Commands Qualified in Cisco IOS XE Catalyst SD-WAN Release 17.x

Qualified CLIs for Cisco IOS XE Catalyst SD-WAN Release 17.2.1r

This section lists the CLIs that are qualified for the CLI add-on feature templates in Cisco IOS XE Catalyst SD-WAN Release 17.2.1r.

Cisco AAA Commands

```
aaa group server tacacs+ tacacs-511
server-private 172.16.0.1 key 7 110a1016141d
ip vrf forwarding 511
!
aaa authentication attempts login 5
aaa authentication login default group tacacs-511
aaa authentication enable default group tacacs-511 enable
aaa authorization config-commands
aaa authorization exec default group tacacs-511 local none
aaa authorization commands 0 default group tacacs-511 local none
aaa authorization commands 1 default group tacacs-511 local none
aaa authorization commands 2 default group tacacs-511 local none
```

```
aaa authorization commands 3 default group tacacs-511 local none
aaa authorization commands 4 default group tacacs-511 local none
aaa authorization commands 5 default group tacacs-511 local none
aaa authorization commands 6 default group tacacs-511 local none
aaa authorization commands 7 default group tacacs-511 local none
aaa authorization commands 8 default group tacacs-511 local none
aaa authorization commands 9 default group tacacs-511 local none
aaa authorization commands 10 default group tacacs-511 local none
aaa authorization commands 11 default group tacacs-511 local none
aaa authorization commands 12 default group tacacs-511 local none
aaa authorization commands 13 default group tacacs-511 local none
aaa authorization commands 14 default group tacacs-511 local none
aaa authorization commands 15 default group tacacs-511 local none
aaa authorization network default local
aaa accounting exec default start-stop group tacacs-511
aaa accounting commands 0 default start-stop group tacacs-511
aaa accounting commands 1 default start-stop group tacacs-511
aaa accounting commands 2 default start-stop group tacacs-511
aaa accounting commands 3 default start-stop group tacacs-511
aaa accounting commands 4 default start-stop group tacacs-511
aaa accounting commands 5 default start-stop group tacacs-511
aaa accounting commands 6 default start-stop group tacacs-511
aaa accounting commands 7 default start-stop group tacacs-511
aaa accounting commands 8 default start-stop group tacacs-511
aaa accounting commands 9 default start-stop group tacacs-511
aaa accounting commands 10 default start-stop group tacacs-511
aaa accounting commands 11 default start-stop group tacacs-511
aaa accounting commands 12 default start-stop group tacacs-511
aaa accounting commands 13 default start-stop group tacacs-511
aaa accounting commands 14 default start-stop group tacacs-511
aaa accounting commands 15 default start-stop group tacacs-511
aaa accounting connection default start-stop group tacacs-511
aaa accounting system default start-stop group tacacs-511
```

Cisco BGP Commands

```
router bgp 64496
neighbor 10.0.0.1 remote-as 64496
bgp graceful-restart
neighbor 10.0.0.1 ha-mode graceful-restart disable

!

router bgp 64496
address-family ipv4 unicast vrf 1
redistribute omp
redistribute static
redistribute connected

!

router bgp 64496
address-family ipv6 unicast vrf 1
redistribute omp
redistribute static
redistribute connected

!

policy-map PMap
class PMap-super-fast
priority level 1
police percent 5
class PMap-fast
```

```
priority level 2
police percent 5

class cos-map-generic
bandwidth remaining percent 5
queue-limit 108 packets
class class-default
bandwidth remaining percent 95
queue-limit 2028 packets
```

IP Commands

```
ip dns server
ip host vrf 1 test_1 192.168.0.{{variable1}}
ip host vrf 1 test_2 192.168.0.{{variable2}}
```

Privilege Exec Show Commands

```
privilege exec level 1 show logging
privilege exec level 1 show sdwan control connections
privilege exec level 1 show sdwan bfd sessions
privilege exec level 1 show sdwan system
```

Qualified CLIs for Cisco IOS XE Release Amsterdam 17.2.1v

This section lists the CLIs that are qualified for the CLI add-on feature templates in Cisco IOS XE Release Amsterdam 17.2.1v.

ACL Commands

```
ip access-list extended acl_1
 11 permit object-group employee_1 any any
!
```

AppNav Commands

```
service-insertion appnav-controller-group scg
  appnav-controller 192.3.3.1 vrf 2
  appnav-controller 192.3.3.2 vrf 2
 !
 service-insertion service-node-group acg1
  service-node 192.3.3.3
 !
 service-insertion service-context waas/1
  appnav-controller-group scg
  service-node-group      acg1
  service-policy          p1
  enable
 !
 service-insertion waas interface Tunnel2
 service-insertion waas interface Tunnel3
 !
```

AppQoE Commands

```
 appqoe
  no tcpopt enable
```

BFD Commands

```
bfd color mpls
  hello-interval 300000
  no pmtu-discovery
  multiplier     60
 !
 bfd color lte
  hello-interval 300000
  pmtu-discovery
  multiplier     60
 !
 bfd color 3g
  hello-interval 300000
  no pmtu-discovery
  multiplier     60
 !
 bfd app-route multiplier 6
 bfd app-route poll-interval 4294967295
```

Cisco BGP Commands

```
router bgp
  address-family no-vrf ipv4
  address-family no-vrf ipv6
  address-family with-vrf ipv4
  address-family with-vrf ipv6
  bgp always-compare-med
  bgp bestpath as-path multipath-relax
  bgp bestpath med missing-as-worst
  bgp deterministic-med
  bgp graceful-restart
  bgp bestpath compare-routerid
  bgp log-neighbor-changes
         bgp router-id

  distance bgp extern-as
  distance bgp internal-as
  distance bgp local
  maximum-paths eibgp
  timers bgp holdtime
  timers bgp keepalive-interval
 neighbor dns-address1 remote-as 999999999

  neighbor dns-address1 ebgp-multihop 255
 neighbor dns-address1 password 7 00141215174C04140B1E1E
 neighbor dns-address1 shutdown
 neighbor dns-address1 timers 65534 65535
 neighbor dns-address2 remote-as 999999
 neighbor dns-address2description test_neighbor_1
 neighbor dns-address2ebgp-multihop 255
 neighbor dns-address2 password 7 13151601181B0B382F1B7A
 neighbor dns-address2 shutdown
 neighbor dns-address2 timers 65534 65535
 neighbor 10.228.0.129 remote-as 999999999
 neighbor 10.228.0.129 advertise-map ADVERTISE non-exist-map NON-EXIST
 neighbor 10.228.0.129 ha-mode graceful-restart disable
  propagate-aspath
```

```
 address-family ipv4 unicast vrf 1
 redistribute connected
 redistribute omp
 redistribute static
 exit-address-family
!
address-family ipv6 unicast vrf 1
 redistribute connected
 redistribute omp
 redistribute static
 exit-address-family
        propagate-aspath
!
address-family ipv4 unicast
 aggregate-address 192.168.51.0 255.255.255.0 as-set summary-only
 aggregate-address 192.168.52.0 255.255.255.0 as-set summary-only
 neighbor 10.0.0.1 advertise-map ADVERTISE non-exist-map NON-EXIST
 neighbor dns-address1 remote-as 999999999
 neighbor dns-address1 activate
 neighbor dns-address1 advertisement-interval 600
 neighbor dns-address1 maximum-prefix 2147483647 100
 neighbor dns-address1 maximum-prefix 769434 100 restart 65535
 neighbor dns-address1 next-hop-self
 neighbor dns-address1 send-community both
 neighbor dns-address2 remote-as 999999
 neighbor dns-address2 activate
 neighbor dns-address2 advertisement-interval 600
 neighbor dns-address2 maximum-prefix 98765 100 restart 65535
 neighbor dns-address2 next-hop-self
 neighbor dns-address2 route-map <route_map_name>
 neighbor dns-address2 send-community both
 neighbor dns-address2 timers 3 9
 network dns-address2  mask 255.255.255.0
 network 192.168.51.0 mask 255.255.255.0
 network 192.168.52.0 mask 255.255.255.0
 exit-address-family
!
timers bgp 60 180
!
```

Class Map Commands

```
class-map match-any BestEffort
 match qos-group 3
!
class-map match-any Bulk
 match qos-group 4
!
class-map match-any Critical
 match qos-group 1
!
class-map match-any Critical-Low
 match qos-group 2
!
class-map match-any BULK
 match qos-group 2
!
class-map match-any CONTROL-SIGNALING
 match qos-group 4
!
class-map match-any CRITICAL-DATA
 match qos-group 1
!
class-map match-any Default
```

```
 match qos-group 5
!
class-map match-any INTERACTIVE-VIDEO
 match qos-group 3
!
class-map match-any LLQ
 match qos-group 0
!
class-map match-any Queue0
 match qos-group 0
!
class-map match-any Queue1
 match qos-group 1
!
class-map match-any Queue2
 match qos-group 2
!
class-map match-any Queue3
 match qos-group 3
!
class-map match-any Queue4
 match qos-group 4
!
class-map match-any Queue5
 match qos-group 5
!
class-map type inspect match-all cmap
 match access-group name cmap
!
   pass
 !
class-map match-any Queue4
 match qos-group 0
!
```

Crypto Commands

```
crypto ikev2 authorization policy li_policy
 exit
 no crypto ikev2 diagnose error
 crypto ikev2 keyring if-ipsec256-ikev2-keyring
  peer if-ipsec256-ikev2-keyring-peer
   address 172.16.93.1
   pre-shared-key cisco123
  !
 !
 crypto ikev2 policy policy1-global
  proposal p1-global
 !
 crypto ikev2 profile if-ipsec256-ikev2-profile
  aaa authorization group psk list default li_policy
  authentication local pre-share
  authentication remote pre-share
  no config-exchange request
  keyring local if-ipsec256-ikev2-keyring
  lifetime 86400
  match identity remote address 172.16.93.2
 !
 crypto ikev2 proposal p1-global
  encryption aes-cbc-128 aes-cbc-256
  group 14 15 16 2
  integrity sha1 sha256 sha384 sha512
 !
```

```
!
crypto ipsec transform-set if-ipsec256-ikev2-transform esp-gcm 256
 mode tunnel
!
crypto ipsec profile if-ipsec256-ipsec-profile
 set ikev2-profile if-ipsec256-ikev2-profile
 set pfs group16
 set transform-set if-ipsec256-ikev2-transform
 set security-association lifetime kilobytes disable
 set security-association lifetime seconds 3600
 set security-association replay window-size 512
!
no crypto isakmp diagnose error
       crypto isakmp aggressive-mode disable
parameter-map type inspect-global
 multi-tenancy
 vpn zone security
!
no crypto ikev2 diagnose error
no crypto isakmp diagnose error
```

EIGRP Commands

```
router eigrp eigrp-name
 address-family ipv4 vrf {{SVPN}} autonomous-system {{SVPN}}
af-interface {{LAN_EIGRP_INT1_name}}
 no dampening-change
 no dampening-interval
 hello-interval 5
 hold-time      15
 split-horizon
 exit-af-interface
!
 af-interface {{LAN_EIGRP_INT2_name}}
  no dampening-change
  no dampening-interval
  hello-interval 5
  hold-time      15
  split-horizon
  exit-af-interface
 !
{{LAN_EIGRP_neighbor1_tf}}  neighbor {{LAN_EIGRP_neighbor1_ip_addr}}
{{LAN_EIGRP_neighbor1_src_int}}
{{LAN_EIGRP_neighbor2_tf}}  neighbor {{LAN_EIGRP_neighbor2_ip_addr}}
{{LAN_EIGRP_neighbor2_src_int}}
{{LAN_EIGRP_neighbor3_tf}}  neighbor {{LAN_EIGRP_neighbor3_ip_addr}}
{{LAN_EIGRP_neighbor3_src_int}}
{{LAN_EIGRP_neighbor4_tf}}  neighbor {{LAN_EIGRP_neighbor4_ip_addr}}
{{LAN_EIGRP_neighbor4_src_int}}
{{LAN_EIGRP_neighbor5_tf}}  neighbor {{LAN_EIGRP_neighbor5_ip_addr}}
{{LAN_EIGRP_neighbor5_src_int}}
network {{LAN_EIGRP_INT1_linknet}}
 network {{LAN_EIGRP_INT2_linknet}}
  topology base
   redistribute omp metric 1000000 255 1 1500
   redistribute static
   exit-af-topology
  !
  exit-address-family
 !
!
```

Global Configuration Commands

```
memory free low-watermark processor 70694
         platform punt-keepalive disable-kernel-core
 no service pad
 no service tcp-small-servers
 no service udp-small-servers
 platform console virtual
 platform qfp utilization monitor load 80
 platform punt-keepalive disable-kernel-core
 hostname myorg
 username admin privilege 15 secret
 username
 username employee1 privilege
 username employee1 secret encryption
 username employee1 secret secret
 clock timezone UTC
 logging monitor
 logging persistent
 logging persistent size 104857600 filesize 10485760
 logging buffered
 logging console
 logging trap errors
 logging rate-limit
 logging host 10.90.9.6 vrf 4
 logging source-interface loopback111 vrf 4
 login on-success log
 no crypto ikev2 diagnose error
 no crypto isakmp diagnose error
 crypto pki trustpoint TP-self-signed-3865005142
  enrollment selfsigned
  revocation-check none
  subject-name     cn=IOS-Self-Signed-Certificate-3865005142
 line con 0
  login authentication default
  speed    9600
  stopbits 1
 !
  login authentication default
  speed    19200
  stopbits 1
 line vty 0 4
  transport input ssh
 line vty 5 80
  transport input ssh
 !mac address-table aging-time <timeout>

 lldp run
```

