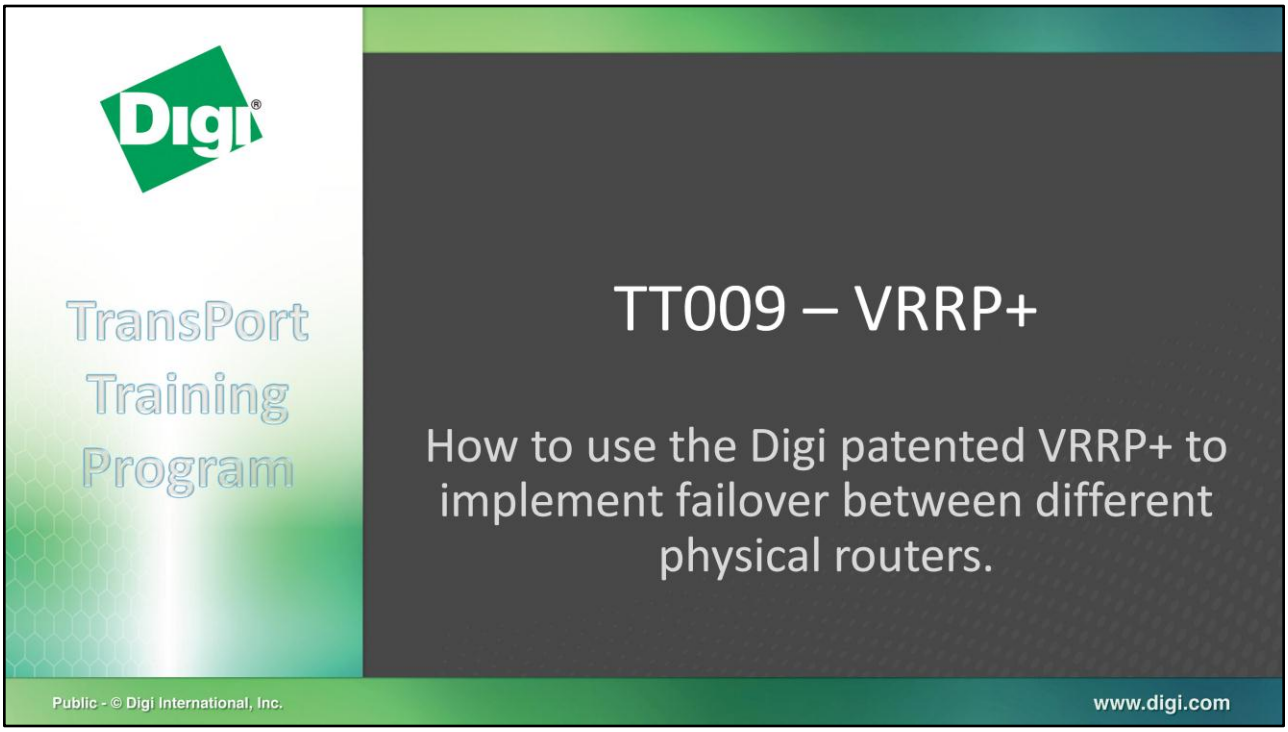

TransPort
Training
Program
TT009 – VRRP+
How to use the Digi patented VRRP+ to implement failover between different physical routers.
Public - © Digi International, Inc.
www.digi.com

TransPort as Default Gateway

- Option 1 of 2:
  Use a TransPort as the default gateway and have it choose the appropriate WAN
  - Advantages: easier to configure and test (possibly), other router does not need to support VRRP
  - Disadvantage: single point of failure
- Or use the “other” router as the default gateway
- Similar in concept to AN41 - **Using Ethernet as the default route with failover to a cellular connection**. Simply use an Ethernet interface (with gateway programmed with IP of other WAN router) instead of either the ADSL or PSTN PPP interfaces.

