

Layer 2 Configuration Guide HP Procurve Switches



Basic Configuration

Command example	Description
<code>configure terminal</code>	Enter configuration mode
<code>exit</code>	Leave configuration mode
<code>hostname myswitch</code>	Set host name
<code>time timezone -480</code>	Set time zone offset (minutes from UTC)
<code>vlan 10</code> <code>name "DATA_VLAN"</code> <code>untagged 1-22</code> <code>tagged 23-24</code> <code>ip address 10.2.3.4 255.255.255.0</code>	Enter configuration for VLAN 10 Assign name to VLAN Specify member ports (no tagging) Trunk ports which will carry this VLAN Set IP address and mask
<code>password manager user-name admin</code>	Set local password for 'admin' user
<code>interface 1-24</code> <code>no lacp</code>	Desactivar LACP en las interfaces 1-24
<code>show running-config</code>	Shows current active config
<code>write memory</code>	Save configuration
<code>show config</code>	Shows the current saved configuration

Spanning Tree Protocol

Command example	Description
<code>spanning-tree protocol-version MSTP</code>	Select Multiple Spanning Tree protocol (needs <i>write mem + reload</i>)
<code>spanning-tree config-name "some-name"</code>	Assign a configuration name (must match in all switches)
<code>spanning-tree config-revision 1</code>	Assign configuration revision (must match in all switches)
<code>spanning-tree instance 1 vlan 10 20</code>	Assign VLANs 10 and 20 to instance 1 of spanning tree
<code>spanning-tree instance 1 priority 0</code>	Assign priority 0 to instance 1 of spanning tree
<code>spanning-tree 1-22 admin-edge-port</code>	Set ports 1-22 as "edge ports" (where end devices are connected)
<code>spanning-tree 1-22 bpdu-protection</code>	Disable ports in range if STP BPDUs are received on those ports

Port Aggregation (LACP)

Command example	Description
<code>Trunk 23-24 trk1 lacp</code>	Establish an LACP trunk called "trk1" using ports 23 and 24

Authentication

Command example	Description
<code>no aaa authentication login privileged mode</code>	Do not honor authentication server's privilege level
<code>aaa authentication {console, ssh} login radius local</code>	{Console, SSH} access uses RADIUS first, then local credentials
<code>radius-server dead-time 5</code>	RADIUS server is considered dead for 5 minutes after a failure to respond to an authentication request
<code>radius-server timeout 3</code>	Wait 3 seconds for authentication response
<code>radius-server retransmit 1</code>	Retry once after not receiving a response from RADIUS server
<code>radius-server key verycomplexkey</code>	Set encryption key for communication with RADIUS server
<code>radius-server host 10.1.2.3.4</code>	Add IP address of RADIUS server

Network Management

Command example	Description
<code>ip icmp burst-normal 20</code>	Drop ICMP packets in excess of 20/sec
<code>ip icmp reply-limit</code>	Enable ICMP reply rate limiting
<code>ip ttl 6</code>	Limit IP packet scope to 6 hops
<code>snmp-server location "Building A"</code>	Set SNMP location
<code>snmp-server contact "noc@mydomain"</code>	Set SNMP contact information
<code>snmp-server community "public" manager restricted</code>	Set the SNMP community and allow read-only access to all MIBs
<code>snmp-server host 10.2.3.4 "public" Not-INFO</code>	Send SNMP traps to IP address with community public. Do not send informational-only messages.
<code>snmp-server enable traps authentication</code>	Send traps about unauthorized access attempts
<code>ip authorized-managers 10.2.3.4 255.255.255.0</code>	Stations in subnet are authorized to manage the switch
<code>no telnet-server</code>	Disable Telnet service
<code>ip ssh key-size 1024</code>	Specify size of SSH key
<code>crypto key generate ssh rsa</code>	Generate RSA key for SSH access
<code>ip ssh</code>	Activate SSH service
<code>dhcp-snooping</code>	Enable Protection for rogue DHCP servers
<code>no dhcp-snooping option 82</code>	Do not add relay information
<code>no dhcp-snooping verify mac</code>	Do not verify that DHCP client address matches source MAC address of packet
<code>dhcp-snooping option 82 untrusted-policy keep</code>	Do not drop DHCP client packets that already contain option 82
<code>interface 24 dhcp-snooping trust</code>	DHCP server replies come in through this port
<code>dhcp-snooping vlan 1-4094</code>	Enable DHCP snooping on all VLANs
<code>timesync sntp</code>	Use Simple Network Time Protocol for time synchronization
<code>sntp server 10.2.3.4</code>	Add SNTP server
<code>sntp unicast</code>	Use unicast delivery for SNTP

Operation and Troubleshooting

Command example	Description
<code>show interfaces [brief]</code>	Shows interface status and counters (or just status with <i>brief</i>)
<code>show interfaces config</code>	Show port settings
<code>show interfaces 23</code>	Show detailed status of port 23
<code>show ip</code>	Show IP configuration
<code>show spanning-tree [detail]</code>	Show status of common spanning tree
<code>show spanning-tree instance 1 [detail]</code>	When using MSTP, show status of instance 1
<code>show vlan [VLAN-ID]</code>	Show VLAN status
<code>show lacp</code>	Show status of LACP trunks
<code>show cdp neighbors</code>	Show neighbor devices discovered via CDP
<code>show lldp info remote-device</code>	Show neighbor devices discovered via LLDP
<code>copy tftp flash 10.2.3.4 myfile primary</code>	Transfer configuration file from TFTP server into flash memory