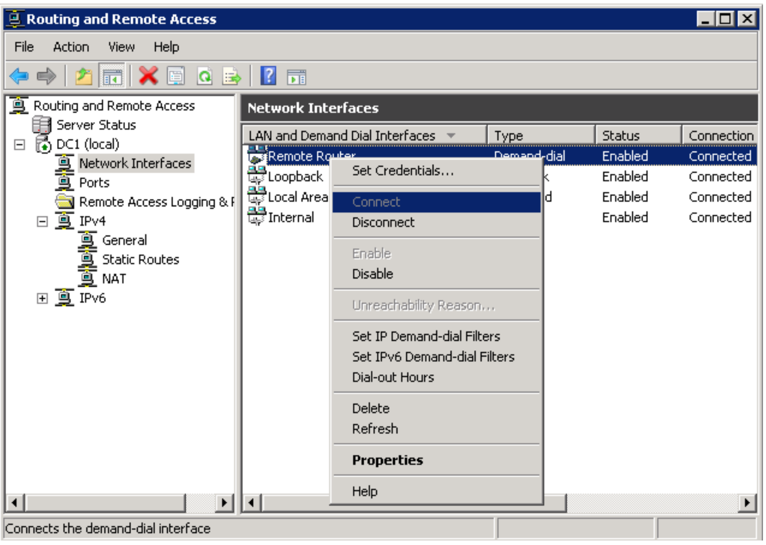
1. On each server to use RRAS, open a command prompt with administrative permissions and enter the following commands.
   Route Print
2. In the resulting text, under 'Interface List' locate the primary network adapter name. E.g. on FGCP VMs this is 'Virtual Network Driver for X64'. Next make a note of the Interface number for this entry e.g. 10

   Note: See KB2161341 for information on why this is important if Clustering is to be installed.

3. Next enter the following command
   Route Add -p <Subnet of target RRAS Server> address of mask 255.255.255.0 <Public IP address of RRAS Server> if <interface number from above>
   e.g.
   Route Add -p 172.16.3.0 mask 255.255.255.0 172.16.41.13 IF 10
   Or
   Route Add -p 172.16.41.0 mask 255.255.255.0 172.16.3.13

Establish the Connection

Expand '<Server name > | Network Interfaces' and right click on 'Remote Router' on the right hand pane and select 'Connect'



It may take a little troubleshooting to get the connection to connect, but if it doesn't start first time try the following.

1. Make sure both nodes in the connection are currently logged on. (It seems that the connection will not be made unless both servers are logged on. Currently rdping to 2nd dc from 1st, logging in and selecting connect. Needs further investigation)
2. Check the Event Viewer on each server for any related events
3. Can you ping the global address of the other node, from the node your on (make sure firewalls allow this)
4. Try restarting both nodes

Deploying an Additional Domain Controller into the new Site.

The above procedure should be sufficient to allow the DC server at the secondary site to join the domain and be promoted to a Global Catalogue Domain Controller.

The detailed steps to do this are outside the scope of this document, but in principal:

1. Ensure the Servers DNS entries, include the IP address of a DNS server in Site1
2. If included as part of your AD Design, ensure a new site exists in AD Sites and Services for the subnet of the new site.
3. Join the Server to the domain and reboot
4. Login to the server with a domain administrator account and enter the command DCPROMO for a cmd prompt
5. Follow the wizard, choosing to join an existing domain, in the new site and include the Global Catalogue server and DNS roles on the current server.
6. Following reboot, log back in as domain administrator and ensure the server has an entry in its DNS list for itself.
7. Ensure DNS is replicating between both sites and both forward and reverse lookup zones exist for the domain.
8. Ensure AD replication is taking place between both sites

Contact

Fujitsu Global Cloud Team
FUJITSU
E-mail: cloud_gsd@au.fujitsu.com
Website: au.fujitsu.com