TransPort with VRRP+

- Option 2 of 2: Use VRRP+
- TransPort shares IP address with other WAN router. Normally other WAN router will have higher VRRP priority, but TransPort will send test packets through other WAN router and raise its priority when other WAN router or other router's WAN network fails.
  - Advantage: no single point of failure
  - Disadvantage: other router must support VRRP

A roadblock to this might be if dynamic routing using proprietary protocols, like EIGRP, are required.

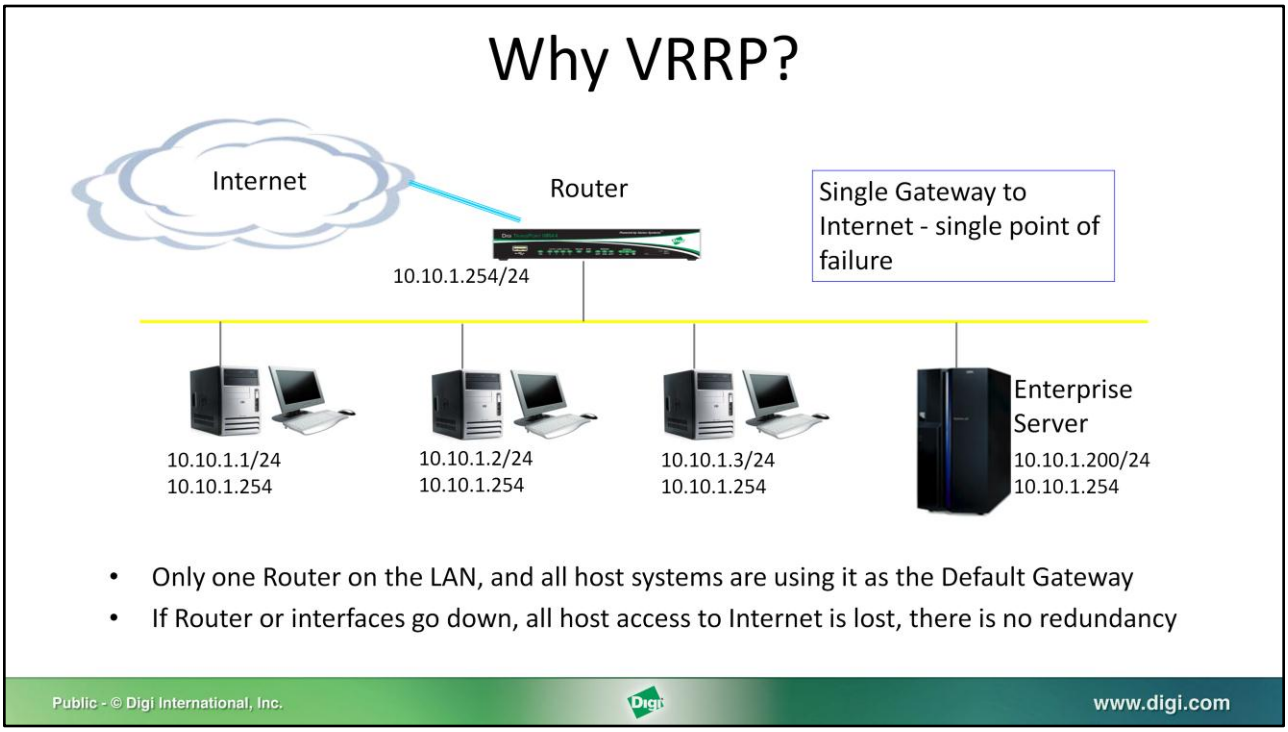
VRRP Overview & Standards

- A non-proprietary redundancy protocol
- Designed to increase the availability of the Default Gateway service for hosts on same subnet
- Uses the concept of a 'Virtual Router'
- Detailed in the IETF RFC 3768
- VRRP can be used over Ethernet and MPLS
- VRRP is widely used, although many vendors have designed their own versions and additions offering improved operation and/or enhanced features
  - E.g., Cisco's HSRP, Nortel's RSMT, Digi's VRRP+

