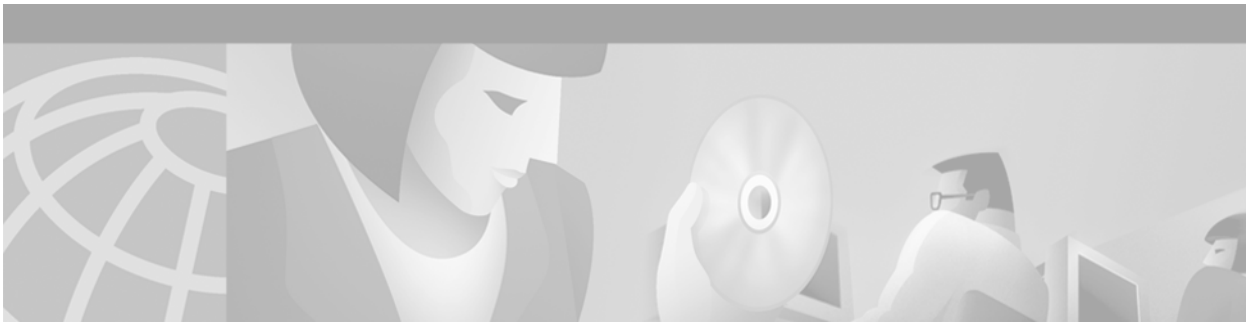


Configuring Dial Backup Using Dialer Watch

This chapter describes how to configure dial backup using the Dialer Watch feature. It includes the following main sections:

- Dialer Watch Overview
- How to Configure Dialer Backup with Dialer Watch
- Configuration Examples for Dialer Watch

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the "Identifying Supported Platforms" section in the "Using Cisco IOS Software" chapter.

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

Dialer Watch Overview

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 permanent virtual circuit (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 whether 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. If 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, meaning the router has a data communications equipment (DCE), terminal adapter, or network termination 1 device attached that supports V.25*bis*.
- The router is configured for DDR. This configuration 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, see the other chapters in the "Dial Backup" part of this publication.

How to Configure Dialer Backup with Dialer Watch

To configure Dialer Watch, perform the following tasks. All tasks are required except the last one to set a disable timer.

- Determining the Primary and Secondary Interfaces (Required)
- Determining the Interface Addresses and Networks to Watch (Required)
- Configuring the Interface to Perform DDR Backup (Required)

- Creating a Dialer List (Required)
- Setting the Disable Timer on the Backup Interface (Optional)

Determining 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.

Determining the Interface Addresses and Networks to Watch

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

Configuring 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, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# dialer watch-group group-number`	Enables Dialer Watch on the backup interface.

Creating a Dialer List

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

Command	Purpose
`Router(config)# dialer watch-list group-number ip ip-address address-mask`	Defines 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** command 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.

Setting 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.

Note The **dialer watch-disable** command used in Dialer Watch configurations was Replaced in Cisco IOS Release 12.3(11)T by the **dialer watch-list delay** command. When using the **dialer watch-list delay** command in software later than Cisco IOS Release 12.3(11)T, you can specify both a connect and disconnect timer for the disable timer. The disconnect time specifies that the disconnect timer is started when the secondary link is up and after the idle timeout period has expired, and only when software has determined that the primary route has come up

In Cisco IOS Software Releases Prior to 12.3(11)T

To apply a disable time, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# dialer watch-disable seconds`	Applies a disable time to the interface.

In Cisco IOS Software Releases After 12.3(11)T

To apply a disable time, use the following command in global configuration mode:

Command	Purpose
`Router(config-if)# dialer watch-list group-number delay {connect connect-time | disconnect disconnect-time}`	Configures a disable time. • *group-number*—Group number assigned to the list. Valid group numbers are from 1 to 255. • **delay**—Specifies that the router will delay dialing the secondary link when the primary link becomes unavailable. • **connect** *connect-time*—Time, in seconds, after which the router rechecks for availability of the primary link. If the primary link is still unavailable, the secondary link is then dialed. Valid times range from 1 to 2147483 seconds. • **disconnect** *disconnect-time*—Time, in seconds, that specifies when to disconnect. Disconnect occurs when the secondary link is up and after the idle timeout period has expired, and only when software has determined that the primary route has come up. Valid times range from 1 to 2147483 seconds.

Configuration Examples for Dialer Watch

The **dialer watch-disable** command used in Dialer Watch configurations was replaced in Cisco IOS Release 12.3(11)T by the **dialer watch-list delay** command. The following sections provide examples of how to configure Dialer Watch in software before and after the **dialer watch-disable** command was replaced.

