!

! This is a template for how to configure a 9300 as a Layer 2 IDF switch.

! Workstations, printers and phones would be connected to this switch.

!

! This is for a 48-port 9300. You will need to change the port references

! for other port configurations, such as a 24-port 9300E.

!

! Items that need to be changed are highlighted in red.

!

! Note - for DHCP snooping, if there are any DHCP servers attached to this

! switch, those interface need to be trusted. This could be the PXE Boot

! servers.

!

no service pad

service tcp-keepalives-in

service timestamps debug datetime msec localtime show-timezone

service timestamps log datetime msec localtime show-timezone

service password-encryption

service compress-config

!

boot-start-marker

boot-end-marker

!

!

vrf definition Mgmt-vrf

!

address-family ipv4

exit-address-family

!

address-family ipv6

exit-address-family

!

no logging console

logging buffered informational

logging monitor debugging

!

**!** **enable secret secret-password**

**!**

**!** **username adminlocal password general-password**

**! They need to be added manually**

**!**

aaa new-model

!

!

aaa group server tacacs+ TACACS-Servers

server name VA-tacacs

server name MO-tacacs

!

aaa group server radius ISE\_SERVERS

!

! For devices west of the Mississippi River swap the 2 statements below

!

server name ISE-Server-VA

server name ISE-Server-MO

!

aaa authentication fail-message ^

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\* \*

\* ACCESS DENIED: Access to this network is restricted to authorized users \*

\* only. The data contained herein is considered to be confidential. \*

\* \*

\* This network is monitored for security and administrative purposes. \*

\* \*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

^

aaa authentication login default group TACACS-Servers local

aaa authentication enable default group TACACS-Servers enable

aaa authentication dot1x default group ISE\_SERVERS

aaa authorization exec default group TACACS-Servers if-authenticated

aaa authorization commands 15 default group TACACS-Servers if-authenticated

aaa authorization network default group ISE\_SERVERS

aaa accounting update newinfo periodic 600

aaa accounting auth-proxy default start-stop group ISE\_SERVERS

aaa accounting dot1x default start-stop group ISE\_SERVERS

aaa accounting exec default start-stop group TACACS-Servers

aaa accounting commands 15 default start-stop group TACACS-Servers

!

aaa server radius dynamic-author

!

! For devices west of the Mississippi River swap the 2 statements below

!

client 30.128.33.197 server-key anth3m!s3

client 10.155.133.65 server-key anth3m!s3

!

aaa session-id common

clock timezone Zulu 0

!

device-sensor filter-list lldp list lldp-list

tlv name system-name

tlv name system-description

!

device-sensor filter-list dhcp list dhcp-list

option name host-name

option name domain-name

option name requested-address

option name parameter-request-list

option name class-identifier

option name client-identifier

!

device-sensor filter-list cdp list cdp-list

tlv name device-name

tlv name address-type

tlv name capabilities-type

tlv name platform-type

tlv name native-vlan-type

tlv number 34

device-sensor filter-spec dhcp include list dhcp-list

device-sensor filter-spec lldp include list lldp-list

device-sensor filter-spec cdp include list cdp-list

device-sensor accounting

device-sensor notify all-changes

!

no ip source-route

no ip gratuitous-arps

ip name-server 198.22.86.53 198.22.86.54

ip domain list mgmt.wellpoint.com

ip domain list wellpoint.com

ip domain list mgmt.internal.das

ip domain list internal.das

ip domain name mgmt.internal.das

ip dhcp snooping vlan 2-3999

no ip dhcp snooping information option

ip dhcp snooping

!

device-tracking tracking auto-source  
!  
device-tracking policy DEVTRK

security-level glean

tracking enable

no protocol ndp

no protocol dhcp6

no protocol udp

!

ip dhcp bootp ignore

!

qos queue-softmax-multiplier 600

vtp version 2

vtp password w3llp01nt

vtp mode transparent

udld aggressive

!

authentication mac-move permit

authentication critical recovery delay 1000

!

dot1x system-auth-control

!

diagnostic bootup level minimal

identity policy webauth-global-inactive

inactivity-timer 3600

!

spanning-tree mode rapid-pvst

spanning-tree loopguard default

spanning-tree portfast default

spanning-tree portfast bpduguard default

spanning-tree extend system-id

!

errdisable recovery cause dhcp-rate-limit

!

redundancy

mode sso

!