Interface GigabitEthernet Commands

```
 no shutdown
  arp timeout
  ip address 192.10.6.5
         vrf forwarding vrf10
         ip address dhcp client-id GigabitEthernet1
  no ip redirects
  ip mtu
  mtu
  ip nat outside
  ip ospf 65535 area 1
  ip ospf authentication message-digest
  ip ospf network     broadcast
```

```
  ip ospf cost
  ip ospf dead-interval
  ip ospf hello-interval
  ip ospf message-digest-key 255 md5 7 00051105005E0D01072846
  ip ospf priority
  ip ospf retransmit-interval
  negotiation auto
  service-policy output  policy_1
         ip tcp adjust-mss 1100
         cdp enable
         ip nat outside
         bandwidth 100000
 vrrp 64 address-family ipv4
   vrrpv2
   track 2 shutdown
   address 10.50.4.3 primary
   priority 11
   timers advertise 1000


interface GigabitEthernet1.101
  no shutdown
  encapsulation dot1Q 101
  vrf forwarding 2
  ip address 192.168.66.1
  no ip redirects
         ip directed-broadcast
  ip mtu    1496
  ipv6 address 2001:DB8::1
  ipv6 enable
  ip nbar protocol-discovery
         ip policy route-map policy_1
         ip helper-address 10.8.4.5
         ip helper-address 10.50.4.6

 tunnel-interface
    encapsulation gre weight 1
           encapsulation ipsec weight 1
    no border
    color lte
    no last-resort-circuit
    no low-bandwidth-link
    max-control-connections       1
    exclude-controller-group-list 1
    no vbond-as-stun-server
    vmanage-connection-preference 5
    port-hop
    carrier                       default
    nat-refresh-interval          5
    hello-interval                1000
    hello-tolerance               12
    no allow-service all
    no allow-service bgp
    allow-service dhcp
    allow-service dns
    allow-service icmp
    no allow-service sshd
    no allow-service netconf
    no allow-service ntp
    no allow-service ospf
    no allow-service stun
    allow-service https
    no allow-service snmp
 bandwidth-downstream 300000000
```

```
 interface GigabitEthernet4.302
   tloc-extension GigabitEthernet
   access-list 4451-Marking-Spoke in

interface Dialer1
  no shutdown
  encapsulation ppp
  ip address negotiated
  ip nat outside
  dialer pool 1
  ppp chap hostname ntt
  ppp chap password ntt
  ppp authentication chap calling

interface Loopback100
 interface VirtualPortGroup0
 interface Vlan1

pppoe enable group global
pppoe-client dial-pool-number

interface Tunnel
 ip unnumbered GigabitEthernet0/2.101
  no ip redirects
  ipv6 unnumbered GigabitEthernet0/2.101
  no ipv6 redirects
  tunnel source GigabitEthernet0/2.101
  tunnel mode sdwan


interface atm 0/3/0
description site1
ip mtu 1496
no shutdown

interface atm 0/3/0.1 point-to-point
description site1
ip mtu 1496
[no] ip address 10.0.0.0 255.255.255.252
no shutdown
load-interval 30
pvc 0/100
  [no] shutdown
  bridge-dot1q encap 1
  encapsulation aal5snap
  dialer pool-member 1
  protocol ppp dialer


interface GigabitEthernet1
description branch1
no ip address
no shutdown
ip mtu 1500

interface GigabitEthernet4.302
description branch1
encapsulation dot1Q 101
pppoe enable group global
pppoe-client dial-pool-number
no shutdown
[no] ip address 192.10.6.5
ip mtu 1496
```

```
interface Dialer1
ip address negotiated
encapsulation ppp
dialer pool 1
dialer-group 1
ppp authentication chap callin
ppp chap hostname ntt
ppp chap password ntt
ppp pap sent-username ntt password ntt
ppp sent-password ntt password 0 ntt
no shutdown

controller VDSL 0/3/0
description branch1
operating mode auto
[no] firmware filename bootflash:firmware
[no] modem auto
[no] sra
no shutdown
training log filename flash:4431.log
[no] bitswap
line-mode single-wire line 0
sync mode none
no diagnostics DELT
```

IP Commands

```
ip dhcp use hardware-address client-id
 no ip dhcp use class
         ip host <vbond ip_address1 ip_address2>
 ip ssh version 2
 ip dhcp use vrf remote
 ip multicast route-limit
 ip route
 ip name-server 10.70.1.2
 ip name-server vrf
         ip prefix-list prfx1  permit 172.16.55.1
 ip bootp server
 no ip source-route
 no ip http server
         ip route vrf Mgmt-intf 172.16.55.10
         ipv6 route vrf Mgmt-intf 2001:DB8:101::1
         ip tcp mss 1200
 no ip http secure-server
 no ip igmp ssm-map query dns
 ip nat settings central-policy
 ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet5 overload
 ip nat translation tcp-timeout
 ip nat translation udp-timeout
 cdp run
 object-group service cdp-service-1
  ip
 ip access-list extended access_list_1
    permit object-group group1 any any
 ip arp proxy disable
 no ip rcmd rcp-enable
 no ip rcmd rsh-enable
 no ip domain lookup
         ip dhcp use class
 ip dhcp pool vrf-1-GigabitEthernet5
  option 150 ip ip-list
  vrf
  lease 365 0 0
```

```
  default-router 10.1.19.15
  dns-server 172.16.79.1
  domain-name dns1
  network 255.255.255.0
 ip http authentication local
 no ip finger
 ip http server
 ip http secure-server
 no ip igmp ssm-map query dns

 ip nat pool natpool-GigabitEthernet0/0/0-0 10.4.1.11 10.4.1.250 prefix-length 24
 ip nat inside source list global-list pool natpool-GigabitEthernet0/0/0-0 overload
egress-interface GigabitEthernet4
 ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet4.101
overload
 ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet4.102
overload
 ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet4.103
overload
 ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet4.104
overload
 ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet4.105
overload
 ip nat translation tcp-timeout 10
 ip nat translation udp-timeout 40
 ip nat route vrf 65529 0.0.0.0 0.0.0.0 global
 ip nat route vrf 2 172.16.200.0 255.255.255.0 global
 ipv6 route vrf 1 2001:DB8:EF::1
 vlan internal allocation policy ascending
 ip redirects
 route-map trigger permit
 match ip address prefix
 line vty 0 4
 access-class
 ipv6 access-class
```

Logging Commands

```
logging trap informational syslog-format rfc5424
logging tls-profile profile1 tls-version TLSv1.1
logging tls-profile profile1 ciphersuite aes-256-cbc-sha
```

NAT Commands

```
nat64 translation timeout tcp 60
nat64 translation timeout udp 1
```

NTP Commands

```
ntp authentication-key 65535 md5 test
 ntp server 10.0.1.1 source GigabitEthernet8 key 65535 prefer version 4
 ntp source GigabitEthernet8
 ntp trusted-key
 ntp access-group peer 25
```

Object Group Commands

```
object-group network Auth-Servers
  host 10.16.137.22
  !
 object-group service ZBF-DIA-External
 tcp 80
```

```
 udp
 tcp range 1024 65535
 tcp source 23
 ip
 icmp
 !
```

OMP Commands

```
omp
   no shutdown
   overlay-as       4294967295
   send-path-limit  16
   ecmp-limit       16
   graceful-restart
   no as-dot-notation
   timers
    holdtime               65535
    advertisement-interval 65535
    graceful-restart-timer 43200
    eor-timer              3600
   exit
   address-family ipv4
    advertise bgp
    advertise ospf external
    advertise connected
    advertise static
    advertise eigrp
    advertise lisp
    advertise isis
   !
   address-family ipv6
    advertise bgp
    advertise connected
    advertise static
    advertise eigrp
    advertise lisp
    advertise isis
```

OSPF Commands

```
router ospf 1 10
  auto-cost reference-bandwidth 100
  timers throttle spf 200 1000 10000
  router-id 10.68.202.1
  compatible rfc1583
          default-information originate
          default-information originate metric-type 1
  distance ospf external 110
  distance ospf inter-area 110
  distance ospf intra-area 110
  redistribute connected subnets
 redistribute nat-route dia
 !
 max-metric router-lsa on-startup 86400
  area 4294967295 nssa no-summary
  area 4294967295 range 10.1.1.0 255.255.255.0 not-advertise
  area 4294967295 range 192.168.1.0 255.255.255.0 cost 16777214
  area 4294967295 range 172.16.5.0 255.255.255.0 advertise
 default-information originate always metric 16777214 metric-type 1
 redistribute static
```

Policy Commands

```
route-map rmap1 deny 10
  match ip address prefix-list prfx1
 !
 route-map rmap1 permit 10
  match as-path 120
  match ip address prefix-list prfx1 !
 route-map clear-df permit 10
 !

parameter-map type inspect-global
  alert on
  log dropped-packets
  multi-tenancy
  vpn zone security
 !

policy
  app-visibility
  flow-visibility
  implicit-acl-logging
  log-frequency        1000
 policer pol1
 rate 500000000
burst 15000
exceed drop
  lists
   data-prefix-list Email-Server
    ip-prefix prfx1



class-map
   class LLQ queue 0
   class Queue0 queue 0
   class VOICE queue 0
   class CRITICAL-DATA queue 1
   class Queue1 queue 1
   class BULK queue 2
   class Queue2 queue 2
   class INTERACTIVE-VIDEO queue 3
   class Queue3 queue 3
   class CONTROL-SIGNALING queue 4
   class Queue4 queue 4
   class Default queue 5
   class Queue5 queue 5
  !
   rewrite-rule Branch-QoS-Rewrite-Template
   class BULK low dscp 10
   class BULK high dscp 10
   class CRITICAL-DATA low dscp 28
   class CRITICAL-DATA high dscp 28
   class INTERACTIVE-VIDEO low dscp 34
   class INTERACTIVE-VIDEO high dscp 34
  !
   access-list acl1
   sequence 10
    match
     destination-ip 172.16.5.10
    !
    action drop
   default-action accept
    action drop
     count 192-167-199-DROP-CNT
```

```
  access-list 4451-Marking-Spoke
   sequence 1
    match
     destination-ip 172.16.10.5
    !
    action accept
     count SSL
     class LLQ
     count EXCHANGE
     class CONTROL-SIGNALING
    action accept
     count RTP
     class LLQ
    action accept
     count HTTP_10K_60K
     class BULK
     action accept
     count HTTP_BROWSING
     class BULK
     count Oracle
     class CRITICAL-DATA
     count Citrix
     class INTERACTIVE-VIDEO
     count SSL
     class BULK
     count EXCHANGE
     class CONTROL-SIGNALING
     count Video
     class INTERACTIVE-VIDEO

"access-list Marking-HQ
   sequence 1
    match
     source-ip 10.74.201.203/32"
 "!
   sequence 21
    match
     source-ip 10.74.201.202/32
    !
    action accept
     set
      dscp 18"
 "policy-map type inspect security-zbfw
    class security-zbfw-seq-1
      inspect"
 "sequence 181
      match
       destination-data-prefix-list QOS-QUALYS-SCANNERS"
 "sequence 11
      match
       destination-ip   10.53.128.23/32
       destination-port 443"
```

Policy Map Commands

```
policy-map type inspect pmap1
 class cos-map-generic inspect
 bandwidth remaining percent 5
 policy-map Branch-QoS-Policy
  class Queue0
   priority level 1
   police rate percent 30
   !
  !
```

```
  class Queue1
   bandwidth remaining ratio 20
   random-detect precedence-based
  !
  class class-default
   bandwidth remaining ratio 10
   random-detect precedence-based
  !
  class Queue3
   bandwidth remaining ratio 20
   random-detect precedence-based
  !
  class Queue4
   bandwidth remaining ratio 10
   random-detect precedence-based
  !
  class Queue5
   bandwidth remaining ratio 10
   random-detect precedence-based
  !
 !
 policy-map shape_GigabitEthernet0/0/1
  class class-default
   service-policy Branch-QoS-Policy
   shape average 1000000000
  !
  class class-default
    drop
  !
 !
```

QOS Policy commands

```
policy-map QOS-POLICY-MAP
 class Queue0
  priority percent 30
 class Queue1
  bandwidth percent 20
 class Queue3
  bandwidth percent 20
 class class-default
  bandwidth percent 30
```

```
policy-map QOS-POLICY-MAP
 class Queue0
  priority percent 30
 class Queue1
  bandwidth percent 20
  random-detect
 class Queue3
  bandwidth percent 20
 class class-default
  bandwidth percent 30
  random-detect
```

```
policy-map QOS-POLICY-MAP
 class Queue0
  priority percent 30
 class Queue1
  bandwidth percent 20
  random-detect
 class Queue3
  bandwidth percent 20
 class class-default
```

```
  bandwidth percent 30
  random-detect
```

```
policy-map QOS-POLICY-MAP
 class Queue0
  priority level 1
  police rate percent 30
 class Queue1
  bandwidth percent 20
  random-detect
 class Queue3
  bandwidth percent 20
 class class-default
  bandwidth percent 30
  random-detect
```

```
policy-map QOS-POLICY-MAP
 class Queue0
  priority level 1
  police rate percent 30
 class Queue1
  bandwidth remaining ratio 20
  random-detect
 class Queue3
  bandwidth remaining ratio 20
 class class-default
  bandwidth remaining ratio 30
  random-detect
```

RADIUS Commands

```
radius-server dead-criteria time 10 tries 3
radius-server deadtime 15
```

Security Commands

```
security
  ipsec
   rekey               1209600
   replay-window       4096
   authentication-type sha1-hmac ah-sha1-hmac ah-no-id
   pairwise-keying
```

SNMP Commands

```
snmp-server community Log view Logging RO
 snmp-server community Trap view Interface RO
 snmp-server contact
 snmp-server enable traps
 snmp-server engineID local
 snmp-server group test_group_v3 v3 noauth read view_test_v3
 snmp-server host 10.100.51.1 vrf 1 version 2c Log udp-port 7081
 snmp-server host 10.1.15.15 version 3 noauth test_user_v3 udp-port 161
 snmp-server community xxxxx view yyyyy RO acl-name1
 snmp-server ifindex persist
 snmp-server location
 snmp-server trap timeout
 snmp-server trap-source Loopback

 snmp-server user test_user_v3 test_group_v3 v3 encrypted
 snmp-server view Interface 1.3.1 included
 snmp-server view Logging 1.4.1 included
 snmp-server view view_test_v3 1.3.6.1 included
```

SSL Proxy Commands

```
sslproxy
  no enable
  rsa-key-modulus      2048
  certificate-lifetime 730
  eckey-type           P256
  ca-tp-label
  settings expired-certificate  drop
  settings untrusted-certificate drop
  settings unknown-status       drop
  settings certificate-revocation-check none
  settings unsupported-protocol-versions drop
  settings unsupported-cipher-suites drop
  settings failure-mode         close
  settings minimum-tls-ver      TLSv1
 no tcpproxy enable
```

System Commands

```
  gps-location latitude 37.368140
  gps-location longitude -121.913658
  system-ip
  overlay-id
  site-id
  port-offset
  control-session-pps
         controller-group-list 1 2
         device-groups  a
  admin-tech-on-failure
  sp-organization-name
  organization-name
         max-omp-sessions      8
  port-hop
  track-transport
  track-default-gateway
  upgrade-confirm
  console-baud-rate
  vbond 192.168.5.4 port 12346
 logging
enable
```

UTD Commands

```
utd multi-tenancy
 utd engine standard multi-tenancy
  utd global
   file-reputation
    cloud-server   cloud-isr-asn.amp.cisco.com
    est-server     cloud-isr-est.amp.cisco.com
    query-interval 300
   !
   file-analysis
    cloud-server panacea.threatgrid.com
   !
  !
  file-analysis profile FILE-ANA-PROFILE1
   file-types
    pdf
    ms-exe
    new-office
    rtf
    mdb
```

```
    mscab
    msole2
    wri
    xlw
    flv
    swf
   !
   alert level critical
  !
  file-reputation profile FILE-REP-PROFILE1
   alert level critical
  !
  file-inspection profile FILE-INS-PROFILE1
   analysis profile FILE-ANA-PROFILE1
   reputation profile FILE-REP-PROFILE1
 !
```

Voice Commands

```
sip-ua
 !
 voice class codec 1000
  codec preference 1 g729r8
  codec preference 2 g711ulaw bytes 160
  codec preference 3 g711alaw bytes 160
  codec preference 4 g722-64 bytes 160
 !
 voice service voip

  allow-connections sip to sip
  no supplementary-service sip handle-replaces
  no supplementary-service sip moved-temporarily
  no supplementary-service sip refer
  sip
   registrar server expires max 300 min 200
  !
 !
 voice register global
  max-dn   200
  max-pool 100
  system message "SRST mode"
 !
 voice register pool 100
  id network 10.0.0.0 mask 255.0.0.0
 !
 dial-peer voice 1000 voip
  description         Branch 1

  destination-pattern 1T
  no shutdown
  voice-class codec 1000
  session transport udp
  session protocol sipv2
  session target ipv4:10.1.101.8
  dtmf-relay rtp-nte digit-drop sip-kpml sip-notify
 !
 dial-peer voice 2000 voip
  description         Branch 1
   destination-pattern 2T
  no shutdown
  voice-class codec 1000
  session transport udp
  session protocol sipv2
  session target ipv4:10.1.101.8
```

```
 dtmf-relay rtp-nte digit-drop sip-kpml sip-notify
!
dial-peer voice 8000 voip
 description         Branch 7
  destination-pattern 8T
 no shutdown
 voice-class codec 1000
 session transport udp
 session protocol sipv2
 session target ipv4:10.1.101.8
 dtmf-relay rtp-nte digit-drop sip-kpml sip-notify
!
dial-peer voice 9000 voip
 description         CallManager for Dial 9

 destination-pattern 9T
 no shutdown
 voice-class codec 1000
 session transport udp
 session protocol sipv2
 session target ipv4:10.1.101.8
 dtmf-relay rtp-nte digit-drop sip-kpml sip-notify
!
```

VRF Commands

```
vrf definition
   address-family ipv4
   address-family ipv6
   description
   rd
   route-target export
   route-target import
 service tcp-keepalives-in
 service tcp-keepalives-out
 service tcp-small-servers
 service udp-small-servers
```

Zone Based Firewall commands

```
zone security LAN
  vpn 2
 !
 zone security WAN
  vpn 0
 !
 zone-pair security ZP_LAN_WAN_test-policy source LAN destination WAN
  service-policy type inspect test-policy
 !
 zone-pair security ZP_WAN_LAN_test-policy source WAN destination LAN
  service-policy type inspect test-policy
```

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.3.1a

Table 1: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	Starting Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, you can use additional commands in CLI Add-on feature templates.