- Dialer Watch Configuration Example Prior to Cisco IOS Release 12.3(11)T, page 463
- Dialer Watch Configuration Example After Cisco IOS Release 12.3(11)T, page 467

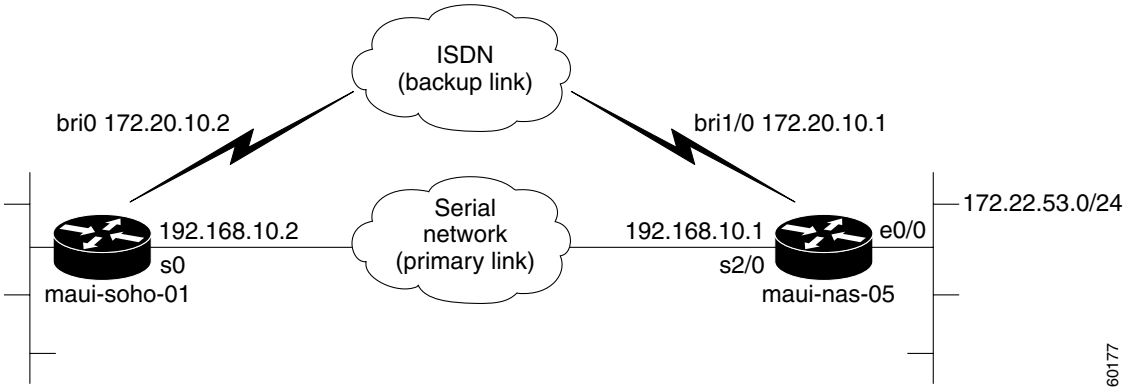
Dialer Watch Configuration Example Prior to Cisco IOS Release 12.3(11)T

In the following example, an ISDN BRI line is used to back up a serial leased line connection by configuring the Dialer Watch feature on a router named maui-soho-01. The Dialer Watch feature enables the router to monitor the existence of a specified route. If that route is not present, the backup interface is activated. Unlike other backup methods, the Dialer Watch feature does not require interesting traffic to activate the backup interface. The configuration shown in Figure 61 uses legacy dial-on-demand routing (DDR) and the Open Shortest Path First (OSPF) routing protocol. Dialer profiles can be used in place of DDR. Once the backup connection is activated, you must ensure that the routing table is updated to use the new backup route. Additional information about the Dialer Watch feature is available at the following website:

http://www.cisco.com/warp/public/129/bri-backup-map-watch.html

For additional information on configuring legacy DDR, dialer profiles, PPP, and traditional dial backup features, see the relevant chapters in this publication.

Figure 61 Dialer Watch for Frame Relay Interfaces



Note The following example uses commands supported in Cisco IOS software prior to Release 12.3(11)T. See the updated example for configuring Dialer Watch after Cisco IOS Release 12.3(11)T that follows this example.