!

lldp run

!

ip telnet source-interface Vlan1500

ip telnet hidden addresses

ip tftp source-interface Vlan1500

ip ftp source-interface Vlan1500

crypto key generate rsa general-keys modulus 1024

ip ssh source-interface Vlan1500

ip ssh version 2

!

class-map match-any mark-voice-20230615

match access-group name qos-mark-dscp-ef-20230615

class-map match-any mark-video-20230615

match access-group name qos-mark-dscp-af41-20230615

class-map match-any mark-signaling-20230615

match access-group name qos-mark-dscp-cs3-20230615

class-map match-any trust-devices-20230615

match access-group name qos-trusted-20230615

!

class-map match-any voice-video-20230615

match dscp cs4 af41 ef

class-map match-any voice-signaling-20230615

match dscp cs3

class-map match-any network-control-20230615

match dscp cs6 cs7

!

policy-map ingress-untrusted-20230615

class mark-voice-20230615

set dscp ef

class mark-video-20230615

set dscp af41

class mark-signaling-20230615

set dscp cs3

class trust-devices-20230615

police cir percent 100

class class-default

set dscp default

!

policy-map egress-queuing-20230615

class voice-video-20230615

priority level 1

queue-buffers ratio 20

class network-control-20230615

bandwidth remaining percent 10

queue-buffers ratio 15

class voice-signaling-20230615

bandwidth remaining percent 10

queue-buffers ratio 15

class class-default

bandwidth remaining percent 35

queue-buffers ratio 25!

!

!

interface GigabitEthernet0/0

vrf forwarding Mgmt-vrf

no ip address

negotiation auto

shutdown

!

!

interface range GigabitEthernet1/1/1 - 4

switchport access vlan 1001

no logging event link-status

no snmp trap link-status

shutdown

!

interface range TenGigabitEthernet1/1/2 - 8

switchport access vlan 1001

no logging event link-status

no snmp trap link-status

shutdown

!

interface range FortyGigabitEthernet1/1/1 - 2

switchport access vlan 1001

no snmp trap link-status

no logging event link-status

shutdown

!

! The configuration below is for trunking the switch to 2 core switches

!

interface TenGigabitEthernet1/1/1

description ININD-MCB-CORE-01 - Gn/n

switchport access vlan 1001

switchport trunk native vlan 998

switchport trunk allowed vlan 1500,2029,2030,3029

switchport mode trunk

logging event link-status

snmp trap link-status

udld port aggressive

spanning-tree portfast disable

spanning-tree bpduguard disable

service-policy output egress-queuing-20230615

ip dhcp snooping trust

no shutdown

!

interface TenGigabitEthernet1/1/2

description ININD-MCB-CORE-02 - Gn/n

switchport access vlan 1001

switchport trunk native vlan 998

switchport trunk allowed vlan 1500,2029,2030,3029

switchport mode trunk

no logging event link-status

snmp trap link-status

udld port aggressive

spanning-tree portfast disable

spanning-tree bpduguard disable

service-policy output egress-queuing-20230615

ip dhcp snooping trust

no shutdown

!

interface Vlan1

no ip address

shutdown

!

