

Network Design Workshop

High Availability

High Availability

- How can we achieve high availability?
 - Protect your network against a single device failure affecting all of your network
 - Introduce hardware resiliency and backup paths
 - Different techniques depending on the layer
 - Relationship between reliability, complexity and cost
 - The trick is to balance all variables and come up ahead

High Availability

- You need to evaluate your needs
 - Minimal need
 - Network just needs to be up for a portion of the day
 - Downtime is easily scheduled after working hours
 - Business is not impacted if the network is down
 - Users' productivity is not impacted by a network failure

High Availability

– Medium need

- Network needs to be available for most of the day
- Only centralized servers need to be up 24 hours/day
- Downtime needs to be scheduled on weekends
- If critical parts of the network fail, the business operation is impacted
- A network failure affects user productivity

High Availability

— High need

- Network needs to be up 24x7
- Downtime needs to be scheduled well in advance and completed within schedule
- A network failure causes major loss of business
- User productivity drastically impacted by a network failure

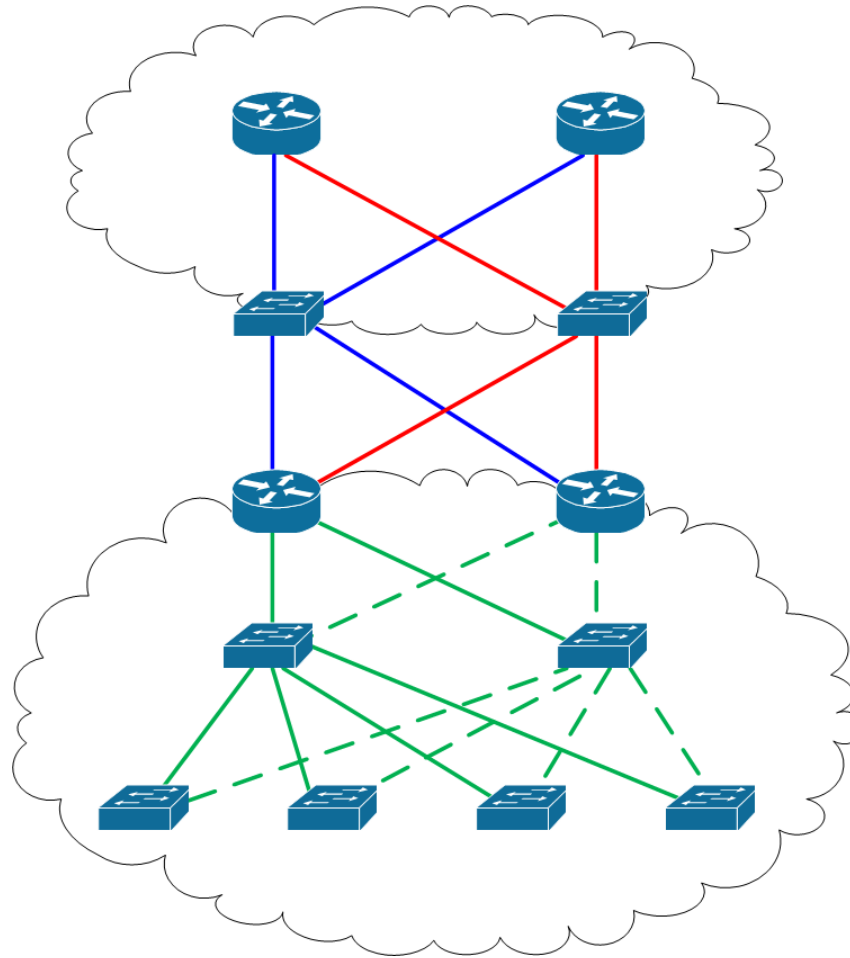
High Availability

- Methods
 - Component Redundancy
 - Duplicate or backup parts
 - Power supplies, fans, processors, etc.
 - Server Redundancy
 - Protect your data with backups
 - Use of hot standby servers
 - Use of load balancers
 - Network Link & Data Path Redundancy
 - Provide physical redundant connections between devices
 - Allow for hot backup paths (STP) and parallelism (routing)