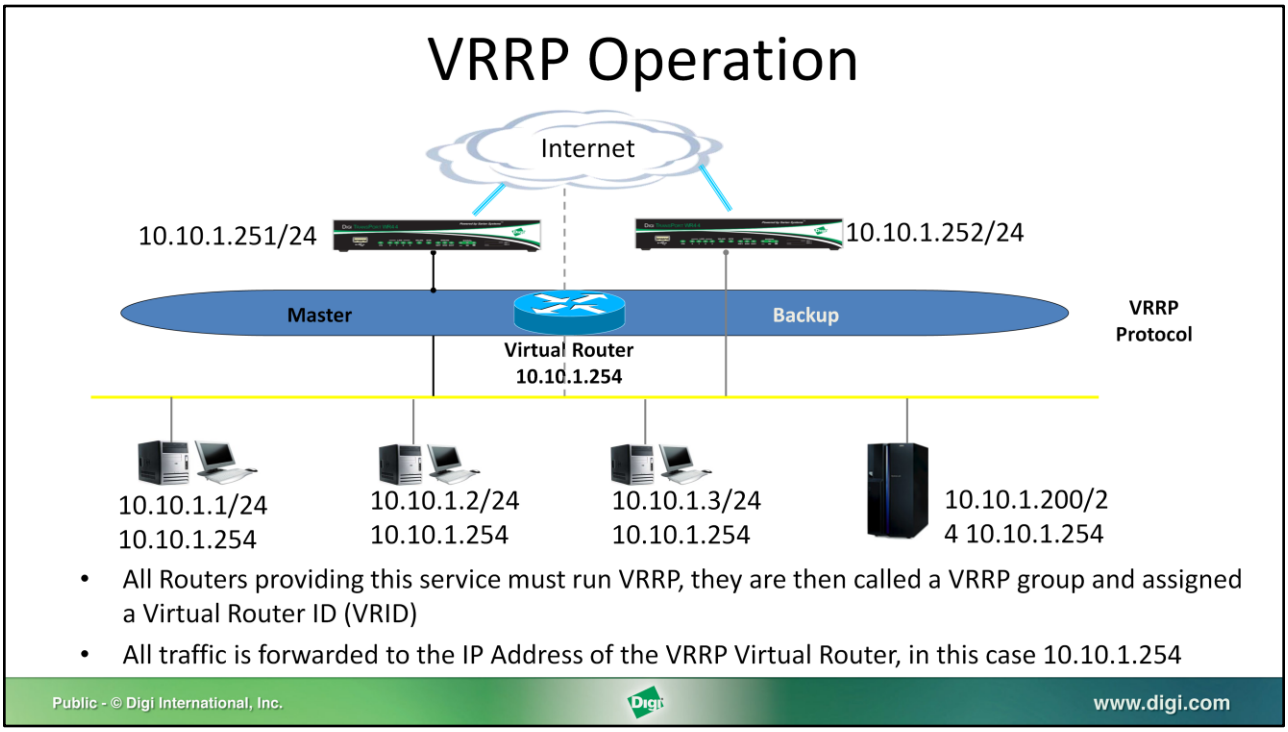
Note: VRRP is not a routing protocol - it does not advertise IP routes or affect the routing table in any way.

(VRRP Can also be used over FDDI/Token Ring)

HSRP (Hot Standby Router Protocol) is the Cisco proprietary Router redundancy protocol and is described in detail in RFC 2281
GLBP (Gateway Load Balancing Protocol) is a Cisco proprietary protocol that attempts to overcome the limitations of existing redundant router protocols by adding basic load balancing functionality
The *Common Address Redundancy Protocol* or CARP is a protocol which allows multiple hosts on the same local network to share a set of IP addresses, OpenBSD developers started CARP as an alternative to the patented VRRP (To avoid the Cisco Patented material in VRRP)
Routed Split Multilink Trunking Nortel Networks proprietary router redundancy solution. Puportedly provides the same services as VRRP, but more efficiently and quicker.

