Contents

Introduction

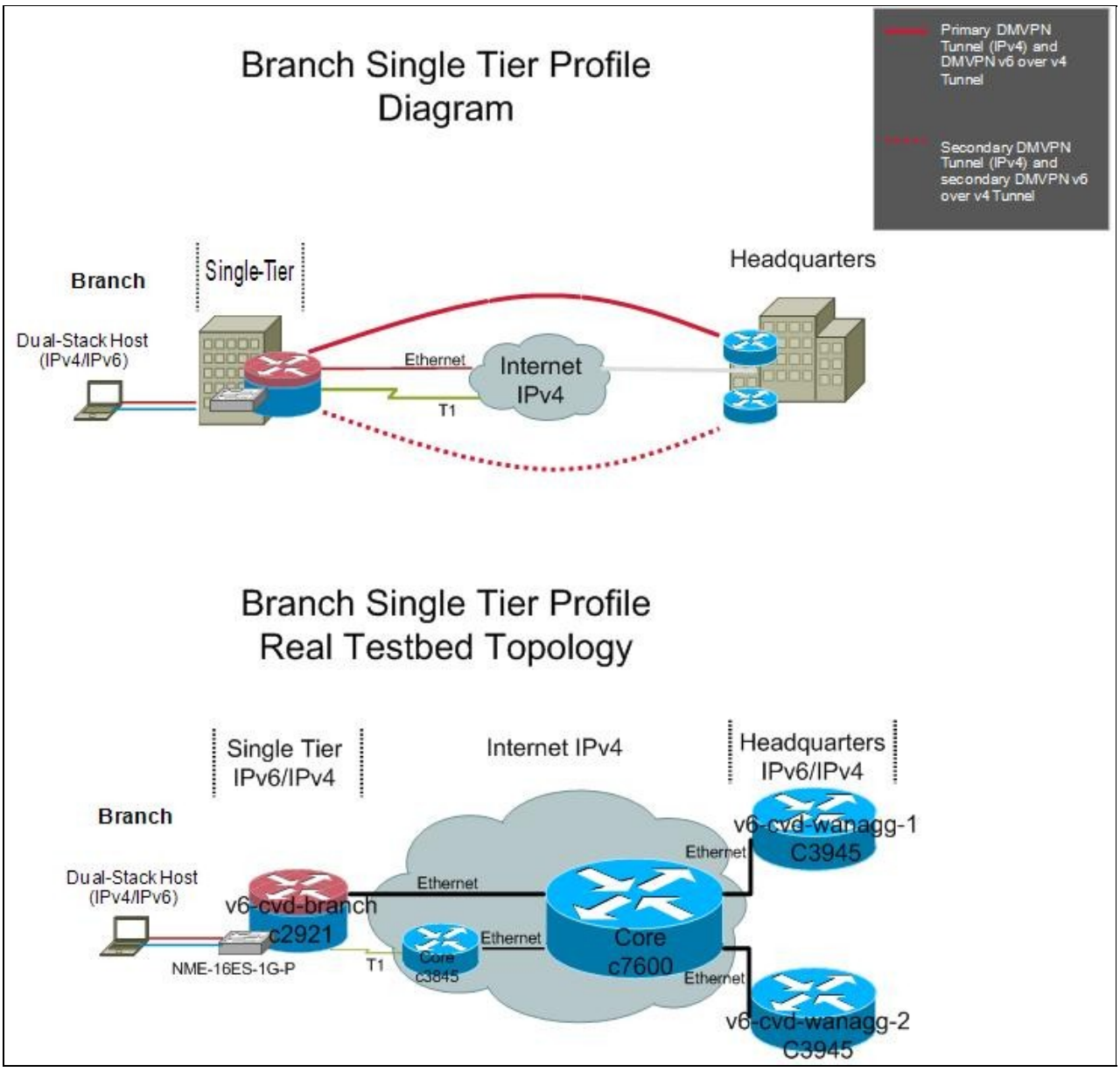
This document is intended to give customers a configuration example when they are planning or deployment IPv6 in their branch networks. This document is not meant to introduce you to branch design fundamentals and best practices, IPv6, transition mechanisms, or IPv4 and IPv6 feature comparisons. The user must be familiar with the Cisco branch design best practices recommendations and the basics of IPv6 and associated transition mechanisms. For information about the enterprise design architecture, refer to the following documents:

- Enterprise Branch Architecture Design Overview
- Enterprise Branch Security Design Guide