!

ip http server

ip http authentication local

ip http secure-server

ip http secure-active-session-modules none

ip http active-session-modules none

!

ip tacacs source-interface Vlan1500

!

ip access-list standard NTP\_SERVERS

permit 30.254.255.124

permit 30.254.255.123

permit 198.22.86.124

permit 198.22.86.123

!

ip access-list extended ACL-DEFAULT

permit ip any any

!

ip access-list extended ACL-LOW-IMPACT

remark DHCP, DNS, ICMP

permit udp any eq bootpc any eq bootps

permit udp any any eq domain

permit tcp any any eq domain

permit udp any any eq 389

permit tcp any any eq 389

remark Allow Microsoft Ports

permit tcp any any eq 88

permit udp any any eq 88

permit icmp any any

permit udp any any eq ntp

remark PXE / TFTP

permit udp any any eq tftp

permit udp any eq 4011 any

permit udp any any eq 4011

permit udp any range 2070 2080 any

permit udp any any range 2070 2080

remark Drop all the rest

deny ip any any

!

ip access-list extended vty-access

permit tcp 30.0.0.0 0.255.255.255 any eq 22

permit tcp 33.0.0.0 0.255.255.255 any eq 22

permit tcp 10.0.0.0 0.255.255.255 any eq 22

permit tcp 172.16.0.0 0.15.255.255 any eq 22

permit tcp 192.168.0.0 0.0.255.255 any eq 22

permit tcp 162.95.0.0 0.0.255.255 any eq 22

permit tcp 22.0.0.0 0.255.255.255 any eq 22

!

ip access-list extended qos-mark-dscp-ef-20230615

remark --- RTP Voice Traffic - Webex

permit udp any range 52000 52099 any eq 5004

permit udp any eq 5004 any range 52000 52099

permit udp any range 52000 52099 any eq 9000

permit udp any eq 9000 any range 52000 52099

remark --- RTP Voice Traffic - MS Teams

permit udp any range 50000 50019 any range 3478 3481

permit udp any range 3478 3481 any range 50000 50019

permit udp any range 50000 50019 any range 50000 50019

remark --- RTP Voice Traffic - Genesys

permit udp any 52.129.96.0 0.0.15.255 range 16384 32768

permit udp any 169.150.104.0 0.0.7.255 range 16384 32768

permit udp any 164.152.64.0 0.0.3.255 range 16384 32768

permit udp 52.129.96.0 0.0.15.255 range 16384 32768 any

permit udp 169.150.104.0 0.0.7.255 range 16384 32768 any

permit udp 164.152.64.0 0.0.3.255 range 16384 32768 any

remark --- Genesys WDE voice ---

permit udp any range 9000 9999 30.136.60.0 0.0.0.255

permit udp any range 9000 9999 30.136.68.0 0.0.0.255

permit udp any range 9000 9999 30.140.60.0 0.0.0.255

permit udp any range 9000 9999 30.140.68.0 0.0.0.255

permit udp 30.136.60.0 0.0.0.255 any range 9000 9999

permit udp 30.136.68.0 0.0.0.255 any range 9000 9999

permit udp 30.140.60.0 0.0.0.255 any range 9000 9999

permit udp 30.140.68.0 0.0.0.255 any range 9000 9999

!

ip access-list extended qos-mark-dscp-af41-20230615

remark --- RTP Video Traffic - Webex

permit udp any range 52100 52299 any eq 5004

permit udp any eq 5004 any range 52100 52299

permit udp any range 52100 52299 any eq 9000

permit udp any eq 9000 any range 52100 52299

remark --- RTP Video Traffic - MS Teams

permit udp any range 50020 50039 any range 3478 3481

permit udp any range 3478 3481 any range 50020 50039

permit udp any range 50020 50039 any range 50020 50039

remark --- RTP Screen Share Traffic - MS Teams

permit udp any range 50040 50059 any range 3478 3481

permit udp any range 3478 3481 any range 50040 50059

permit udp any range 50040 50059 any range 50040 50059

!

