CISCO VALIDATED PROFILE

# Configuration Snippets

April 2017

# Table of Contents


Configuration Snippets ..... 1

EnergyWise Use Case ..... 1

ACL Use Case ..... 2

CISF Use Case ..... 3

IPv6 FHS Use Case ..... 4

IBNS2.0 Mode Use Case ..... 5

Auth-Manager Mode Use Case ..... 8

Guest Access (LWA) Use Case ..... 10

Guest Access (CWA) Use Case ..... 12

TrustSec (Static) Use Case ..... 13

TrustSec (Dynamic) Use Case ..... 15

TrustSec (Dynamic over SXP) Use Case ..... 16

VRF-Lite Use Case ..... 17

Private VLAN Use Case ..... 18

WCCP Use Case ..... 19

Q-in-Q Use Case ..... 20

Multicast Data/Video Use Case ..... 20

OSPF and BGP Use Case ..... 22

QoS (AutoQoS/ Custom QoS) Use Case ..... 23

QoS–3750X Use Case ..... 27

CoPP Use Case ..... 28

NetFlow Use Case ..... 28

VSS Use Case ..... 31

HSRP Use Case ..... 32

Etherchannel Use Case ..... 33

SDG Use Case ..... 34

Smart Install Use Case ..... 36

AutoConf Use Case ..... 38

ASP Use Case ..... 38
SPAN, RSPAN Use Case ..... 40
Wireshark Use Case ..... 41
GRE Use Case ..... 42
MPLS L3VPN Use Case ..... 42
MVPN Use Case ..... 45
MCASToGRE Use Case ..... 47
BFD Use Case ..... 48
DNS-AS Use Case ..... 48
Named VLAN Use Case ..... 49
FIPS Use Case ..... 49
AVC Use Case ..... 51
AVC Protocol Pack Update Use Case ..... 52
LACP Rate Fast Use Case ..... 52
VRRPv3 Use Case ..... 52
V6VACL Use Case ..... 53
CISP/NEAT Use Case ..... 53
OGACL Use Case ..... 55
CTS Dot1x MACsec Use Case ..... 58
DHCP v6 Snooping, ND Inspection, and RA Guard ..... 58
iPXE Use Case ..... 60
Netconf/Yang Use Case ..... 60
V-Net Use Case ..... 61

# Configuration Snippets

This document contains sample configuration snippets to give you a general idea about the configuration used in some of the use cases. Your actual configuration would require further customization for actual deployments. For detailed configuration options/best practices, refer to the CCO documentation.

## ENERGYWISE USE CASE

```
energywise domain <> security shared-secret 0 <>
energywise allow query save
energywise allow endpoint-notify domain
energywise endpoint security none


!
interface GigabitEthernet<>
 description Connected to IP Phones
switchport port-security maximum <>
switchport port-security
switchport port-security aging time <>
switchport port-security violation restrict
switchport port-security aging type inactivity
 energywise level <0/10> recurrence importance <1-100> at <mins> <hours> <days-
of-month> <month> <weekdays>
 storm-control broadcast level <> <>
 storm-control multicast level <> <>
!
```

# ACL USE CASE

## VACL

```
!! define an IP and MAC acl's!!
ip access-list extended net_10
  permit ip 10.0.0.0 0.255.255.255 any
mac access-list extended MACFilter
  permit 123.456.000 000.000.fff any

!! define a VLAN map with action !!
vlan access-map  sample_name
match ip address net_10
match mac address MACFilter
action forward

!! apply to a list of vlan(s)!!
vlan filter sample_name vlan-list <>
```

## RACL/PACL

```
!! define the ipv4 or ipv6 access list and apply to interface!!
ip access-list extended ACL_IPv4
 permit ip host 101.3.1.2 host 61.3.1.2
 permit ip host 102.3.1.2 host 62.3.1.2
.
.

ipv6 access-list ACL_IPV6
 permit ipv6 2020:198:664:27::/64 2009:197:17:138::/64
 permit ipv6 2020:537:81:67::/64 2009:886:61:281::/64
 permit ipv6 2020:704:446:79::/64 2009:694:7:124::/64
.
.

Interface GigabitEthernet<>
 ip access-group ACL_IPv4 <in/out>
 ipv6 traffic-filter ACL_IPv6 <in/out>
```

## CISF USE CASE

```
ip dhcp snooping
ip dhcp snooping vlan <>

interface <>
description enable storm-control-port security
 switchport access vlan <>
 switchport mode access
 switchport port-security maximum <>
 switchport port-security
 switchport port-security aging time <>
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 storm-control broadcast level <> <>
 storm-control multicast level <> <>
 storm-control action shutdown

ip arp inspection validate src-mac dst-mac
!
interface <>
 description enable IPSG
 switchport access vlan <>
 switchport mode access
 storm-control broadcast level <> <>
 storm-control multicast level <> <>
 storm-control action trap
 ip verify source mac-check

interface Port-channel<>
 description Connected to Dist-Layer - Cat4k
 switchport trunk allowed vlan <>
 switchport mode trunk
 ip arp inspection trust
 ip dhcp snooping trust
end
```

# IPV6 FHS USE CASE

## DHCPv6 Guard/RA Guard

```
ipv6 dhcp guard policy Univ-v6-DHCPG-Client-Policy1
!
ipv6 dhcp guard policy Univ-v6-DHCPG-Server-Policy1
 device-role server
!
ipv6 nd raguard policy Univ_IPv6_RA_Policy_Host
!
 ipv6 nd raguard policy Univ_IPv6_RA_Policy_Router
 device-role router
!
device-tracking policy My_IP_DeviceTracking_Policy
 security-level glean
 no protocol udp
 tracking enable

vlan configuration <>
 device-tracking attach-policy My_IP_DeviceTracking_Policy
 ipv6 dhcp guard attach-policy Univ-v6-DHCPG-Client-Policy1

!
interface Port-channel82
 description Connected to Dist-Layer - Cat4k
 switchport trunk allowed vlan <>
 switchport mode trunk
 ip arp inspection trust
 ipv6 nd raguard attach-policy Univ_IPv6_RA_Policy_Router
 ipv6 dhcp guard attach-policy Univ-v6-DHCPG-Server-Policy1
 device-tracking attach-policy My_IP_DeviceTracking_Policy
 no keepalive
 ip dhcp snooping trust

Interface <>
 description -  IPv6 FHS RA Guard Attacker
```

```
 switchport access vlan <>
 switchport mode access
ipv6 nd raguard attach-policy Univ_IPv6_RA_Policy_Host
end
```

### IPv6 Source Guard/Destination Guard

```
ipv6 source-guard policy Univ-v6-IPSG-Policy2
 validate address
 validate prefix
!
ipv6 destination-guard policy Univ-v6-IPDG-Policy1
!

interface <>
 description Connected to host - IPv6 IPSG
 switchport access vlan <>
 switchport mode access
ipv6 destination-guard attach-policy Univ-v6-IPDG-Policy1
 ipv6 source-guard attach-policy Univ-v6-IPSG-Policy2
end
```

## IBNS2.0 MODE USE CASE

### AAA Configuration

```
!
aaa authentication dot1x default group <group_name>
aaa authorization network default group <group_name> local
aaa accounting Identity default start-stop group radius
username lab privilege 15 password 0 lab
!
!
!
!
aaa server radius dynamic-author
 client <server-ip> server-key radius
 auth-type any
```

```
!
!
radius server ISE
 address ipv4 <server-ip> auth-port 1645 acct-port 1646
 key radius
!
radius-server retransmit 12
!
aaa group server radius <group_name>
 server name ISE
!
!
!
aaa new-model
aaa session-id common
!
```

