

WHITE PAPERS from the files of Networking Unlimited, Inc.

WebQuery@NetworkingUnlimited.com

14 Dogwood Lane, Tenafly, NJ 07670

Phone: +1 201 568-7810

FAX: +1 201 568-7269

Using Dial-on-Demand Routing to Trigger Backup Links on Cisco Routers

Dr. Vincent C. Jones, PE

Version 1.1 -- 3 June 2000

Copyright © 1999,2000 Networking Unlimited, Inc. All Rights Reserved.

Cisco provides backup interface commands to support dial backup and bandwidth-on-demand. While these commands work well, particularly for bandwidth-on-demand, the requirement that the CSU/DSU lose carrier in order to trigger backup can result in unnecessary network outages. This white paper shows how floating static routes can be used with Cisco Dial-on-Demand Routing (DDR) to initiate dial backup based on routing table changes, a much more dependable source of reachability data.

Background

ISDN is frequently used to back up frame relay and other permanent links. However, use of the standard Cisco *backup interface* commands results in a solution which only backs up failures which cause the local frame relay interface to report failure. In the event of a failure which prevents communications but leaves the local line protocol up, such as a switch failure inside the frame relay network, the backup commands are not activated and communications remain down. While these modes of failure are far less frequent than local loop failure (which is handled correctly by the backup interface command set), they do occur in the real world and should trigger an ISDN call to route around the failure.

Cisco has recognized this shortcoming and introduced the *dialer watch* feature in IOS 12.0 to provide the ability to trigger backup action based on changes in the EIGRP routing tables. However, you do not need to upgrade to IOS 12 and change your routing protocol to EIGRP if you need this capability. With a little extra effort, dial-on-demand routing can be used to provide the same functionality with any current IOS release using any dynamic routing protocol. The trick is to use floating static routes to trigger dial-on-demand routing to bring up the ISDN link. Nor is the technique limited to ISDN backup of frame relay on Cisco routers. Any "dial-on-demand" capable interface from switched T1 to analog modems on the AUX port can be used to back up any "permanent" connectivity such as leased line, frame relay, or ATM.

Figure 1: Simple ISDN backup topology for frame relay

Figure 1 illustrates a simple scenario where two sites are connected by frame relay using ISDN for backup. While this configuration is simpler than most real networks, it shows how the theory of dial-on-demand backup functions without the distraction of additional connectivity. In practice, this technique can be applied to arbitrarily complex topologies limited only by the stability of the configuration and time available for design and implementation. The technique can be extended to allow automatically calling diverse locations to provide additional redundancy.

While this example uses a 2500 series remote and a 4700 series central router, the actual configuration is model independent. If other routers are used, the configurations would need to be modified to

match their requirements, however the general philosophy will remain consistent. Lets see how this works in practice.

Dial Backup using the Backup Interface Commands

Listings 1 and 2 show how the remote and core routers could be configured using the *backup interface* command set. This is the traditional way of configuring link restoral and works well for most failure modes. However, as already mentioned, failures which do not cause the local interface to fail will not be recognized and will not trigger the backup call. In addition, the backup link can only be used to back up one interface and testing of the ISDN interface is difficult to automate. On the other hand, if automated bandwidth augmentation is required, the *backup load* command remains the appropriate solution and dial-on-demand backup can not be used.

```
version 11.2
hostname Remote2524
!
username Core4700 password mumble
!
interface Ethernet0
 ip address 192.168.2.1 255.255.255.0
!
interface Serial0
 no ip address
 encapsulation frame-relay
!
interface Serial0.1 point-to-point
 ip address 192.168.1.5 255.255.255.252
 backup interface bri0
 backup delay 0 120
 frame-relay interface-dlci 101 broadcast
!
interface BRI0
 ip unnumbered Ethernet0
 encapsulation ppp
 no keepalive
 isdn spid1 20123456780000
 isdn spid2 20123456790000
 dialer idle-timeout 170
 dialer map ip 192.168.3.1 name Core4700 speed 56
 broadcast 12125551234
 dialer hold-queue 10
 dialer-group 1
 ppp authentication chap
!
router eigrp 1
 network 192.168.1.0
 network 192.168.2.0
 no auto-summary
!
ip host TestISDN 10.99.99.99
ip classless
```

```

ip route 0.0.0.0 0.0.0.0 192.168.3.1 150
ip route 192.168.3.1 255.255.255.255 BRI0
ip route 10.99.99.99 255.255.255.255 BRI0
!
dialer-list 1 protocol ip permit
!
line con 0
  password mumble
  login
line aux 0
  password mumble
  login
line vty 0 4
  password mumble
  login
!
scheduler interval 500
end