ip access-list extended qos-mark-dscp-cs3-20230615

remark --- SIP Signaling UDP

permit udp any any eq 5060

permit udp any eq 5060 any

permit udp any any eq 5061

permit udp any eq 5061 any

remark --- SIP Signaling TCP

permit tcp any any eq 5060

permit tcp any eq 5060 any

permit tcp any any eq 5061

permit tcp any eq 5061 any

remark --- Genesys SIPS Signaling

permit tcp any any eq 8061

permit tcp any eq 8061 any

permit udp any any eq 3478

permit udp any eq 3478 any

!

ip access-list extended qos-trusted-20230615

remark reserved for Cisco AP

permit udp any any range 5246 5247

permit udp any range 5246 5247 any

remark ThousandEyes\_Agent\_VAASH-WDC04

permit ip any host 10.152.128.18

permit ip host 10.152.128.18 any

remark ThousandEyes\_Agent\_VAHAR-MAI

permit ip any host 30.236.14.55

permit ip host 30.236.14.55 any

remark ThousandEyes\_Agent\_VARIC-DCS

permit ip any host 30.230.15.148

permit ip host 30.230.15.148 any

remark ThousandEyes\_Agent\_MOSTL-CHE

permit ip any host 30.232.14.41

permit ip host 30.232.14.41 any

remark ThousandEyes\_Agent\_VAVAB-AME

permit ip any host 30.96.14.132

permit ip host 30.96.14.132 any

!

ip radius source-interface Vlan1500

!