## Enable dot1x Globally

```
dot1x system-auth-control
```

## Define Policy

```
policy-map type control subscriber ACCESS-IDENTITY-POLICY
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
 event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template CRITICAL_AUTH_VLAN_Gi1/0/1
   20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
```

```
  20 authorize
 30 class DOT1X_NO_RESP do-until-failure
  10 terminate dot1x
  20 authenticate using mab priority 20
 40 class MAB_FAILED do-until-failure
  10 terminate mab
  20 authentication-restart 60
 50 class NRH do-until-failure
  10 terminate webauth
  20 authentication-restart 60
 60 class NRH do-until-failure
  10 terminate webauth
  20 authentication-restart 60
 80 class WEBAUTH_FAILED do-until-failure
  10 terminate webauth
  20 authentication-restart 60
 90 class always do-until-failure
  10 terminate dot1x
  20 terminate mab
  30 terminate webauth
  40 authentication-restart 60
event agent-found match-all
 10 class always do-until-failure
  10 terminate mab
  20 terminate webauth
  30 authenticate using dot1x priority 10
event authentication-success match-all
event violation match-all
 10 class always do-until-failure
  10 replace
!
```

### Apply on Interface

```
interface <>
 switchport access vlan <>
 switchport mode access
 switchport voice vlan <>
 authentication periodic
 authentication timer reauthenticate server
 access-session host-mode multi-domain
 access-session closed
 access-session port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast
 service-policy type control subscriber ACCESS-IDENTITY-POLICY
```

## AUTH-MANAGER MODE USE CASE

### AAA Configuration

```
!
aaa authentication dot1x default group <group_name>
aaa authorization network default group <group_name>
aaa authorization auth-proxy default group <group_name>
aaa accounting network default start-stop group <group_name>
username lab privilege 15 password 0 lab
!
!
!
!
aaa server radius dynamic-author
 client <server ip> server-key radius
 auth-type any
!
!
radius server ISE
 address ipv4 <server-ip> auth-port 1645 acct-port 1646
 key radius
```

```
!
radius-server dead-criteria time 10 tries 1
radius-server deadtime 1
!
aaa group server radius <group_name>
 server name ISE
!
!
!
aaa new-model
aaa session-id common
!
```

## Enable dot1x Globally

```
dot1x system-auth-control
```

## Apply on Interface

```
interface <>
 switchport access vlan <>
 switchport mode access
 switchport voice vlan <>
 authentication host-mode multi-domain
 authentication order dot1x mab webauth
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 mab
 dot1x pae authenticator
 storm-control broadcast level 10.00 5.00
 storm-control multicast level 20.00 10.00
 storm-control action shutdown
 spanning-tree portfast
end
```

# GUEST ACCESS (LWA) USE CASE

## AAA Configuration

```
aaa authentication login default local
aaa authentication dot1x default group <AAA-RADIUS-GROUP>
aaa authorization network default local group <AAA-RADIUS-GROUP>
aaa accounting Identity default start-stop group <AAA-RADIUS-GROUP>
username <cisco123> password 0 <cisco123>

aaa server radius dynamic-author
 client <> server-key radius
!

radius server <ISE>
 address ipv4 <> auth-port 1645 acct-port 1646
 key radius
!
 aaa group server radius <AAA-RADIUS-GROUP>
 server name <ISE>

aaa local authentication default authorization default
aaa new-model
aaa session-id common
```

## Define Policy

```
policy-map type control subscriber <WebAuth_POLICY_LWA_CUSTOM>
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using webauth parameter-map <LWA_WebAuth_Map_Custom>

policy-map type control subscriber <WebAuth_POLICY_LWA_global>
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using webauth

parameter-map type webauth global
```

```
 type webauth
 timeout init-state sec 3000
 virtual-ip ipv4 <>

parameter-map type webauth LWA_WebAuth_Map_Custom
 type webauth
 custom-page login device flash:<web-login.html>
 custom-page success device flash:<web-success.html>
 custom-page failure device flash:<web-fail.html>
 custom-page login expired device flash:<web-expired.html>
```

## Apply on Interface

```
interface <>
 description Connected to Laptop For WebAuth LWA
 switchport access vlan <>
 switchport mode access
 access-session port-control auto
 service-policy type control subscriber <WebAuth_POLICY_LWA_CUSTOM>

interface <>
 description Connected to Laptop For WebAuth LWA
 switchport access vlan <>
 switchport mode access
 access-session port-control auto
 service-policy type control subscriber <WebAuth_POLICY_LWA_global>

interface <>
 description Client SVI VLAN
 ip address <>
 ip helper-address <>
```

# GUEST ACCESS (CWA) USE CASE

## Define Policy

```
policy-map type control subscriber <WebAuth_POLICY_CWA>
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using mab


ip access-list extended <My_CWA_Redirect_ACL>
 permit tcp any any eq www
 permit tcp any any eq 443
 deny   ip any host <ISE IP>
 deny   ip any host <DHCP IP>
```

## Apply on Interface

```
interface GigabitEthernet<>
 description Connected to Laptop For WebAuth CWA
 switchport access vlan <>
 switchport mode access
 access-session port-control auto
 mab
 dot1x pae authenticator
  service-policy type control subscriber <WebAuth_POLICY_CWA>

interface <>
 description Client SVI VLAN
 ip address <>
 ip helper-address <>
```

# TRUSTSEC (STATIC) USE CASE

## Cisco Catalyst 4k

```
!
interface <>
no switchport
no ip address
cts manual
  sap pmk 00000000000000000000000000000000000000000000000000000000000123456 mode-
list no-encap
 channel-group <> mode desirable
!

! Enable Global enforcement for L2 & L3
!
cts role-based enforcement
cts role-based enforcement vlan-list <>
!

! IP-SGT
!
cts role-based sgt-map <src-IP> sgt <SGT>
!
! Vlan-SGT
!
cts role-based sgt-map vlan-list <vlan-ID> sgt <SGT>
!
! Subnet -SGT
!
cts role-based sgt-map <ip subnet> sgt <SGT>
!

! Static role-based ACLS
!
ip access-list role-based RBACL_ICMP
permit ip
```

```
!
! Static role-based permissions
!
cts role-based permissions from <src-SGT> to <dst-SGT> RBACL_ICMP
!
```

## Cisco Catalyst 3850

```
interface <>
no switchport
no ip address
cts manual
  sap pmk 00000000000000000000000000000000000000000000000000000000000123456 mode-
list no-encap
 channel-group <> mode desirable
!


! Enable Global enforcement for L2 & L3
!
cts role-based enforcement
cts role-based enforcement vlan-list <>
!
! IP-SGT
!
cts role-based sgt-map <> sgt <>
!
! Vlan-SGT
!
cts role-based sgt-map vlan-list <VLAN-id> sgt <SGT>
!
! Subnet –SGT
!
cts role-based sgt-map <IPsubnet> sgt <SGT>
!


! Static role-based ACLS
!
```

```
ip access-list role-based RBACL_ICMP
permit ip
!
! Static role-based permissions
!
cts role-based permissions from <srcSGT> to <dstSGT> RBACL_ICMP
!
```