```

Listing 1: Backup interface remote router configuration

```

version 11.2 hostname Core4700
!
username Remote2524 password mumble
!
isdn switch-type primary-dms100
controller T1 0
  framing esf
  linecode b8zs
  pri-group timeslots 1-24
!
interface Loopback99
  ip address 10.99.99.99 255.255.255.255
!
interface Ethernet0
  ip address 192.168.3.1 255.255.255.0
  ip access-group 199 in
  ip access-group 99 out
!
interface Serial0
  no ip address
  encapsulation frame-relay
!
interface Serial0.1 point-to-point
  ip address 192.168.1.6 255.255.255.252
  bandwidth 56
  ip access-group 199 in
  ip access-group 99 out
  frame-relay interface-dlci 17
!
interface Serial0:23
  ip unnumbered Ethernet0
  encapsulation ppp
  bandwidth 100
  no keepalive
  dialer idle-timeout 300

```

```

dialer map ip 192.168.2.1 name Remote2524 speed 56
broadcast
dialer-group 1
ppp authentication chap
!
router eigrp 1
network 192.168.1.0
network 192.168.3.0
distribute-list 99 out Ethernet0
distribute-list 99 out Serial0.1
no auto-summary
!
ip classless
!
access-list 99 deny 10.99.99.99
access-list 99 permit any
access-list 199 deny ip any host 10.99.99.99
access-list 199 permit ip any any
dialer-list 1 protocol ip permit
!
line con 0
password mumble
login
line aux 0
password mumble
login
line vty 0 4
password mumble
login
!
scheduler interval 500
end

```

Listing 2: Backup interface core router configuration

Obviously system names, passwords, SPID numbers, ISDN switch type, and dialer map phone numbers need to be adjusted to match the local environment. Make sure that names and passwords are exactly the same, including matching case. Even though CHAP is not case sensitive on the system name, the dialer maps can be, which can create strange failures. The *speed 56* keyword in the dialer map is almost always required for North American inter-LATA ISDN calls. The default is to use the full 64Kbps ISDN bandwidth, which is rarely available on long distance calls and may not always be available even on local calls. Specifying *speed 56* ensures that the link will come up whether or not the connection is a 64Kbps clear channel.

Other ports, including con, aux and vtys should be configured to match local standards and have no impact on the ISDN backup and are included here only to provide a complete implementation example. Similarly, SNMP, logging, and other protocols should be specified as required.

Note that this sample configuration for the core router extracted from a production environment includes two "features" not in the published Cisco examples. First is the deliberate weighting of the ISDN link on the core side so it will be preferred to the frame link if both are up simultaneously. This should only be done if backup interface is being used only to backup the frame relay and not for bandwidth augmentation. Its primary function is to enable simplified testing using the Loopback99 IP address discussed in the next paragraph, but it also serves to enhance reliability by ensuring that the ISDN link is used immediately without waiting for the routing protocol to time out in the event that the frame relay failure detected by the remote has not yet propagated to the core router interface.

The second "feature" is the strange definition of Loopback99. This address is defined, then filtered out of all EIGRP advertisements and blocked at all interfaces except ISDN. Its function is to provide a target that can be pinged from a remote router after bringing up the ISDN link that will only succeed if the IP packets to and from the core actually travel over the ISDN link. Otherwise, the only way to be sure the ISDN link is truly working is to shutdown the frame link and wait for the ISDN link to come up and then communicate over it. This mode of testing is clearly not appropriate while production traffic is present so we provide a non-destructive mode of testing that we can be confident will actually prove that the ISDN link is capable of carrying traffic.

Note that if your core routers do not have the CPU capacity to handle all the filtering, the filters could be moved to the remote routers. If all routers are so overburdened that the extra loopback and filters can not be tolerated, there are other ways to check to see if the ISDN line is apparently functional, such as checking EIGRP neighbors, but they are nowhere near as convenient and much harder to automate.)