logging history informational

logging trap debugging

logging source-interface Vlan1500

logging host 30.254.254.12

access-list 61 permit 198.22.81.135

access-list 61 permit 198.22.81.137

access-list 61 permit 22.140.128.22

access-list 61 permit 22.112.8.97

access-list 61 permit 22.140.128.21

access-list 61 permit 30.132.129.14

access-list 61 permit 30.128.133.13

access-list 61 permit 30.192.196.13

access-list 61 permit 30.199.5.254

access-list 61 permit 30.236.128.72

access-list 61 permit 30.128.200.107

access-list 61 permit 22.136.128.33

access-list 61 permit 30.130.38.248

access-list 61 permit 30.196.132.28

access-list 61 permit 30.230.144.32

access-list 61 permit 30.230.144.33

access-list 61 permit 30.128.190.106

access-list 61 permit 30.230.144.34

access-list 61 permit 30.249.9.165

access-list 61 permit 30.230.144.35

access-list 61 permit 30.230.144.36

access-list 61 permit 30.130.38.247

access-list 61 permit 30.230.144.37

access-list 61 permit 30.230.144.38

access-list 61 permit 10.40.105.30

access-list 61 permit 30.135.254.5

access-list 61 permit 30.128.241.10

access-list 61 permit 10.44.5.79

access-list 61 permit 30.122.31.9

access-list 61 permit 30.230.144.27

access-list 61 permit 30.230.144.28

access-list 61 permit 30.128.190.85

access-list 61 permit 10.100.140.151

access-list 61 permit 30.230.144.29

access-list 61 permit 30.230.144.30

access-list 61 permit 192.251.12.64

access-list 61 permit 30.230.144.31

access-list 61 permit 30.233.128.13

access-list 61 permit 162.95.82.208

access-list 61 permit 30.96.13.247

access-list 61 permit 30.144.8.10

access-list 61 permit 2.136.12.10

access-list 61 permit 30.129.1.19

access-list 61 permit 30.144.8.9

access-list 61 permit 30.128.241.251

access-list 61 permit 30.144.50.40

access-list 61 permit 22.140.36.43

access-list 61 permit 172.29.124.80

access-list 61 permit 30.132.128.187

access-list 61 permit 22.136.48.15

access-list 61 permit 2.136.12.36

access-list 61 permit 30.144.56.16

access-list 61 permit 30.132.128.188

access-list 61 permit 22.140.36.23

access-list 61 permit 22.140.36.16

access-list 61 permit 30.134.20.34

access-list 61 permit 30.135.163.139

access-list 61 permit 22.141.36.12

access-list 61 permit 192.168.248.36

access-list 61 permit 2.136.41.22

access-list 61 permit 2.136.41.21

access-list 61 permit 2.176.0.5

access-list 61 permit 30.230.14.76

access-list 61 permit 30.122.194.29

access-list 61 permit 30.230.14.77

access-list 61 permit 30.144.56.9

access-list 61 permit 30.231.128.185

access-list 61 permit 30.231.128.184

access-list 61 permit 30.124.251.81

access-list 61 permit 30.124.251.83

access-list 61 permit 30.124.251.82

access-list 61 permit 30.231.128.181

access-list 61 permit 30.231.128.183

access-list 61 permit 30.231.128.182

access-list 61 permit 30.124.251.75

access-list 61 permit 162.95.82.124

access-list 61 permit 30.128.82.20

access-list 61 permit 30.152.114.40

access-list 61 permit 30.42.128.104

access-list 61 permit 30.152.114.41

access-list 61 permit 30.128.82.19

access-list 61 permit 30.160.192.158

access-list 61 permit 30.36.202.18

access-list 61 permit 30.160.192.157

access-list 61 permit 30.118.189.61

access-list 61 permit 30.96.132.21

access-list 61 permit 30.188.20.71

access-list 61 permit 10.152.128.188

access-list 61 permit 10.158.7.150

access-list 61 permit 33.0.1.30

access-list 61 permit 33.0.1.31

access-list 61 permit 30.129.33.0 0.0.0.255

access-list 61 permit 30.133.33.0 0.0.0.255

access-list 61 permit 30.117.33.0 0.0.0.255

access-list 61 permit 30.129.52.0 0.0.0.255

access-list 61 permit 30.133.52.0 0.0.0.255

access-list 61 permit 10.155.85.0 0.0.0.255

access-list 61 permit 10.22.144.0 0.0.0.255

access-list 61 permit 10.22.145.0 0.0.0.255

access-list 61 permit 10.22.17.0 0.0.0.255

access-list 62 permit 30.128.241.10

access-list 62 permit 30.132.128.187

access-list 62 permit 30.132.128.188

access-list 62 permit 30.133.33.67

access-list 62 permit 30.129.33.68

access-list 62 permit 30.129.33.67

access-list 62 permit 30.133.33.68

!

snmp-server view fullview iso included

snmp-server view partialview iso included

! Below excludes routing table (1.3.6.1.2.1.4.21)

! snmp-server view partialview ipRouteTable excluded

snmp-server view partialview 1.3.6.1.2.1.4.21 excluded

! Below excludes arp table (1.3.6.1.2.1.4.22)

! snmp-server view partialview ipNetToMediaTable excluded

snmp-server view partialview 1.3.6.1.2.1.4.22 excluded

! Below excludes arp table (1.3.6.1.2.1.3)

snmp-server view partialview at excluded

! Below excludes user table for SNMP (1.3.6.1.6.3.15)

! snmp-server view partialview snmpUsmMIB excluded

snmp-server view partialview 1.3.6.1.6.3.15 excluded

! Below excludes view-based access control model for SNMP (1.3.6.1.6.3.16)

! snmp-server view partialview snmpVacmMIB excluded

snmp-server view partialview 1.3.6.1.6.3.16 excluded

! Below excludes community strings for SNMP (1.3.6.1.6.3.18)

! snmp-server view partialview snmpCommunityMIB excluded

snmp-server view partialview 1.3.6.1.6.3.18 excluded

snmp-server view partialview\_w\_route iso included

snmp-server view partialview\_w\_route at excluded

snmp-server view partialview\_w\_route snmpUsmMIB excluded

snmp-server view partialview\_w\_route snmpVacmMIB excluded

snmp-server view partialview\_w\_route snmpCommunityMIB excluded

snmp-server view partialview\_w\_route ip.22 excluded

snmp-server view noview iso exclude

snmp-server group grpallRO v3 priv read fullview write noview notify fullview access 61

