

Configuring Dial Backup Using Dialer Watch

This chapter describes how to configure dial backup using Dialer Watch.

For a complete description of the dial backup commands used to configure Dialer Watch, refer to the *Dial Solutions Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Dialer Watch is a backup feature that integrates dial backup with routing capabilities. Prior dial backup implementations used the following conditions to trigger backup:

- Interesting packets were defined at central and remote routers using Dial on Demand routing (DDR).
- Connection loss occurred on a primary interface using a back up interface with floating static routes.
- Traffic thresholds were exceeded using a dialer load threshold.

Prior backup implementations may not have supplied optimum performance on some networks, such as those using Frame Relay multipoint subinterfaces or Frame Relay connections that do not support end-to-end PVC status updates.

Dialer Watch provides reliable connectivity without relying solely on defining interesting traffic to trigger outgoing calls at the central router. Dialer Watch uses the convergence times and characteristics of dynamic routing protocols. Integrating backup and routing features enables Dialer Watch to monitor every deleted route. By configuring a set of watched routes that define the primary interface, you are able to monitor and track the status of the primary interface as watched routes are added and deleted. Monitoring the watched routes is done in the following sequence:

- 1 Whenever a watched route is deleted, Dialer Watch checks to see if there is at least one valid route for any of the defined watched IP addresses.
- 2 If no valid route exists, the primary line is considered down and unusable.
- 3 If a valid route exists for at least one of the defined IP addresses, and if the route is pointing to an interface other than the backup interface configured for Dialer Watch, the primary link is considered up.
- 4 In the primary link goes down, Dialer Watch is immediately notified by the routing protocol and the secondary link is brought up.
- 5 Once the secondary link is up, at the expiration of each idle timeout, the primary link is rechecked.
- 6 If the primary link remains down, the idle timer is indefinitely reset.

- 7 If the primary link is up, the secondary backup link is disconnected. Additionally, you can set a disable timer to create a delay for the secondary link to disconnect, after the primary link is reestablished.

Dialer Watch provides the following advantages:

- Routing—Backup initialization is linked to the dynamic routing protocol, rather than a specific interface or static route entry. Therefore, both primary and backup interfaces can be any interface type, and can be used across multiple interfaces and multiple routers. Dialer Watch also relies on convergence, which is sometimes preferred over traditional DDR links.
- Routing protocol independent—Static routes or dynamic routing protocols, such as Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP) or Open Shortest Path First (OSPF) can be used.
- Nonpacket semantics—Dialer Watch does not exclusively rely on interesting packets to trigger dialing. The link is automatically brought up when the primary line goes down without postponing dialing.
- Dial backup reliability—DDR redial functionality is extended to dial indefinitely in the event that secondary backup lines are not initiated. Typically, DDR redial attempts are affected by enable-timeouts and wait-for-carrier time values. Intermittent media difficulties or flapping interfaces can cause problems for traditional DDR links. However, Dialer Watch automatically reestablishes the secondary backup line on ISDN, synchronous, and asynchronous serial links.

The following prerequisites apply to Dialer Watch:

- The router is dial backup capable. This means the router has a DCE, TA, or NT1 device attached that supports V.25bis.
- The router is configured for DDR. This includes traditional commands such as **dialer map** and **dialer in-band** commands, and so on.
- Dialer Watch is only supported for IP at this time.

For information on how to configure traditional DDR for dial backup, refer to the “Dial Backup” chapter in the *Dial Solutions Configuration Guide* for Cisco IOS Release 11.3.

Configuration Tasks

Perform the following tasks to configure Dialer Watch. All tasks are required except the last task to set a disable timer.

- Determine the Primary and Secondary Interfaces
- Determine the Interface Addresses and Networks to Watch
- Configure the Interface to Perform DDR Backup
- Create a Dialer List
- Set the Disable Timer on the Backup Interface (optional)

Determine the Primary and Secondary Interfaces

Decide which interfaces on which routers will act as primary and secondary interfaces. Unlike traditional backup methods, you can define multiple interfaces on multiple routers instead of a singly defined interface on one router.

Determine the Interface Addresses and Networks to Watch

Determine which addresses and networks are to be monitored or watched. Typically, this will be an interface on a remote router or a network advertised by a central or remote router.

Configure the Interface to Perform DDR Backup

To initiate Dialer Watch, you must configure the interface to perform DDR and backup. Use traditional DDR configuration commands, such as dialer maps, for DDR capabilities. To enable Dialer Watch on the backup interface, perform the following task in interface configuration mode:

Command	Purpose
dialer watch-group <i>group-number</i>	Enable Dialer Watch on the backup interface.

Create a Dialer List

To define the IP addresses you want watched, use the following command in global configuration mode:

Command	Purpose
dialer watch-list <i>group-number</i> ip <i>ip-address</i> <i>address-mask</i>	Define all IP addresses to be watched.

The **dialer watch-list** command is the means to detect if the primary interface is up or down. The primary interface is determined to be up when there is an available route with a valid metric to any of the addresses defined in this list, and it points to an interface other than the interface on which the **dialer watch-group** is defined. The primary interface is determined to be down when there is no available route to any of the addresses defined in the **dialer watch-list** command.