This document contents a dual stack ipv4/ipv6 single-tier branch profile. A single-tier dual stack ipv4/ipv6 single-tier branch profile is a fully integrated solution. The requirements for LAN and WAN connectivity and security are met by a single Integrated Services Router (ISR). WAN connectivity via an Ethernet links to an Internet Service Provider (ISP). This Ethernet is used as the primary link to the headquarters (HQ) site. For WAN redundancy, a backup connection is made via T1. IPv4 connectivity to the HQ site is provided by IPv4 IPSec using Dynamic Multi-Point Virtual Private Network (DMVPN) technologies. IPv6 connectivity to the HQ site is provided by using DMVPN v6 over v4. LAN connectivity is provided by an integrated switch module (EtherSwitch Service Module). Dual-stack (running both IPv4 TCP/IP stack and IPv6 TCP/IP stack) is used on the VLAN interfaces at the branch.

In addition to all of the security policies in place at the HQ, local security for both IPv4 and IPv6 is provided by a common set of infrastructure security features and configurations in addition to the use of the Cisco IOS Firewall.
QoS for IPv4 and IPv6 is integrated into a single policy.

Design



Configuration

This configuration uses the following features:

Routing Protocol	EIGRP IPv6
	EIGRP IPv4
Multicast	PIM-SSM (IPv4)
	MLDv2 (IPv6)
DMVPN	IPv4 / IPv6
WAN Access	Ethernet Handoff (Primary)
	T1 (Backup)
QoS (IPv6 / IPv4)	Classification (DSCP, ACL)
	Marking
	Queuing (CBWFQ, LLQ)

	Shaping
	HQOS (2-level HQOS)
Security	First Hop Security
Firewall	Zone Based Firewall (IPv6 and IPv4)
DHCP	DHCP (IPv6 and IPv4)
SSH	SSH (IPv6 and IPv4)
FTP	FTP
SNMP	SNMP
Access Lists	Standard and extended ACL

The links take you to the Configuration Guide (or other document) for information on configuring the features.

The router is a Cisco 2921 running c2900-universalk9-mz.SPA.151-3.T

Related show Commands

The feature documentation in the table above contains references to appropriate show commands for the features.

Certain show commands are supported by the Output Interpreter Tool (registered customers only), which allows you to view an analysis of show command output.