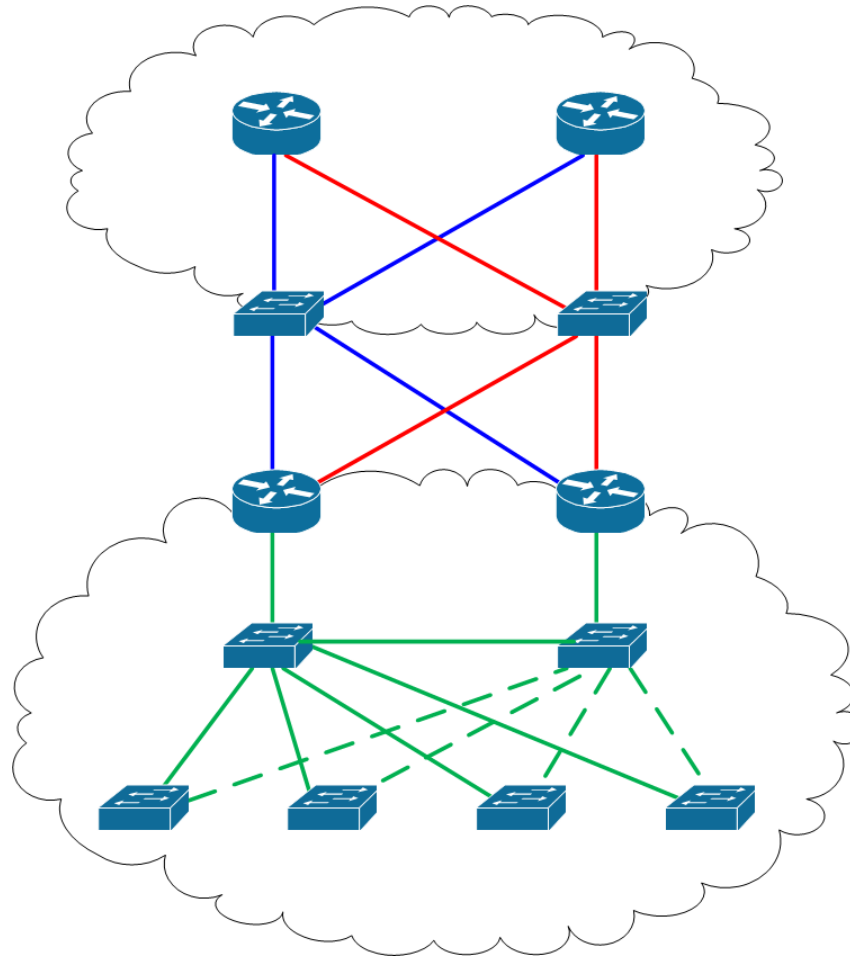
High Availability

- At core and distribution layers
 - Add redundant routers and provide dual paths to each from the lower layer
 - Make sure that you have redundant power supplies in your devices
 - This also assumes two different sources of power
 - Think about the possibility of dual routing/forwarding engines
 - Weigh this against the use of two devices
 - Or just throw that in there as yet another layer of reliability

