
TransPort
Training
Program
TT010 – SRI and SureLink
Stateful Route Inspection
Surelink
Public - © Digi International, Inc.
www.digi.com

Stateful Route Inspection

- The Digi routing code stack contains a sophisticated scripted “Stateful Firewall” and “Route Inspection” engine.
- Stateful inspection is a powerful tool that allows the unit to keep track of a TCP/UDP or ICMP session and match packets based on the state of the connection on which they are being carried.
- In addition to providing sophisticated Firewall functionality the SF/RI engine also provides a number of facilities for tracking the “health” of routes, marking “dead” routes as being Out Of Service (OOS) and creating rules for the automatic status checking of routes previously marked as OOS (for use in multilevel backup/restore scenarios)

Stateful Route Inspection

- The firewall may be used to place interface into an OOS state and also control how the interfaces return to service. When an interface goes OOS, all routes configured to use that interface will have their route metric set to 16 (the maximum value), meaning that some other route with a lower metric will be selected.

Stateful Route Inspection

- When a firewall stateful inspection rule expires, a decision is made as to whether the traffic being allowed to pass by this rule completed successfully or not.
- For example, if the stateful rule monitors SYN and FIN packets in both directions for a TCP socket then that rule will expire successfully.
- However, if a SYN is seen to pass in one direction but no SYN ACK pass in the other direction, the stateful rule will expire and the unit will tag this as a failure.

Stateful Route Inspection

- The following conditions tag a stateful rule as a failure:
  - Packets have only passed in one direction
  - 10 packets have passed in one direction with no return packets (for TCP the packets must also be re-transmits)

  All of the SRI features depend upon the stateful inspection capabilities of the firewall engine, so the firewall needs to be enabled for these features to be used.

SureLink / Dead-Link Detection

- Dead link detection is used on working PPP connections
- Cellular TransPort routers will monitor the PPP connection attempts by default
- If a cellular PPP connection fails to connect after 10 attempts, the cellular module will be power cycled.
  - This helps recover from an error condition in the module and also causes the module to re-register with the network in attempt to get a working PPP connection
  - This is configurable
- Cellular module power cycling will be seen in the event log as **GPRS link failed -> power cycle**

SureLink / Dead-Link Detection

- SureLink and the following dead-link detection methods all use the firewall and stateful route inspection.

Dead-Link Scenario

- Problems may occur with an interface that does not result in the interface disconnecting or an interface deactivation failure.
  - i.e. The TransPort thinks it still has a valid IP connection, but something has happened and no traffic is able to pass.
  - This is known as a *dead-link* scenario.
- Site visits to reboot a unit are very expensive!
- TransPort routers have several different mechanisms for detecting and recovering from such a network problem.
- It is recommended that every cellular configuration contain dead-link detection.

SureLink Wizard

- SureLink wizard makes configuration of these dead-link detection methods simpler.
- SureLink will detect when IP traffic is unable to use the WAN link. Traffic is seemingly sent, but link is dead.
- Time based, passive and active methods.
- Can monitor 2 way UDP traffic.
- Can deactivate the PPP link when an IPsec VPN fails to establish after a specified number of attempts.

SureLink

- The modemcc entity will monitor the activation and connection attempts to the mobile network (RF level).
- If 10 network connection attempts fail, the cellular module will be power-cycled.

  The PPP entity can be configured to reboot the router after a specified number of PPP connection failures.
  In theory, this should not be required as disconnecting the PPP interface and power-cycling the cellular module should fix nearly all problems connecting to the network.

SureLink and Dual SIM

As we work though, notice that:

the **SureLink / Dead-Link detection** feature

and

the **Dual SIM failover** configuration

Use many of the same configuration parameters.

- This will help with understanding the configuration.

Detecting a dead-link

- The solution is to detect the dead-link and deactivate the interface.
- There are two main types of dead-link detection
  - Active

    Generate ICMP traffic
  - Passive

    Monitor TCP or UDP traffic

    Time based, expects the router to *receive* traffic within a specified number of seconds

Active link failure detection

- An active detection mechanism sends traffic out the interface in order to test it.
  - This has the advantage of working whether or not the interface is being used for normal traffic.
- It does not matter from which end (site or central location) normal traffic is initiated
- There can be a cost associated with sending data to test the link, depending on how the wireless WAN plan is billed

Passive link failure detection

- A passive detection mechanism will monitor the IP traffic and detect if there is a problem with it.
  - Such as a TCP connection failure or excessive TCP re-transmits
- Passive detection only works if LAN hosts behind the TransPort router *initiate* the IP traffic.
- IPsec Tunnels have detection available via Dead Peer Detection.
  - The parameter 'Disconnect interface after this many consecutive auto-negotiation failures' (or 'go out of service after x consecutive auto negotiation failures') will cause the PPP link to disconnect if an IPsec VPN fails to be established after the specified number of tries.
- Time based option will disconnect the PPP interface is no traffic is received within a specified number of seconds. This may result in the PPP interface being disconnected when it didn't need to be.