If other routers or routing protocols are used, the configurations would need to be modified to match their requirements, however the general philosophy will remain consistent. As we shall see when we implement dial-on-demand backup for higher reliability, one major advantage of the backup interface command set is its simplicity, reducing the probability of configuration errors and simplifying maintenance.

Dial Backup Using Dial-on-Demand Routing

Dial-on-Demand Routing (DDR) depends upon "interesting" packets to destinations known to be at the other end of the dial link to bring up the dial link (and to keep it up). Since we can not be sure that there will be interesting traffic occurring naturally, we include a logging specification in the remote configuration with a target on the core LAN.

That way, even if there is a natural pause in normal traffic at the same time as the frame link fails, the syslog entries reporting the state change will force the ISDN link up immediately, minimizing the delays seen when normal data traffic resumes.

On the remote system which will be placing the call we define interesting as any packets other than EIGRP routing protocol packets (access list 102, see Listing 3). The time-out before dropping the link should be adjusted with care. Too long and money is wasted keeping up an ISDN link after it is no longer required. Too short, and the link may drop while there is still traffic to be carried or if the frame relay link "hiccups" on the way back up. The 170 second value was chosen in this case because the local telco billed a flat rate for the first three minutes. This value allowed testing the link at minimum cost, yet kept the link up as long as possible otherwise to minimize the potential of premature drops.

```
version 11.2 hostname Remote2524
!
username Core4700 password mumble
!
interface Ethernet0
 ip address 192.168.2.1 255.255.255.0
!
interface Serial0
 no ip address
 encapsulation frame-relay
!
interface Serial0.1 point-to-point
 ip address 192.168.1.5 255.255.255.252
 bandwidth 56
 frame-relay interface-dlci 101 broadcast
!
interface BRI0
 ip unnumbered Ethernet0
 encapsulation ppp
 bandwidth 20
 no keepalive
 isdn spid1 20123456780000
 isdn spid2 20123456790000
 dialer idle-timeout 170
 dialer map ip 192.168.3.1 name Core4700 speed 56
 broadcast 12125551234
 dialer hold-queue 10
 dialer-group 1
 ppp authentication chap
!
router eigrp 1
 network 192.168.1.0
 network 192.168.2.0
 no auto-summary
!
ip host TestISDN 10.99.99.99
```

```

ip classless
ip route 0.0.0.0 0.0.0.0 192.168.3.1 150
ip route 192.168.3.1 255.255.255.255 BRI0
ip route 10.99.99.99 255.255.255.255 BRI0
!
access-list 102 deny eigrp any any
access-list 102 permit ip any any
!
logging 192.168.3.99
dialer-list 1 protocol ip list 102
!
line con 0
  password mumble
  login
line aux 0
  password mumble
  login
line vty 0 4
  password mumble
  login
!
scheduler interval 500
end

```

Listing 3: Dial-on-Demand Routing remote router configuration

The changes to the configuration, while at first glance superficial, are quite critical. Two lines are removed (the *backup interface* and *backup delay* lines on the frame relay interface) and a number of lines are added. The added lines implement two functions to control the utilization of the ISDN line. The *bandwidth* statements added to the frame relay and ISDN interface definitions assure that all traffic to the core will flow over the frame relay interface if it is up. If the ISDN link was considered better than or equal to the frame relay link (which it would if we used "honest" bandwidth statements), traffic would never stop flowing through the ISDN link once it came up and it would never drop regardless of the state of frame relay.

The *access-list 102* and its assignment to the dialer prevent the EIGRP multicasts which are always being generated by the ISDN interface from bringing up the link. The EIGRP multicasts are not actually blocked, as we need the routing protocol to function over the ISDN link. The *dialer-list* definition just defines them as "not interesting" and all other IP traffic as "interesting" and worthy of bringing up and keeping up the ISDN link.