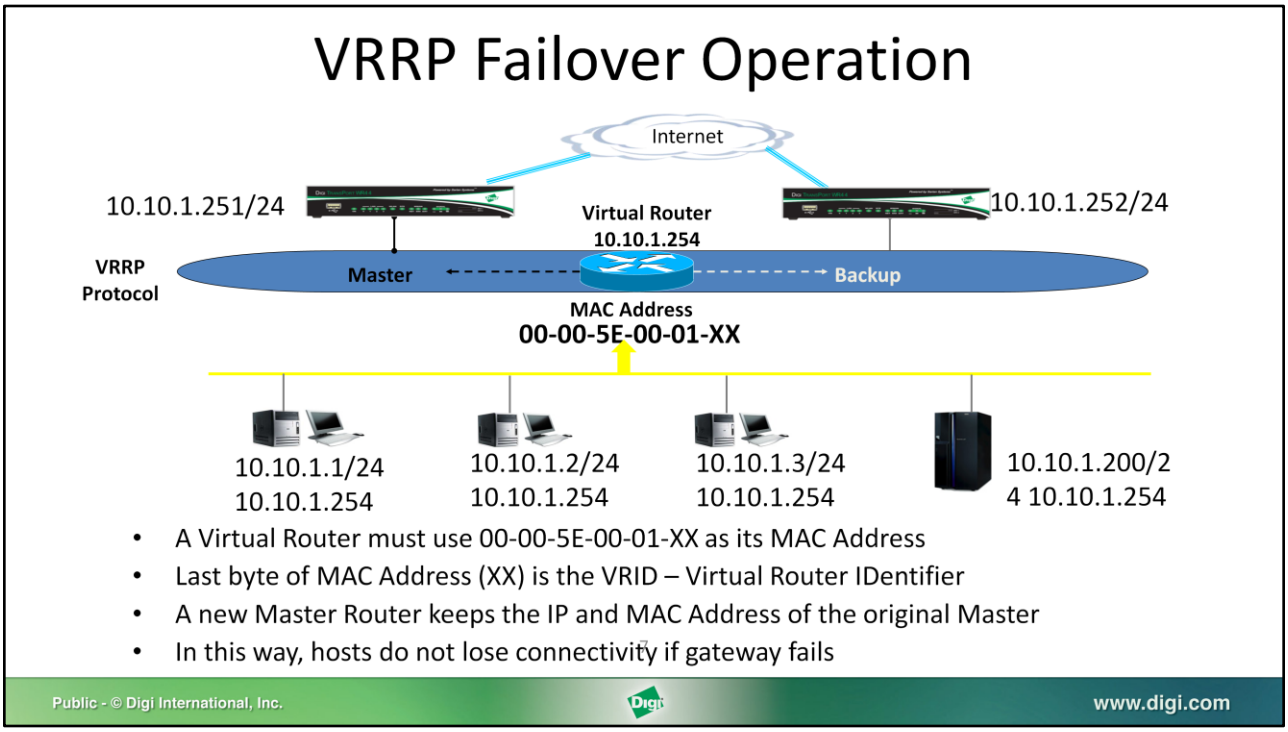


Short for ***V**irtual **R**outer **R**edundancy **P**rotocol*, an election protocol that dynamically assigns responsibility for one or more virtual router(s) to the VRRP router(s) on a LAN, allowing several routers on a multiaccess link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP setup, one router is elected as the master router with the other routers acting as backups in case of the failure of the master router.



•Here we have a diagram that is used to illustrate how VRRP works, not how it would necessarily be implemented
•VRRP allows a failover mechanism for the default router without hosts having to re-configure
•All of The routers involved in this must run the VRRP protocol
•They are then referred to as a VRRP virtual router group, and are assigned a Virtual Router ID (VRID)
•A virtual router group is a group of routers having a logical association and reducing the risk of a single point of failure
•Election of the master and backups in the event of a failure is by administratively assigned priorities (1-255, 0 has special significance), the IP address is used a tie breaker if priorities are the same
•The master is responsible for responding to ARP requests for the IP Address of the virtual router, and this also implies it has the responsibility to forward the packets forwarded to the Virtual MAC Address of the virtual router