AAA Commands

- `aaa authentication password-prompt <>`
- `aaa authentication username-prompt <>`
- `aaa authentication login default group tacacs+ local`
- `aaa authentication enable default group tacacs+ enable`
- `aaa authorization console`
- `aaa authorization config-commands`
- `aaa authorization exec default local group tacacs+`
- `aaa authorization commands 15 default local group tacacs+`
- `aaa accounting connection default stop-only group tacacs+`
- `aaa accounting exec default start-stop group tacacs+`
- `aaa accounting commands 15 default start-stop group tacacs+`
- `aaa authorization network default local`
- `aaa accounting system default start-stop group tacacs+`
- `aaa authentication attempts login`
- `aaa authentication ppp dialinppp local`
- `login block-for <> attempts <> within`
- `login quiet-mode access-class <ACL>`
- `tacacs server server name`
- `tacacs server server name`
  `address ipv4 192.0.2.1`
- `ip tacacs source-interface Loopback0`
- `tacacs server server-name`
  `key Ys6WhgHS40`

ACL Commands

- `ip access-list standard <>`
- `ip access-list standard 15 permit <>`
- `ip access-list standard 15 deny <>`
- `ip access-list standard 15 deny any <>`
- `ip access-list extended <>`
- `ip access-list extended 105 <> ip any any`
- `ip access-list extended 105 deny <> any any`
- `ip access-list extended 105 deny ip <> any`
- `ip access-list extended 105 deny ip any <>`
- `ip access-list extended EXTACL deny ip any any <>`
- `ip access-list extended DSCP-OUT-SAA <> udp any range 64001 64005 any`
- `ip access-list extended DSCP-OUT-SAA permit <> any range 64001 64005 any`
- `ip access-list extended DSCP-OUT-SAA permit udp <> range 64001 64005 any`
- `ip access-list extended DSCP-OUT-SAA permit udp any range <> 64005 any`
- `ip access-list extended DSCP-OUT-SAA permit udp any range 64001 <> any`
- `ip access-list extended BGP-D1 permit tcp any eq <> any`
- `ip access-list extended DSCP-OUT-SAA permit udp any range 64001 64005 <>`
- `ip access-list extended DSCP-OUT-SAA permit icmp host <> any`
- `ip access-list extended DSCP-OUT-SAA permit udp any any range <> 64005`
- `ip access-list extended DSCP-OUT-SAA permit udp any any range 64001 <>`
- `ip access-list extended DSCP-OUT-SAA permit udp any range 64001 64005 any <>`
- `ip access-list extended BGP-D1 permit tcp any any eq <>`

ATM Commands

- `interface ATM <>`
- `interface ATM 0/0/0`
  `ip <>`
- `interface ATM 0/0/0`
  `atm <>`
- `interface ATM 0/0/0`
  `<>`
- `interface ATM 0/2/0.1 <>`
- `interface ATM 0/2/0.1 point-to-point`
  `pvc 0/1`
  `encapsulation aal5mux <>`
- `interface ATM 0/2/0.1 point-to-point`
  `pvc 0/1`
  `encapsulation <>`
- `interface ATM 0/2/0.1 point-to-point`
  `pvc 0/1`
  `vbr-nrt <> 48 1`
- `interface ATM 0/2/0.1 point-to-point`
  `pvc 0/1`
  `vbr-nrt 48 <> 1`
- `interface ATM 0/2/0.1 point-to-point`
  `service-policy output <>`
- `interface ATM 0/2/0.1 point-to-point`
  `<>`
- `interface ATM 0/2/0.1 point-to-point`
  `pvc 0/1`
  `oam-pvc <>`
- `interface ATM 0/2/0.1 point-to-point`
  `pvc 0/1`
  `oam-pvc manage <>`
- `interface ATM 0/2/0.1 point-to-point`
  `pvc 0/1`
  `oam retry <>`

Frame Relay Commands

- `interface Serial 0/1/0`
  `encapsulation frame-relay <ietf>`
- `interface Serial 0/1/0`
  `frame-relay lmi-type <ansi>`
- `interface Serial 0/1/0`
  `frame-relay intf-type <dte>`
- `interface Serial 0/1/0`
  `frame-relay intf-type <dce>`

- `interface Serial 0/1/0`
  `frame-relay interface-dlci <>`
- `interface Serial 0/1/0`
  `< >`
- `interface Serial 0/1/0.2 point-to-point`
  `ip address <192.0.2.1> 255.255.255.0`
- `interface Serial 0/1/0.2 point-to-point`
  `frame-relay interface-dlci <>`
- `interface Serial 0/1/0.2 point-to-point`
  `<>`
- `interface Serial 0/0/1:5`
  `ip address <192.0.2.1> 255.255.255.0`
- `interface Serial 0/0/1:5`
  `encapsulation frame-relay`
- `interface Serial 0/0/1:5`
  `frame-relay intf-type <dte>`
- `interface Serial 0/0/1:5`
  `frame-relay intf-type <dce>`
- `interface Serial 0/0/1:5`
  `<>`
- `interface MFR<>`
- `interface MFR 1`
  `ip address <192.0.2.1> 255.255.255.0`
- `interface MFR 1`
  `frame-relay multilink bandwidth-class <a>`
- `interface MFR 1`
  `frame-relay multilink bandwidth-class <b>`
- `interface MFR 1`
  `frame-relay multilink bandwidth-class c <>`
- `interface MFR 1`
  `frame-relay intf-type <dte>`
- `interface MFR 1`
  `frame-relay intf-type <dce>`
- `interface MFR 1`
  `frame-relay interface-dlci <>`
- `interface MFR 1`
  `<>`

HTTP Commands

- `no ip http server`
- `no ip http secure-server`

Interface Commands

- `configure interface  <id> mtu <size>`
- `configure interface  <id> mtu <size greater than 1500 and upto 9000>`
- `configure interface <id> ip mtu <size>`
- `configure interface <id> description`
- `configure interface <id> hold-queue in`
- `configure interface <id> hold-queue out`
- `configure interface <id> no shutdown`
- `configure interface ATM <id> encapsulation dot1Q <vlan-id>`
- `configure interface Ethernet <id> encapsulation dot1Q <vlan-id>`

IP Commands

- ```
  interface GigabitEthernet2.1
  encapsulation dot1Q 1
  ip address <> 255.255.255.0
  ```
- ```
  interface GigabitEthernet 3
  ip address <> 255.255.255.0
  ```
- ```
  interface ATM0/3/0
  ip address <> 255.255.255.0
  ```
- ```
  interface ATM0/3/0.1
  ip address <> 255.255.255.0
  ```
- ```
  interface Serial2/0
  ip address <> 255.255.255.0
  ```
- ```
  interface Loopback 2
  ip address <> 255.255.255.0
  ```
- ```
  interface Dialer2
  ip address <> 255.255.255.0
  ```
- ```
  interface Vlan 1
  ip address <> 255.255.255.0
  ```
- ```
  interface Dialer 2
  ip unnumbered <>
  ```
- `ip route 192.0.2.1 255.255.255.0 198.51.100.1 track <>`
- `ip route 192.0.2.1 255.255.255.0 Dialer2 198.51.100.1 tag <>`
- `ip route 192.0.2.1 255.255.255.0 198.51.100.1 tag <>`
- `ip route 192.0.2.1 255.255.255.0 Dialer2 tag <>`
- `ip route 192.0.2.1 255.255.255.0 Dialer2 198.51.100.1 <>`
- `ip route 192.0.2.1 255.255.255.0 198.51.100.1 <>`
- `ip route 192.0.2.1 255.255.255.0 Dialer2 <>`
  ```

- `ip route 192.0.2.1 255.255.255.0 GigabitEthernet2 <>`
- `ip route 192.0.2.1 255.255.255.0 <>`
- `ip route vrf 1 192.0.2.1 255.255.255.0 198.51.100.1 track <>`
- `ip route vrf 1 192.0.2.1 255.255.255.0 198.51.100.1 tag <>`
- `ip route vrf 1 192.0.2.1 255.255.255.0 198.51.100.1 <>`
- `ip route vrf 1 192.0.2.1 255.255.255.0 GigabitEthernet2 <>`
- `ip route vrf 1 192.0.2.1 255.255.255.0 <>`
- `ip icmp rate-limit unreachable <>`
- `interface Dialer 2`
  `ip <>`
- `interface GigabitEthernet 2.100`
  `ip <>`
- `interface GigabitEthernet 2`
  `ip <>`
- `ip <>`
- `ip icmp redirect <host>`
- `ip icmp redirect <subnet>`
- `interface Tunnel 10`
  `ip <>`
- `ip ftp <>`
- `ip rcmd <>`
- `interface Dialer 2`
  `ip address <>`
- `interface GigabitEthernet 2`
  `ip address <>`
- `interface Virtual-Template 2`
  `ip address <>`

IPoE MTU

- `mtu<size>`
- `ip mtu <size>`

IPv6 Commands

- `no ipv6 source-route`
- `interface GigabitEthernet 2`
  `ipv6 <>`
- `interface GigabitEthernet 2.100`
  `ipv6 <>`

- `interface GigabitEthernet 2`
  `ipv6 nd ra suppress <>`
- `interface GigabitEthernet 2`
  `ipv6 nd prefix <>`
- `interface GigabitEthernet 2`
  `ipv6 nd router-preference <>`
- `interface GigabitEthernet 2`
  `ipv6 address autoconfig`
- `interface GigabitEthernet 2`
  `ipv6 nd other-config-flag`

Line Commands

- `line console 0`
  `transport <>`
- `line vty 0 4`
  `transport <>`
- `line console 0`
  `transport output <ssh>`
- `line vty 0 4`
  `transport output <ssh>`

Logging Commands

- `logging console <>`
- `logging monitor <>`
- `logging <>`
- `banner login <>`

PPP Commands

- `interface Dialer 1`
  `encapsulation ppp`
- `interface Dialer 2`
  `encapsulation ppp`
  `ppp authentication chap <>`
- `interface Dialer 3`
  `encapsulation ppp`
  `ppp chap hostname <>`
- `interface Dialer 4`
  `encapsulation ppp`
  `ppp chap password 0 <>`
- `interface ATM 0/3/0`
  `pvc 0/1`
  `encapsulation aal5mux ppp <>`

- interface ATM 0/3/0.1 point-to-point
  pvc 0/20
  encapsulation aal5mux ppp <>
- interface ATM 0/3/0
  pvc 0/1
  encapsulation aal5mux ppp Virtual-Template <>

PPPoEoVlan - Chap Commands

- policy-map COS-OUT-SHAPED
- class class-default
- set cos {dot1P_Value}
- interface {Ethernet_Interface}
- mtu 1774
- no ip address
- no shutdown pppoe enable group global
- pppoe-client dial-pool-number 1
- pppoe-client ppp-max-payload 1766
- service-policy output COS-OUT-SHAPED
- no shutdown
- interface Dialer1
- mtu 1766
- ip unnumbered Loopback0
- encapsulation ppp
- dialer pool 1
- ppp authentication chap callin
- ppp chap hostname {Usename}
- ppp chap password {Chap_Password}
- no shutdown

Routemap Commands

- route-map <>
- route-map abc <permit> 10
- route-map def <deny> 20
- route-map abc permit <>
- route-map map-tag deny <>

- `route-map map-tag permit 25`
  `match length <> 2147483647`
- `route-map map-tag permit 30`
  `match length 1 <>`
- `route-map map-tag permit 35`
  `match ipv6 address prefix-list <>`
- `route-map map-tag permit 40`
  `match ipv6 address <>`
- `route-map map-tag permit 311`
  `set ipv6 next-hop <2::2>`
- `route-map map-tag permit 45`
  `set ipv6 precedence <>`
- `route-map map-tag permit 50`
  `set interface Dialer <1>`
- `route-map map-tag permit 55`
  `set interface GigabitEthernet <3>`
- `route-map map-tag permit 60`
  `set interface Tunnel <1>`
- `route-map map-tag permit 251`
  `set ipv6 default  next-hop <1::1>`
- `route-map map-tag permit 56`
  `set default interface GigabitEthernet <3>`
- `route-map map-tag permit 79`
  `set default interface Tunnel <11>`
- `route-map map-tag permit 75`
  `set vrf <1>`
- `interface GigabitEthernet 3`
  `ipv6 policy route-map <>`
- `ipv6 local policy route-map <>`

Security Commands

To configure posture assessment use the CLI Add-on template in Cisco vManage.

Configure IEEE 802.1x authentication and authorization

```
policy-map type control subscriber simple_dot1x
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x
!
interface GigabitEthernet0/1/7
 switchport access vlan 22
 switchport mode access
 access-session closed
 access-session port-control auto
 dot1x pae authenticaton
 service-policy type control subscriber simple_dot1x
!
```

```
interface Vlan22
 ip address 198.51.100.1 198.51.100.254
```

Configure device tracking

```
!
device-tracking policy tracking_test
 security-level glean
 no protocol ndp
 no protocol dhcp6
 tracking enable
!
interface GigabitEthernet0/1/7
 device-tracking attach-policy tracking_test
```

SHDSL Commands

- ```
  Router# config-transaction
  Router(config)# controller shdsl 0/1/0
  Router(config-controller)# termination cpe
  ```
- ```
  Router# config-transaction
  Router(config)# controller shdsl 0/1/0
  Router(config-controller)# termination <cpe/co>
  Router(config-controller)# mode atm
  ```
- ```
  Router# config-transaction
  Router(config)# controller shdsl 0/1/0
  Router(config-controller)# termination cpe
  Router(config-controller)# mode efm
  ```
- ```
  Router# config-transaction
  Router(config)# controller shdsl 0/1/0
  Router(config-controller)# termination cpe
  Router(config-controller)# mode atm
  Router(config-controller)# dsl-group 0 pairs 0
  Router(config-controller-dsl-group)#
  ```
- ```
  Router# config-transaction
  Router(config)# controller shdsl 0/1/0
  Router(config-controller)# termination cpe
  Router(config-controller)# mode atm
  Router(config-controller)# dsl-group auto
  Router(config-controller-dsl-group)#
  ```
- ```
  Router(config)# controller shdsl 0/1/0
  Router(config-controller)# termination cpe
  Router(config-controller)# mode atm
  Router(config-controller)# dsl-group 0 pairs 0-3 m-pair
  Router(config-controller-dsl-group)#
  ```
- ```
  Router(config)# controller shdsl 0/1/0
  Router(config-controller)# termination cpe
  Router(config-controller)# mode efm
  Router(config-controller)# dsl-group 0 pairs 0-3 efm-bond
  Router(config-controller-dsl-group)#
  ```
- ```
  Router(config)# controller shdsl 0/1/0
  Router(config-controller)# termination cpe
  Router(config-controller)# mode atm
  Router(config-controller)# dsl-group 0 pairs 0
  Router(config-controller)# dsl-group 1 pairs 2-3 m-pair
  ```

```
Router(config)# controller shdsl 0/1/0
Router(config-controller)# termination cpe
Router(config-controller)# mode efm
Router(config-controller)# dsl-group 0 pairs 0
Router(config-controller)# dsl-group 1 pairs 1-2 efm-bond
Router(config-controller)# dsl-group 3 pairs 3
```

- ```
  Router# configure terminal
  Enter configuration commands, one per line. End with CNTL/Z.
  Router(config)#controller shdsl 0/1/0
  Router(config-controller)#firmware phy?
  filename filename to read firmware

  Router(config-controller)# firmware phy filename ?

  flash: Download fw file name
  bootflash: Download fw file name

  Router(config-controller)#firmware phy filename
  bootflash:IDC_192.0.2.1_DFE_1.1-1.8.1__001.pkg
  ```
- ```
  shdsl annex { annex standard } [ coding < tcpam >]
  ```

```
Router(config-controller-dsl-group)# shdsl annex ?