## TRUSTSEC (DYNAMIC) USE CASE

### Cisco Catalyst 4k

```
interface GigabitEthernet1/1/1
no switchport
no ip address
cts manual
  sap pmk 00000000000000000000000000000000000000000000000000000000000123456 mode-list no-encap
 channel-group <> mode desirable
!

! Enable Global enforcement for L2 & L3
!
cts role-based enforcement
cts role-based enforcement vlan-list <>
!

! SGT mapping and SGACL polices will come dynamically through ISE
```

### Cisco Catalyst 3850

```
interface <>
no switchport
no ip address
cts manual
  sap pmk 00000000000000000000000000000000000000000000000000000000000123456 mode-list no-encap
 channel-group <> mode desirable
!




! Enable Global enforcement for L2 & L3
!
cts role-based enforcement
cts role-based enforcement vlan-list <>
!


! SGT mapping and SGACL polices will come dynamically through ISE
```

## TRUSTSEC (DYNAMIC OVER SXP) USE CASE

### Cisco Catalyst 4k

```
! Enable global sxp and configure sxp link
!
cts sxp enable
cts sxp connection peer <peerIP> source <srcIP> password none mode local listener hold-time 1000 2000
!


! Enable Global enforcement for L2 & L3
!
cts role-based enforcement
cts role-based enforcement vlan-list <>
!


SGT mapping and SGACL polices will come dynamically through ISE
```

## Cisco Catalyst 3850

```
! Enable global sxp and configure sxp link
!
cts sxp enable
cts sxp connection peer <peerIP> source <srcIP> password none mode local speaker hold-time 0
!
! Enable Global enforcement for L2 & L3
!
cts role-based enforcement
cts role-based enforcement vlan-list <>
!

! SGT mapping and SGACL polices will come dynamically through ISE
```

## VRF-LITE USE CASE

```
ip vrf vrf1
  description vrf1
  rd 100:1
  route-target export 100:1
  route-target import 100:1
 !

interface Port-channel55
 no switchport
 ip vrf forwarding vrf1
 ip address 33.0.0.1 255.255.255.0
!
```

## PRIVATE VLAN USE CASE

```
vlan 20
private-vlan primary
vlan 201-203
private-vlan community
vlan 204
private-vlan isolated
!
vlan20
private-vlan association 201-204

interface <>
description community port on vlan201
switchport private-vlan host-association 20 201
 switchport mode private-vlan host
!

interface <>
description promiscuous port
 switchport private-vlan mapping 20 201-204
 switchport mode private-vlan promiscuous

interface Vlan20
 description primary vlan20
 ip address 20.0.0.1 255.0.0.0
 private-vlan mapping 201-204
```

# WCCP USE CASE

## Cisco Catalyst 3850

```
ip wccp check services all
ip wccp web-cache group-address 224.0.1.1 password 0 systest
ip wccp 70 group-address 224.0.1.70 password 0 systest
ip wccp 80 group-address 224.0.1.80 password 0 systest
ip wccp 90 group-address 224.0.1.90 password 0 systest


interface GigabitEthernet3/0/14
 description HTTP client
 no switchport
 ip address 172.31.30.1 255.255.255.0
 ip wccp web-cache redirect in
 ip wccp 70 redirect in
 ip wccp 80 redirect in
 ip wccp 90 redirect in
```

## Cisco Catalyst 4k

```
ip wccp check services all
ip wccp web-cache group-address 224.0.1.1 password 0 systest
ip wccp 53 group-address 224.0.1.53 password 0 systest
ip wccp 60 group-address 224.0.1.160 password 0 systest
ip wccp 70 group-address 224.0.1.70 password 0 systest
ip wccp 80 group-address 224.0.1.80 password 0 systest
ip wccp 81 group-address 224.0.2.81 password 0 systest
ip wccp 82 group-address 224.0.2.81 password 0 systest
ip wccp 90 group-address 224.0.1.90 password 0 systest

interface <>
 description WCCP CE-facing interface
 no switchport
 ip address 49.4.4.81 255.255.255.0
 ip wccp web-cache group-listen
 ip wccp 53 group-listen
```

```
 ip wccp 60 group-listen
 ip wccp 70 group-listen
 ip wccp 80 group-listen
 ip wccp 81 group-listen
 ip wccp 82 group-listen
 ip wccp 90 group-listen
```

## Q-IN-Q USE CASE

```
interface <>
 switchport trunk native vlan 999
 switchport mode trunk
 switchport vlan mapping 200 dot1q-tunnel 102
 switchport vlan mapping 201 dot1q-tunnel 102
 switchport vlan mapping 202 dot1q-tunnel 103
 switchport vlan mapping 203 dot1q-tunnel 104
;
```

## MULTICAST DATA/VIDEO USE CASE

### Cisco Catalyst 3850

```
ip multicast-routing
ip multicast multipath s-g-hash next-hop-based

interface <>
 description Connected to Receiver Host1
 switchport access vlan <>
 switchport mode access

interface <>
 description Connected to Receiver Host2
 switchport access vlan <>
 switchport mode access

interface <>
 description Connected to Receiver Host3
 switchport access vlan <>
 switchport mode access
```

## Cisco Catalyst 4k

```
interface <>
 description Multicast VLAN
 ip address <>
 ip helper-address <>
 ip pim sparse-dense-mode

ip multicast-routing
ip pim rp-address <> override

interface Port-channel <>
 description Connected to Cat6k Core
 ip address <>
 ip pim sparse-dense-mode

interface <>
 description Connected to Cat6k Core
 no switchport
 no ip address
 ip pim sparse-dense-mode
 channel-group <> mode active
```

## Cisco Catalyst 6k

```
ip multicast-routing
ip pim rp-address <> override

interface Port-channel<>
 description downlink to the Cat4k Distribution
 ip address <>
 ip pim sparse-dense-mode


interface <>
 description downlink to the Cat4k Distribution
 no ip address
 ip pim sparse-dense-mode
```

```
 channel-group <> mode active

interface <>
 description Connected to Video Source
 ip address <>
 ip pim sparse-dense-mode
```

## OSPF AND BGP USE CASE

```
router ospf 100
 router-id 3.2.1.2
 ispf
 nsf
 timers throttle spf 40 120 10000
 timers throttle lsa 10 100 10000
 ;
 network 3.2.1.2 0.0.0.0 area 0
 network 3.2.1.3 0.0.0.0 area 102
 network 3.10.1.0 0.0.0.255 area 0
 network 3.11.1.0 0.0.0.255 area 0
network 3.13.1.0 0.0.0.255 area 0
 ;
 maximum-paths 8
 bfd all-interfaces
!

interface GigabitEthernet2/2/12
 no switchport
 ip address 3.13.1.1 255.255.255.252
 ip pim sparse-dense-mode
 ipv6 address 3:13:1::1/126
 ipv6 enable
 ospfv3 1 ipv6 area 0
!

router bgp 100
 bgp log-neighbor-changes
```

```
 neighbor 3.3.1.1 remote-as 100
 neighbor 3.3.1.1 fall-over bfd
 neighbor 3.3.1.1 route-reflector-client
 neighbor 3.3.1.2 remote-as 100
 neighbor 3.3.1.2 update-source Loopback100
 neighbor 3.3.1.2 fall-over bfd
!
```