The IPSec (eroute) detection mechanism uses DPD. So it somewhat blurs the line between passive and active since the DPD function does generate active data. The current SureLink wizard has this function listed under Active configuration.

The IPSec "Go out of service if automatic establishment fails" applies to the eroute. However it is NOT related to dead link detection or SureLink.

"Disconnect interface after this many consecutive auto-negotiation failures" – refers to the PPP interface not the Eroute. In the current Web GUI (as of firmware version 5139) this parameter has been unhelpfully renamed to "go out of service after x consecutive auto negotiation failures" in the new web GUI.

Detecting a dead-link

- Link failure detection is often done with help of the firewall.
- Before looking at the methods, a quick overview of the firewall rule used of link failure detection will help.

```
pass out break end on ppp 1 proto tcp from any
to 82.68.226.27 port=http flags S!A inspect-
state oos 1 t=5 c=2 d=2
```

This firewall rule is allowing traffic outbound to a web server.

The dark blue syntax is what we're interested in now.

Detecting a dead-link

```
pass out break end on ppp 1 proto tcp from any
to 82.68.226.27 port=http flags S!A inspect-
state oos 1 t=5 c=2 d=2
```

oos secs {t=secs} {c=count} {d=count}

This parameter allows the stateful inspect engine to mark as "out of service" any routes that are associated with the specified interface and also to control how and the interfaces are returned to service. Such routes will only be marked as out of service if the specified oos option parameters are met.

Detecting a dead-link

```
pass out break end on ppp 1 proto tcp from any
to 82.68.226.27 port=http flags S!A inspect-
state oos 1 t=5 c=2 d=2
```

oos secs {t=secs} {c=count} {d=count}

This puts the associated routes out of service for 1 second only.

This is fine, because the following syntax will be deactivating the PPP link.

Detecting a dead-link

```
pass out break end on ppp 1 proto tcp from any
to 82.68.226.27 port=http flags S!A inspect-
state oos 1 t=5 c=2 d=2
```

oos secs {t=secs} {c=count} {d=count}

This specifies the length of time in seconds the unit will wait for a response the packet that matched the rule.

Detecting a dead-link

```
pass out break end on ppp 1 proto tcp from any
to 82.68.226.27 port=http flags S!A inspect-
state oos 1 t=5 c=2 d=2
```

oos secs {t=secs} {c=count} {d=count}

This specifies the number of times that the stateful inspection engine must trigger on the rule before the **route** is marked as out of service.

2 packets without a response = failure

Detecting a dead-link

```
pass out break end on ppp 1 proto tcp from any
to 82.68.226.27 port=http flags S!A inspect-
state oos 1 t=5 c=2 d=2
```

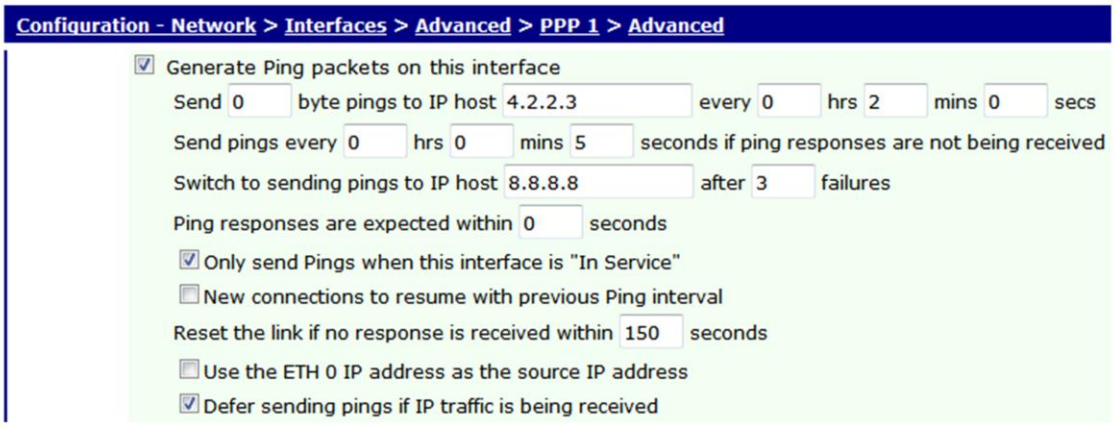
oos secs {t=secs} {c=count} {d=count}

This specifies the number of times that the stateful inspection engine must trigger on the rule before the **interface** is deactivated.

