Cisco Virtual Office: Dial Backup Deployment Guide

Introduction

This deployment guide provides detailed design and implementation information for deployment of Dial Backup with the Cisco® Virtual Office. Please refer to the Cisco Virtual Office overview (http://www.cisco.com/go/cvo) for further information about the solution, its architecture, and all of its components.

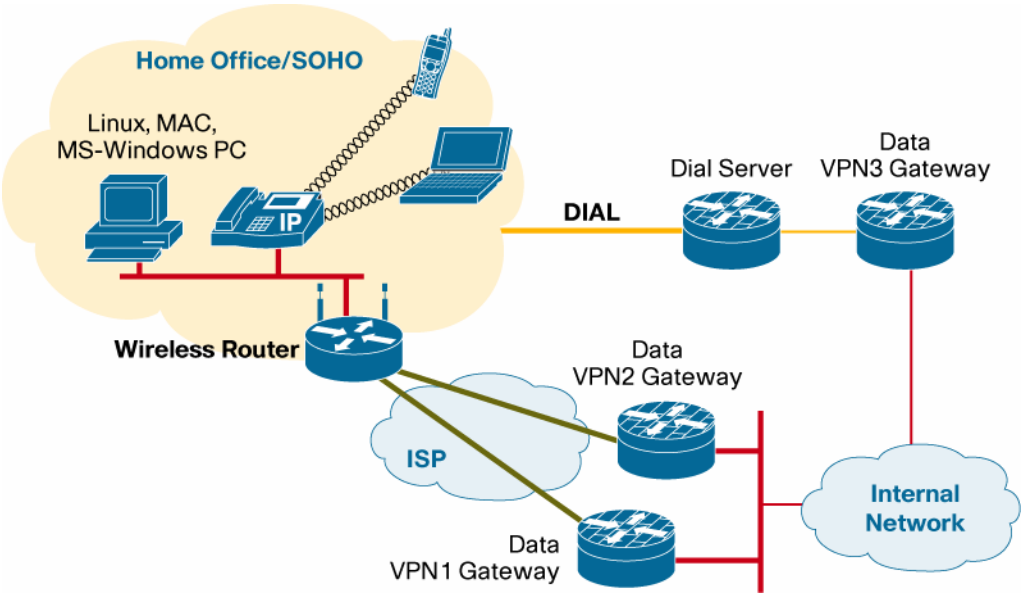
Dial Backup provides backup connectivity using dial network-to-corporate network connections if the Internet service provider (ISP) connection from spoke to hub fails. In the Cisco Virtual Office solution, which encompasses Dynamic Multipoint VPN (DMVPN) architecture for data gateway infrastructure, the Dial Backup feature provides connectivity to the data gateways using the dial network if the ISP connection fails. The bandwidth and speed provided by dial networks is low and should be used mainly to provide secondary connectivity. Whenever connection to the ISP restores, the tunnel to the data gateway through the dial network is torn down and the tunnel through the ISP is restored.

Topology

In DMVPN deployment, Dial Backup is incorporated on spokes. Figure 1 shows the connectivity between spoke and data gateways in the current Cisco Virtual Office deployment.

The dial server is introduced and a new hub is created to handle all DMVPN tunnels originating from the dial network.

Figure 1. Deploying Dial Backup in Cisco Virtual Office Environment



Initially connectivity to the internal network is through the data gateways VPN1 and VPN2 . These gateways provide redundant connectivity to the internal network. Although the primary path to

reach the internal network is provided by one VPN gateway (say VPN1), VPN2 gateway takes over if VPN1 gateway is unusable because of system abnormality or router reload. By providing a dial backup, the redundancy is taken to the next level, where connectivity to the internal network is transparently provided if ISP connectivity fails.

When the spoke recognizes that connectivity to VPN1 and VPN2 gateways is unavailable, the spoke triggers the dial process and attempts to reach the dial server. The spoke has two paths to reach the VPN gateways -- the path through the ISP and the path through the dial network. On the spoke, the path through the ISP is given higher priority than the path through the dial network. When the spoke does not find the path to the gateway through the primary path (because of a missing entry in the routing table or Internet Control Message Protocol [ICMP] ping failure), it triggers the dial process. The spoke gets a dynamic address from the dial server and reaches the VPN gateway through the dial server.

The spoke then initiates Next Hop Resolution Protocol (NHRP) registration and subsequently brings up a DMVPN tunnel with VPN3 gateway and thereby provides connectivity to the internal network. When the ISP connection is up again, the DMVPN tunnel to VPN1 and VPN2 gateways is brought up and the DMVPN tunnel to VPN3 is torn down.

