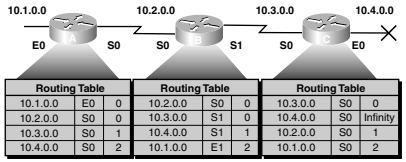
Example of Route Poisoning

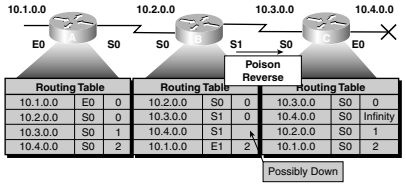


The figure provides the following example: When network 10.4.0.0 goes down, Router C "poisons" its link to network 10.4.0.0 with an infinite cost (marked as unreachable).

Router C is no longer susceptible to incorrect updates about network 10.4.0.0 coming from neighboring routers that might claim to have a valid alternative path. After the hold-down timer expires (which is just longer than the time to convergence), Router C begins accepting updates again.

Poison Reverse

When Router B sees the metric to 10.4.0.0 jump to infinity, it sends a return message (overriding split horizon) called a *poison reverse* back to Router C, stating that network 10.4.0.0 is inaccessible. This message ensures that all routers on that segment have received information about the poisoned route.



Avoiding Routing Loops with Triggered Updates

A triggered update is sent immediately in response to a change in the network. The router detecting the change immediately sends an update message to adjacent routers, which then generate their own triggered updates. This continues until the network converges. There are two problems with triggered updates:

- The update message can be dropped or corrupted.
- The updates do not happen instantly. It is possible that a router issued a regular update before receiving the triggered update. If this happens, the bad route can be reinserted into a router that received the triggered update.

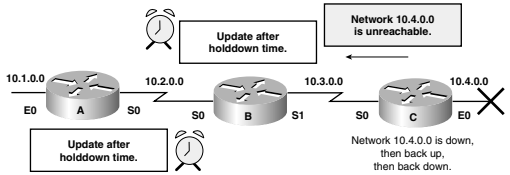
The solution is as follows: Hold-down timers dictate that when a route is invalid, no new route with a same or worse metric will be accepted for the same destination for a certain period of time. This allows the triggered update to propagate throughout the network.

Characteristics of Hold-Down Timers

- They are used to prevent regular update messages from inappropriately reinstating a route that might have gone bad.
- Hold-down timers force routers to hold any changes for a period of time.
- The hold-down period should be calculated to be just greater than the amount of time it takes for updates to converge.

Hold-Down Implementation Process

1. When a router receives an update that a network is down, the router marks the route as inaccessible and starts a hold-down timer.



2. If an update is received from a neighboring router with a better metric, the router removes the timer and uses the new metric.
3. If an update with a poorer metric is received before the hold-down timer expires, the update is ignored.
4. During the hold-down period, routes appear in the routing table as "possibly down."

Distance Vector Routing Summary

- Distance vector routing protocols maintain routing information by updating routing tables with neighboring routing tables.
- Defining a max count prevents infinite loops.
- Split horizon solves routing loops by preventing routing updates from being sent back in the same direction from which they came.
- Route poisoning sets downed routes to infinity to make that route unreachable.
- A triggered update is sent immediately in response to a change. Each router receiving a triggered update sends its own until the network converges.
- Hold-down timers prevent regular update messages from reinstating failed routes.
- More than one loop-preventing solution can be implemented on networks that have multiple routes.