## QOS (AUTOQOS/ CUSTOM QOS) USE CASE

### AutoQoS

```
interface <>
 description autoqos cisco-phone
 switchport access vlan <>
 switchport mode access
 switchport voice vlan <>
 trust device cisco-phone
 auto qos voip cisco-phone
 spanning-tree portfast
 service-policy input AutoQos-4.0-CiscoPhone-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy

interface <>
 description autoqos ip-camera
 switchport access vlan <>
 switchport mode access
 switchport voice vlan <>
 trust device ip-camera
 auto qos video ip-camera
 service-policy input AutoQos-4.0-Trust-Dscp-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
```

## Custom QoS

```
interface <>
 switchport access vlan <>
 switchport mode access
spanning-tree portfast
 service-policy input WIRED-INGRESS-POLICY
 service-policy output WIRED-EGRESS-POLICY


policy-map WIRED-INGRESS-POLICY
 class VVLAN-VOIP
  police 128000 8000 conform-action transmit  exceed-action drop
 class VVLAN-SIGNALING
  police 32000 8000 conform-action transmit  exceed-action drop
 class MULTIMEDIA-CONFERENCING
  police 5000000 8000 conform-action transmit  exceed-action drop
 class SIGNALING
  police 32000 8000 conform-action transmit  exceed-action drop
 class TRANSACTIONAL-DATA
  police 10000000 8000 conform-action transmit  exceed-action set-dscp-transmit
dscp table policed-dscp
 class BULK-DATA
  police 10000000 8000 conform-action transmit  exceed-action set-dscp-transmit
dscp table policed-dscp
 class SCAVENGER
  police 10000000 8000 conform-action transmit  exceed-action drop
 class DEFAULT
  police 10000000 8000 conform-action transmit  exceed-action set-dscp-transmit
dscp table policed-dscp
!


policy-map WIRED-EGRESS-POLICY
 class AutoQos-4.0-Output-Priority-Queue
  priority level 1 percent 10
 class AutoQos-4.0-Output-Control-Mgmt-Queue
  bandwidth remaining percent 10
 class AutoQos-4.0-Output-Multimedia-Conf-Queue
  priority level 2 percent 20
```

```
 class AutoQos-4.0-Output-Trans-Data-Queue
  bandwidth remaining percent 10
 class AutoQos-4.0-Output-Bulk-Data-Queue
  bandwidth remaining percent 5
 class AutoQos-4.0-Output-Scavenger-Queue
  bandwidth remaining percent 5
 class AutoQos-4.0-Output-Multimedia-Strm-Queue
  bandwidth remaining percent 10
 class class-default
  bandwidth remaining percent 60
!
```

## Access-list Definitions

```
ip access-list extended MULTIMEDIA-CONFERENCING
permit udp any any range 16384 32767
!
ip access-list extended SCAVENGER
permit tcp any any range 2300 2400
permit udp any any range 2300 2400
permit tcp any any range 6881 6999
permit tcp any any range 28800 29100
permit tcp any any eq 1214
permit udp any any eq 1214
permit tcp any any eq 3689
permit udp any any eq 3689
permit tcp any any eq 11999
!
ip access-list extended SIGNALING
permit tcp any any range 2000 2002
permit tcp any any range 5060 5061
permit udp any any range 5060 5061
!
ip access-list extended TRANSACTIONAL-DATA
permit tcp any any eq 443
permit tcp any any eq 1521
permit udp any any eq 1521
```

```
permit tcp any any eq 1526
permit udp any any eq 1526
permit tcp any any eq 1575
permit udp any any eq 1575
permit tcp any any eq 1630
permit udp any any eq 1630
!
ip access-list extended BULK-DATA
permit tcp any any eq 22
permit tcp any any eq 465
permit tcp any any eq 143
permit tcp any any eq 993
permit tcp any any eq 995
permit tcp any any eq 1914
permit tcp any any eq ftp
permit tcp any any eq ftp-data
permit tcp any any eq smtp
permit tcp any any eq pop3
!
```

## Class-map Definitions

```
class-map match-any VVLAN-VOIP
 match ip dscp ef

class-map match-any VVLAN-SIGNALING
 match ip dscp cs3
!
class-map match-any MULTIMEDIA-CONFERENCING
 match access-group name MULTIMEDIA-CONFERENCING
!
class-map match-any SIGNALING
 match access-group name SIGNALING
!
class-map match-any TRANSACTIONAL-DATA
 match access-group name TRANSACTIONAL-DATA
!
```

```
class-map match-any BULK-DATA
 match access-group name BULK-DATA
!
class-map match-any SCAVENGER
 match access-group name SCAVENGER
!
```

## QOS–3750X USE CASE

```
mls qos srr-queue input bandwidth 70 30
mls qos srr-queue input threshold 1 80 90
mls qos srr-queue input priority-queue 2 bandwidth 30
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 48 56
mls qos srr-queue input dscp-map queue 2 threshold 3 32 40 46
mls qos srr-queue output dscp-map queue 2 threshold 1 26 28 30 34 36
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 56
mls qos srr-queue output dscp-map queue 3 threshold 3 0
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 100 100
mls qos queue-set output 1 threshold 2 80 90 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 100 100 400
mls qos queue-set output 1 buffers 15 30 35 20
mls qos

interface <>
 switchport access vlan <>
 switchport mode access
 switchport voice vlan <>
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 spanning-tree portfast
!
```

## COPP USE CASE

```
macro global apply system-cpp

access-list 140 deny tcp host 10.1.1.1 any eq telnet
access-list 140 deny tcp host 10.1.1.2 any eq telnet
access-list 140 permit tcp any any eq telnet

class-map telnet-class
match access-group 140

policy-map system-cpp-policy
class telnet-class
police 80000 1000 conform transmit exceed drop
```

## NETFLOW USE CASE

### Exporter Definition

```
flow exporter <export_prime_nf9>
destination <ip_address>
source GigabitEthernet<>
transport udp 9991  <=== 9991 required if PRIME is used the collector
option exporter-stats timeout <>
!
```

### Monitor Definition

```
flow monitor <monitor_ipv4>
 exporter <export_local_nf9>
 cache timeout active <>
 record <record_ipv4>
!

flow monitor <monitor_ipv6>
 exporter <export_local_nf9>
 cache timeout active <>
 record <record_ipv6>
!
```

## Record Definition

```
flow record <record_ipv4>
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface output
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute first
 collect timestamp absolute last


flow record <record_ipv6>
 match ipv6 version
 match ipv6 traffic-class
 match ipv6 protocol
 match ipv6 hop-limit
 match ipv6 source address
 match ipv6 destination address
 match interface output
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute first
 collect timestamp absolute last
!
```

## Sampler Definition

```
sampler <govt_sampler>
 mode <random> 1 out-of <2>
```

## Apply on Interface

```
!
interface GigabitEthernet<>
 no switchport
 ip flow monitor <monitor_ipv4> sampler <govt_sampler> output
 ip address 20.1.1.1 255.255.255.0
 ip access-group 2001 in
 ip access-group 2001 out
ipv6 address 2000::1/64
 ipv6 eigrp 10
 auto qos trust
 service-policy input AutoQos-4.0-Trust-Dscp-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
end

!
interface GigabitEthernet<>
 no switchport
 ipv6 flow monitor <monitor_ipv6> sampler <govt_sampler> output
 ip address 21.1.1.1 255.255.255.0
ipv6 address 2001::1/64
 ipv6 eigrp 10
 ipv6 traffic-filter v6-b in
 ipv6 traffic-filter v6-a out
end
```