In testing Dial Backup in Cisco Virtual Office setup, only analog modems were used. In the spoke router, you can use platforms such as modular integrated services routers, which have internal modems; for platforms such as the Cisco 881 Integrated Services Routers, which do not have and internal modem, you must use an external modem. If you use an external modem, be sure to adjust the speed and other parameters on the spoke router to match the speed that the modem is configured to work with.

Images

The dial server is supported on many platforms. For testing we limited the dial server and spoke platforms and images as follows:

- Dial server platform: Cisco 3845 Integrated Services Router; image: Cisco IOS® Software Release 12.4(15)T5 or later
- Spoke platform: Cisco 1841 Integrated Services Router; image: Cisco IOS Software Release 12.4(15)T5 or later

For the Cisco 880 Series Integrated Services Routers, you must use Cisco IOS Software Release 12.4(20)T or later.

Limitations

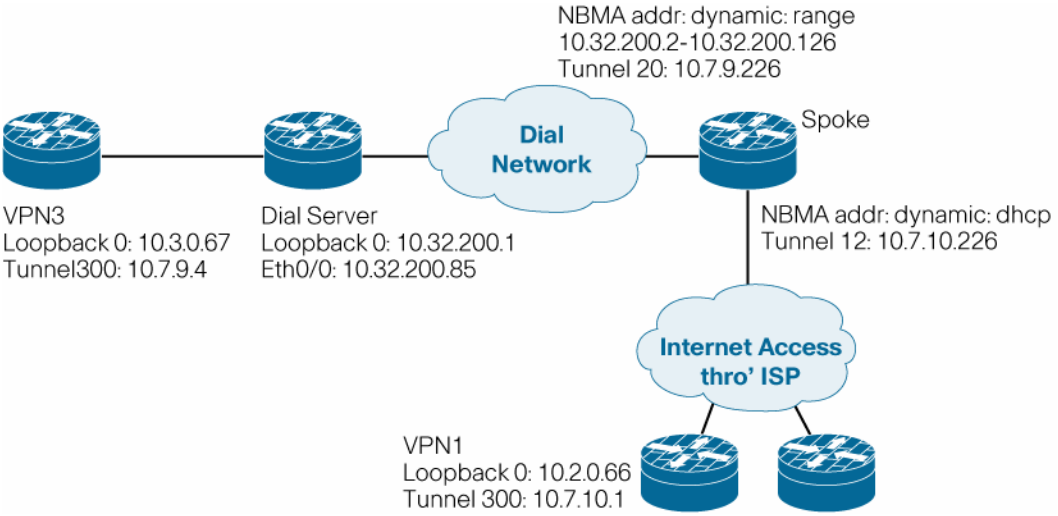
- When a DMVPN tunnel is established using Dial Backup, only the hub-to-spoke topology is supported.
- The testing was performed with an in-house dial server; the setup has not been tried with dialup service provided by ISPs.
- While configuring the Cisco 800 Series for Dial Backup, **do not** use the console. Always perform Telnet to the router and then configure the modem commands and other commands for the Dial Backup feature. Because the Cisco 800 Series routers do not have an internal modem, connect the console port on the Cisco 800 with an external analog modem.

Because the Cisco 1841 uses a modem WAN interface card (WIC), connect the phone cable to the ports on the WIC.

Configuration

Figure 2 gives the sample topology with IP address corresponding to the node, to map with the configuration that follows.