•**Optional discussion (Load sharing)**
•One of problems is that 2nd router (or more) is completely idle, a waste of resources
•Could assign the 2nd router as a default router to a number of other hosts
•This effectively establishes a load-sharing scheme
•However this would not afford failover protection to the 2nd group of hosts
•So what we would need to do is create a 2nd Virtual Router Group, and in the diagram the master of the 2nd group would be 10.10.1.252 and the backup would be the master of the 1st group
•With this arrangement, we establish a load sharing mechanism, and a failover protection for each group. Obviously there may be some service degradation if one of the routers fails

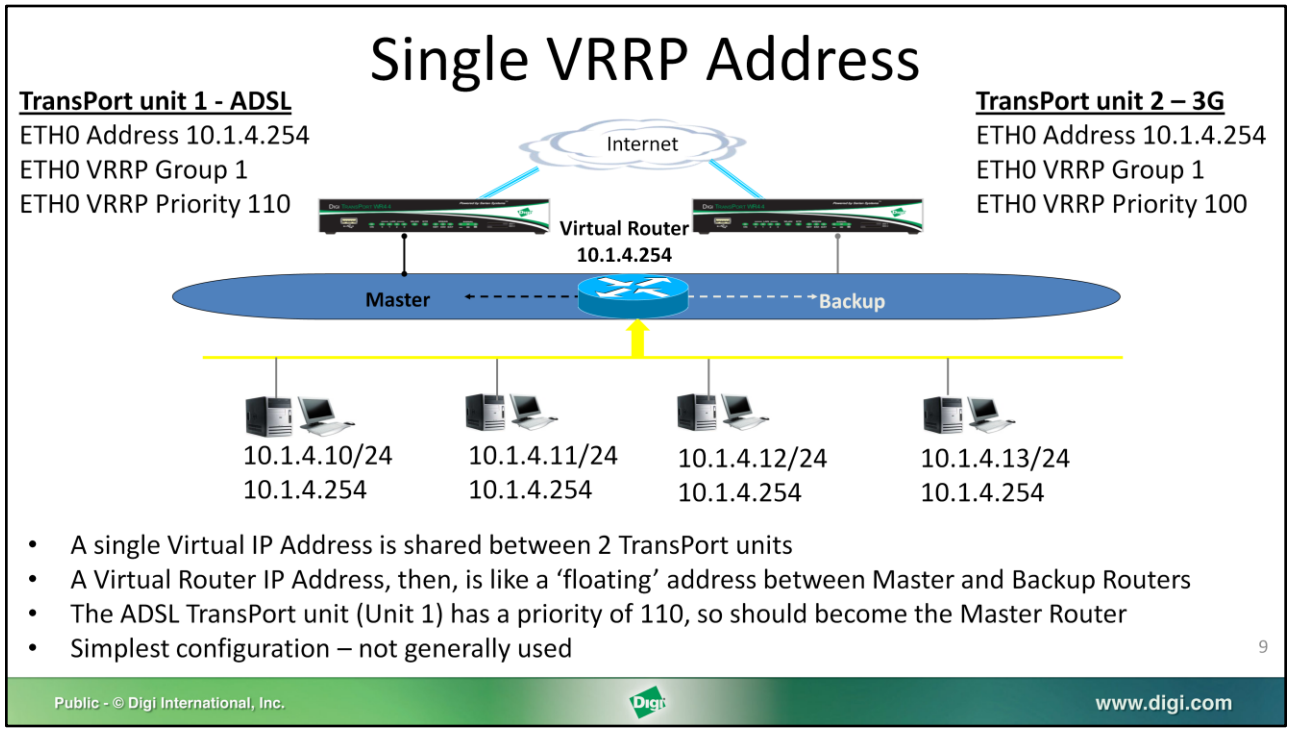


A virtual router must use 00-00-5E-00-01-XX as its Media Access Control (MAC) address. The last byte of the address (XX) is the Virtual Router IDentifier (VRID), which is different for each virtual router in the network. This address is used by only one physical router at a time, and is the only way that other physical routers can identify the master router within a virtual router. Physical routers acting as a virtual routers must communicate within themselves using packets with multicast IP address 224.0.0.18 and IP protocol number 112.
Master routers have a priority of 255 and backup router(s) can have priority between 1-254. When a planned withdraw of a master router is to take place, it changes its priority to zero which forces a backup router to take up the master router status more quickly. This is in order to reduce the black hole period.