# VSS USE CASE

## Cisco Catalyst 4k

```
switch virtual domain 100
 switch mode virtual
 switch 1 priority 200
 mac-address use-virtual

interface Port-channel10
 switchport
 switch virtual link 1
!
interface Port-channel20
 switchport
 switch virtual link 2

interface <>
 no lldp transmit
 no lldp receive
 no cdp enable
 channel-group 10 mode on
 service-policy output VSL-Queuing-Policy
end

interface <>
 no lldp transmit
 no lldp receive
 no cdp enable
 channel-group 10 mode on
 service-policy output VSL-Queuing-Policy
end

interface <>
 no lldp transmit
 no lldp receive
 no cdp enable
```

```
 channel-group 20 mode on
 service-policy output VSL-Queuing-Policy
end

interface <>
 no lldp transmit
 no lldp receive
 no cdp enable
 channel-group 20 mode on
 service-policy output VSL-Queuing-Policy
end
```

## HSRP USE CASE

### Switch 1

```
interface Vlan<x>
 ip address 10.60.1.102 255.255.255.0
 standby version 2
 standby 1 ip 10.60.1.1
 standby 1 preempt
 standby 1 authentication md5 key-string 7 <>
 ipv6 address 2060::102/64
!
interface Vlan<y>
 ip address 10.61.1.102 255.255.255.0
 standby 2 ip 10.61.1.1
 standby 2 preempt
 standby 2 authentication md5 key-string 7 <>
 ipv6 address 2061::102/64
!
```

### Switch 2

```
interface Vlan<x>
 ip address 10.60.1.202 255.255.255.0
 standby version 2
 standby 1 ip 10.60.1.1
 standby 1 preempt
 standby 1 authentication md5 key-string 7 <>
 ipv6 address 2060::202/64
!
interface Vlan<y>
 ip address 10.61.1.202 255.255.255.0
 standby 2 ip 10.61.1.1
 standby 2 preempt
 standby 2 authentication md5 key-string 7 <>
 ipv6 address 2061::202/64
!
```

## ETHERCHANNEL USE CASE

### L3 Portchannel

```
!
interface Port-channel<21>
 no switchport
 ip address 32.1.1.2 255.0.0.0
 speed 1000
 duplex full
 ipv6 address 3201::1/64
 ipv6 eigrp 10
 !
```

## Member Link Interface Configuration

```
interface GigabitEthernet<>
 no switchport
 no ip address
 speed 1000
 duplex full
 channel-group <21> mode active
!
```

## L2 EtherChannel

```
!
interface Port-channel<1>
 switchport trunk allowed vlan 1-100
 switchport mode trunk
```

## Member Link Interface Configuration

```
!
interface GigabitEthernet<>
 switchport trunk allowed vlan 1-100
 switchport mode trunk
 auto qos classify
 channel-group <1> mode passive
 service-policy input AutoQos-4.0-Classify-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
!
```

# SDG USE CASE

```
service-list mdns-sd <3850-MA1-PERMIT-LIST1> permit 10
 match message-type query
!
service-list mdns-sd <3850-MA1-PERMIT-LIST1> deny 20
!

service-list mdns-sd <3850-MA2-PERMIT-LIST2> permit 10
 match message-type query
!
```

```
service-list mdns-sd <3850-MA2-PERMIT-LIST2> permit 20
 match message-type announcement
 match service-type _smb._tcp.local
!
service-list mdns-sd <3850-MA2-PERMIT-LIST2 > permit 30
 match message-type announcement
 match service-type _afpovertcp._tcp.local
!
service-list mdns-sd <3850-MA2-PERMIT-LIST2> permit 40
 match message-type announcement
 match service-type _printer._tcp.local
!
service-list mdns-sd <3850-MA2-PERMIT-LIST2> permit 50
 match message-type announcement
 match service-type _ipp._tcp.local
!

service-list mdns-sd <3850-MA2-PERMIT-LIST2> deny 60
!

service-list mdns-sd <PERMIT-ALL> permit 10

service-list mdns-sd <ACTIVE-QUERY1> query
 service-type _printer._tcp.local
 service-type _ipp._tcp.local
 service-type _afpovertcp._tcp.local
 service-type _smb._tcp.local
 service-type _raop._tcp.local
!

service-routing <mdns-sd>
 service-policy-query <ACTIVE-QUERY1> 900
!

interface <>
 description Connecting the Access Switch1 VLAN
```

```
 ip address <>
 service-routing mdns-sd
 service-policy <3850-MA1-PERMIT-LIST1> IN
 service-policy <PERMIT-ALL> OUT
!
interface <>
 description Connecting the Access Switch2 VLAN
 ip address <>
 service-routing mdns-sd
 service-policy <3850-MA2-PERMIT-LIST2> IN
 service-policy <PERMIT-ALL> OUT
!
```

## SMART INSTALL USE CASE

### Cisco Catalyst 4k––Director Switch Configuration

```
!
interface Vlan110
 description vstack vlan
 ip address 4.1.110.1 255.255.255.0
 ipv6 address 4:1:110::1/120
 ipv6 enable
!


!
vstack vlan 110
!
vstack group custom C1_3750x_acc2 stack
 image tftp://4.1.71.2/c3750e-universalk9-tar.152-2.2.48.E.tar
 config bootflash:C1_3750X_acc2-stack.cfg
 match 1 3750x 24poe
 match 2 3750x 24poe
 match 3 3750x 24
 match 4 3750x 24
 match 5 3750x 24
!
```

```
vstack group custom C1_2960X_acc3 stack
 image tftp://4.1.71.2/c2960x-universalk9-tar.152-2.2.24.E.tar
 config tftp://4.1.71.2/c1_2960x_acc3-stack-confg
 match 1 2960x 48-2sfp-poe
 match 3 2960x 48-2sfp-poe
!
vstack group custom belvedere product-id
 image tftp://4.1.71.2/c3560cx-universalk9-tar.152-3.1.70.E1.tar
 match WS-C3560CX-8PT-S
!
!
vstack group built-in 2960x 48-2sfp-poe
 image bootflash:c2960x-universalk9-tar.152-2.1.99.PI3.tar
 config bootflash:vstack/C1_2960X_acc3-stack-7010.5c72.c200.REV2
!
vstack group built-in 2960c 12-poe
 image bootflash:c2960c405-universalk9-tar.152-2.2.8.PI3.tar
!
vstack group built-in 3560c 8-pd-poe
 image tftp://4.1.71.2/c3560c405ex-universalk9-tar.152-2.2.31.E.tar
!
vstack group built-in 4500 sup8-e 4510r+e
 image tftp://4.1.71.2/cat4500es8-universalk9.SSA.03.06.34.E.152-2.2.34.E.bin
!
!
vstack dhcp-localserver smi
 address-pool 4.1.110.0 255.255.255.0
 file-server 10.105.33.135
!
vstack director 4.1.110.1
vstack basic
vstack startup-vlan 110
vstack backup file-server tftp://4.1.71.2/
!
```

# AUTOCONF USE CASE

## Global Configuration

```
autoconf enable
```

## Builtin-Policy-map

```
policy-map type control subscriber BUILTIN_AUTOCONF_POLICY
  event identity-update match-all
    10 class always do-until-failure
      10 map attribute-to-service table BUILTIN_DEVICE_TO_TEMPLATE
```

## Derived-Configuration after Applying the AutoConf

```
interface GigabitEthernet<>
 switchport mode access
 switchport port-security maximum <>
 switchport port-security maximum <> vlan access
 switchport port-security aging time <>
 switchport port-security
 storm-control broadcast level pps <>
 storm-control multicast level pps <>
 storm-control action trap
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input AutoConf-4.0-CiscoPhone-Input-Policy
 service-policy output AutoConf-4.0-Output-Policy
 ip dhcp snooping limit rate <>
```