Show running-config

```
v6-cvd-branch#show running-configuration
Building configuration...

Current configuration : 28169 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname v6-cvd-branch
!
boot-start-marker
boot system flash0:c2900-universalk9-mz.SPA.151-3.T
boot-end-marker
!
!
card type t1 0 0
logging buffered 1000000
!
no aaa new-model
!
no network-clock-participate wic 0
!
ipv6 unicast-routing
ipv6 dhcp pool DATA_VISTA
 address prefix 2001:DB8:CAFE:1000::/64
 dns-server 2001:DB8:CAFE:10:20D:9DFF:FE93:B25D
 dns-server 2001:DB8:CAFE:10:51A1:5B1:4A85:B3DA
```

```
 domain-name cisco.com
!
ipv6 cef
ipv6 multicast-routing
ip source-route
ip cef
!
!
ip nbar port-map cifs tcp 137 139 445 445
ip nbar port-map custom-03 tcp 5554 9996
ip nbar port-map custom-02 udp 1434
ip nbar port-map netbios tcp 137 139 445
!
ip multicast-routing
ip dhcp relay information trust-all
no ip dhcp use vrf connected
!
ip dhcp pool DATA_LAN
   network 10.124.1.0 255.255.255.128
   dns-server 10.121.10.7
   default-router 10.124.1.1
   domain-name cisco.com
!
ip dhcp pool VOICE_LAN
   network 10.125.1.0 255.255.255.0
   dns-server 10.121.10.7
   default-router 10.125.1.1
   option 150 ip 10.121.10.7
   domain-name cisco.com
!
ip dhcp pool PRINTER_LAN
   network 10.124.1.128 255.255.255.128
   dns-server 10.121.10.7
   default-router 10.124.1.129
!
!
no ip bootp server
no ip domain lookup
ip domain name cisco.com
login block-for 30 attempts 3 within 200
login delay 2
!
multilink bundle-name authenticated
!
parameter-map type inspect global
 sessions maximum 1000
 alert off
 one-minute low 2000
 one-minute high 2000
parameter-map type inspect alart-on
 alert on
parameter-map type inspect default
 tcp max-incomplete host 100 block-time 0
parameter-map type urlf-glob MSN
 pattern msn.cisco.com

parameter-map type protocol-info msn-p
 server name msn.cisco.com

parameter-map type protocol-info msn-servers
 server name messenger.hotmail.com
 server name gateway.messenger.hotmail.com
 server name webmessenger.msn.com
```

```
!
!
!
!
!
key chain ESE
 key 1
  key-string 7 111B180B101719
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-1729957883
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1729957883
 revocation-check none
 rsakeypair TP-self-signed-1729957883
!
!
crypto pki certificate chain TP-self-signed-1729957883
 certificate self-signed 01
  3082024C 308201B5 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31373239 39353738 3833301E 170D3036 30363134 31353432
  33375A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 37323939
  35373838 3330819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100D428 80941683 0170D8DE 030D2C3C 33A07D6F 6CD1C01F E5356009 24ED5755
  D7485842 1C02DB49 A2A51B2B 5A68D212 898A916A A3458FA1 38E6994C F5715130
  35AB574D FC8A0C23 6E397EDB 4AAE2A38 1A2CC8D5 547B3745 83D11BCE 69E7F491
  090137C4 EA5863C0 2ABB64AF F985967A 2B170738 F4BF28B6 56009BA5 BEEC7C1E
  94350203 010001A3 74307230 0F060355 1D130101 FF040530 030101FF 301F0603
  551D1104 18301682 14323835 312D6272 312D312E 63697363 6F2E636F 6D301F06
  03551D23 04183016 801497B3 EB034DE7 C5481685 6DF51BA1 9C26CFD4 DA17301D
  0603551D 0E041604 1497B3EB 034DE7C5 4816856D F51BA19C 26CFD4DA 17300D06
  092A8648 86F70D01 01040500 03818100 92D03B85 6E53F61E 3FD536AD 0B5C2C94
  25E6A607 DD31170F 236B50F3 8A77685A 548164EC 022D262A EC26695F A26584EB
  469EA2AE 52878DA3 18A35708 BE9A1184 59D65E6B 652D8B6F E4392602 2E82F88F
  B57277C5 C4DE7908 82844EEA 06D079C1 B8190635 3268AEE8 A196FB1A A606C35C
  484DC275 D0F47913 1157FC30 BAFEAE13
        quit
voice-card 0
!
!
!
!
!
!
!
license udi pid CISCO2921/K9 sn FTX1435AJE2
hw-module pvdm 0/0
!
hw-module sm 1
!
!
!
username cisco privilege 15 password 0 cisco
!
redundancy
!
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
  key-string
   30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
   00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
   17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
```

```
   B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
   5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
   FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
   50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
   006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
   2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
   F3020301 0001
  quit
!
!
!
!
controller T1 0/0/0
 cablelength long 0db
 channel-group 1 timeslots 1-24
!
controller T1 0/0/1
 cablelength long 0db
 channel-group 1 timeslots 1-24
!
ip ftp source-interface Loopback0
ip ftp username cisco
ip ftp password 7 071D2042490C0B
ip ssh time-out 60
ip ssh authentication-retries 2
ip ssh source-interface Loopback0
ip ssh version 2
!
class-map type inspect match-all MSN-map
 match protocol msnmsgr
class-map type inspect match-any v6-class
 match protocol tcp
 match protocol udp
 match protocol icmp
 match protocol ftp
class-map type inspect match-all Y-map
 match protocol ymsgr
class-map type inspect match-all v6-map
 match class-map v6-class
 match access-group name ZFWv6
class-map type inspect match-any v4-map
 match protocol tcp
 match protocol udp