A Annex A of G.991.2 standard
A-F Annex A/F of G.991.2 standard
B Annex B of G.991.2 standard
B-G Annex B/G of G.991.2 standard
F Annex F of G.991.2 standard
G Annex G of G.991.2 standard

Router(config-controller-dsl-group)# shdsl annex F coding ?

128-TCPAM 128-TCPAM line coding
16-TCPAM 16-TCPAM line coding
32-TCPAM 32-TCPAM line coding
4-TCPAM 4-TCPAM line coding
64-TCPAM 64-TCPAM line coding
8-TCPAM 8-TCPAM line coding


Router(config-controller-dsl-group)# shdsl annex F coding 32-TCPAM
```

- ```
  Router (config-controller-dsl-group)# shdsl rate <rate>
  ```
- ```
  Router(config-controller-dsl-group)# handshake ?

  auto Initiate auto handshake
  ieee Initiate IEEE handshake
  itut Initiate ITUT handshake
  ```
- ```
  CPE(config-controller-dsl-group)# shdsl 4-wire mode enhanced
  ```
- ```
  CPE(config-controller-dsl-group)# ignore
  ```
- ```
  CPE(config-controller-dsl-group)# shutdown
  ```

SNMP Commands

- ```
  snmp-server packetsize <>
  ```

- `snmp-server view supriya iso <>`
- `snmp-server user  SNMP_V3_User SNMP_Group_Name v3 auth sha sha_pwd priv aes 128 aes_pwd access ipv6 <>`
- `snmp-server engineID local  <123456ABCD>`
- `snmp mib community-map SNMP_V2c_Community_String  engineid <12345ABCD6>`
- `snmp-server community <>`
- `snmp-server community MyROCommunity ro <>`
- `snmp-server community someword1 view someword2 ro <>`
- `snmp-server group someword v3 priv read someword access <>`
- `snmp-server group someword v3 priv read someword access ipv6  <>`
- `snmp-server file-transfer access-group <>`
- `snmp-server enable traps snmp authentication`
- `snmp-server enable traps snmp coldstart`
- `snmp-server enable traps snmp linkdown`
- `snmp-server enable traps snmp linkup`
- `snmp-server enable traps snmp warmstart`

TCP Commands

- `service tcp-keepalives-in`
- `service tcp-keepalives-out`
- `service tcp-small-servers`
- `service udp-small-servers`
- `ip finger`

VDSL Commands

- `config-transaction`

  `controller VDSL slot/subslot/port`

  `operating mode auto`
- `line-mode single-wire line line-number`
- `line-mode bonding`
-
```
Router# config-transaction
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#controller shdsl 0/1/0
Router(config-controller)#firmware phy?
filename filename to read firmware

Router(config-controller)# firmware phy filename ?
```

- `sra`
- `bitswap`
- `modem <keyword>`
- `description <string>`
- `diagnostics DELT`
- `training log filename flash:<filename>`
- `sync mode`
- `sync interval`

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.4.1a

Table 2: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	Starting Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, you can use additional commands in CLI Add-on feature templates.

AAA and DOT1X Global Configuration

```
aaa group server radius radius-0
 server-private {ise_server} auth-port 1812 acct-port 1813 timeout 5 retransmit 3 key
cisco123

aaa authorization network default group radius-0
aaa authentication dot1x default group radius-0
aaa accounting dot1x default start-stop group radius-0

dot1x system-auth-control
radius-server dead-criteria time 10 tries 3
radius-server deadtime 15
```

AAA Tacacs and Radius

```
aaa group server radius rad123
 server-private 10.255.255.254
ip radius source-interface GigabitEthernet0/0/1
 radius-server key 0
$CRYPT_CLUSTER$a8YJvVLAFYXnoYOhLUMO5Q==$6tofKux6yYsQ42+nYL9FGf3wg4cKWLxB4O5zdWoFvmY=
aaa group server tacacs+ tac123
 server-private 10.255.255.254 key 0
$CRYPT_CLUSTER$a8YJvVLAFYXnoYOhLUMO5Q==$6tofKux6yYsQ42+nYL9FGf3wg4cKWLxB4O5zdWoFvmY=
ip tacacs source-interface GigabitEthernet0/0/1
aaa authentication login default group rad123 group tac123 local
username admin privilege 15 secret 5 $1$XQJ4$VxlKu0qZFDzNz8PjZqFSF1
```

CFM CLI List

```
ethernet cfm ieee
ethernet cfm global
ethernet cfm traceroute cache
ethernet cfm logging
ethernet cfm traceroute cache size entries
ethernet cfm traceroute cache hold-time minutes
snmp-server enable traps ethernet cfm cc
snmp-server enable traps ethernet cfm crosscheck
ethernet evc evc-id
ethernet cfm domain domain-name level level-id
 id dns dns-name
 mep ccm-hold-time hours
 mep ccm-fastage enable
 mep archive-hold-time minutes
 sender-id chassis
 service vpn-id vpn-id port
 service vlan-id vlan-id port
 service number MA-number port
 service short-ma-name port
 service short-ma-name evc evc-name vlan vlanid direction down
  continuity-check
  continuity-check [interval cc-interval]
  continuity-check loss-threshold threshold
  ais period 1 or 60
  ais level 0-7
  ais expiry-threshold 0-255
  ais suppress-alarms
  maximum meps 1-65535
  sender-id chassis
  offload sampling sample
Interface interface-name
 cfm mep domain domain-name mpid id service service-name
  alarm notification all*
  cos 0-7
 ethernet oam
 ethernet oam mode passive
 ethernet oam remote-loopback supported
 ethernet loopback permit external
```

CXP Branch DIA

```
class-map match-any ART_APPLICATIONS
 match protocol attribute application-group ms-cloud-group
!
performance monitor context sdwanarts profile sdwan-performance
 exporter destination local-sdwan source Null0
 traffic-monitor art-cor-saas class-and ART_APPLICATIONS ipv4
!
performance monitor sampling-rate 10
performance monitor apply sdwanarts color-all-dia|color
!
```

CXP Gateway

```
class-map match-any ART_APPLICATIONS
 match protocol attribute application-group ms-cloud-group
!
performance monitor context sdwanarts profile sdwan-performance
 exporter destination local-sdwan source Null0
 traffic-monitor art-cor-saas class-and ART_APPLICATIONS ipv4
!
performance monitor sampling-rate 10
```

```
interface GigabitEthernetx/x/x
 performance monitor context sdwanarts
!
```

DSL NIM Support

```
controller VDSL 0/1/0
line-mode single-wire line
no shutdown/shutdown
operating mode auto/adsl1/adsl2/adsl2+/auto adsl/auto adsl2/auto adsl2+/vdsl2
sra
bitswap
description VADSL_Ping_Test
training log filename bootflash:testlog.bin
firmware phy filename bootflash:nim_vab_phy_fw_A38q_B39x3.pkg
!
interface ATM0/1/0
description Atm_Main_intf
no shutdown
ip mtu 1500
mtu 1500
!
interface ATM0/1/0.303 point-to-point
description Atm_Sub_intf
no shutdown
ip address 192.0.2.254 255.255.255.0
ip mtu 1492
pvc 20/60
encapsulation aal5snap/aal5mux ppp dialer
protocol ppp dialer/dialer pool-member 1
!
!
interface Ethernet0/1/0
description Ethernet_Main_intf
no shutdown
mtu 1500
!
interface Ethernet0/1/0.303
description Ethernet_Sub_intf
no shutdown
encapsulation dot1Q 303
ip address 192.0.2.254 255.255.255.0
ip mtu 1492
pppoe enable
pppoe-client dial-pool-number 30
pppoe-client ppp-max-payload 1708
!
interface GigabitEthernet0/0/0
no shutdown
arp timeout 1200
ip address 192.0.2.254 255.255.255.0
no ip redirects
ip mtu 1500
mtu 1500
negotiation auto
!
interface Loopback1
description intf_loop_1
no shutdown
ip address 192.0.2.254 255.255.255.0
!
interface Loopback2
description intf_loop_2
no shutdown
```

```
ip address 192.0.2.254 255.255.255.0
!
interface Dialer30
no shutdown
encapsulation ppp
ip unnumbered Loopback1/Loopback2/GigabitEthernet0/0/0
dialer pool 30
ppp chap hostname cisco
ppp chap password 0 sisco
ppp pap sent-username cisco password sisco
ppp authentication chap pap callin
!
interface Tunnel0
no shutdown
ip unnumbered GigabitEthernet0/0/0
no ip redirects
ipv6 unnumbered GigabitEthernet0/0/0
no ipv6 redirects
tunnel source GigabitEthernet0/0/0
tunnel mode sdwan
!
interface Tunnel3
no shutdown
ip unnumbered Dialer30
tunnel source Dialer30
tunnel mode sdwan
!
sdwan
interface GigabitEthernet0/0/0
tunnel-interface
encapsulation ipsec weight 1
no border
color mpls
no last-resort-circuit
no low-bandwidth-link
no vbond-as-stun-server
vmanage-connection-preference 5
port-hop
carrier default
nat-refresh-interval 5
hello-interval 1000
hello-tolerance 12
allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
allow-service sshd
allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
no allow-service snmp
no allow-service bfd
!
interface Dialer30
tunnel-interface
encapsulation ipsec
color biz-internet
allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns
```

```
allow-service icmp
allow-service sshd
allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
no allow-service snmp
no allow-service bfd
!
!
```

FNF Support for IPv6

```
app-visibility-ipv6
flow-visibility-ipv6
ip visibility cache entries
ipv6 visibility cache entries
```

GRE/IPSec LoadBalancing Using ECMP to Zscaler ZEN Node

```
interface Tunnel100512
 tunnel route-via GigabitEthernet1 mandatory
ip sdwan route vrf 1 0.0.0.0/0 service sig
sdwan service sig vrf global
 ha-pairs
  interface-pair Tunnel100511 active-interface-weight 100 Tunnel100512 backup-interface-weight
 200
```

IPSLA IPv4

```
ip sla 1
  icmp-echo 203.0.113.255
  vrf 100
ip sla schedule 1 life forever start-time now
track 1 ip sla 1 state
ip sla 2
  icmp-echo 203.0.113.255
  vrf 300
ip sla schedule 2 life forever start-time now
track 2 ip sla 2 state
ip access-list extended test300
 100 permit ip any 203.0.113.255 255.255.255.0
ip access-list extended test100
 100 permit ip any 192.0.2.254 255.255.255.0
!
class-map match-any test300
 match access-group name test300
class-map match-any test100
 match access-group name test100
!
policy-map type epbr test300
 class test300
  set ipv4 vrf 300 next-hop verify-availability 192.0.2.254 10 track 2
policy-map type epbr test100
 class test100
  set ipv4 vrf 100 next-hop verify-availability 192.0.2.254 10 track 1
!
interface GigabitEthernet0/0/1
 service-policy type epbr input test300
interface GigabitEthernet0/0/2
 service-policy type epbr input test100
!
```

IPv4 EPBR

```
ip access-list extended test300
 100 permit ip any 0.0.0.2 255.255.255.0
ip access-list extended test100
 100 permit ip any 0.0.0.2 255.255.255.0
!
class-map match-any test300
 match access-group name test300
class-map match-any test100
 match access-group name test100
!
policy-map type epbr test300
 class test300
  set ipv4 vrf 300 next-hop 203.0.113.255
policy-map type epbr test100
 class test100
  set ipv4 vrf 100 next-hop 203.0.113.255
!
interface GigabitEthernet0/0/1
 service-policy type epbr input test300
interface GigabitEthernet0/0/2
 service-policy type epbr input test100
```

IPv6 EPBR

```
ipv6 access-list test300_v6
  sequence 100 permit ipv6 any 2003::2/64
ipv6 access-list test100_v6
 sequence 100 permit ipv6 any 2001::2/64
!
class-map match-any test300_v6
 match access-group name test300_v6
class-map match-any test100_v6
 match access-group name test100_v6
!
policy-map type epbr test300_v6
 class test300_v6
  set ipv6 vrf 300 next-hop 2003::2
policy-map type epbr test100_v6
 class test100_v6
  set ipv6 vrf 100 next-hop 2001::2
!
interface GigabitEthernet0/0/1
 service-policy type epbr input test300_v6
interface GigabitEthernet0/0/2
 service-policy type epbr input test100_v6
```

Loopback Ports

```
interface Loopback100
 ip mtu 2000
```

Multi-SN (SC CLI List)

```
vrf definition 300
rd 1:300
address-family ipv4
route-target export 1:300
route-target import 1:300
exit-address-family
!
address-family ipv6
```

```
exit-address-family
interface TenGigabitEthernet0/1/2
no shutdown
arp timeout 1200
vrf forwarding 300
ip address 10.255.255.254 255.255.255.0
ip mtu 1496
ip nbar protocol-discovery
mtu 1500
exit
service-insertion appnav-controller-group appqoe ACG-APPQOE
appnav-controller 10.255.255.254 vrf 300
!
service-insertion service-node-group appqoe SNG-APPQOE
service-node 10.255.255.254
service-node 10.255.255.254
!
service-insertion service-context appqoe/1
appnav-controller-group ACG-APPQOE
service-node-group SNG-APPQOE
cluster-type service-controller
enable
vrf global
!
policy
app-visibility
app-visibility-ipv6
flow-visibility
flow-visibility-ipv6
no implicit-acl-logging
log-frequency 1000
!
```

Multi-SN (SN CLI List)

```
interface GigabitEthernet2
no shutdown
arp timeout 1200
ip address 10.255.255.254 255.255.255.0
no ip redirects
ip mtu 1500
mtu 1500
negotiation auto
interface VirtualPortGroup2
no shutdown
ip address 192.168.2.1 255.255.255.0
service-insertion appqoe
service-insertion service-node-group appqoe SNG-APPQOE
device-role service-node
service-node 192.168.2.2
```

Per-Class App Aware Routing

```
policy
sla-class sla1
loss 10
jitter 10
latency 10
app-probe-class apc1
!
sla-class sla2
loss 50
jitter 50
```