# ASP USE CASE

## Global Configuration

```
macro auto global processing
```

## Builtin-Macro for Phone

```
macro auto execute CISCO_PHONE_EVENT builtin CISCO_PHONE_AUTO_SMARTPORT ACCESS_
VLAN=10 VOICE_VLAN=20


!
interface gigabitethernet<>
switchport access vlan 10
switchport mode access
switchport voice vlan 20
switchport port-security maximum <>
switchport port-security
switchport port-security aging time <>
switchport port-security violation restrict
switchport port-security aging type inactivity
auto qos voip cisco-phone
qos trust device cisco-phone
neighbor device type phone
macro description CISCO_PHONE_EVENT
spanning-tree portfast
spanning-tree bpduguard enable
service-policy input AutoQos-VoIP-Input-Cos-Policy
service-policy output AutoQos-VoIP-Output-Policy
end
!
```

## Builtin-Macro for IP Camera

```
Switch(config)#macro auto execute CISCO_IPVSC_EVENT builtin CISCO_IP_CAMERA_AUTO_
SMARTPORT  ACCESS_VLAN=10


!
interface gigabitethernet<>
switchport access vlan 10
switchport mode access
switchport voice vlan 20
switchport port-security maximum <>
switchport port-security
switchport port-security aging time <>
```

```
switchport port-security violation restrict
switchport port-security aging type inactivity
qos trust device ip-camera
 dot1x pae authenticator
 auto qos video ip-camera
 macro description CISCO_IPVSC_EVENT
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input AutoQos-4.0-Trust-Dscp-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
!
```

## SPAN, RSPAN USE CASE

### Cisco Catalyst 3850

```
monitor session 10 source interface <>
monitor session 10 destination interface <>
monitor session 10 filter ip access-group span-filter-acl1
monitor session 20 source interface <>
monitor session 20 destination interface <>
monitor session 20 filter mac access-group span-filter-macl1
monitor session 30 source interface <> rx
monitor session 30 destination interface <>
monitor session 40 source interface <>
monitor session 40 destination remote vlan 4001

vlan <4001>
 name RSPAN_VLAN
 remote-span

ip access list span-filter-acl1
    10 permit ip any host 169.1.1.112
    20 permit ip any host 169.1.1.120

mac access list span-filter-macl1
    permit any host 0000.b1b1.b1b1
    permit any host 0000.b1b1.b1ba
```

### Cisco Catalyst 4k

```
monitor session 1 destination interface <>
monitor session 1 source remote vlan 4001
monitor session 1 filter packet-type good rx

vlan 4001
 name RSPAN_VLAN
 remote-span
```

## WIRESHARK USE CASE

### Data Plane Capture

#### File Capture Configuration

(Captures the pcap file and saves it at a file/location)

```
monitor cap cap1 interface <> both match any file location flash:pcap.pcap
```

#### Buffer Capture Configuration

(Captures the pcap file and saves it in buffer)

```
monitor cap cap2 interface <> both match any
```

#### Buffer Capture Configuration with Duration Limit

```
monitor cap cap3 interface <> both match any limit duration <seconds>
```

#### Buffer Capture Configuration with Size Limit

```
monitor cap cap4 interface <> both match any buffer size <MB>
```

### Control Plane Capture

#### File Capture Configuration

```
monitor capture cap5 control-plane both file location flash:pcap2.pcap match any
```

#### Buffer Capture Configuration

```
monitor capture cap6 control-plane both match any
```

#### Buffer Capture Configuration with Duration Limit

```
monitor capture cap7 control-plane both match any limit duration <seconds>
```

### Buffer Capture Configuration with Size Limit

```
monitor capture cap8 control-plane both match any buffer size <MB>
```

## GRE USE CASE

### Layer 3 GRE Tunnel Non-VRF Environment

```
interface tunnel <>
ip address <>
tunnel source <>
tunnel destination <>
tunnel  mode gre ip
```

### Layer 3 GRE Tunnel Interface in VRF Environment

```
vrf definition <>
address-family ipv4
exit-address-family

interface tunnel <>
vrf forwarding <>
ip address <>
tunnel source <>
tunnel destination <>
tunnel mode gre ip
```

## MPLS L3VPN USE CASE

### PE (Provider Edge)

```
ip routing
mpls label range <min> <max> static <min-static-label>  <max-static-label>
mpls label protocol ldp
mpls static
mpls ldp graceful-restart
mpls ldp router-id <interface> force

interface <interface-name>
 description "Connection to Core P"
no switchport
```

```
 ip address <ip address> <netmask>
 mpls ip
 mpls label protocol ldp

vrf definition <vpn-name>
 rd  <ASN>:<nn>
 route-target export <ASN>:<nn>
 route-target import <ASN>:<nn>
 !
 address-family ipv4
  route-target export <ASN>:<nn>
  route-target import <ASN>:<nn>
 exit-address-family
end

vlan <Customer vlan-id>

interface <vlan-id>
 vrf forwarding <vpn-name>
 ip address <ip address> <netmask>

interface <interface name>
 description "Con to CE"
 switchport trunk allowed vlan <vlan-id>
 switchport mode trunk
end

router ospf <> vrf <vpn-name>
nsr
 nsf
 network <network> <wildcard bits> area <>

router <igp-routing-protocol> < >
 router-id <interface ip>
 nsr
 nsf
```

```
network <network> <wildcard bits> area <>

router bgp <AS number>
 bgp router-id <interface ip>
 bgp log-neighbor-changes
 bgp graceful-restart
 neighbor <peer-ip> remote-as <>
 neighbor <peer-ip> update-source <>
 !
 address-family ipv4
  neighbor <peer-ip> activate
 exit-address-family
 !
 address-family vpnv4
  neighbor <peer-ip> activate
  neighbor <peer-ip> send-community extended
 exit-address-family

 address-family ipv4 vrf <>
  redistribute connected
  redistribute static
  redistribute ospf <> match internal external 1 external 2
 exit-address-family
```

## P (Core)

```
ip routing
mpls label range <min> <max> static <min-static-label>  <max-static-label>
mpls label protocol ldp
mpls static
mpls ldp graceful-restart
mpls ldp router-id <interface> force

interface <interface-name>
description "Con to Provider Edge PE"
no switchport
 ip address <ip address> <netmask>
```

```
 mpls ip
 mpls label protocol ldp

router <igp-routing-protocol> < >
 router-id <interface ip>
 nsr
 nsf
network <network> <wildcard bits> area <>
```

## MVPN USE CASE

Multicast VPNs are configured over the Unicast MPLS L3VPN backbone. Here incremental MVPN specific configuration is specified.