2 packets without a response = failure

Auto Ping – Active method (manual configuration)

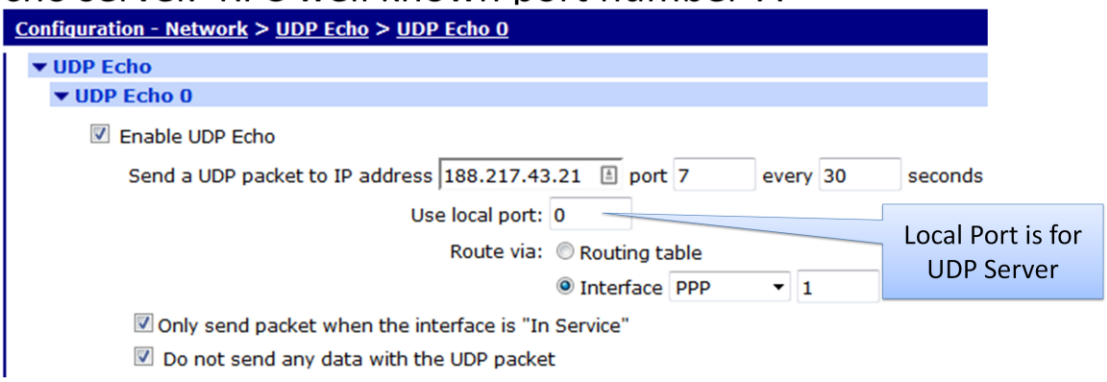
- ***Configuration - Network > Interfaces > Advanced > PPP 1 > Advanced***



This method does not require the use of the firewall. All the configuration is done in this part of the GUI.
However, it IS possible to just configure the auto pings with an IP address and a ping interval, this will generate pings. The firewall can then be used to monitor the pings.

UDP Echo – Active method (manual configuration)

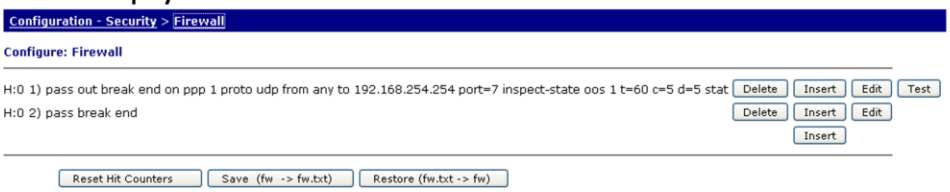
- ***Configuration - Network > UDP Echo > UDP Echo 0***
- Configure the UDP client to send UDP packets to a UDP echo server. RFC well known port number 7.



It may be preferable to send UDP echoes through a an IPsec VPN to a server on a remote LAN.
Windows PCs will respond to UDP echo on port 7, just enable Simple TCP/UDP services.

UDP Echo – Active method (manual configuration)

- This UDP traffic must be monitored using the TransPort firewall.
- Configure the firewall to monitor the UDP packets and drop the link after 5 no replies in a row allowing 60 seconds for each reply.

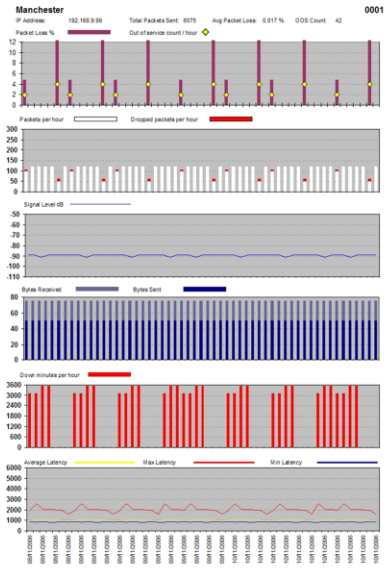



```
pass out break end on ppp 1 proto udp from any
to xxx.xxx.xxx.xxx port=7 inspect-state oos 1
t=60 c=5 d=5 stat
```

UDP Echo – Active method (manual configuration)

- When using UDP echo technique with the ‘stat’ keyword, Digi Remote Manager can collect stats and draw performance graphs for each site

- There is a separate module covering Remote Manager.



Monitoring TCP traffic

- This is a PASSIVE technique
- It requires that outbound TCP connections are routinely initiated from hosts behind the TransPort router.

Monitoring TCP traffic

- The following rule will detect:
  - A failure for a TCP/23 (telnet) connection to establish.

```
pass out break end on ppp 1 proto tcp from any to 192.168.254.60 port = 23 flags
S!A inspect-state oos 1 t=10 c=2 d=2
```

  - 10 seconds are allowed for the TCP connection to be established
  - 2 attempts in a row fail must fail (allowing 10 seconds for each attempt) then the interface will be deactivated and the route will be set OOS until the interface comes back up again.