```
latency 50
app-probe-class apc2
!
app-route-policy _vpn_1_list_perclassaar_policy_vpn_1_list
vpn-list vpn_1_list
sequence 1
match
source-ip 10.0.0.0/8
!
action
sla-class sla1
!
!
sequence 11
match
source-ip 10.0.0.0/8
!
action
count counter2
sla-class sla1
!
!
default-action sla-class sla2
!
lists
site-list site_all_app_regr
site-id 100
site-id 400
site-id 500
site-id 600
!
app-probe-class apc1
forwarding-class class3
color lte dscp 10
color 3g dscp 11
color red dscp 12
color gold dscp 13
!
app-probe-class apc2
forwarding-class class5
color lte dscp 20
color 3g dscp 21
!
vpn-list vpn_1_list
vpn 1
!
!
!
apply-policy
site-list site_all_app_regr
app-route-policy _vpn_1_list_perclassaar_policy_vpn_1_list
bfd color lte
dscp 35
bfd color 3g
dscp 36
bfd default-dscp 28
!
!
```

PMTU Configuration

```
bfd color lte
hello-interval 1000
```

```
pmtu-discovery
multiplier 1
```

POE

```
interface {intf-name}
power inline auto max <4000-60000>
power inline auto
power inline never
```

Policy Based SIG

```
policy
data-policy sig_ha_zscaler_data_policy_vedg
  vpn-list vpn_1
   sequence 90
    match
     destination-ip 10.255.255.254/32
    action accept
     count seqcnt_90
     sig
   sequence 100
    match
     destination-ip 10.255.255.254/32
    action accept
     count seqcnt_100
     sig
   sequence 110
    match
     destination-ip 10.255.255.254/32
    action accept
     count seqcnt-110
     sig
   default-action accept
 lists
  vpn-list vpn_1
   vpn 1
  site-list vedge_1
   site-id 500
   site-id 600
apply-policy
 site-list vedge_1
  data-policy sig_ha_zscaler_data_policy_vedg from-service
```

Routed Ports

```
interface GigabitEthernet0/0/1
ip mtu 9000
mtu 9216
```

SLA IPv6

```
ip sla 3
  icmp-echo 2001::2
  vrf 100
ip sla schedule 3 life forever start-time now
track 3 ip sla 3 state
ip sla 4
  icmp-echo 2003::2
  vrf 300
ip sla schedule 4 life forever start-time now
track 4 ip sla 4 state
ipv6 access-list test300_v6
```

```
  sequence 100 permit ipv6 any 2003::2/64
ipv6 access-list test100_v6
 sequence 100 permit ipv6 any 2001::2/64
!
class-map match-any test300_v6
 match access-group name test300_v6
class-map match-any test100_v6
 match access-group name test100_v6
!
policy-map type epbr test300_v6
 class test300_v6
  set ipv6 vrf 300 next-hop verify-availability 2003::2 10 track 4
policy-map type epbr test100_v6
 class test100_v6
  set ipv6 vrf 100 next-hop verify-availability 2001::2 10 track 3
!
!
interface GigabitEthernet0/0/1
 service-policy type epbr input test300_v6
interface GigabitEthernet0/0/2
 service-policy type epbr input test100_v6
!
```

SNMP

- snmp-server community 0 $CRYPT_CLUSTER$IXnkuKPGacBNK+bXDmIq4Q==$msxENYwt8IX5ylClfcb+rA== view 4431_view ro
  snmp-server host 10.255.255.254 0 $CRYPT_CLUSTER$IXnkuKPGacBNK+bXDmIq4Q==$msxENYwt8IX5ylClfcb+rA== udp-port 100 version 2csnmp-server view 4431_view iso included
- snmp-server host 10.255.255.254 vrf Mgmt-intf 0 $CRYPT_CLUSTER$IXnkuKPGacBNK+bXDmIq4Q==$msxENYwt8IX5ylClfcb+rA==snmp-server host 10.255.255.254 vrf Mgmt-intf 0 $CRYPT_CLUSTER$IXnkuKPGacBNK+bXDmIq4Q==$msxENYwt8IX5ylClfcb+rA== udp-port 15
- snmp-server host 10.1.1.1 vrf vrf-name informs version 2c priv 0 $CRYPT_CLUSTER$IXnkuKPGacBNK+bXDmIq4Q==$msxENYwt8IX5ylClfcb+rA== udp-port 15
- snmp mib community-map 0 $CRYPT_CLUSTER$IXnkuKPGacBNK+bXDmIq4Q==$msxENYwt8IX5ylClfcb+rA==
- snmp-server community 0 $CRYPT_CLUSTER$IXnkuKPGacBNK+bXDmIq4Q==$msxENYwt8IX5ylClfcb+rA==> ro acl-name

Spanning Tree

```
spanning-tree mode rapid-pvst
interface {intf-name}
spanning-tree portfast
```

SVI Ports

```
interface Vlan25
ip mtu 1600
```

Switchport Interface Configuration

- interface {intf-name}
  switchport mode access
  switchport access vlan {vlan_id}
  dot1x pae authenticator
  authentication order dot1x mab

```
authentication host-mode single-host
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown
```

- `interface {intf-name}`
  `speed {value}`
  `duplex {value}`
  `mtu {value}`
  `switchport mode trunk`
  `switchport trunk allowed vlan {vlans}`
  `switchport trunk native vlan {vlans_id}`
  `no shutdown`
- `mac address-table static {mac1} vlan {intf_vlan} interface {intf_name}`

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.5.1a

Table 3: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Release 17.5.1	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Additional commands are qualified for use in Cisco vManage CLI templates.

Application-Aware Routing

```
fallback-best-tunnel
criteria jitter
```

Application Performance Monitoring

```
performance monitor context 175_SDWAN profile sdwan-performance
exporter destination 10.0.1.128 source GigabitEthernet9 port 2055
traffic-monitor application-response-time
traffic-monitor media
!
performance monitor apply 175_SDWAN sdwan-tunnel
```

Multicast PIM BSR Dynamic RP

```
ip pim vrf 1 bsr-candidate GigabitEthernet5
ip pim vrf 1 rp-address 172.16.255.116
ip pim vrf 1 rp-candidate GigabitEthernet5 interval 10 priority 5

ip pim sparse-mode

spt-only
```

Data Policy Next-hop

```
next-hop-loose
```

DCA

```
platform resource service-plane-heavy
platform resource data-plane-heavy
```

DIA - DDOS Visibility

```
policy
implicit-acl-logging
log-frequency  <int value>
```

DRE

Service Node Configuration

```
interface VirtualPortGroup2
no shutdown
ip address 192.168.2.1 255.255.255.0
service-insertion appqoe
exit
interface VirtualPortGroup3
no shutdown
ip address 192.168.3.1 255.255.255.252
exit

app-hosting appid dreopt
app-vnic gateway0 virtualportgroup 3 guest-interface 1
guest-ipaddress 192.168.3.2 netmask 255.255.255.252
!
start
!

dual-side optimization enable
```

Integrated Service Node Configuration

```
interface VirtualPortGroup2
no shutdown
ip address 192.168.2.1 255.255.255.0
service-insertion appqoe
exit
interface VirtualPortGroup3
no shutdown
ip address 192.168.3.1 255.255.255.252

service-insertion appnav-controller-group appqoe ACG-APPQOE
appnav-controller 192.168.2.1
!
service-insertion service-node-group appqoe SNG-APPQOE
service-node 192.168.2.2
!
service-insertion service-context appqoe/1
appnav-controller-group ACG-APPQOE
service-node-group SNG-APPQOE
cluster-type integrated-service-node
enable
vrf global
!
iox
app-hosting appid dreopt
```

```
app-vnic gateway0 virtualportgroup 3 guest-interface 1
guest-ipaddress 192.168.3.2 netmask 255.255.255.252
!
start
!
dreopt enable
!
dual-side optimization enable
!
```

Office 365: Dynamic NBAR Mapping

```
service-area exchange
```

Geo Filter

```
object-group geo DST_GEO_LIST1
 country FLK
 country UZB
 country YEM
!
object-group geo SELF_ZONE_RULES-seq-Rule_5-geo-dstn-og_
 country MYT
 country TCD
 continent OC
!
object-group geo master-seq-Rule_11-geo-dstn-og_
 group-object DST_GEO_LIST1
!

object-group geo master-seq-Rule_11-geo-src-og_
 group-object GEO_SRC_LIS1
 group-object GEO_SRC_LIST2
!
object-group geo ruleset-RS4-R1-geo-dstn-og_
 continent NA
!
object-group geo ruleset-RS5-R1-geo-dstn-og_
 country FIN
 country FRA
!
ip access-list extended LAN_to_WAN_and_DIA-seq-Rule_11-acl_
 17 permit object-group LAN_to_WAN_and_DIA-seq-Rule_11-service-og_ geo-group
master-seq-Rule_11-geo-src-og_ object-group master-seq-Rule_11-network-dstn-og_
 18 permit object-group LAN_to_WAN_and_DIA-seq-Rule_11-service-og_ geo-group
master-seq-Rule_11-geo-src-og_ fqdn-group master-seq-Rule_11-fqdn-dstn-og_
 19 permit object-group LAN_to_WAN_and_DIA-seq-Rule_11-service-og_ geo-group
master-seq-Rule_11-geo-src-og_ geo-group master-seq-Rule_11-geo-dstn-og_
!
ip access-list extended SELF_ZONE_RULES-seq-Rule_5-acl_
 15 permit object-group SELF_ZONE_RULES-seq-Rule_5-service-og_ any geo-group
SELF_ZONE_RULES-seq-Rule_5-geo-dstn-og_
!
ip access-list extended ruleset-RS4-acl_
 175 permit object-group ruleset-RS4-R1-service-og_ geo-group ruleset-RS4-R1-geo-src-og_
object-group master-ruleset-RS4-R1-network-dstn-og_
 200 permit object-group ruleset-RS4-R1-service-og_ geo-group ruleset-RS4-R1-geo-src-og_
fqdn-group master-ruleset-RS4-R1-fqdn-dstn-og_
 225 permit object-group ruleset-RS4-R1-service-og_ geo-group ruleset-RS4-R1-geo-src-og_
geo-group ruleset-RS4-R1-geo-dstn-og_
!
ip access-list extended ruleset-RS5-acl_
 125 permit object-group ruleset-RS5-R1-service-og_ any geo-group ruleset-RS5-R1-geo-dstn-og_
```

```
!
geo database
```

GRE Tunnel from the Service Side

```
interface Tunnel100512
no shutdown
vrf forwarding 1
ip address 192.168.0.1 255.255.255.248
no ip clear-dont-fragment
ip tcp adjust-mss 1387
ip mtu              1500
tunnel source 10.0.3.55
tunnel destination 10.0.3.149
exit
```

Note This can also be used with an Amazon Web Services (AWS) transit gateway (TGW) running a GRE tunnel.

NetAdmin

Authorization

```
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group tacacs-0 local
aaa authorization commands 15 default group tacacs-0 if-authenticated
```

Accounting

```
aaa accounting exec default start-stop group tacacs-0
aaa accounting commands 15 default start-stop group tacacs-0
aaa accounting commands 1 default start-stop group tacacs-0
aaa accounting network default start-stop group tacacs-0
aaa accounting system default start-stop group tacacs-0
```

PPPoE

- `bandwidth 500`
- `bandwidth qos-reference 100000`
- `ip access-group 1 out`
  `ipv6 enable`
  `keepalive 60`
- `ppp ipcp mask request`
- `ppp ipcp dns request`

Security

```
snmp
no shutdown
view v2
oid 1.3.6.1
!
view v3
oid 1.3.6.1
!
```

```
community $CRYPT_CLUSTER$i7nR7D99DSlEy4fF/WLdKA==$Vi0BKsnRfjxxiniO4bGutg==
view v2
authorization read-only
!
community $CRYPT_CLUSTER$kISnggeJ63senHxHbOCp0g==$PQAGFWVSrWCPpLJ5Au1mYw==
view v3
authorization read-only
!
ipv6 shutdown
```

Service Side Static NAT

Static NAT Inside Mapped to Inside Pool

```
ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 27
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf overload
!
ip nat inside source static 192.168.11.10 11.11.11.10 vrf 1 match-in-vrf pool natpool1
```

Static NAT Outside Mapped to Outside Pool

```
ip nat pool natpool1 10.21.21.1 10.21.21.30 prefix-length 27
ip nat outside source list global-list pool natpool1 vrf 1 overload match-in-vrf
!
ip nat outside source static 192.168.21.10 10.21.21.10 vrf 1 match-in-vrf pool natpool1
```

Port-forwarding Mapped to Inside Pool

```
ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 27
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf overload
!
ip nat inside source static tcp 192.168.11.10 80 10.11.11.10 8080 vrf 1 match-in-vrf pool
natpool1
```

SLE

Direct Connect Mode

```
license smart transport smart
license smart url smart https://smartreceiver-stage.cisco.com/licservice/license
ip name-server  172.16.168.183
ip http client source-interface GigabitEthernet0/0/2
```

Indirect Connect Mode

```
license smart transport cslu
license smart url cslu http:10.195.85.83:8182/cslu/v1/pi
ip name-server 172.20.168.183
ip http client source-interface GigabitEthernet0/0/2
```

Indirect Connect Mode

```
license smart transport off
```

Spanning Tree

```
spanning-tree guard root
spanning-tree bpdu guard enable
```

TCP MSS

```
ip tcp adjust-mss 1300
```

TrustSec

```
ip access-list role-based CTS_ACCESS_LIST
 10 permit ip
 20 permit tcp
 30 deny icmp
!
aaa group server radius radius-1
 server-private 77.251.1.1 timeout 5 retransmit 3 pac key 6 cd[UCLCiMIM^HTXbigAKUf[VJKJPSOQfD

 ip radius source-interface GigabitEthernet0/0/2
 ip vrf forwarding 1
!
aaa server radius dynamic-author
 client 77.251.1.1 vrf 1 server-key 6 gWTLbecJKOQcFcIbJNR[]WKP_g^TRacRF
!
key chain key1 tcp
 key 1000
  cryptographic-algorithm hmac-sha-256
  key-string 6 _RPB[dVI]SO^BAOVNMKATgOZKMXFGXFTa
  accept-lifetime local 18:00:00 Jan 12 2021 06:00:00 Jan 12 2022
  send-lifetime local 18:00:00 Jan 12 2021 01:00:00 Jan 12 2022
  send-id 215
  recv-id 215
  exit
!
cts authorization list cts-mlist
cts role-based permissions from 300 to 500 CTS_ACCESS_LIST
cts role-based enforcement
cts role-based sgt-map vrf 1 77.29.1.2 sgt 5
cts role-based sgt-map vrf 1 77.29.1.4 sgt 10
cts sxp node-id ipv4 77.29.1.1
cts sxp default password 6 LZcdEUScdLSVZceMAJ_R[cJgb^NbWNLLC
cts sxp default source-ip 77.29.1.1
cts sxp default key-chain key1
cts sxp connection peer 77.201.1.2 source 77.29.1.1 password key-chain mode local both vrf
 1
cts sxp enable
cts credentials id cEDGE4 password 6 RX^ASQVgfFV^EOAeQWVZ]VFQ_hcLDdgJJ
```

Interface Level Enforcement

```
cts role-based enforcement
```

Voice

```
rel1xx disable
header-passing
```

Commands Under Interface Serial

```
[no] cdp enable
snmp ifindex <clear | persist>
```

ISDN Commands Under Interface Serial

```
isdn map address <digit-string> plan [data | isdn | national | privacy | reserved/10 |
reserved/11 |
reserved/12 | reserved/13 | reserved/14 | reserved/2 | reserved/5 | reserved/6 | reserved/7
 | telex |
unknown] type [abbreviated | international | national | reserved/5 | subscriber | unknown]
```

```
isdn outgoing ie <called-number | called-subaddr | caller-number | caller-subaddr |
connected-number |
 connected-subaddr | display |  extended-facility | facility | high-layer-compat |
low-layer-compat |
```

Commands Under Trunk Group Hunt-Scheme