Configuration for maui-soho-01

```
maui-soho-01# show running-config

Building configuration...

Current configuration : 1546 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname maui-soho-01
!
logging rate-limit console 10 except errors
aaa new-model
aaa authentication login default local
aaa authentication login NO_AUTHEN none
aaa authentication ppp default local
```

```
!This is basic AAA configuration for PPP calls.
enable secret 5 <deleted>
!
username maui-nas-05 password 0 cisco
!Username for remote router (maui-nas-05) and shared secret.
!Shared secret(used for CHAP authentication) must be the same on both sides.
ip subnet-zero
no ip finger
!
isdn switch-type basic-ni
!
interface Loopback0
 ip address 172.17.1.1 255.255.255.0
!
interface Ethernet0
 ip address 172.16.1.1 255.255.255.0
!
interface Serial0
!Primary link.
 ip address 192.168.10.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
interface BRI0
 ip address 172.20.10.2 255.255.255.0
!IP address for the BRI interface (backup link).
 encapsulation ppp
 dialer idle-timeout 30
!Idle timeout(in seconds)for this backup link.
!Dialer watch checks the status of the primary link every time the
!idle-timeout expires.
 dialer watch-disable 15
!Delays disconnecting the backup interface for 15 seconds after the
!primary interface is found to be up.
 dialer map ip 172.20.10.1 name maui-nas-05 broadcast 5550111
!Dialer map for the BRI interface of the remote router.
 dialer map ip 172.22.53.0 name maui-nas-05 broadcast 5550111
!Map statement for the route/network being watched by the
!dialer watch-list command.
!This address must exactly match the network configured with the
!dialer watch-list command.
!When the watched route disappears, this dials the specified phone number.
 dialer watch-group 8
!Enable Dialer Watch on this backup interface.
!Watch the route specified with dialer watch-list 8.
 dialer-group 1
!Apply interesting traffic defined in dialer-list 1.
 isdn switch-type basic-ni
 isdn spid1 51255522220101 5550112
 isdn spid2 51255522230101 5550112
 ppp authentication chap
!Use chap authentication.
!
router ospf 5
 log-adjacency-changes
 network 172.16.1.0 0.0.0.255 area 0
 network 172.17.1.0 0.0.0.255 area 0
 network 172.20.10.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.3 area 0
!
ip classless
no ip http server
!
```

```
dialer watch-list 8 ip 172.22.53.0 255.255.255.0
!This defines the route(s) to be watched.
!This exact route(including subnet mask) must exist in the routing table.
!Use the dialer watch-group 8 command to apply this list to the backup interface.
access-list 101 remark Define Interesting Traffic
access-list 101 deny   ospf any any
!Mark OSPF as uninteresting.
!This will prevent OSPF hellos from keeping the link up.
Access-list 101 permit ip any any
dialer-list 1 protocol ip list 101
!Interesting traffic is defined by access-list 101.
!This is applied to BRI0 using dialer-group 1.
!
line con 0
 login authentication NO_AUTHEN
 transport input none
line vty 0 4
!
end
```

Configuration for maui-nas-05

```
maui-nas-05# show running-config

Building configuration...

Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname maui-nas-05
!
aaa new-model
aaa authentication login default local
aaa authentication login NO_AUTHEN none
aaa authentication ppp default local
! -- This is basic AAA configuration for PPP calls.
Enable secret 5 <deleted>
!
username maui-soho-01 password 0 cisco
!Username for remote router (maui-soho-01) and shared secret.
!Shared secret(used for CHAP authentication) must be the same on both sides.
!
ip subnet-zero
!
isdn switch-type basic-ni
!
interface Loopback0
 ip address 172.22.1.1 255.255.255.0
!
interface Ethernet0/0
 ip address 172.22.53.105 255.255.255.0
!
interface Ethernet0/1
 no ip address
 shutdown
!
interface BRI1/0
!Backup link.
 ip address 172.20.10.1 255.255.255.0
 encapsulation ppp
```

```
 dialer map ip 172.20.10.2 name maui-soho-01 broadcast
!Dialer map with IP address and authenticated username for remote destination.
!The name should match the authentication username provided by the remote side.
!The dialer map statement is used even though this router is not dialing out.
 Dialer-group 1
!Apply interesting traffic defined in dialer-list 1.
 isdn switch-type basic-ni
 isdn spid1 51255501110101 5550111
 isdn spid2 51255501120101 5550112
 ppp authentication chap
!
.
.
.
!
interface Serial2/0
 ip address 192.168.10.1 255.255.255.252
 encapsulation ppp
 clockrate 64000
 ppp authentication chap
!
.
.
.
!
router ospf 5
 network 172.20.10.0 0.0.0.255 area 0
 network 172.22.1.0 0.0.0.255 area 0
 network 172.22.53.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.3 area 0
 default-information originate
!
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet0/0
no ip http server
!
dialer-list 1 protocol ip permit
!This defines all IP traffic as interesting.
!
line con 0
 login authentication NO_AUTHEN
 transport input none
line 97 102
line aux 0
line vty 0 4
!
end
```

Dialer Watch Configuration Example After Cisco IOS Release 12.3(11)T

The following example shows how to configure Dialer Watch using the **dialer watch-list delay** command that replaced the **dialer watch-disable** command.

