**STP**

(config mode)

* spanning-tree vlan 1 root primary (*need to do for each vlan if there’s multiple vlans*)
* spanning-tree vlan 1 root secondary

(int range fa0/1-3)

* spanning-tree portfast (*removes the delay and forces it to forwarding state imm.*)
* spanning-tree bpduguard enable (*Spanning-tree BPDU guard can be enabled on each individual port*)
* spanning-tree portfast bpduguard default (*Enable BPDU guard on all PortFast enabled ports, use the global configuration command*)
* spanning-tree guard root (*deployed toward ports that connect to switches*)

Verify - show spanning-tree

**VTP**

VTP server switch

(Config mode)

1. vtp mode server
2. vtp domain TESTDOMAIN
3. vtp password cisco (*not necessary*)

VTP client switch

(Config mode)

1. vtp mode client
2. vtp domain TESTDOMAIN
3. vtp password cisco

verify – show vlan brief

**Switch/Router Security**

Port Security: Storm control, MAC address sticky… (int range fa0/1-3)

* storm-control broadcast level 50 (*50 is the percent rising suppression level*)
* storm-control multicast level pps 2k 1k *(highest,lowest)*
* storm-control action trap/shutdown
* switchport port-security (*implement port security* ***IMPORTANT***)
* switchport port-security maximum 2 (*maximum number of learned MAC address*)
* switchport port-security mac-address sticky (*allow the MAC address to be learned dynamically*)
* switchport port-security violation shutdown (*setting of violation; shutdown, restrict, protect*)
* switchport port-security aging time 120 (time is in minutes)

verify- show port-security, show port-security addresses

Syslog, NTP, SSH, AAA

NTP & Syslog (config mode)

1. ntp server 192.168.1.5 (*ntp server ip*)
2. ntp update-calendar
3. service timestamps log datetime msec
4. logging on
5. logging 192.168.1.6 (*log to a remote host/ syslog server*)
6. logging trap debugging

SSH (config-mode)

1. ip domain-name ccnasecurity.com (*IMPORTANT)*
2. username SSHadmin privilege 15 secret ciscosshpa55 (*15 is highest user privilege level*)
3. line vty 0 4 (vty) (line con 0 *console*)
4. login local
5. transport input ssh
6. exit
7. crypto key generate rsa (*remember to enter the modulus bits eg 512 1024*)
8. ip ssh version 2
9. ip ssh authentication-retries 2
10. ip ssh time-out 90

Verify - show ip int brief

AAA

Local AAA authentication

1. aaa new-model
2. aaa authentication login default local-case
3. aaa local authentication attempts max-fail 10

Named list AAA

1. aaa new-model
2. aaa authentication login default local-case enable
3. aaa authentication login TELNET-LOGIN local-case
4. line vty 0 4
5. login authentication TELNET-LOGIN

**HSRP**

Commands done in interface configuration

Main Router: ( int g0/0.10) (vlan 10)

* standby version 2 (*not necessary*)
* standby 10 ip 192.168.1.1 (*virtual IP*) (*standby 1 - need to change number for each VLAN*)
* standby 10 priority 120 (*default priority 100, higher better*)
* standby 10 preempt *(when down n back up connection go back to main router)*

Backup Router: ( int g0/0.10) (vlan 10)

* standby version 2
* standby 10 ip 192.168.1.1 *(virtual IP same as main router)*

verify – show standby

**Etherchannel** (*group up switch ports into one logical connection*)

PAgP (Cisco proprietary [desirable, auto])

* channel-group 1 mode desirable
* channel-group 1 mode auto (*by right both side shouldn’t be desirable but see the result %*)

LACP (Open-source[active,passive])

* channel-group 1 mode active
* channel-group 1 mode passive

Etherchannel (config mode) (let fa0/1-2 be in group 1)

1. int range fa0/1-2
2. switchport mode trunk
3. switchport trunk native vlan 99
4. switchport trunk allowed vlan 10,20
5. channel-group 1 mode passive *(can be also active, desirable, auto)*
6. int port-channel 1
7. switchport mode trunk
8. switchport trunk native vlan 99
9. switchport trunk allowed vlan 10,20

verify – show eth summary

**Trunking/Inter-VLAN Routing/VLAN configuration**

Create VLANs on switch (config mode )

1. vlan 10
2. name guests
3. int fa0/1 (*interface pointing to end device*)
4. switchport mode access
5. switchport access vlan 10 (switchport voice vlan [id])
6. vlan 20
7. name HQ
8. int fa0/2
9. switchport mode access
10. switchport access vlan 20
11. int fa0/4 (*interface pointing to switches/routers*)
12. switchport mode trunk
13. switchport trunk native vlan 99
14. switchport trunk allowed vlan 10,20

* int vlan 100 (virtual interface)
* ip address 192.168.1.254. 255.255.255.0

reset port – **go into int**, no switchport mode access

delete vlan – no vlan [id]

Configure router on a stick on router

* int g0/0/0
* no shut
* int g0/0/0.10
* encapsulation dot1Q 10
* ip address 192.168.0.1 255.255.255.0
* int g0/0/0.20
* encapsulation dot1Q 20
* ip address 192.168.1.1 255.255.255.0
* int g0/0/0.30
* encapsulation dot1Q 30
* ip address 192.168.2.1 255.255.255.0

**ACLs** (*Standard Destination Extended Source*) (RMB TO PERMIT IP ANY ANY)

No name: no **ip**

Named: **ip** access-list...