```
hunt-scheme <least-used | round-robin | sequential> [both | even | odd] [up | down]
```

SCCP Commands

```
bind interface <interface-name-slot/bay/port>
keepalive retries <1-32> default 3
keepalive timeout <0-180> default 10

sccp ip precedence <1-7> default is 5
```

Weighted Load Balancing for SaaS Traffic

```
probe-path load-balance-dia latency-variance 50
probe-path load-balance-dia loss-variance 30
probe-path load-balance-dia source-ip-hash false
```

Zscaler Location Based API

```
zscaler-location-settings
datacenters primary-data-center vie1-vpn.zscalerthree.net
auth-required false
ssl-scan-enabled false
xff-forward-enabled false
surrogate ip false
surrogate idle-time 0
surrogate display-time-unit MINUTE
surrogate ip-enforced-for-known-browsers false
surrogate refresh-time 0
surrogate refresh-time-unit MINUTE
ofw-enabled false
ips-control false
aup disabled
aup block-internet-until-accepted false
aup force-ssl-inspection false
aup timeout 0
caution-enabled false
!
tunnel-options tunnel-set secure-internet-gateway-zscaler tunnel-dc-preference primary-dc
source-interface GigabitEthernet1
exit
tunnel-options tunnel-set secure-internet-gateway-zscaler tunnel-dc-preference secondary-dc
 source-interface GigabitEthernet2
exit
zscaler organization cisco-dev.com
zscaler partner-base-uri admin.zscalerthree.net/api/v1
zscaler partner-key SAGv4U2lwh9R
zscaler username sig-dev@cisco-dev.com
zscaler password $8$O0i/6etiDQSqcm+B4yetJDPaYBx1x0wQujnz3pqQG7s=
```

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.6.1a

Table 4: Feature History

Feature Name	Release Information	Description
Qualified Configurations for Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Additional commands are qualified for use in Cisco vManage CLI templates.

IP SLA

```
ip sla responder

ip sla 6001
 udp-jitter 172.31.11.85 44444 source-ip 172.31.17.220 num-packets 100
  request-data-size 64
  tag 6001:UDP64 HNZ-H7Z
  frequency 300

ip sla schedule 6001 life forever start-time now
ip sla 7001
 icmp-echo 172.31.17.222 source-ip 172.31.17.216
  request-data-size 64
  tag 7001:AVAILABILITY DSO-D7S
  frequency 30

ip sla schedule 7001 life forever start-time now
ip sla reaction-configuration 6001 react rtt threshold-value 40 40 threshold-type immediate
 action-type trapAndTrigger
ip sla reaction-configuration 6001 react timeout threshold-type immediate action-type
trapAndTrigger
ip sla reaction-configuration 6001 react packetLossDS threshold-value 1 1 threshold-type
immediate action-type trapAndTrigger
ip sla reaction-configuration 6001 react packetLossSD threshold-value 1 1 threshold-type
immediate action-type trapAndTrigger
ip sla reaction-configuration 7001 react timeout threshold-type immediate action-type
trapAndTrigger
```

AppQoE for RA user

SD-WAN Datacenter

```
hostname SDWAN-DC-B40
!
interface Loopback1
description apple.com DC-LAN
vrf forwarding 10
ip address 196.168.1.1 255.255.255.0
end
!
interface Loopback2
description google.com DC-LAN
vrf forwarding 20
ip address 197.168.1.1 255.255.255.0
end
```

```
!
interface GigabitEthernet4
description shared-service VPN (RADIUS server)
vrf forwarding 1
ip address 77.27.11.1 255.255.255.0
end
!
interface GigabitEthernet2 -> Internet TLOC
 tunnel-interface
 encapsulation ipsec
 color biz-internet restrict
!
interface GigabitEthernet5 -> MPLS TLOC
 tunnel-interface
 encapsulation ipsec
 color mpls restrict
```

Interface Configuration

```
interface GigabitEthernet2
description INTERNET-LINK(TLOC)
ip address 77.27.5.2 255.255.255.0
ip nat outside
negotiation auto
end
!
interface GigabitEthernet2 -> Internet TLOC
 tunnel-interface
 encapsulation ipsec
 color biz-internet restrict
!
interface GigabitEthernet7 -> MPLS TLOC
 tunnel-interface
 encapsulation ipsec
 color mpls restrict
!
interface GigabitEthernet4
description shared-service VPN
vrf forwarding 1
ip address 77.27.13.1 255.255.255.0
end
```

DIA configuration

```
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet2 overload

ip nat route vrf 10 0.0.0.0 0.0.0.0 global
```

IKEv2/IPsec FlexVPN RA server configuration with Preshared-key

```
crypto ikev2 profile prof

description RA-SERVER common profile
match identity remote email domain apple.com
match identity remote email domain google.com
authentication remote pre-share key cisco
authentication local pre-share key cisco
aaa authorization user psk list AUTHORIZE name-mangler server
virtual-template 1
!
crypto ipsec profile prof
set ikev2-profile prof
!
interface Virtual-Template1 type tunnel
no ip address
tunnel mode ipsec ipv4
```

```
tunnel protection ipsec profile prof
!
```

IKEv2/IPsec FlexVPN RA server configuration with PKI

```
For any PKI configuration to work properly, the "clock" of the device should be set.

All the devices in the topology should be sync using NTP and the "show ntp status" should
be synchronized.

cry key generate rsa modulus 2048 label test-key

crypto pki trustpoint tp
enrollment url http://10.0.149.205:80/certsrv/mscep/mscep.dll
usage ike
fingerprint 32AE15680731AD3E91A612A72A35419D
subject-name CN=R1 C=pki
revocation-check none
rsakeypair tp 2048
auto-enroll 80
end

crypto pki trustpoint tp
enrollment url http://10.0.149.205:80
end
```

Routes to push to RA clients

```
ip access-list standard 98 (For google.com)
10 permit 197.168.0.0 0.0.255.255
!
ip access-list standard 99 (For apple.com)
20 permit any
!
```

IP pools to assign IP to RA clients

```
ip local pool apple 10.0.0.4 10.0.0.10 (For apple.com)
ip local pool google 20.0.0.4 20.0.0.10 (For google.com)
!
```

AAA configuration

```
aaa new-model
!
aaa group server radius RADIUS_PSK
server-private 77.27.11.2 key cisco
ip vrf forwarding 1
ip radius source-interface GigabitEthernet4
!
aaa authorization network AUTHORIZE group RADIUS_PSK
!
```

PKI Server config

For any PKI configuration to work properly, the "clock" of the device should be set. All the devices in the topology should be sync using NTP and the "show ntp status" should be synchronized. PKI server should **`ip http server`** config as a prerequisite.

RootCA:

```
crypto pki server ROOTCA
database level complete
database archive pkcs12 password 0 cisco123
grant auto
hash sha256
```

```
lifetime certificate 365
auto-rollover 0 0 20
no shutdown
```

```
hostname SOHO-RA-CLIENT
```

Configuration for apple.com

```
interface Loopback1

description APPLE.COM client-LAN
vrf forwarding 10
ip address 199.168.1.1 255.255.255.0
!
interface GigabitEthernet3
description INTERNET LINK FOR APPLE.COM
ip address 192.167.1.33 255.255.255.0
end
!
ip access-list standard 99
10 permit 199.168.0.0 0.0.255.255
!
crypto ikev2 authorization policy apple
route set interface
route set access-list 99
!
crypto ikev2 authorization policy google
route set interface
route set access-list 98
!
crypto ikev2 profile apple
description RA-CLIENT profile for apple.com
match identity remote any
identity local email abc@apple.com
authentication remote pre-share key cisco
authentication local pre-share key cisco
aaa authorization group psk list mylist apple
!
crypto ipsec profile apple
set ikev2-profile apple
!
interface Tunnel10
description SVTI-TUNNEL for apple.com
vrf forwarding 10
ip address negotiated
tunnel source GigabitEthernet3
tunnel mode ipsec ipv4
tunnel destination 77.27.5.2
tunnel protection ipsec profile apple
end
!
```

Configuration for google.com

```
interface Loopback2

description GOOGLE.COM client-LAN
vrf forwarding 20
ip address 199.170.1.1 255.255.255.0
end
!
interface GigabitEthernet4
description INTERNET LINK FOR GOOGLE.COM
ip address 194.167.1.33 255.255.255.0
negotiation auto
no mop enabled
```

```
no mop sysid
end
!
ip access-list standard 98
10 permit 199.170.0.0 0.0.255.255
!
crypto ikev2 profile google
description RA-CLIENT profile for google.com
match identity remote any
identity local email xyz@google.com
authentication remote pre-share key cisco
authentication local pre-share key cisco
aaa authorization group psk list mylist google
!
crypto ipsec profile google
set ikev2-profile google
!
interface Tunnel20
description SVTI-TUNNEL for google.com
vrf forwarding 20
ip address negotiated
tunnel source GigabitEthernet4
tunnel mode ipsec ipv4
tunnel destination 77.27.5.2
tunnel protection ipsec profile google
end
!
```

Carrier Supporting Carrier

```
interface GigabitEthernet2

no shutdown
mpls bgp forwarding
ip address 10.1.17.15 255.255.255.0

interface GigabitEthernet3
no shutdown
mpls bgp forwarding
ip address 10.1.19.15 255.255.255.0

router bgp 10
bgp router-id 10.1.1.15
neighbor 10.1.17.14 remote-as 100
neighbor 10.1.19.16 remote-as 100

address-family ipv4 unicast
maximum-paths 4
neighbor 10.1.17.14 activate

neighbor 10.1.17.14 as-override
neighbor 10.1.17.14 allowas-in

neighbor 10.1.17.14 advertisement-interval 30
neighbor 10.1.17.14 send-label explicit-null
neighbor 10.1.19.16 activate
neighbor 10.1.19.16 advertisement-interval 30
neighbor 10.1.19.16 send-community both
neighbor 10.1.19.16 send-label explicit-null
redistribute connected
redistribute static
exit-address-family
!
```

Cisco SD-WAN Etherchannel

```
interface Port-channel2
 ip address 10.0.0.1 255.255.255.0
 no negotiation auto
!

interface GigabitEthernet2/1/0
 no ip address
 negotiation auto
 cdp enable
 channel-group 2
!
interface GigabitEthernet2/1/1
 no ip address
 negotiation auto
 cdp enable
 channel-group 2
!
```

Cloud onRamp Over SIG Tunnels

```
probe-path branch sig-tunnel-list Tunnel100015 Tunnel100016
probe-path branch all-auto-sig-tunnels
```

Collect-tos/DSCP

```
Policy
 cflowd-template cflowd_server
  flow-active-timeout    60
  flow-inactive-timeout  30
  flow-sampling-interval 10
  protocol               ipv4
  collector vpn 0 address 10.0.100.1 port 4739 transport transport_udp
 customized-ipv4-record-fields
   collect-tos
   collect-dscp-outputpath
```

Cloud onRamp-SaaS gateway interface

```
probe
vanalytics-url https://us01.cloudservice.cisco.com
saas office365_apps
saas amazon_aws_apps
saas box_net_apps
saas dropbox_apps
saas intuit_apps
saas concur_apps
saas google_apps
!
```

```
probe-path gateway color-list <color>
```

or

```
probe-path gateway color-list <color>
```

DRE Profiles

```
interface VirtualPortGroup3
 no shutdown
 ip address 192.168.3.1 255.255.255.252
exit
```

```
platform resource service-plane-heavy
iox
app-hosting appid dreopt
 app-resource package-profile medium
 app-vnic gateway0 virtualportgroup 3 guest-interface 1
  guest-ipaddress 192.168.3.2 netmask 255.255.255.252
 start
```

The following CLI command can be configured on a vSmart.

```
policy
 data-policy _v1_dataPolicy
  vpn-list v1
    sequence 1
     match
      …
     !

     action accept
      dre-optimization
     !
    !

  default-action drop
 !
```

Geofencing with SD-WAN Edges

```
system
 gps-location latitude 37.416399
 gps-location longitude -121.918717
 gps-location geo-fencing-enable
 gps-location geo-fencing-config
  geo-fencing-range 200
  sms
   sms-enable
   mobile-number +14080000000
   !
  !
 !
!
```

Implicit ACL on Loopback Interface

```
sdwan
interface Loopback100
  tunnel-interface
   [bind interface-name]
   encapsulation ipsec
   color mpls
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  exit
```

Per VPN QoS

```
class-map match-all Queue0
match qos-group 0
class-map match-all Queue2
match qos-group 2
class-map match-all Queue3
match qos-group 3
class-map match-all Queue5
match qos-group 5
class-map match-all Queue7
match qos-group 7
!

class-map match-any Tenant-1
match packet-tag 1 11 65535
match packet-tag 1 12 65535
!
class-map match-any VPN_100
match packet-tag 1 100 65535
!

policy-map qos_1_500000 // generate specific qos_1 policy for 500000kbps
class Queue0
  priority level 1
policer rate 100000000 // priority queue policer rate 100Mbps = 500Mbps * 20%
class Queue3
  bandwidth remaining ratio 30
class Queue7
  bandwidth remaining ratio 35
class class-default
  bandwidth remaining ratio 15
!

policy-map qos_1_300000 // generate specific qos_1 policy for 300000kbps
class Queue0
  priority level 1
policer rate 60000000 // priority queue policer rate 60Mbps = 300Mbps * 20%
class Queue3
  bandwidth remaining ratio 30
class Queue7
  bandwidth remaining ratio 35
class class-default
  bandwidth remaining ratio 15
!

policy-map qos_2_200000 // generate specific qos_2 policy for 200000kbps
class Queue0
  priority level 1
policer rate 70000000 // priority queue policer rate 70Mbps = 200Mbps * 35%
class Queue5
  bandwidth remaining ratio 45
class class-default
  bandwidth remaining ratio 20
!

policy-map VPN_Policy
class Tenant-1
  bandwidth remaining ratio 50 // configured bandwidth 500000kbps
   service-policy qos_1_500000
class VPN_100
  bandwidth remaining ratio 20 // configured bandwidth 200000kbps
shape average 300000000    // configured maximum bandwidth 300000kbps
   service-policy qos_2_200000
```

```
class class-default
  bandwidth remaining ratio 30 // rest of 300000kbps (1000000kbps - 500000kbps - 200000kbps)

   service-policy qos_1_300000
!

policy-map Phy_WAN_Policy
class class-default
  shape average 1000000000
   service-policy VPN_Policy
!

interface GigabitEthernet2
service-policy output Phy_WAN_Policy
!

sdwan
 vpn packet-tag 1



ipsec
rekey 86400
replay-window 512
extended-ar-window 256
authentication-type ah-sha1-hmac sha1-hmac
!
!
```

QoS Commands

```
policy
 cloud-qos
 cloud-qos-service-side
 class-map
  class Queue0 queue 0
  class Queue3 queue 3
  class Queue4 queue 4
  class queue4 queue 4
 !

 qos-scheduler ut-qos-222_0
  class Queue0
  bandwidth-percent 5
  buffer-percent 10
  scheduling llq
 !

 qos-scheduler ut-qos-222_3
  class Queue3
  bandwidth-percent 30
  buffer-percent 30
 !

 qos-scheduler ut-qos-222_4
  class Queue4
  bandwidth-percent 1
  buffer-percent 50
  drops red-drop
 !
 qos-map ut-qos-222
  qos-scheduler ut-qos-222_4
```

Route Leaking

```
track 1 ip route 12.1.1.0 255.255.255.0 reachability
 ip vrf red
```

vrrp-v3 configuration