### PE (Provider Edge)

```
ip routing
ip multicast-routing
ip pim rp-address <Core PIM RP address>

interface <interface-name>
 description "Connection to Core P"
no switchport
 ip address <ip address> <netmask>
ip pim sparse-mode
mpls ip
 mpls label protocol ldp

vrf definition <vpn-name>
 rd  <ASN>:<nn>
 route-target export <ASN>:<nn>
 route-target import <ASN>:<nn>
 !
 address-family ipv4
  mdt default <mcast group address>
  mdt data <mcast group address> <wildcat bits>  threshold <>
  route-target export <ASN>:<nn>
  route-target import <ASN>:<nn>
```

```
 exit-address-family
end

ip  multicast-routing vrf  <vrf-name>
ip pim vrf <vrf-name> rp-address <vrf rp ip address>

vlan <Customer vlan-id>

interface <vlan-id>
 vrf forwarding <vpn-name>
 ip address <ip address> <netmask>
 ip pim sparse-mode

interface <loopback number>
 ip address <ip address> <net mask>
 ip pim sparse-mode

router ospf <> vrf <vpn-name>
nsr
 nsf
 network <network> <wildcard bits> area <>

router <igp-routing-protocol> < >
 router-id <interface ip>
 nsr
 nsf
network <network> <wildcard bits> area <>

router bgp <AS number>
 bgp router-id <interface ip>
 bgp log-neighbor-changes
 bgp graceful-restart
 neighbor <peer-ip> remote-as <>
 neighbor <peer-ip> update-source <>
 !
address-family ipv4 mdt
```

```
  neighbor <peer-ip> activate
  neighbor <peer-ip> send-community both
exit-address-family
```

## P (Core)

```
ip routing
ip multicast-routing
ip pim rp-address <Core PIM RP address>

interface <interface-name>
description "Con to Provider Edge PE"
no switchport
 ip address <ip address> <netmask>
ip pim sparse-mode
 mpls ip
 mpls label protocol ldp

interface <loopback number>
 ip address <ip address> <net mask>
 ip pim sparse-mode
```

## MCASTOGRE USE CASE

```
SW1: (Source)
interface <interface-name>
 description MCASToGRE Src
 no switchport
 ip address <ip address> <netmask>
 ip pim sparse-dense-mode/sparse-mode/dense-mode
end

interface Tunnel<>
 bandwidth <>
 ip address <ip address> <netmask>
 ip pim sparse-dense-mode/sparse-mode/dense-mode
 tunnel source <interface>
 tunnel destination <ip address>
```

```
end

SW2: (Receiver)
interface <interface name>
 description Con to MCASToGRE Rcv
 no switchport
 ip address <ip address> <netmask>
 ip pim dense-mode
end
interface Tunnel <tunnel interface number>
 bandwidth <>
 ip address <ip address> <netmask>
 ip pim dense-mode
 tunnel source <interface>
 tunnel destination <ip address>
end
```

## BFD USE CASE

```
interface <interface-name>
 no switchport
 ip address <ip address> <netmask>
bfd interval <> min_rx <> multiplier <>
end

router <routing-protocol> <>
bfd all-interfaces
```

## DNS-AS USE CASE

```
ip name-server <>

avc dns-as client enable
avc dns-as client trusted-domains
 domain www.campus.com
 domain www.education.com
 domain www.facebook.com
```

```
interface <interface name>
 description <>
 switchport access vlan <>
 switchport mode access
 service-policy input DNS-AS
end
```

## NAMED VLAN USE CASE

```
vlan <vlan-id>
 name DATA_VLAN
vlan <vlan-id>
 name VOICE_VLAN
interface  <interface-name>
switchport access vlan name DATA_VLAN
switchport voice vlan name VOICE_VLAN
```

## FIPS USE CASE

Enable FIPS on the switch-member stacks.

```
fips authorization-key <32-bit key>
```

### IKEV2

```
ip access-list extended <ikev2_acl_name>
permit ip any any
crypto ikev2 proposal <name>
 encryption aes-cbc-256
 integrity sha256
 group <group_num>

crypto ikev2 policy <ike_v2_policy>
 proposal ikev2proposal

crypto ikev2 keyring <ike_v2_key>
 peer <peer_switch>
  address <peer_ip_address>
  pre-shared-key <password>
```

```
crypto ikev2 profile <profile_name>
 match identity remote address <ip_address> <subnet_mask>
 authentication local pre-share
 authentication remote pre-share
 keyring local <key>

crypto ipsec transform-set aes256-sha1 esp-aes 256 esp-sha-hmac
 mode tunnel

crypto map <ikev2_cryptomap_name> <number> ipsec-isakmp
 set peer <ip_address>
 set transform-set aes256-sha1
 set ikev2-profile <profile_name>
 match address <ikev2_acl_name>

interface <interface name>
 no switchport
 ip address <ip4_address> <subnet_mask>
 crypto map <ikev2_cryptomap_name>
```

## SSHv2

```
crypto key generate rsa usage-keys label sshkeys modulus <2048>

aaa new-model

ip ssh rsa keypair-name sshkeys
ip ssh version 2
ip ssh dh min size <2048>
ip ssh logging events
ip ssh server algorithm encryption aes128-cbc aes256-cbc aes192-cbc aes256-ctr
aes128-ctr aes192-ctr
username <username> privilege 15 password 0 <password>
```

## AVC USE CASE

```
ip nbar http-services
```

Enable custom application to monitor user-defined custom application using IP addresses (8 custom IP-addresses allowed).

```
ip nbar custom <custom_app_name> ip any id <id_num>
 ip address <ip_address_1> <ip_address_2> <ip_address_3> <ip_address_4> <ip_address_5> <ip_address_6> <ip_address_7> <ip_address_8>
```

Define IP NBAR flow records, exporter, and monitors.

```
!
flow record <record_name>
 match ipv4 version
 match ipv4 protocol
 match connection client ipv4 address
 match connection server ipv4 address
 match connection server transport port
 match flow observation point
 match application name
 collect flow direction
 collect connection initiator
 collect connection client counter packets long
 collect connection client counter bytes network long
 collect connection server counter packets long
 collect connection server counter bytes network long
 collect timestamp absolute first
 collect timestamp absolute last
 collect connection new-connections

flow exporter <exporter_name>
 destination <ip_address_of_exporter_device>
 transport udp <udp_port_of_exporter_device>

flow monitor <monitor_name>
 exporter <exporter_name>
 cache timeout active 60
 record <record_name>
```

```
Interface command for enabling AVC

interface <interface name>
 switchport mode dynamic desirable
 ip flow monitor <monitor_name> input
 ip nbar protocol-discovery
!
interface <interface name>
 switchport mode dynamic desirable
 ip nbar protocol-discovery
!
```

## AVC PROTOCOL PACK UPDATE USE CASE

```
ip nbar protocol-pack flash:<filename> force
```

## LACP RATE FAST USE CASE

```
interface <interface name>
 switchport trunk allowed vlan <vlan-number>
 switchport mode trunk
 channel-group <group_num> mode active
 lacp rate fast
```

## VRRPV3 USE CASE

```
fhrp version vrrp v3

interface Vlan<vlan_number>
 ip address <ip_v4_address> <subnet_mask>
 ipv6 address <ip_v6_address/mask>

vrrp <vrrp_group> address-family ipv4
  priority <priority_number>
  address <ip_v4_address> primary

vrrp <vrrp_group> address-family ipv6
  priority <priority_number>
  address <ip_v6_address> primary
```

# V6VACL USE CASE

## Define V6-VACL Access Lists

```
ipv6 access-list <v6-acl-name>
 <permit/deny> ipv6 host <> any
permit ipv6 host <> any
```

## Define VLAN Access-Maps to Forward/Drop Traffic

```
vlan access-map <vlan-vacl-name> <sequence number>
 match ipv6 address <v6-acl-name>
 action [forward|drop]
```