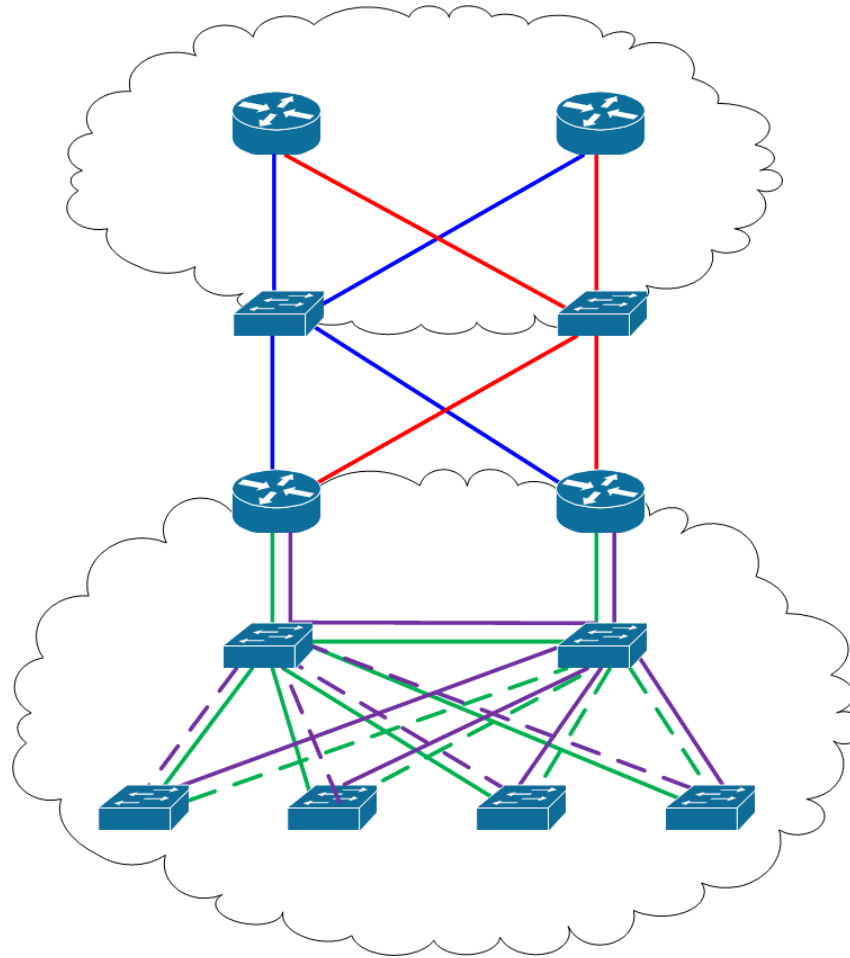
High Availability



High Availability



High Availability



Last Hop Redundancy

- So I built all this redundancy and high availability in my network, how can my end users take advantage of it?
 - You are already providing more than one router for a segment
 - You want to provide your users with a way to move their traffic from one default gateway to another

Last Hop Redundancy

- If one of the routers fails the other one will continue to provide services to the segment
 - Be aware that redundancy is not the same as load balancing

Last Hop Redundancy

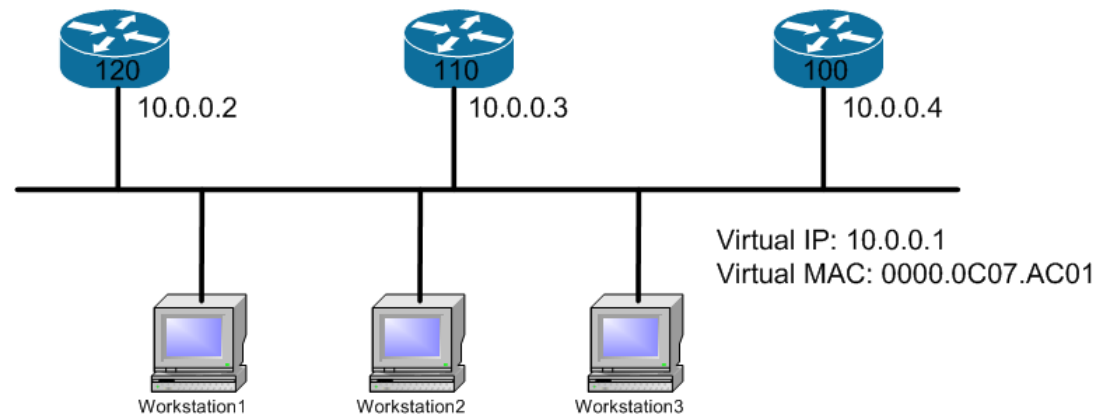
- Current solutions:
 - Hot Standby Redundancy Protocol – HSRP (Cisco Proprietary, RFC2281)
 - Virtual Router Redundancy Protocol – VRRP (RFC3768)
 - Gateway Load Balancing Protocol – GLBP (Cisco Proprietary)

Last Hop Redundancy

- The concept is very similar in all three
 - Workstations get configured with a single default gateway
 - Routers negotiate who will be the default gateway
 - They keep track of the state of the other routers
 - On router failure, standby router becomes the primary/active
 - Traffic from the workstations will go to the primary/active router
 - Incoming traffic into the segment will follow the routing decisions made by routers in the network