VRRP is a protocol between IP routers that allows backup routers to monitor the status of a master router. When the master router fails, the backup router can take over the function of the master router. The new master router keeps the IP and MAC address of the original master, so that hosts that are configured with a single default gateway do not have their network connectivity disrupted if the gateway fails.
With VRRP enabled, the master router sends out regular VRRP packets to indicate that it is alive. If the VRRP packets stop, the backup router adopts the IP and MAC address of the master, in addition to its own IP and MAC addresses. If you have more than one backup router, the router with the highest priority becomes the master router

TransPort VRRP Implementations

- You can implement VRRP on the TransPort units in a number of different ways depending on requirements
  - Single VRRP Address
  - Dedicated VRRP Address
  - The TransPort VRRP+ Implementation



This uses a single Virtual IP address shared between two units.

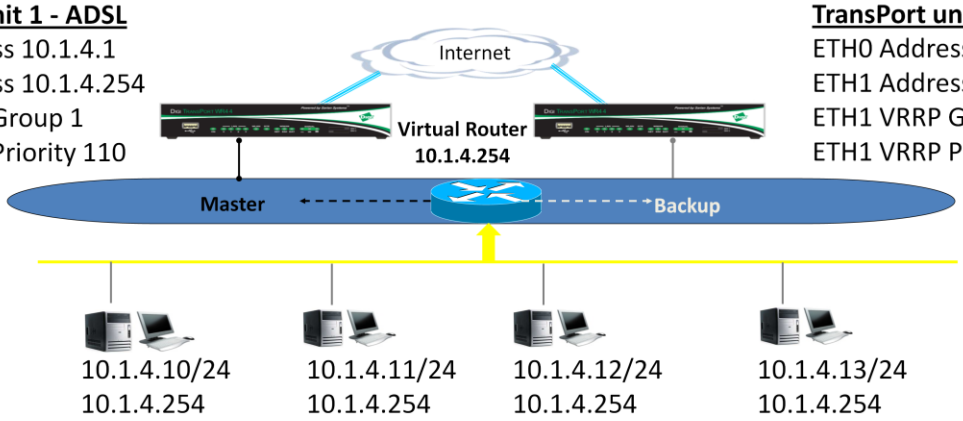
This will mean that the IP Address 10.1.4.254 is not assigned to any one unit but floats between them depending on which is the VRRP master router. If both ETH0 interfaces are connected to hub/switch along with a client then the client will be able to always see a router at the 10.1.4.254 address.
Unit_1 has a priority of 110 so should become the VRRP master router over Unit_2 which has a lower priority of 100.

This is the simplest configuration but it is not generally adopted as it means that you can only attach to the unit that is the VRRP master at any one time which is no good for administration and monitoring of both the units.

Dedicated VRRP Address

TransPort unit 1 - ADSL
ETH0 Address 10.1.4.1
ETH1 Address 10.1.4.254
ETH1 VRRP Group 1
ETH1 VRRP Priority 110

TransPort unit 2 – 3G
ETH0 Address 10.1.4.2
ETH1 Address 10.1.4.254
ETH1 VRRP Group 1
ETH1 VRRP Priority 100