Set the Disable Timer on the Backup Interface

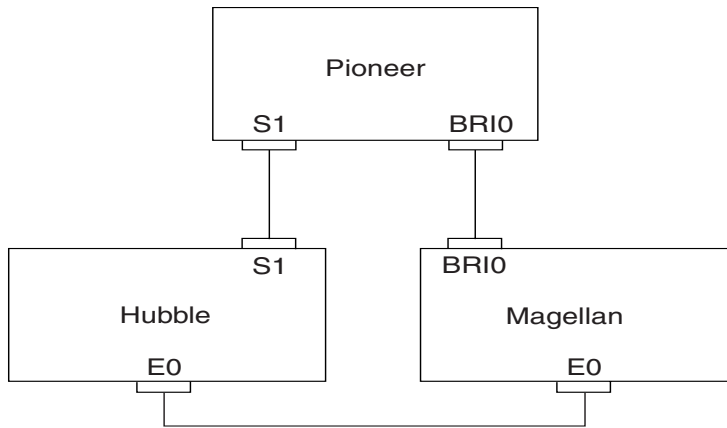
This task is optional. Under some conditions, you may want to implement a delay before the backup interface is dropped once the primary interface recovers. This delay can ensure stability, especially for flapping interfaces or interfaces experiencing frequent route changes. To apply a disable time, use the following command in interface configuration mode:

Command	Purpose
dialer watch-disable <i>seconds</i>	Apply a disable time to the interface.

Dialer Watch Configuration Examples

In the following example, Pioneer and Hubble are connected via Frame Relay. Magellon is configured to perform Dialer Watch and it will watch networks 3.0.0.0, 4.0.0.0, and 5.0.0.0. If routing updates are deleted for these three networks, Magellon will implement Dialer Watch by initiating the call to Pioneer. Comments precede the configuration commands and are noted by an exclamation mark (!). Refer to Cisco IOS Release 11.3 configuration guides and command references for additional information on configuring Frame Relay, PPP, and traditional dial backup features. Figure 301 shows Dialer Watch configured to backup primary interfaces that are configured for Frame Relay.

Figure 301 Dialer Watch for Frame Relay Interfaces



10110

Configuration for Hubble Router

```

interface Ethernet0
 ! Hubble and magellan are on same LAN
 ip address 172.21.24.85 255.255.255.0

interface serial1
 ! This is the Primary multipoint interface
 ip address 3.1.1.1 255.255.255.0
 encapsulation frame-relay
 frame-relay map ip 3.1.1.1 100
 frame-relay map ip 3.1.1.2 200
 frame-relay map ip 3.1.1.3 300

 ! The interfaces are configured to use EIGRP routing
router eigrp 190
network 3.0.0.0
network 172.21.0.0
 !
end
  
```

Configuration for Magellan Router

```

 ! Remote site username and shared password. Password is not encrypted to show
 ! that the password is shared between the routers
username pioneer password starz
interface Ethernet0
 ! This is in the same LAN as Hubble Ethernet 0
 ip address 172.21.24.86 255.255.255.0
 !
interface bri0
 ! This is the secondary backup line
 ip address 7.1.1.2 255.255.255.0
 encapsulation ppp
 dialer idle-timeout 5
 ! Use a dialer map for the IP address/network which is the same network as
 ! being watched
 dialer map ip 3.1.1.0 name pioneer 60079 broadcast
 ! Add a dialer map for remote end's IP address to make routing work over this
interface
 dialer map ip 7.1.1.3 name pioneer 60079 broadcast
 dialer-group 1
  
```

```

! Enable Dialer Watch on this interface
dialer watch-group 1
ppp authentication chap
!
! The interfaces are configured to use EIGRP routing
router eigrp 190
network 7.0.0.0
network 172.21.0.0
!
access-list 100 deny eigrp any any
access-list 100 permit ip any any
! Watch IP networks 3.1.1.0, 4.1.1.0, and 5.1.1.0
dialer watch-list 1 ip 3.1.1.0 255.255.255.0
dialer watch-list 1 ip 4.1.1.0 255.255.255.0
dialer watch-list 1 ip 5.1.1.0 255.255.255.0
dialer-list 1 protocol ip list 100
!
end

```

Configuration for Pioneer Router

```

! Remote site username and shared password. Password is not encrypted to show that
! the password is shared between the routers
username magellon password starz
interface ethernet0
 ip address 182.21.75.21 255.255.255.0
interface serial1
 ! This is Primary interface on the remote end
 ip address 3.1.1.2 255.255.255.0
 encapsulation frame-relay
 frame-relay map ip 3.1.1.1 100
!
interface bri0
 ! This is where the secondary dials in. This router does not require a dialer map
 ! statement because it is receiving the call.
 ip address 7.1.1.3 255.255.255.0
 encapsulation ppp
 ! The dialer idle-timeout command prevents premature hangup
 dialer idle-timeout 10000
 dialer-group 1
 ppp authentication chap
!
access-list 100 permit ip any any
dialer-list 1 protocol ip list 100
!
! The interfaces are configured to use EIGRP routing
router eigrp 190
network 3.0.0.0
network 7.0.0.0
network 182.21.0.0
!
end

```