```
interface GigabitEthernet7
 vrf forwarding 100
 ip address 13.1.1.1 255.255.255.0
 negotiation auto
 vrrp 2 address-family ipv4
  vrrpv2
  priority 220
  track 1 decrement 25
  preempt delay minimum 30
  address 13.1.1.100 primary
exit
```

vrf configuration

```
vrf definition 100
 !
 address-family ipv4
 exit-address-family
sdwan
  omp
    no shutdown
    graceful-restart
    no as-dot-notation
    timers
      holdtime               15
      graceful-restart-timer 120
exit
    address-family ipv4
       distance 100
       advertise bgp
    !
    address-family ipv6
      distance 100
      advertise bgp
    !
    address-family ipv4 vrf 1
       distance 200
       advertise bgp
    !
    address-family ipv6 vrf 1
      distance 200
      advertise bgp
    !
  !
```

SD-WAN Multitenancy

```
clear sdwan reverse-proxy context
clear sdwan certificate reverse-proxy
show sdwan certificate reverse-proxy
```

SNMP Commands

```
snmp ifmib ifindex persist
snmp-server community private view v3 ro 5
snmp-server community public view v2 ro
snmp-server contact MY_CONTACT_NAME
snmp-server context MY_CONTEXT
```

```
snmp-server enable traps alarms informational
snmp-server enable traps bgp state-changes limited
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps entity-state
snmp-server enable traps snmp authentication coldstart linkdown linkup warmstart
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps sdwan
snmp-server enable traps bgp state-changes limited
snmp-server group groupAuthNoPriv v3 auth read v3
snmp-server group groupAuthPriv v3 priv read v3
snmp-server group groupNoAuthNoPriv v3 noauth read v3
snmp-server host 172.27.54.199 vrf 172 version 2c public udp-port 162
snmp-server host 172.27.214.64 vrf 172 version 2c public udp-port 16664
snmp-server location sjc-20
snmp-server packetsize 1300
no snmp-server sparse-tables
no snmp-server trap authentication unknown-context
snmp-server trap-source Loopback0
snmp-server view v2 1.3.6.1 included
snmp-server view v3 1.3.6.1 included
snmp-server view v3 internet included
```

UCSE as AppQoE Service Node

```
platform resource app-heavy

service-insertion service-context appqoe/1
  cluster-type hybrid
  appnav-controller-group ACG-APPQOE
  service-node-group SNG-APPQOE1
  service-node-group SNG-APPQOE2
  vrf global
  enable

 !
```

Unified Security Policy

Policy CLI

```
parameter-map type inspect-global
log dropped-packets
multi-tenancy
vpn zone security
alert on
utd-policy AIP_1

parameter-map type inspect AIP_1-pmap_
utd-policy AIP_1

policy-map type inspect FW_UNIFIED_POLICY_1
class type inspect FW_UNIFIED_POLICY_1-seq-1-cm_
inspect AIP_1-pmap_
class class-default
drop

zone security ZONE_1_2
vpn 1
vpn 2
```

```
zone-pair security ZP_ZONE_1_2_ZONE_1_2_F_671459382 source ZONE_1_2 destination ZONE_1_2
service-policy type inspect FW_UNIFIED_POLICY_1
```

UTD CLI

```
utd engine standard unified-policy
web-filter block page profile block-URLF_UNIFIED_1
text Access to the requested page has been denied.Blocked by admin
web-filter url profile URLF_UNIFIED_1
alert all
categories block
sports
gambling
block page-profile block-URLF_UNIFIED_1
log level error
reputation
block-threshold low-risk
threat-inspection profile IPS_UNIFIED_1
threat detection
policy security
logging level info
utd global
file-analysis
apikey 0 <apikey>
cloud-server isr.api.threatgrid.eu
file-reputation
cloud-server cloud-isr-asn.amp.cisco.com
est-server cloud-isr-est.amp.cisco.com
file-analysis profile AMP_UNIFIED_1-fa-profile
alert level info
file-types
pdf
ms-exe
file-reputation profile AMP_UNIFIED_1-fr-profile
alert level info
file-inspection profile AMP_UNIFIED_1-fi-profile
reputation profile AMP_UNIFIED_1-fr-profile
analysis profile AMP_UNIFIED_1-fa-profile
tls-decryption profile TLS_UNIFIED_1-tls-profile
categories never-decrypt
financial-services
log level error
reputation
decrypt-threshold low-risk
sourcedb fail decrypt
policy AIP_1
file-inspection profile AMP_UNIFIED_1-fi-profile
tls-decryption profile TLS_UNIFIED_1-tls-profile
tls-decryption action decrypt
threat-inspection profile IPS_UNIFIED_1
web-filter url profile URLF_UNIFIED_1
```

Wireless Management on Cisco 1000 Series Integrated Services Routers

Radio Profile Definition

```
radio-profile 24ghz
 channel auto
 channel-bandwidth auto

radio-profile 5ghz
 channel auto
 channel-bandwidth auto
```

WLAN Profile Definition

```
wlan-profile TEST-Enterprise
 radio-band all
 vlan-id 300
 ssid TEST-Enterprise
 data-security enterprise
 aaa radius-server 192.168.100.20 auth-port 1812 shared-secret 6
XEJ_TKR[gATN^EOAJfVKBTdcIAeEFHBC^
 qos-type silver
```

```
wlan-profile TEST-Personal
 radio-band all
 ssid TEST-Personal
 data-security personal
 passphrase 6 EJcWJK]F_aNQUZBdCDW[aJOKRAHdELKOY
 qos-type silver
```

General Wireless LAN Settings

```
wireless-lan mgmt ip address 192.168.1.11 255.255.255.0 default-gateway 192.168.1.1
 wireless-lan mgmt credential username admin password 6
IPSWCKabbF_OHgaVHZADPAg]UiWLcK]Q^IZKBVS
 wireless-lan country US
```

Qualified Commands for Cisco IOS XE Release 17.6.4

Table 5: Feature History

Feature Name	Release Information	Description
Qualified Configurations for Cisco IOS XE Release 17.6.4	Cisco IOS XE Release 17.6.4	Additional commands are qualified for use in Cisco vManage CLI templates.

Network Address Translation (NAT) Commands

```
ip nat log translations flow-export v9 udp destination IPv4address-port source interface-name
 interface-number
```

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.7.1a

Table 6: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	Additional commands are qualified for use in Cisco vManage CLI templates.

Cisco Unified Border Element Commands

```
address-hiding
anat
```

```
answer-address
application (global)
asserted id
asymmetric payload
audio forced
authentication
bind
block
call spike
call threshold global
call treatment action
call treatment cause-code
call treatment isdn-reject
call treatment on
callmonitor
call-route
clid
codec preference
codec profile
codec transparent
connection-reuse
contact-passing
cpa
credentials
crypto signaling
dial-peer cor custom
dial-peer cor list
dspfarm profile
dtmf-interworking
early-media update block263
early-offer
emergency
error-code-override
error-passthru
g729-annexb override
gcid
header-passing
host-registrar
http client connection idle timeout
http client connection persistent
http client connection timeout
ip qos dscp
localhost
max-conn
media
media-address voice-vrf
media disable-detailed-stats
media-inactivity-criteria
media profile asp
media profile nr
media profile stream-service
media profile video
media-renegotiate
midcall-signaling
min-se
notify redirect
num-exp
options-ping
outbound-proxy
pass-thru content
privacy
privacy-policy
progress_ind
protocol mode
```

```
reason-header override
redirect ip2ip
redirection
referto-passing
registrar
rel1xx
remote-party-id
requri-passing
retry bye
rtcp all-pass-through
rtcp keepalive
rtp payload-type
rtp-media-loop count
rtp-port
rtp-ssrc multiplex
session refresh
session transport
set pstn-cause.
set sip-status
signaling forward
silent discard untrusted
sip-server
srtp
stun
stun usage firewall-traversal flowdata
supplementary-service
timers
transport
uc secure-wsapi
uc wsapi
update-callerid
url (SIP)
vad
voice cause code
voice class codec
voice class dpg
voice class e164-pattern-map
voice class media
voice class server-group
voice-class sip options-keepalive
voice class sip-copylist
voice class sip-event-list
voice class sip-hdr-passthrulist
voice class sip-profiles
voice class srtp-crypto
voice class uri
voice iec syslog
voice statistics iec
```

Cloud onRamp SaaS Commands

```
probe saas-app webex
```

Crypto Commands

```
crypto pki import
```

Dual Endpoint DIA Tracker Commands

```
system
endpoint-tracker tracker-name
    endpoint-dns-name dns-name
```

```
endpoint-ip ip-address
endpoint-api-url api-url
interval seconds
multiplier number
threshold milliseconds
  endpoint-tracker <group-name>  boolean or|and
    tracker-elements <tracker1-name> <tracker2-name>
    tracker-type tracker-group
  interface interface-name
    ip nat outside
        endpoint-tracker  <tracker-group-name>
endpoint-ip <ipv4 address> tcp|udp <port number>
```

Event Commands

```
event ipsla
event manager applet
event manager session cli username
event none
event routing
event syslog
event timer
event track
```

HSRP Commands

```
standby authentication
standby follow
standby ip
standby ipv6
standby mac-address
standby mac-refresh
standby name
standby preempt
standby priority
standby timers
standby track
standby version
show standby
show standby neighbors
```

IP Commands

```
DHCPv6
address prefix
ipv6 address dhcp client request
ipv6 dhcp relay destination
ipv6 dhcp-relay option vpn
ipv6 dhcp client pd
ipv6 dhcp pool
ipv6 dhcp server
ipv6 address autoconfig
prefix-delegation
prefix-delegation pool
vendor-specific
```

Packet Capture Commands

```
monitor capture match ipv4
```

NAT Commands

```
nat66 outside
nat66 prefix
nat66 nd enable
nat66 max-vpn
nat66 route
```

```
show commands:
show nat66 prefix
show nat66 statistics
show nat66 dia route
show platform hardware qfp active feature nat66 datapath prefix
show platform hardware qfp active feature nat66 datapath statistics
show platform software nat66 fp active prefix-translation
show platform software nat66 rp active prefix-translation
clear platform hardware qfp active feature nat66 datapath stat
```

Routing Information Protocol Commands

```
address-family ipv4 vrf
auto-summary (RIP)
default-information originate (RIP)
default-metric (RIP)
distance (IP)
distribute-list (RIP)
input-queue
ip rip advertise
ip rip receive version
ip rip send version
maximum-paths
neighbor (RIP)
network (RIP)
offset-list (RIP)
omp-route-tag
output-delay
passive-interface
redistribute
router rip
timers basic (RIP)
traffic-share min
validate-update-source
version (RIP)
show ip protocols
show ip rip database
show ip rip neighbors
show ip route vrf
```

SNMP Commands

```
snmp-server enable traps config-copy
snmp-server enable traps config-ctid
snmp-server enable traps cpu
snmp-server enable traps event-manager
snmp-server enable traps flash
snmp-server enable traps memory
snmp-server enable traps syslog
snmp-server sparse-tables
snmp trap link-status
```

System Commands

```
gps-location (system)
```

Tracker Commands

```
boolean
endpoint-api-url
endpoint-dns-name
endpoint-ip
endpoint-tracker
interval
multiplier
threshold
tracker-elements
tracker-type
tracker-type
show endpoint-tracker
show ip sla summary
```

Unified Logging for Security Connection Events

```
ZBFW
Use this configuration to enable Unified Logging for ZBFW at a global level.
Device(config)# parameter-map type inspect-global
Device(config-profile)# log flow
```

```
UTD
Use this configuration to enable Unified Logging for all UTD features.
Device(config)# utd engine standard unified-policy
Device(config-utd-unified-policy)# utd global
Device(config-utd-mt-global)# flow-logging all
Device(config-utd-mt-global)# flow-logging all {file-inspection threat-inspection
web-filtering}
```

```
Configure Netflow
Use this configuration to enable Netflow to export log data of ZBFW and UTD features to an
 external collector
Device(config)# flow exporter exporter-name
Device(config-flow-exporter)# description description
Device(config-flow-exporter)# destination IP address
Device(config-flow-exporter)# export-protocol netflow-v9
Device(config-flow-exporter)# transport udp udp-port
```

```
show performance monitor context temp0 configuration
show performance monitor context temp1 exporter
show performance monitor context temp1 traffic-monitor sdwan-fnf-vpn0-stats cache
```

VRRP Commands

```
object (tracking)
track interface
track list
track service
tloc-change increase-preference
vrrp address-family
vrf forwarding
show vrrp
```

Troubleshooting Commands

```
monitor capture match ipv4
show autoip status
show crypto key mypubkey rsa
```

```
show crypto pki certificates
show crypto session
show endpoint-tracker
show flow monitor sdwan_flow_monitor cache
show ip protocols
show ip rip database
show ip rip neighbors
show ip route rip
show ip route vrf
show ip sla summary
show ipv6 dhcp binding
show ipv6 dhcp database
show ipv6 dhcp interface
show ipv6 dhcp pool
show platform hardware qfp active classification class-group-manager class-group client cce
 name
show platform hardware qfp active feature firewall drop
show platform hardware qfp active feature nat66 datapath prefix
show platform hardware qfp active feature nat66 datapath statistics
show platform software nat66 fp active
show platform software nat66 rp active
show policy-firewall config
show policy-map type inspect
show nat66 dia route
show nat66 nd
show nat66 prefix
show nat66 statistics
show sdwan bfd sessions region-access
show sdwan bfd sessions region-core
show sdwan cloudexpress applications
show sdwan omp cloudexpress
show sdwan omp peers
show standby
show standby neighbors
show track
show vrrp
```

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

Table 7: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	Additional commands are qualified for use in Cisco vManage CLI templates.

Access Point Name (APN) Commands

```
profile id <id> apn <name> authentication <type> pdn-type <type>
```

Cloud onRamp for SaaS Commands

```
probe saas-app <applist name>
app <app1>
```

```
app <app2>
endpoint-fqdn   DNS name of saas-app endpoint
endpoint-ip     IP address of saas-app endpoint
endpoint-url    API url of saas-app endpoint
```

Hierarchical SD-WAN Commands

```
region <region_id> [secondary-region <region_id>]
region (secondary-shared | secondary-only)
omp best-path region-path-length ignore
transport-gateway enable
omp best-path transport-gateway [prefer | ecmp-with-direct-path]
match route transport-gateway-reoriginated
affinity-group <number>
affinity-group-preference <number1> <number2> …
filter route outbound affinity-group preference
```

IP Commands

```
ip cef load-sharing algorithm src-only [id]
ipv6 cef load-sharing algorithm src-only
ip load-sharing algorithm src-ip-only
ipv6 load-sharing algorithm src-ip-only
```

Network Address Translation (NAT) Commands

```
ip nat inside source static 10.0.0.1 12.0.0.1 vrf 1 match-in-vrf track  <track-id>
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf overload track
<track-id>
```

Routing Information Protocol Next Gen (RIPng) Commands

```
ipv6 rip vrf-mode enable
ipv6 rip enable
ipv6 router rip sdwan
address-family ipv6 vrf <vpn-id>
omp-route-tag
distribute-list prefix-list <ipv6-prefix-list-name> {in | out}
redistribute {omp | static | connected | ospf <id>} [route-map <route-map-name>] [metric
<1-15>]
ipv6 rip default-information {only | originate} [metric <1-15>]
ipv6 rip metric-offset <value>
ipv6 rip summary-address <ipv6-add>
```

Voice Commands