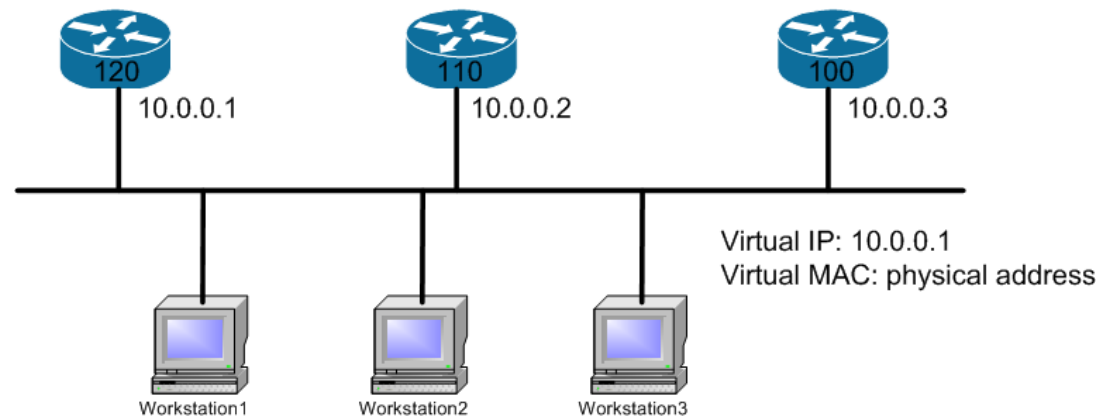
Last Hop Redundancy

HSRP



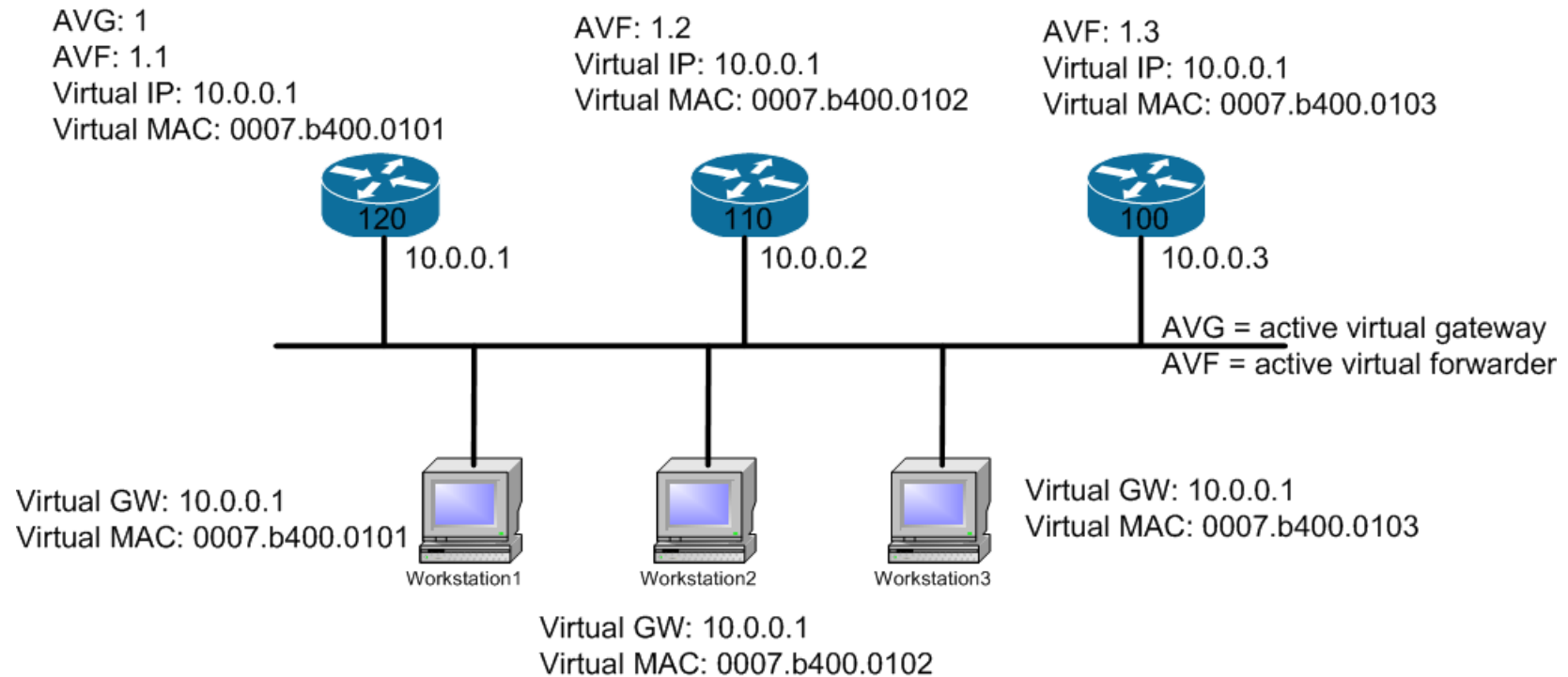
Last Hop Redundancy

VRRP



Last Hop Redundancy

GLBP



Last Hop Redundancy

- Which one should I use?
 - They all allow for a common default gateway and MAC address
 - VRRP is standardized
 - HSRP & GLBP are Cisco proprietary
 - GLBP provides load balancing
 - HSRP & VRRP do not (without introducing complexity)

Last Hop Redundancy

- VRRP can reuse the default gateway IP
 - HSRP does not
- HSRP/GLBP support IPv6
 - VRRP does not (yet)
- VRRP uses protocol 112 & 224.0.0.18
 - HSRP uses UDP/1985 & 224.0.0.2
 - GLBP uses UDP/3222 & 224.0.0.102

High Availability

- All this redundancy and high availability is not going to do you any good if:
 - You don't test it
 - Make sure that it actually works the way you expect
 - You don't monitor it
 - If the redundant devices or links are down, it won't work!