## Apply the VACL to VLAN

```
vlan filter < vlan-vacl-name> vlan-list <vlan_number>
```

### Interface VLAN Configuration

```
interface Vlan<vlan_number>
 ip address <ipv4_address> <subnet_mask>
 ipv6 address <ipv6_address/mask>
```

# CISP/NEAT USE CASE

## Authenticator

```
Switch#show running-config | sec cisp
cisp enable
policy-map type control subscriber CISP
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
 event authentication-failure match-all
  1 class always do-until-failure
   1 authentication-restart 10


Authenticator#show running-config int <interface num>
 switchport mode access
 access-session port-control auto
```

```
 dot1x pae authenticator
 storm-control broadcast level 30.00
 storm-control action trap
 no macro auto processing
 spanning-tree portfast trunk
 service-policy type control subscriber CISP
end
```

## Supplicant

Global configuration

```
cisp enable
Switch#show running-config | sec CRED
dot1x credentials CRED
 username user1
 password 0 Public123
 dot1x credentials CRED
Switch#show running-config | sec md5
eap profile md5
 method md5
 dot1x supplicant eap profile md5
```

## Interface Configuration

```
Switch#show running-config int tenGigabitEthernet <interface num>
 switchport mode trunk
 switchport voice vlan <xxx>
 dot1x pae supplicant
 dot1x credentials CRED
 dot1x supplicant eap profile md5
 spanning-tree portfast
end
```

## OGACL USE CASE

```
SWITCH#sh run | sec object
object-group service allowed-applications
 igmp
 udp range 10 999
 tcp range 10 999
 udp range 5456 5490
object-group network zone31-traffic
 8.31.0.0 255.255.255.0
 8.31.1.0 255.255.255.0
object-group network zone33-traffic
 8.33.0.0 255.255.255.0
 8.33.1.0 255.255.255.0
 host 8.33.6.1
 host 8.33.7.28
 8.33.100.0 255.255.255.0
object-group network zone41-traffic
 host 8.41.0.110
 8.41.0.0 255.255.255.0
 8.41.1.0 255.255.255.0
object-group network zone51-traffic
 8.51.0.0 255.255.255.0
 host 8.51.100.161
object-group network zone91-traffic
 8.91.110.0 255.255.255.0
object-group network allowed-traffic
 description all host based traffic
 group-object zone31-traffic
 group-object zone33-traffic
 group-object zone41-traffic
 group-object zone51-traffic
 group-object zone91-traffic
object-group service denied-applications
 tcp eq telnet
 udp range 1000 65535
 tcp range 1000 65535
```

```
 udp range 1000 1999
 udp range 3000 5000
 udp range 7000 65535
 tcp range 1000 2050
 tcp range 2051 3000
 tcp range 21000 54345
 udp eq sunrpc
 udp eq xdmcp
 udp eq non500-isakmp
 udp eq netbios-ss
 udp eq netbios-ns
 udp eq netbios-dgm
 tcp eq cmd
 tcp eq chargen
object-group network zone31-denied-hosts
 host 8.31.0.1
object-group network zone41-denied-hosts
 host 8.41.0.1
object-group network other-denied-hosts
 host 8.61.1.1
object-group network denied-hosts
 group-object zone31-denied-hosts
 group-object zone41-denied-hosts
 group-object other-denied-hosts
object-group service host-allowed-services
 description host-allowed-service
 ip
 icmp echo
 group-object allowed-applications
object-group service host-denied-services
 description host-denied-service
 ipinip
 icmp traceroute
 icmp redirect
 nos
 pcp
```

```
 ahp
 esp
 gre
 group-object denied-applications
object-group network mgmt-hosts
 87.20.20.0 255.255.255.0
 87.20.0.0 255.255.255.0
object-group network zone-mixed-denied-hosts
 host 8.46.1.10
 host 8.41.2.40
object-group network zoneC-real-traffic-allowed-networks
 87.9.40.0 255.255.255.0
object-group network zoneC-real-traffic-denied-networks
 97.9.40.0 255.255.255.0
object-group service zoneC-real-trafic-denied-applications
 tcp eq 333
 deny   object-group host-denied-services object-group allowed-traffic any
 deny   object-group host-allowed-services object-group denied-hosts any log
 permit object-group host-denied-services object-group mgmt-hosts any
 permit object-group host-allowed-services object-group mgmt-hosts any
 permit object-group host-denied-services object-group zoneC-real-traffic-al-
lowed-networks any
 permit object-group host-allowed-services object-group zoneC-real-traffic-al-
lowed-networks any
 deny   object-group zoneC-real-trafic-denied-applications host 87.9.41.2 any log
 deny   object-group zoneC-real-trafic-denied-applications object-group zoneC-
real-traffic-denied-networks any log
```

## CTS DOT1X MACSEC USE CASE

```
interface GigabitEthernet <interface number>
 no switchport
 no ip address
 cts dot1x
  sap mode-list gcm-encrypt
 channel-group 24 mode on
!
interface GigabitEthernet <interface number>
 no switchport
 no ip address
 cts dot1x
  sap mode-list gcm-encrypt
 channel-group 24 mode on
!
```

## DHCP V6 SNOOPING, ND INSPECTION, AND RA GUARD

### Global Configuration

```
ip dhcp snooping vlan <snoopvlan>
ip dhcp snooping
ip dhcp excluded-address <excluded_address>

ip dhcp pool dhcp_pool_name
 network <networkIP> 255.255.255.0
!

ipv6 nd inspection policy ipv6nd_inspection_policy
 validate source-mac
 limit address-count 1
 drop-unsecure
 tracking enable
!
ipv6 nd raguard policy ra_guard_policy
 trusted-port
 hop-limit maximum 1
```

```
!
ipv6 unicast-routing
ipv6 dhcp guard policy dhcpv6_trust_policy
 trusted-port
!
ipv6 dhcp pool dhcp6_pool_name
 address prefix <v6network> lifetime 360 240
!
```

## Interface Configuration

```
interface GigabitEthernet <interface number>
 switchport access vlan 50
 switchport mode access
 ipv6 nd inspection attach-policy inspection_policy
 ipv6 nd raguard attach-policy ra_guard_policy
 ipv6 nd ra-throttler
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order mab dot1x
 authentication priority mab dot1x
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity 30
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 4
 storm-control broadcast level 0.10
 storm-control action trap
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet <interface number>
 switchport access vlan 50
 switchport mode access
```

```
 ipv6 nd inspection attach-policy inspection_policy
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order mab dot1x
 authentication priority mab dot1x
 authentication port-control auto
 authentication timer reauthenticate server
 authentication timer inactivity 30
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 4
 storm-control broadcast level 0.10
 storm-control action trap
 spanning-tree bpduguard enable
 ip dhcp snooping limit rate 100
!
```

## IPXE USE CASE

```
boot ipxe timeout 120
```

## NETCONF/YANG USE CASE

```
netconf-yang
```

# V-NET USE CASE

## V-NET Configuration

```
vrf definition <>
 vnet tag <>
 rd <>:<>
 route-target export <>:<>
 route-target import <>:<>
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
```

## Assigning V-NET Configurations to Interface and OSPF

```
interface <>
 description <>
vnet trunk
 ip address <> <>
 ip ospf 20 area 0
 vnet name <>
  ip address <> <>
 !
```

Please use the feedback form to send comments and suggestions about this guide.


**Americas Headquarters**
Cisco Systems, Inc.
San Jose, CA

**Asia Pacific Headquarters**
Cisco Systems (USA) Pte. Ltd.
Singapore

**Europe Headquarters**
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.