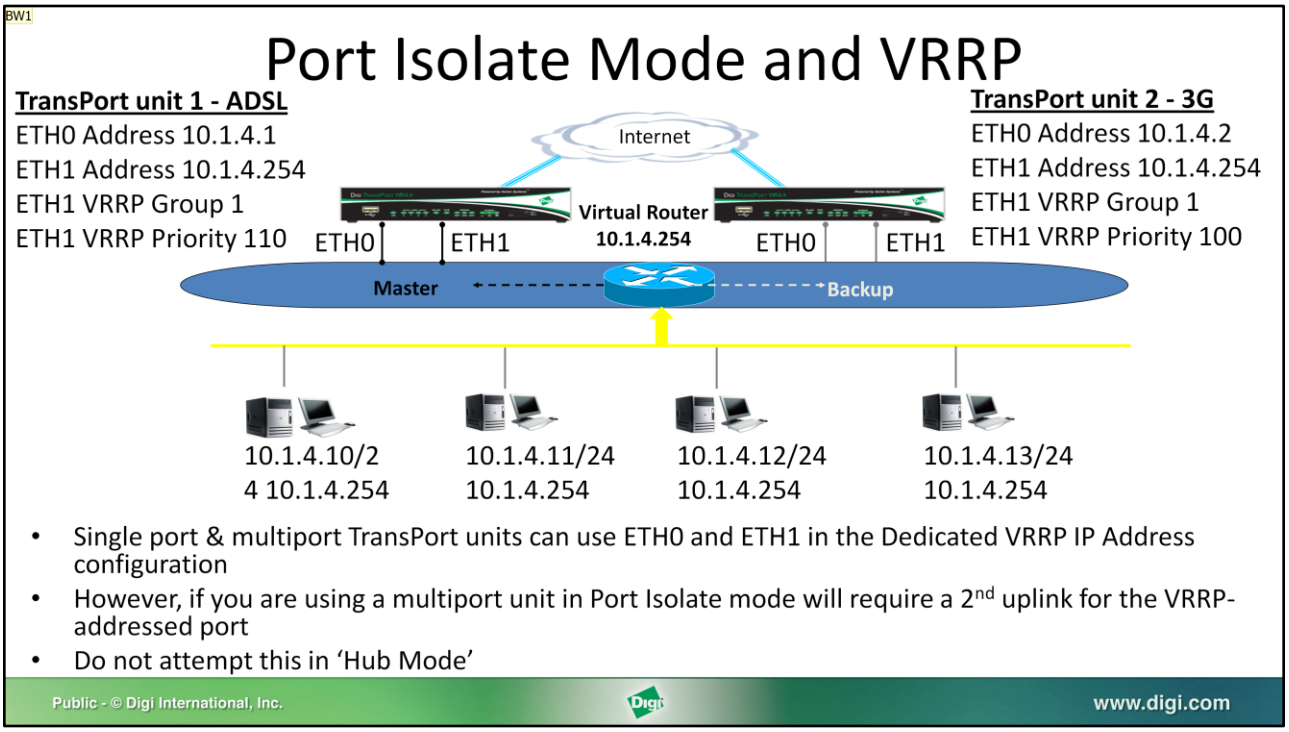


- Each TransPort unit has its own IP Address so can be now reached on their own IP Addresses on ETH0
- A different IP Address is used for VRRP
- A more widely used solution

A more common solution would be to have an IP address for each unit and then a third address for VRRP e.g.

So as before the 10.1.4.254 VRRP address floats between the two routers on ETH1 and can be used by the clients as a default gateway, but the routers can also be reached on their own IP addresses on ETH0.

See the next slide for restrictions on this configuration.