Every project is different and the values for t, c and d should be chosen carefully after testing.

Hand-On Practical Session – Dead-Link Detection

Create a firewall rule to detect a problem with a TCP connection and automatically deactivate the PPP link

Hand-On Practical Session – Dead-Link Detection

1. Configure the WAN interface to connect to the Internet in "always on" mode
2. Turn on the firewall for the WAN interface
3. Choose an address to establish a TCP connection to e.g. a web server. Ensure you have some means to disable this address.
4. Add a TCP firewall rule to monitor the connection

example :

```
pass out break end on ppp 1 proto tcp from any to
192.168.254.60 port = 80 flags S!A inspect-state oos
1 t=5 c=2 d=2
```

Hand-On Practical Session – Dead-Link Detection

- Check that you can connect to the TCP host
- Disable the TCP host
- Try to connect again and monitor the status of the WAN interface
- Inspect the event log

Hand-On Practical Session – SureLink

- Reset the config to remove the previous settings.
- Use the SureLink Wizard to configure the router to monitor the same TCP session to the same web server.
- The SureLink Wizard makes configuration easier.

End of Hand-On Practical Session

Advanced Automatic Failover

Advanced Automatic Failover

- From the last section, the TransPort firewall can be used to detect errors on the primary interface (which can be most any interface).
- TransPort firewall monitors the primary connection. If the test fails:

1. Primary interface is marked *out of service* (OOS)
2. Secondary interface is then used to route IP data
3. Primary interface is re-connected and continually tested (Tests can use ICMP or TCP data)
4. Primary interface is brought back into service only when tests complete successfully

Advanced Automatic Failover

- This same concept is used for SIM failover

AN14 - Configure a dual SIM cellular router to automatically failover to a 2nd SIM unit a timeout occurs, then revert to SIM 1

AN15 - Configure a dual SIM cellular router to automatically failover to a 2nd SIM and remain using SIM 2 until a failure occurs, then revert to SIM 1

Error Detection, Testing and Recovery

```
pass out break end on ppp 1 proto tcp from any to
82.68.226.27 port=http flags S!A inspect-state
oos 1 t=5 c=2 d=2 r=tcp,120,10 rd =1 dt=1
```

- The above example will demonstrate how the firewall can be used to spot a TCP connection to a nominated web server failing and back up to an alternative interface

- The firewall rule includes a recovery capability which means that it will test the TCP connection before allowing the interface to come back into service

Error Detection, Testing and Recovery

```
pass out break end on ppp 1 proto tcp from any to
82.68.226.27 port=http flags S!A inspect-state
oos 1 t=5 c=2 d=2 r=tcp,120,10 rd =1 dt=1
```

OOS time is 1 second

5 Seconds are allowed for a response packet

2 consecutive failed packets before route is set OOS

2 consecutive failed packets before interface is down

Error Detection, Testing and Recovery

```
pass out break end on ppp 1 proto tcp from any to
82.68.226.27 port=http flags S!A inspect-state
oos 1 t=5 c=2 d=2 r=tcp,120,10 rd=1 dt=1
```

This specifies the recovery procedures will consist of TCP connection attempts executed at 2 minute (120 second) intervals.

10 seconds will be allowed for each recovery attempt. (You may wish to allow extra interface activation time in the case of the oos interface being deactivated.)

Error Detection, Testing and Recovery

```
pass out break end on ppp 1 proto tcp from any to
82.68.226.27 port=http flags S!A inspect-state
oos 1 t=5 c=2 d=2 r=tcp,120,10 rd=1 dt=1
```

Sometimes it may be desirable to deactivate the interface when the testing is complete. If this is required then the following options are available:

rd=1 (deactivate after a recovery failure)

rd=2 (deactivate after a recovery success)

rd=3 (deactivate after either recovery success or recovery failure)

Error Detection, Testing and Recovery

```
pass out break end on ppp 1 proto tcp from any to
82.68.226.27 port=http flags S!A inspect-state
oos 1 t=5 c=2 d=2 r=tcp,120,10 rd=1 dt=1
```

This option indicates the interface is to remain out of service when it is disconnected. If it is not an always-on interface, this specifies the time in seconds at which the interface is reactivated for testing.

Hand-On Practical Session – Failover and recovery

Complete one or more of the following:

- Failover from Ethernet to cellular
  - see AN41
- ADSL Backup to PSTN, ISDN or Cellular
  - For failover to PSTN or ISDN see AN34;
  - to cellular use AN 35
- Dual SIM failover
  - see AN14 and AN15
  - Hint: use the **Wizard**, then look at details

End of Hands-On Practical Session