The configuration of the core side is unchanged. This allows the same core configuration to support both dial-on-demand and backup interface modes. The 300 second idle time-out at the core should

never be invoked, as the remote system will drop the link after only 170 seconds of inactivity. It is included, however, because networks do not always work properly and you do not want to leave an unneeded link up forever simply because the remote failed to drop the line. The time-out can also be a good way to spot configuration or router errors. If a remote starts calling in with a series of five minute calls, you know that something is wrong and that while the remote thinks the link is up, the core is not using it.

The static routes at the remote are essential. They are the only way the remote router knows that the dial link can be used to reach the destination until the link comes up and routing tables are exchanged. This configuration assumes a hub and spokes architecture where all non-local traffic from a remote must be routed through the core regardless. Conversely, if there are multiple frame relay links to the remote, the dial-on-demand configuration can be configured to respond either when any link goes down (choosing the dialer map for the appropriate destination) or only when all links are down (ensuring that the remote is never totally cut off). The former situation would be most useful when the remote is carrying transit traffic for delivery to other remotes.

Backup Interface versus Dial-on-Demand Trade-offs

Typical of most network decisions, the choice of backup interface command set or dial-on-demand routing command set to implement link backup is not always a clear choice. Each approach has its advantages and its disadvantages, and whether a particular feature is an advantage or a disadvantage will depend upon the application. Some of the more critical trade-offs include speed of response to failure, reliability of response to failure, call stability, testability, and link performance.

Speed of Response to Failure: When properly configured, either approach will respond immediately to the remote's frame relay link going down hard. However, with dial-on-demand, the first few data packets following a failure could be delayed or lost if event logging or the equivalent is not configured to force dialing.

Reliability of Response to Failure: Backup Interface commands will only respond to an interface failure which the router can detect as a physical or link layer down on the interface. Any event which can trigger the backup interface commands will also immediately remove the associated destinations from the routing tables and generate a syslog entry forcing dial-on-demand to immediately raise the link. Conversely, failures inside the WAN which do not cause the router

interface to go down will eventually be detected by the routing protocol, so that dial-on-demand will still bring up the link after the routing protocol discovers the failure whereas IOS 12.0 is required to get this functionality for backup interface.

Call Stability: Backup interface will keep the dial link up until the link being backed up is returned to service. If there is very little traffic, this could mean that the link is being kept up unnecessarily. On the other hand, dial-on-demand requires traffic to keep the link up, so if there is insufficient traffic the link may drop when it should be up. Taking advantage of the cost savings possible with dial-on-demand also requires configuring the core router to allow it to dial out to the remote unless either all traffic originates from the remote or there is enough traffic to ensure the link will never drop while required.

Testability: Testing the ISDN link when using backup interface requires going into configuration mode on the remote router, removing the backup interface command from the running configuration, verifying that the ISDN link comes up correctly and the remote can ping the ISDN test address, then restoring all backup interface commands defined on the interface. This is not only a cumbersome procedure, but also a risky one from the viewpoint of security, as it requires the ability to reconfigure the router and there is nothing to prevent adjusting other parameters other than the integrity of the operator or script writer. Alternatively, backup interface can be tested by downing the frame relay interface and waiting for ISDN backup to restore communications. However, this mode of testing disrupts production traffic, particularly if the ISDN tests uncovers a problem with ISDN backup.

Testing the ISDN link when using dial-on-demand merely requires logging into the remote router and executing the command "ping TestISDN" at the command prompt. If the ping succeeds, the ISDN link is functional and able to carry traffic when required. Executive mode is not required nor is production traffic affected while the testing is executed, even if the testing is automated and executed while the ISDN link is already in use carrying production traffic.

Link Performance: Backup interface has the advantage that the ISDN line can be used not only for backup, but also for bandwidth augmentation. The ability to use the ISDN line for additional bandwidth is lost when using dial-on-demand. On the other hand, when using dial-on-demand, the same ISDN line can be used to back up multiple interfaces.

Summary

In many scenarios, using dial-on-demand routing for backing up permanent links can be a superior solution to the backup interface command approach, particularly if the goal is to maximize network reliability and uptime. However, the decision must be made with full knowledge of the strengths and weaknesses of both approaches, and the correct approach will be strongly dependent upon the network architecture, user requirements, and typical and worst case traffic flows. While example configurations for both approaches are provided for illustration, there are many variations possible depending upon specific requirements and the examples should only be considered a starting point.