snmp-server group grppartialRO v3 priv read partialview write noview notify partialview access 61

snmp-server group grppartial\_w\_route\_RO v3 priv read partialview\_w\_route write noview notify partialview\_w\_route access 61

snmp-server group grpallRW v3 priv read fullview write fullview access 62

snmp-server user primea grpallRW v3 auth sha Th0usaND3y3s priv aes 128 s0v3ryCrypt1c

snmp-server user anthemnmsa grpallRO v3 auth sha 1nSid3rs! priv aes 128 Scr@mb13Min3

snmp-server user qualysa grppartialRO v3 auth sha 1nTrud3rs priv aes 128 Scr@mb13Min3

snmp-server user tddma grppartial\_w\_route\_RO v3 auth sha fr0gl@rv@ priv aes 128 Scr@mb13Min3

snmp-server user netflowa grppartialRO v3 auth sha bitStr3@ms priv aes 128 Scr@mb13Min3

snmp-server user cactia grppartialRO v3 auth sha s@sp@ri110 priv aes 128 Scr@mb13Min3

snmp-server user cspca grppartialRO v3 auth sha Fri3ndlygh0st priv aes 128 Scr@mb13Min3

snmp-server user iseappla grppartialRO v3 auth sha Fri3ndlygh0st priv aes 128 Scr@mb13Min3

snmp-server community aicinfo RO 61

snmp-server community Th0usaND3y3s RW 62

snmp-server trap-source Vlan1500

!

! The contact string should be the SNOW group name of who supports the device

!

snmp-server contact DATA NTWK SUPPORT ENTERPRISE

snmp-server enable traps bgp

snmp-server enable traps bridge

snmp-server enable traps config

snmp-server enable traps envmon

snmp-server enable traps hsrp

snmp-server enable traps memory

snmp-server enable traps ospf

snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message

snmp-server enable traps snmp

snmp-server enable traps stpx

snmp-server enable traps tty

snmp-server enable traps vtp

snmp-server host 30.254.254.13 public

snmp ifmib ifindex persist

tacacs server VA-tacacs

address ipv4 30.128.33.150

key w3llp01nt

tacacs server MO-tacacs

address ipv4 30.132.52.211

key w3llp01nt

tacacs-server directed-request

!

radius-server attribute 6 on-for-login-auth

radius-server attribute 8 include-in-access-req

radius-server attribute 25 access-request include

radius-server attribute 31 mac format ietf upper-case

radius-server attribute 31 send nas-port-detail mac-only

radius-server dead-criteria time 5 tries 2

radius-server deadtime 10

!

radius server ISE-Server-MO

address ipv4 10.155.133.65 auth-port 1812 acct-port 1813

automate-tester username radius-test

key anth3m!s3

!

radius server ISE-Server-VA

address ipv4 30.128.33.197 auth-port 1812 acct-port 1813

automate-tester username radius-test

key anth3m!s3

!

banner motd ^

Attention:

This is a restricted computer system and is for authorized use only.

Unauthorized use of this system may result in disciplinary action

and/or civil and criminal penalties. Failure to maintain the

confidentiality of sensitive information may subject the user to

penalties under applicable law.

By using this system, the user consents to monitoring, inspection,

and disclosure of all activity for security purposes.

^

!

line con 0

session-timeout 15

exec-timeout 15 0

logging synchronous

transport preferred ssh

transport output telnet ssh

stopbits 1

line vty 0 4

session-timeout 15

access-class vty-access in

exec-timeout 15 0

logging synchronous

transport preferred ssh

transport input ssh

transport output telnet ssh

line vty 5 15

no exec

transport input none

transport output none

!

ntp authentication-key 1 md5 w3llp01nt

ntp authenticate

ntp trusted-key 1

ntp source Vlan1500

ntp access-group peer NTP\_SERVERS

ntp server 198.22.86.123 key 1

ntp server 198.22.86.124 key 1

!

End