Configuration for maui-soho-01

```
maui-soho-01# show running-config
Building configuration...

Current configuration : 1546 bytes
!
version 12.4
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname maui-soho-01
!
logging rate-limit console 10 except errors
aaa new-model
aaa authentication login default local
aaa authentication login NO_AUTHEN none
aaa authentication ppp default local
!This is basic AAA configuration for PPP calls.
enable secret 5 <deleted>
!
username maui-nas-05 password 0 cisco
!Username for remote router (maui-nas-05) and shared secret.
!Shared secret(used for CHAP authentication) must be the same on both sides.
ip subnet-zero
no ip finger
!
isdn switch-type basic-ni
!
interface Loopback0
 ip address 172.17.1.1 255.255.255.0
!
interface Ethernet0
 ip address 172.16.1.1 255.255.255.0
!
interface Serial0
!Primary link.
 ip address 192.168.10.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
interface BRI0
 ip address 172.20.10.2 255.255.255.0
!IP address for the BRI interface (backup link).
 encapsulation ppp
 dialer idle-timeout 30
!Idle timeout(in seconds)for this backup link.
!Dialer watch checks the status of the primary link every time the
!idle-timeout expires.
 dialer map ip 172.20.10.1 name maui-nas-05 broadcast 5550111
!Dialer map for the BRI interface of the remote router.
 dialer map ip 172.22.53.0 name maui-nas-05 broadcast 5550111
!Map statement for the route/network being watched by the
!dialer watch-list command.
!This address must exactly match the network configured with the
!dialer watch-list command.
```

```
!When the watched route disappears, this dials the specified phone number.
 dialer watch-group 8
!Enable Dialer Watch on this backup interface.
!Watch the route specified with dialer watch-list 8.
 dialer-group 1
!Apply interesting traffic defined in dialer-list 1.
isdn switch-type basic-ni
 isdn spid1 51255522220101 5552222
 isdn spid2 51255522230101 5552223
 ppp authentication chap
!Use chap authentication.
dialer watch-list 8 delay disconnect 15
!Delays disconnecting the backup interface for 15 seconds after the
!primary interface is found to be up.
!
router ospf 5
 log-adjacency-changes
 network 172.16.1.0 0.0.0.255 area 0
 network 172.17.1.0 0.0.0.255 area 0
 network 172.20.10.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.3 area 0
!
ip classless
no ip http server
!
dialer watch-list 8 ip 172.22.53.0 255.255.255.0
!This defines the route(s) to be watched.
!This exact route(including subnet mask) must exist in the routing table.
!Use the dialer watch-group 8 command to apply this list to the backup interface.
access-list 101 remark Define Interesting Traffic
access-list 101 deny   ospf any any
!Mark OSPF as uninteresting.
!This will prevent OSPF hellos from keeping the link up.
Access-list 101 permit ip any any
dialer-list 1 protocol ip list 101
!Interesting traffic is defined by access-list 101.
!This is applied to BRI0 using dialer-group 1.
!
line con 0
 login authentication NO_AUTHEN
 transport input none
line vty 0 4
!
end
```

Configuration for maui-nas-05

```
maui-nas-05# show running-config
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname maui-nas-05
!
aaa new-model
aaa authentication login default local
aaa authentication login NO_AUTHEN none
aaa authentication ppp default local
```

```
! -- This is basic AAA configuration for PPP calls.
Enable secret 5 <deleted>
!
username maui-soho-01 password 0 cisco
!Username for remote router (maui-soho-01) and shared secret.
!Shared secret(used for CHAP authentication) must be the same on both sides.
!
ip subnet-zero
!
isdn switch-type basic-ni
!
interface Loopback0
 ip address 172.22.1.1 255.255.255.0
!
interface Ethernet0/0
 ip address 172.22.53.105 255.255.255.0
!
interface Ethernet0/1
 no ip address
 shutdown
!
interface BRI1/0
!Backup link.
 ip address 172.20.10.1 255.255.255.0
 encapsulation ppp
 dialer map ip 172.20.10.2 name maui-soho-01 broadcast
!Dialer map with IP address and authenticated username for remote destination.
!The name should match the authentication username provided by the remote side.
!The dialer map statement is used even though this router is not dialing out.
 Dialer-group 1
!Apply interesting traffic defined in dialer-list 1.
 isdn switch-type basic-ni
 isdn spid1 51255501110101 5550111
 isdn spid2 51255501120101 5550112
 ppp authentication chap
!
! <<-- irrelevant output removed
!
interface Serial2/0
 ip address 192.168.10.1 255.255.255.252
 encapsulation ppp
 clockrate 64000
 ppp authentication chap
!
! <<-- irrelevant output removed
!
router ospf 5
 network 172.20.10.0 0.0.0.255 area 0
 network 172.22.1.0 0.0.0.255 area 0
 network 172.22.53.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.3 area 0
 default-information originate
!
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet0/0
no ip http server
!
dialer-list 1 protocol ip permit
!This defines all IP traffic as interesting.
!
line con 0
 login authentication NO_AUTHEN
 transport input none
line 97 102
```

```
line aux 0
line vty 0 4
!
end
```