Figure 2. Sample Topology



Configuration on the Dial Server

Note: In the configuration that follows, a dedicated dial server was used. In general you can use any public ISP dial server.

```
Building configuration...

Current configuration : 4598 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dial-server1
!
boot-start-marker
boot system flash c3640-ik9o3s-mz.123-9
boot-end-marker
!
logging buffered 65555 debugging
enable secret 5 <removed>
!
clock timezone PST -8
clock summer-time PDT recurring
aaa new-model
```

```
!
! Defines a RADIUS type server group
!
aaa group server radius dial-server
 server-private 10.4.1.1 auth-port 1812 acct-port 1813 key mypasswd
!
! Specifies one or more AAA authentication methods for use on serial
interfaces running Point-
! to-Point Protocol (PPP)
!
aaa authentication ppp default group dial-server
aaa session-id common
ip subnet-zero
!
!
ip cef
no ip domain lookup
ip domain name cisco.com
!
ip audit po max-events 100
no ftp-server write-enable
!  The following example specifies ISDN PRI on T1 slot 1, port 0, and
configures voice and data
!   bearer capability on time slots 1 through 24:


isdn switch-type primary-5ess
!
controller T1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
interface Loopback0
 ip address 10.32.200.1 255.255.255.128
 ip ospf network point-to-point
!
interface Ethernet0/0
 ip address 10.34.200.85 255.255.255.240
 ip access-group fw_acl out
 full-duplex
!  In a dedicated configuration, we assume the 24th timeslot will be
used by ISDN.
!  Serial interface 0:23 is created for configuring ISDN parameters.
!
interface Serial1/0:23
 no ip address
 encapsulation ppp
 dialer rotary-group 1
 dialer-group 1
 isdn switch-type primary-5ess
```

```
 isdn incoming-voice modem
 no isdn outgoing ie redirecting-number
 no isdn incoming alerting add-PI
 no fair-queue
 no cdp enable
!
! Create an asynchronous group interface
!
interface Group-Async1
 ip unnumbered Loopback0
 encapsulation ppp
 async mode interactive
 peer default ip address pool dialin_pool
 ppp authentication chap callin
 group-range 97 114
!
router ospf 5
 log-adjacency-changes
 area 24 nssa
 passive-interface Serial1/0:23
 passive-interface Group-Async1
 passive-interface Dialer1
 network 10.32.200.0 0.0.0.127 area 24
 network 10.34.200.80 0.0.0.7 area 24
!
! configure a local pool of IP addresses to be used when a remote peer
connects to a
! point-to-point interface.
!
ip local pool dialin_pool 10.32.200.2 10.32.200.126
!
! Define a DDR dialer list to control dialing by protocol or by a
combination of a protocol and
! a previously defined access list
!
dialer-list 1 protocol ip permit
no cdp log mismatch duplex
! Configure  line interface for the AUX port. enable incoming and
outgoing calls.
line con 0
 exec-timeout 0 0
line 97 114
 exec-timeout 0 0
 modem InOut
 modem autoconfigure discovery
 autoselect during-login
 autoselect ppp
line aux 0
!
ntp clock-period 17180022
```

```
ntp server 192.168.203.5
!
end
```

Configuration on the VPN3 Data Gateway

Note: The following configuration is mainly for the Dial Backup feature. For a complete DMVPN gateway configuration, please refer to the Cisco Virtual Office overview available at http://www.cisco.com/go/cvo.

```
version 12.4
service timestamps debug uptime
service timestamps log uptime
!
hostname vpn3-data-gw
!
ip domain name dmvpn.com
!
crypto pki trustpoint certificate-server
enrollment url http://192.168.203.12:80
 serial-number
 revocation-check crl
 auto-enroll 70
!
! The certificates are generated automatically after the registration
with the CA
crypto pki certificate chain TEST-CA
certificate <removed>
certificate ca <removed>
!--- Certificate is abbreviated for easier viewing
!
crypto isakmp policy 1
 encr 3des
!
crypto isakmp policy 2
 encr 3des
!
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
 mode transport
crypto ipsec transform-set t2 esp-3des esp-sha-hmac
crypto ipsec transform-set t3 esp-3des esp-sha-hmac
 mode transport require
!
! Create an IPSec profile to be applied dynamically to the GRE over
! IPSec tunnels.

crypto ipsec profile dialbackup
 set transform-set t3 t1 t2
!
```

```
interface Loopback0
ip address 10.3.0.67 255.255.255.255
!
! This is the mGRE interface for dynamic GRE tunnels via the dial
!
interface Tunnel300
 bandwidth 1900
 ip address 10.7.9.4 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim nbma-mode
 ip pim sparse-dense-mode
 ip multicast rate-limit out 768
 ip nhrp map multicast dynamic
 ip nhrp network-id 1234
 ip nhrp holdtime 600
 ip nhrp server-only
 ip tcp adjust-mss 1360
 no ip split-horizon eigrp 7
 ip nhrp redirect
 no ip mroute-cache
 delay 2000
 tunnel source Loopback1
 tunnel mode gre multipoint
 tunnel key 100
tunnel protection ipsec profile dialbackup
!
interface Ethernet0
ip address 172.17.0.1 255.255.255.252
!
interface Ethernet1
ip address 192.168.0.1 255.255.255.0
!
! Enable a routing protocol to send/receive dynamic updates about the
private networks over the
! tunnels
!
router eigrp 7
network 10.7.8.0 0.0.1.255
distribute-list split_out in Tunnel300
 no auto-summary
!
ntp server 192.168.203.5
end
```