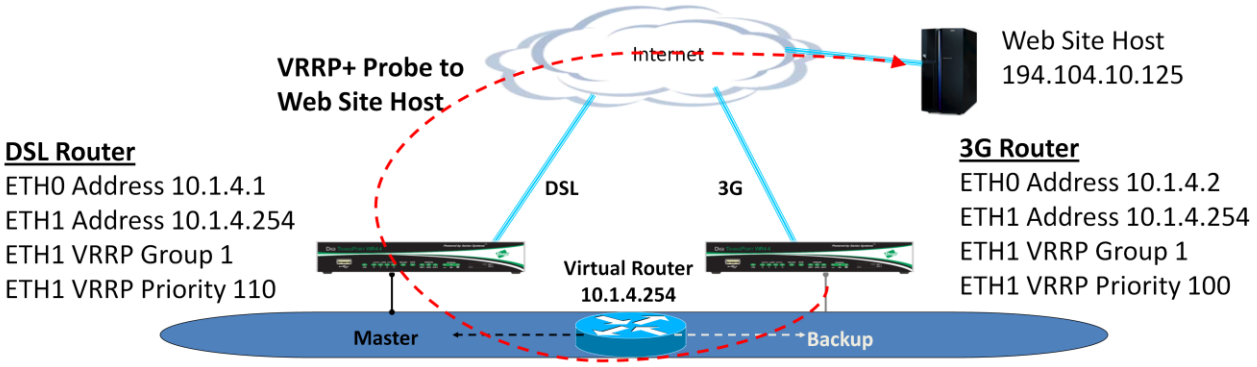
Depending on the TransPort model, you can implement VRRP in different ways. E.g., if you have a unit with a single LAN port (e.g. WR41) then you can use ETH0 and ETH1 in the Dedicated IP Address configuration, if you have a unit with multiple ports (e.g. WR44) in 'Hub Mode' then the same applies.

However, If you are using a multi port unit in 'Port Isolate Mode' then you will need to provide a second uplink for the VRRP-addressed port:

NOTE: Do not try this configuration in 'Hub Mode' otherwise a network loop will form with undesirable consequences.

This may not be practical so a better solution would be to keep the unit in Hub Mode and use the Group feature to make each port a member of a different hub group but have the ETH0 and ETH1 ports in the same group for VRRP.

The TransPort VRRP+ Extension



- An extension to VRRP developed by Digi
- Allows other devices to be monitored eg. Internet host systems
- Enables the changing of VRRP router priorities thus achieving logical redundancy
- Based on status of connections behind the TransPort Router
- TransPort's VRRP+ provides for intelligent failover scenarios

VRRP+ is an extension to VRRP developed by Sarian Systems, it allows other devices to be monitored and alter the priorities of the VRRP routers. For example, if a host becomes unreachable on the far end of a network link then the default router can be changed by adjusting the VRRP priority of the router connected to that failing link.
In this case we are able to achieve logical redundancy in addition to the physical redundancy provided by basic VRRP and fail over based on the status of connections behind the router.

VRRP+ is an innovation of Sarian Systems (now Digi International) and allows VRRP to be extended to provide intelligent fail over scenarios.
For example, if you have two routers that connect to the internet, a DSL router and an ISDN router that you want to use as backup.
In addition to the ISDN router taking over if the DSL router fails completely it is also desirably to swap over if the DSL line fails or the DSL ISP has some kind of fault to prevent access to the Web Site Host.

To achieve this the DSL router is set to use VRRP+ probing to send ICMP (ping) packets to the web site host on 192.32.42.133.
In the event of a failure of a ping, the VRRP Priority on the DSL Router will be decremented by 20, giving it a VRRP priority of 90. This makes it lower than the priority of the 3G router (100) will cause the 3G router to become the VRRP Master Router and take all the traffic bound for the internet.

In addition to this the DSL router (which is now a VRRP Backup Router) will attempt to periodically contact the Web Site Host via ICMP and upon restoring the connection the VRRP Priority will be restored to 110 and the DSL router will once again become the VRRP Master Router.
It is possible that the Web Site Host is behind a firewall and configured not to respond to ICMP (ping) requests, this can be overcome by setting the router to probe port 80 (HTTP/Web) on the Web Site Host instead.

Summary

- VRRP Overview & Standards
- VRRP Operation
- VRRP Failover Operation
- TransPort VRRP Implementations
- Single VRRP Address
- Dedicated VRRP Address
- TransPort Unit in Port Isolate mode and VRRP
- The TransPort VRRP+ Extension

HANDS-ON PRACTICAL SESSION VRRP

For reference, see Application Note 31 VRRP and VRRP+

HOPS - VRRP

- This practical session covers:

Configure a pair of TransPort devices to operate VRRP to demonstrate switchover

HOPS Summary

- Summary of Practical session
- Issues?
- Observations?
- Suggestions?