R&S Quick Notes ? Security & IP Services

Security] - Know how to use extended access-lists in distribute-lists, see Brian McGahan @INE article.] - Know how to use extended access-lists instead of prefix-lists, see Brian Dennis @ INE article.] - Dont forget to allow IGP's, BGP, Multicast , IPv6 and any other needed protocols when adding ACL to a interface. - Know when to use the ?established? keyword. - When matching Multicast traffic in a extended ACL, remember that Multicast traffic can NEVER be a source. - Allowing Telnet to a local router on a port other then 23: Option 1- Rotary command or Option 2- Port NAT. - NBAR can be used if you not forbidden from using ACL's. You can also map undefined custom ports with ?ip nbar port-map custom? - Dynamic ACL time-outs specified in the acl: ?dynamic NAME timeout {x} permit tcp any any eq 80?. - When configuring SSH, don't forget to specify a Domain-name and generate your RSA keys. **IP-Services**] - ?no service config? ? Disables the router from auto-answering for tftp config files - WCCP uses udp port 2048 and protcol 47-GRE - If talk about router discovery > IRDP - DNS server config : ?ip dns server? & ?ip host? - DNS client config : ?ip domain-lookup? & ?ip name-server? - DHCP stands for Dont Hit Computer People - DHCP option-82 = dhcp-relay. - DHCP option-66 = Hand out IP address off TFTP server - When configuring DHCP and earlier in the swithcing section you configured DHCP snooping you must enable the port connecting to the DHCP server as trusted. - Incase DHCP was configured you need either ?no ip dhcp snooping info option? on the switch OR ?ip dhcp relay information trust? on the dhcp router. - HSRP timers only need to be configure on one of the participating routers. - HSRP uses UDP port 1984. - When using HSRP with earlier configured port-security, you might need to allow you HSRP MAC 0000.0c07.acxx ? where XX is the group number in hex.