Standard ACL(1-99)

* access-list 10 permit host 198.168.10.10
* access-list 10 permit 192.168.20.0 0.0.0.255 (*wildcard subnet mask*)
* Int se0/1/0
* Ip access-group 10 out

Named Standard ACL

* ip access-list standard PERMIT-ACCESS
* permit host 198.168.10.10
* permit 192.168.20.0 0.0.0.255 (*wildcard subnet mask*)
* Int se0/1/0
* Ip access-group PERMIT-ACCESS out

Extended ACL(100-199)

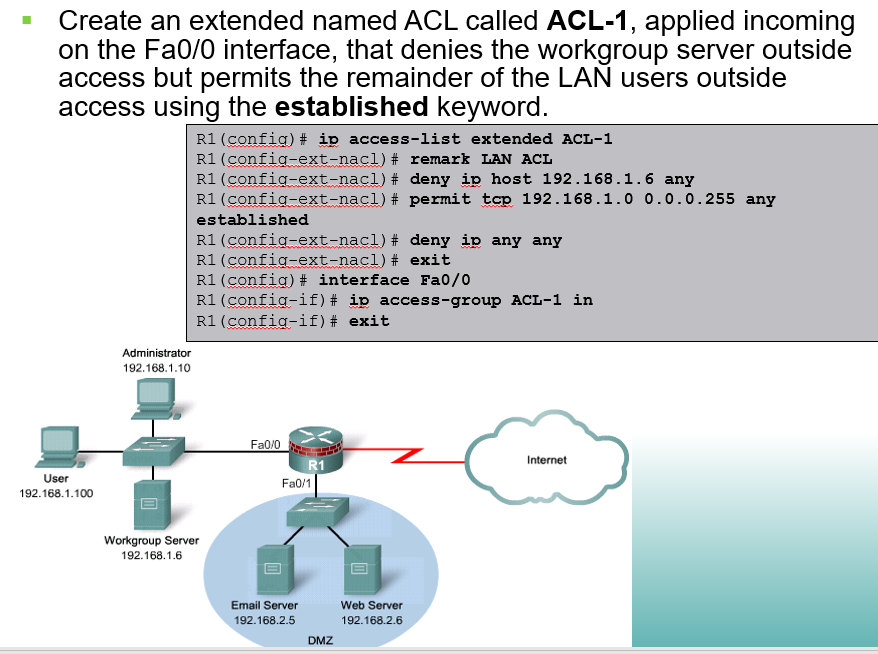
* Access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80

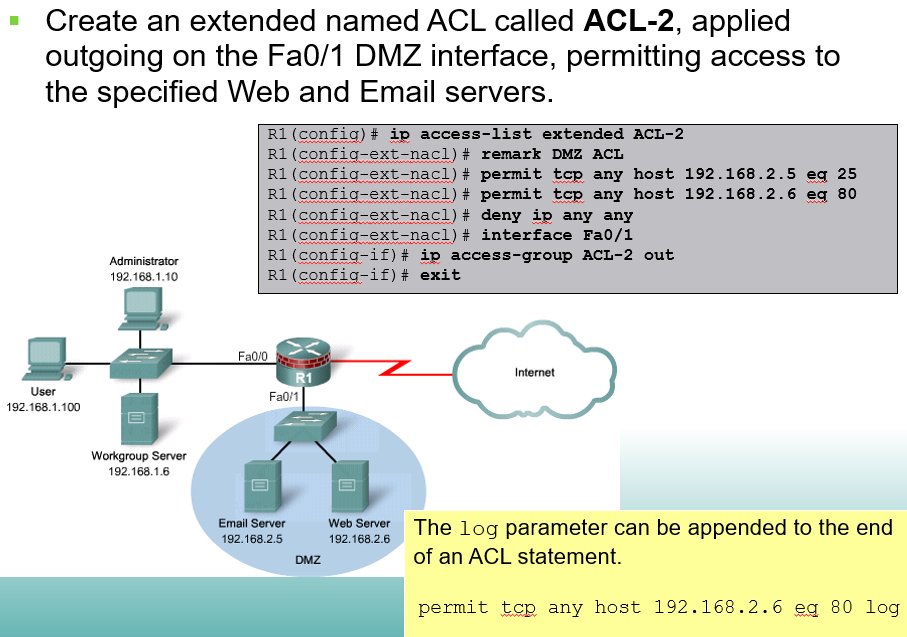
*(Permitting tcp traffic for network 192.168.30.0 from any ip add as long as using http)*

Ssh(22) Https(443) Http(80)

*EstablishedText

Description automatically generated*





**disable dns lookup cisco - ‘no ip domain-lookup’**