```
caller-id alerting dsp-pre-allocate
caller-id alerting line-reversal
caller-id alerting pre-ring
caller-id alerting ring [ 1 | 2 | 3 | 4 ]
caller-id block
caller-id format 911
caller-id mode {BT | FSK | DTMF [start | end {# | * | A | B | C | D}]}
clid dtmf-codes <start-code><redirect-code><end-code>
```

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

Table 8: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	Additional commands are qualified for use in Cisco vManage CLI templates.

AppQoE Commands

```
sdwan appqoe tcptopt http-connect port port-number
```

Cisco SD-WAN Identity-Based Firewall Policy Commands

```
identity
  pxgrid
    server-address name>
    username name>
    password name>
    subscriptions {user-identity | sgt}
    domain-name domain-name>
    vpn 0

class-map type inspect match-any cm3
    match identity user-group source Engineering
    match identity user-group source Security
    match identity user source Jim

class-map type inspect match-all cm4
    match access-group name group-name>
    match application-class>
    match protocol-class>
    match identity-class-cm3>

policy-map type inspect pm1
    class type inspect cm4
         inspect
```

Network Address Translation (NAT) Commands

```
ip nat service all-algs
ip nat service dns tcp
ip nat service dns udp
ip nat service ftp
ip nat service sip tcp port port-number
ip nat service sip udp port port-number


ip nat inside source static tcp ip-address port ip-address port egress-interface
interface-type-number
ip nat inside source static tcp ip-address port interface interface-type-number

ip nat outside source static ip-address ip-address vrf vrf-name redundancy
```

```
hsrp-standby-group-name match-in-vrf

ip nat log translations flow-export v9 udp destination IPv4address-port source interface-name
 interface-number
```

Policy Configuration Tagging Commands

```
tag-instances [tag-instance] [lists]

tag-instance tag-instance-name [id global-unique-id][app-list app-list-name] [data-prefix-list
 prefix-list-name] [data-ipv6-prefix-list ipv6-prefix-list-name]

lists [app-list app-list-name] [data-prefix-list prefix-list-name] [data-ipv6-prefix-list
ipv6-prefix-list-name]

match [destination-tag-instance dest-tag-name | source-tag-instance src-tag-name]

match [destination-tag-instance dest-tag-name | source-tag-instance  src-tag-name |
tag-instance  tag-name]

match[destination-tag-instance dest-tag-name | source-tag-instance src-tag-name | tag-instance
  tag-name]

access-list acl-name sequence sequence-number match source-tag-instance src-tag-name

access-list acl-name sequence sequence-number match destination-tag-instance dest-tag-name
```

Route Leaking Between Service VPNs

```
route-replicate from vrf source-vrf-name unicast protocol [route-map map-tag]

redistribute vrf vrf-name protocol subnets [route-map map-tag]
```

Qualified Commands for Cisco IOS XE Release 17.10.1a

Table 9: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Additional commands are qualified for use in Cisco vManage CLI templates.

AAA Commands

```
no ip scp server enable
no ip http tls-version TLSv1.1
no ip http tls-version TLSv1.0
ip http tls-version TLSv1.2
no snmp-server system-shutdown
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
aaa group server tacacs+ tacacs-100
tacacs server <server name>
port <xx> timeout <xx>
aaa accounting connection default start-stop group
aaa authorization credential-download [default | <string>] <group-name>
```

Cisco SD-WAN Identity-Based Firewall Policy Commands

```
identity
  pxgrid
    server-address name>
    username name>
    password name>
    subscriptions {user-identity | sgt}
    domain-name domain-name>
    vpn 0
class-map type inspect match-any cm3
    match identity user-group source Engineering
    match identity user-group source Security
    match identity user source Jim
class-map type inspect match-all cm4
    match access-group name group-name>
    match application-class>
    match protocol-class>
    match identity-class-cm3>
object-group security sec-source
    security-group tag 100
    security-group tag 200
    security-group tag 300
object-group security sec-dest
    security-group tag 400
    security-group tag 500
policy-map type inspect pm1
    class type inspect cm4
         inspect
```

CUBE Commands

```
conn-reuse
disable-early-media 180
gw-accounting
handle-replaces
max-forwards
nat
notify ignore substate
notify telephone-event
permit hostname
random-contact
retry invite
srtp negotiate
stun flowdata shared-secret
video codec
voice class codec preference
voice class tls-cipher
voice class tls-profile
xfer target

credentials
security-policy (voice register global)
translation-profile (voice register)
```

DHCP Commands

```
ip dhcp client vendor-class
ipv6 dhcp client vendor-class
```

Network Address Translation (NAT) Commands

```
ip nat settings preserve-sdwan-ports
nat64 route
nat64 settings
nat64 settings mtu (mtu keyword added for 17.10.1.a)
nat64 provisioning
```

Security Command

```
threat-inspection custom-signature profile
```

System Commands

```
system
gps-location latitude 32.0
gps-location longitude -100.0
system-ip 172.16.255.14
domain-id 1
site-id 400
ipv6-strict-control true
admin-tech-on-failure
organization-name "vIPtela Inc Regression"
vbond vbond
!
```

Underlay Measurement and Tracing Services Commands

```
sdwan
umts
monitor
periodicity 30
local-color-all
remote-color-all
remote-system-ip-all
!
event
event-type tunnel-sla-change
local-color-all
remote-color-all
remote-system-ip-all
!
event-type tunnel-pmtu-change
local-color-all
remote-color-all
remote-system-ip-all
!
```

Qualified Commands for Cisco IOS XE Release 17.11.1a

Table 10: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	Additional commands are qualified for use in Cisco vManage CLI templates.

IP Commands

```
ntp disable ip/ipv6
radius server <server-name>
ipv6 nd autoconfig default-route
aaa group server tacacs+
ip tacacs source-interface
server-private (TACACS+)
tacacs server address ipv4
aaa group server radius
ip radius source-interface
ipv6 tcp adjust-mss
ipv6 radius source-interface
ipv6 address dhcp
ipv6 tacacs source-interface
ipv6 address dhcp client request
ipv6 access-class
ipv6 address autoconfig
ipv6 dhcp client pd
ipv6 enable
ntp access-group
ntp server


object-group v6-network ipv6-og1 host 2001:DB8:1::1 2002::1/64
object-group v6-network ipv6-og2 host 2001:DB8:2::1 2003::1/64
ipv6 access-list ipv6acl permit ipv6 ::2 2001:3c0:1::64/128
ipv6 access-list ipv6-acl2
permit tcp object-group ipv6-og1 object-group ipv6-og2
class-map type inspect match-any ipv6cm
match access-group name ipv6acl
match access-group name ipv6acl2
policy-map type inspect ipv6pm

 class type inspect ipv6cm
inspect
zone security inside
  vpn 1
zone security outside
   vpn 0
zone-pair security zp source-zone inside destination-zone outside
service-policy type inspect ipv6pm

Firewall Support for Dual Stack of IPv4 and IPv6

object-group network ipv4-og1
host 192.168.12.10 host 192.168.12.11
object-group network ipv4-og2 host 192.168.12.12
host 192.168.12.13
object-group v6-network ipv6-og1
host 2001:DB8:1::1 2002::1/64
object-group v6-network ipv6-og2
host 2001:DB8:2::1 2003::1/64

ip access-list extended ipv4acl
permit tcp 0.0.0.2 255.255.255.0 0.0.0.3 255.255.255.0
ipv6 access-list ipv6acl
permit ipv6 ::2 ::3
ip access-list extended ipv4-acl2
permit udp object-group ipv4-og1 object-group ipv4-og2
ipv6 access-list ipv6-acl2
permit tcp object-group ipv6-og1 object-group ipv6-og2
class-map type inspect match-any dualcm

 match access-group name ipv4acl
```

```
 match access-group name ipv6acl

 match access-group name ipv4-acl2

 match access-group name ipv6-acl2
policy-map type inspect dualpm

 class type inspect dualcm
  inspect
zone security inside
   vpn 1
zone security outside
   vpn 0
zone-pair security zp source-zone inside destination-zone outside

 service-policy type inspect dualpm
```

Multicast Commands

```
multicast
 address-family ipv4 vrf 1
 replicator
 spt-only
 msdp-interworking
```

Multi-Region Fabric Commands

```
advertise aggregate prefix <pfx> … [region <access | core>]

system
 host-name             vm9
 gps-location latitude 45.0
 gps-location longitude -122.0
 system-ip             172.16.255.19
 site-id               100
 tloc-color-compatibility
  compatible lte private1
  !
  compatible private1 private2
  !
  incompatible lte default
  !
  incompatible lte 3g
  !
 !

omp
  no shutdown
  ecmp-limit       6
  graceful-restart
  no as-dot-notation
  timers
   holdtime                       15
   tloc-color-cap-update-interval 120
   graceful-restart-timer         120
  exit

show running-config policy
policy
 control-policy test-affinity
  sequence 1
```

```
   match route
    site-id 100
   !
   action accept
    set
     affinity-group-number 2
    !
   !
  !
  sequence 2
   match tloc
    tloc 172.16.255.21 color lte encap ipsec
   !
   action accept
    set
     affinity-group-number 5
    !
   !
  !
  default-action reject
 !
!
```

NAT Commands

```
ip nat service all-algs
ip nat service H225
ip nat service ras
ip nat service pptp
ip nat service tftp
ip nat service sunrpc tcp
ip nat service sunrpc udp


ip nat inside source static tcp 10.0.0.12 8080
interface Loopback15 8585 vrf 1 egress-interface GigabitEthernet3
```

Policy Commands

```
Device(config)# policy log-rate-limit

(<1..10000> logs per second. Default is 25) (25):



Device# show sdwan running-config policy
policy
no app-visibility
no app-visibility-ipv6
no flow-visibility
no flow-visibility-ipv6
no implicit-acl-logging
log-frequency        1000
log-rate-limit    25
access-list ACL1
  sequence 1
   match
    dscp 10
   !
   action accept
    count CNT2
    log
   !
  !
```

```
  default-action drop
!
!
```

Tunnel Interface Commands

```
gre-in-udp
```

```
match-inner ipv4
match-inner ipv6
mpls match-inner ipv4
allow-no-label
mpls match-inner ipv6
mpls <label> <depth> match-inner ipv4
mpls <label> <depth> match-inner ipv6
```

Zone Based Firewall Commands

```
parameter-map type inspect-global
log flow-export v9 udp destination 10.10.10.50 5050 source interface GigabitEthernet0/0/5
log flow-export v9 udp destination 10.10.10.51 5050 source interface GigabitEthernet0/0/5
log flow-export v9 udp destination 10.10.10.52 5050 source interface GigabitEthernet0/0/5
log flow-export v9 udp destination 10.10.10.53 5050 source interface GigabitEthernet0/0/5
```

```
logging host 10.10.10.1 source-interface Loopback10
```

Qualified Commands for Cisco IOS XE Release 17.12.1a

Table 11: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Additional commands are qualified for use in Cisco SD-WAN Manager CLI templates.

AAA Commands

```
 aaa
lockout-policy
fail-attempts 3 fail-interval 300 lockout-interval 100
num-inactive-days days
multi-factor-auth
duo
api-hostname name
secret-key s-key
integration-key i-key
proxy proxy-url
```

Hub and Spoke Commands

```
topology hub-and-spoke enable
```

IP Commands

```
ip virtual-reassembly
```

MACsec Commands

```
key chain mac_chain macsec
key 1234abcd5678
key-string 12345678123456781234567812345678 cryptographic-algorithm AES-128-CMAC
key-string 11111111111111111111111111111111 cryptographic-algorithm aes-256-cmac
lifetime 05:00:00 20 february 2015 12:00:00 30 september 2016
mka policy MKAPolicy
confidentiality-offset
key-server priority 1
delay-protection
mka policy 2
include-icv-indicator
macsec-cipher-suite gcm-aes-256
sak-rekey interval 300
use-updated-eth-header
mka pre-shared-key key-chain kc1
macsec access-control must-secure
macsec access-control should-secure
macsec replay-protection window-size 10
eapol eth-type 0xB860
eapol destination-address 0018.b967.3cd0
eapol destination-address bridge-group-address
eapol destination-address broadcast-address
eapol destination-address lldp-multicast-address
cryptographic-algorithm aes-128-cmac
macsec-cipher-suite gcm-aes-128
macsec-cipher-suite gcm-aes-256
macsec-cipher-suite gcm-aes-xpn-128
macsec-cipher-suite gcm-aes-xpn-256
send-secure-announcements
macsec disable-sci
macsec replay-protection window-size 1024
macsec dot1q-in-clear
```

NAT Commands

```
nat66 prefix inside 2001:DB8::/32 outside 2001:DB8::/48 vrf 1 egress-interface GigabitEthernet
 3

nat66 prefix inside 2001:DB8::/32 outside 2001:DB8::/48 egress-interface GigabitEthernet 3
```

Routing Commands

```
affinity-group preference-auto
affinity-per-vrf
redistribute omp translate-rib-metric
```

Transport Gateway Commands

```
site-type
```

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.13.1a

Table 12: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	Additional commands are qualified for use in Cisco SD-WAN Manager CLI templates.

Interface Commands

```
  interface  GigabitEthernet  slot/subslot/port
 no ip address
 channel-group  channel-group-number  mode { active  passive}
 exit
lacp  system-priority  priority
 interface  GigabitEthernet  slot/subslot/port
 lacp  port-priority  priority
config-transaction
 interface  GigabitEthernet  slot/subslot/port
 no ip address
 channel-group  channel-group-number
```

IP Commands

```
ip dhcp smart-relay
```

Multi-Region Fabric Commands

```
management-gateway
management-region
```

NAT Commands

```
nat66 prefix inside source-prefix outside interface interface-name

nat66 prefix inside source-prefix outside interface interface-name vrf 1
```

SD-WAN Tunnel Interface Commands

```
interface  Tunnel  tunnel-number
 ip unnumbered  Port-channel channel-group-number
 no ip redirects
 tunnel source   Port-channel channel-group-number
 tunnel mode sdwan
 interface  Port-channel  channel-group-number
 tunnel-interface
 encapsulation { ipsec gre}
 color { public-internet mpls biz-internet lte}
```

Tracker Commands

```
tracker-type interface-icmp

tracker-type ipv6-interface-icmp

icmp-interval

endpoint-tracker-settings dia-stabilize-status
```

Service Insertion Commands

```
service-chain
service-chain-affect-bfd
service-chain-description
service-chain-enable
service-chain-vrf
service-track-enable
```

Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.14.1a

Table 13: Feature History

Feature Name	Release Information	Description
Qualified Commands for Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	Additional commands are qualified for use in Cisco SD-WAN Manager CLI templates.

Interface Commands

```
port-channel load-balance-hash-algo sdwan
ip load-sharing algorithm src-dst-ip

port-channel load-balance-hash-algo sdwan
ipv6 load-sharing algorithm ip-and-ports
```

L2VPN Commands

```
l2vpn sdwan instance 10 point-to-point
l2vpn sdwan instance 11 multipoint

interface GigabitEthernet7
 service instance 20 ethernet
  encapsulation dot1q 200
  !
 service instance 21 ethernet
  encapsulation dot1q 201
  !
bridge-domain 30
 member GigabitEthernet7 service-instance 20
 member sdwan-instance 10  remote-site 2 vc-id 1 single-homing
```

```
bridge-domain 31
 member GigabitEthernet7 service-instance 21
 member sdwan-instance 11 vc-id 1 single-homing
```

NAT Commands

```
nat66 prefix inside source-prefix outside interface interface-name
```

```
nat66 prefix inside source-prefix outside interface interface-name vrf 1
```

Policy Commands

```
policy app-agg-node max-records-per-minute
```

Tracker Commands

```
endpoint-tracker-sla-profile sla_agg
loss 10
latency 300
jitter 80
sla-mode aggressive
```