Configuration on the Spoke Router

Note: For this configuration the Cisco 1841 is used as a spoke. The following configuration is mainly for the Dial Backup feature. For a complete spoke configuration, please refer to the Cisco Virtual Office overview at http://www.cisco.com/go/cvo.

```
version 12.4
service timestamps debug uptime
service timestamps log uptime
!
hostname spoke1
!
ip domain name dmvpn.com
!
!
crypto pki trustpoint TEST-CA
enrollment mode ra
enrollment url http://192.168.203.12:80/certsrv/mscep/mscep.dll
serial-number
password dmvpntest
crl optional
auto-enroll 70
! The certificates are generated automatically after the registration
with the CA
crypto pki certificate chain TEST-CA
certificate <removed>
certificate ca <removed>
!--- Certificate is abbreviated for easier viewing.
crypto isakmp policy 1
 encr 3des
crypto isakmp keepalive 10
crypto isakmp nat keepalive 10
!
crypto ipsec security-association lifetime kilobytes 530000000
crypto ipsec security-association lifetime seconds 14400
!
crypto ipsec transform-set stealth-3des esp-3des esp-sha-hmac
crypto ipsec transform-set t1 esp-3des esp-sha-hmac
 mode transport
!
! Create an IPSec profile to be applied dynamically to the GRE over
! IPSec tunnels.
!
crypto ipsec profile dialprofile
 set transform-set stealth-3des
!
crypto ipsec profile proftest
 set transform-set t1
!
```

```
! This is the mGRE interface for dynamic GRE tunnels via the ISP
!
interface Tunnel12
description Tunnel to primary hubs vpn1 and vpn2
 bandwidth 2000
 ip address 10.7.10.226 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim sparse-dense-mode
 ip multicast rate-limit out 128
 ip nhrp map 10.7.10.1 10.2.0.66
 ip nhrp map multicast 10.2.0.66
 ip nhrp map 10.7.10.5 10.2.0.65
 ip nhrp map multicast 10.2.0.65
 ip nhrp network-id 2345
 ip nhrp holdtime 300
 ip nhrp nhs 10.7.10.1
 ip nhrp nhs 10.7.10.5
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
 ip tcp adjust-mss 1360
 load-interval 30
 delay 2000
 qos pre-classify
 tunnel source FastEthernet0/1
 tunnel mode gre multipoint
 tunnel key 101
 tunnel protection ipsec profile proftest
!
! This is the mGRE interface for dynamic GRE tunnels via the dial
!
interface Tunnel20
 description tunnel to dial backup hub vpn3
 bandwidth 2000
 ip address 10.7.9.226 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip pim sparse-dense-mode
 ip multicast rate-limit out 128
 ip nhrp map 10.7.9.4 10.3.0.67
 ip nhrp map multicast 10.3.0.67
 ip nhrp network-id 1234
 ip nhrp holdtime 300
 ip nhrp nhs 10.7.9.4
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
 ip tcp adjust-mss 1360
```

```
 load-interval 30
 delay 2000
 qos pre-classify
 tunnel source Async0/1/0
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile dialprofile
!
interface FastEthernet0/1
description outside interface
ip address dhcp
!
interface FastEthernet0/0
description inside interface
ip address 192.168.1.1 255.255.255.0
!
interface Async0/1/0
 ip address negotiated
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 300
 dialer fast-idle 10800
 dialer enable-timeout 6
 dialer wait-for-carrier-time 75
 dialer string 4441234
 dialer hold-queue 100 timeout 75
 dialer-group 1
 async dynamic address
 async dynamic routing
 async mode dedicated
 no fair-queue
 ppp chap hostname dialuser
 ppp chap password 7 12171A1D
!
router eigrp 7
 passive-interface FastEthernet0/0
 passive-interface FastEthernet0/1
 network 10.7.8.0 0.0.1.255
 network 10.7.10.0 0.0.1.255
 no auto-summary
 no eigrp log-neighbor-changes

ip classless
ip route 10.2.0.64 255.255.255.248 Async0/1/0 200
ip route 171.69.1.9 255.255.255.255 Async0/1/0
!
end
```

Troubleshooting and Show Commands

To debug Dial Backup problems, use the following commands on the hub and spoke:

- **debug async framing**
- **debug async packet**
- **debug async state**

To disable debugging, use the “no” form of these commands.

The show commands follow:

- Issue **show ip interface brief** and check to make sure the asynchronous interface has been assigned an IP address.
- Use the commands **show crypto isa sa** and **show crypto ipsec sa** and check to make sure the DMVPN tunnel to VPN3 has been established using the source interface Async 0/1/0.
- Use the commands **show ip nhrp**, **show crypto ipsec sa**, and **show crypto isa sa** on the hub to see if the spoke has registered successfully.
- Use the **show ip route eigrp** command on the spoke to make sure the Enhanced IGRP (EIGRP) routes are populated through tunnel 20.

References

- Cisco Virtual Office Deployment Guide: http://www.cisco.com/go/cvo

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C07-492501-00 08/08