 match protocol dns
 match protocol icmp
 match protocol kazaa2
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
 match protocol ssh
 match protocol ftp
 match protocol https
 match protocol gdoi
 match protocol ipsec-msft
 match protocol isakmp
 match protocol bgp
 match protocol router
 match protocol ntp
 match protocol tacacs
 match protocol radius
class-map type inspect msnmsgr match-any MSN-class
class-map match-any BRANCH-BULK-DATA
 match access-group name BULK-DATA-APPS
 match access-group name BULK-DATA-APPS-V6
```

```
class-map type inspect http match-all HTTP
 match  request port-misuse any
 match  request method connect
class-map type inspect msnmsgr match-any MSN-c
 match  service any
class-map match-all SQL-SLAMMER
 match protocol custom-02
 match packet length min 404 max 404
class-map match-all BULK-DATA
 match  dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match  dscp af41  af42
class-map match-any BRANCH-SCAVENGE
class-map type inspect match-all v6-map-in
 match protocol icmp
 match access-group name FWIN
class-map match-any CALL-SIGNALLING
 match  dscp cs3
 match  dscp af31
class-map type inspect match-all HTTP-s
 match access-group 10
 match protocol http
class-map type inspect match-any HTTP-map
 match protocol http
class-map type inspect match-any im-aol
 match protocol aol
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol citrix
 match protocol ldap
 match protocol sqlnet
 match access-group name BRANCH-TRANSACTIONAL-V6
 match protocol http url "*cisco.com"
class-map type inspect ymsgr match-any YAHOO
 match  service any
class-map type inspect msnmsgr match-any MSN
class-map match-any BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
 match access-group name MISSION-CRITICAL-V6
class-map match-any WORMS
 match protocol http url "*.ida*"
 match protocol http url "*cmd.exe*"
 match protocol http url "*root.exe*"
 match protocol http url "*readme.eml*"
 match class-map SQL-SLAMMER
 match protocol exchange
 match protocol custom-03
class-map match-all VOICE
 match  dscp ef
class-map match-all MISSION-CRITICAL-DATA
 match  dscp 25
class-map match-any BRANCH-NET-MGMT
 match protocol snmp
 match protocol syslog
 match protocol telnet
 match protocol nfs
 match protocol dns
 match protocol icmp
 match protocol tftp
 match access-group name BRANCH-NET-MGMT-V6
class-map match-all ROUTING
 match  dscp cs6
class-map match-all SCAVENGER
 match  dscp cs1
class-map type inspect match-any telnet-s
```

```
class-map match-all NET-MGMT
 match  dscp cs2
class-map type inspect match-any VPN-in
 match access-group name ZBFW-v6-in
 match access-group name ZBFW-in
class-map match-any BRANCH-SCAVENGER
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
 match access-group name BRANCH-SCAVENGER-V6
class-map type inspect match-all v4-in
 match protocol icmp
class-map match-all TRANSACTIONAL-DATA
 match  dscp af21  af22
class-map type inspect match-any im-MSN
 match protocol msnmsgr msn-servers
class-map type inspect match-any route-v4-v6
 match access-group name v4-route
 match access-group name v6-route
!
!
policy-map type inspect FWIN
 class type inspect v4-in
  inspect
 class type inspect v6-map-in
  inspect
 class class-default
  drop
policy-map type inspect http HTTP
 class type inspect http HTTP
  allow
policy-map BRANCH-LAN-EDGE-IN-CHILD
 class WORMS
  drop
 class class-default
  set dscp default
policy-map BRANCH-WAN-EDGE-CHILD
 class VOICE
  priority percent 18
 class INTERACTIVE-VIDEO
  priority percent 15
 class CALL-SIGNALLING
  bandwidth percent 5
 class ROUTING
  bandwidth percent 3
 class NET-MGMT
  bandwidth percent 2
 class SCAVENGER
  bandwidth percent 1
 class MISSION-CRITICAL-DATA
  bandwidth percent 15
  random-detect dscp-based
 class TRANSACTIONAL-DATA
  bandwidth percent 12
  random-detect dscp-based
 class BULK-DATA
  bandwidth percent 4
  random-detect dscp-based
 class class-default
  bandwidth percent 25
  random-detect
policy-map BRANCH-LAN-EDGE-OUT
 class class-default
  set cos dscp
```

```
policy-map type inspect im YAHOO
 class type inspect ymsgr YAHOO
  allow
policy-map type inspect ZBP
 class type inspect v4-map
  inspect
 class type inspect v6-map
  inspect
 class type inspect HTTP-s
  inspect alart-on
 class type inspect telnet-s
  inspect alart-on
 class type inspect Y-map
  inspect
  service-policy im YAHOO
 class type inspect HTTP-map
  inspect
  service-policy http HTTP
 class type inspect im-MSN
  drop log
 class type inspect im-aol
  inspect alart-on
 class type inspect VPN-in
  pass
 class type inspect route-v4-v6
  pass
 class class-default
  drop
policy-map BRANCH-LAN-EDGE-IN-PARENT
 class BRANCH-MISSION-CRITICAL
  set dscp 25
 class BRANCH-TRANSACTIONAL-DATA
  set dscp af21
 class BRANCH-NET-MGMT
  set dscp cs2
 class BRANCH-BULK-DATA
  set dscp af11
 class BRANCH-SCAVENGER
  set dscp cs1
 class class-default
  set dscp default
  service-policy BRANCH-LAN-EDGE-IN-CHILD
policy-map type inspect im MSN
 class type inspect msnmsgr MSN
policy-map type inspect im MSN-policy
 class type inspect msnmsgr MSN-c
policy-map BRANCH-WAN-EDGE-PARENT
 class class-default
  shape average percent 90
  service-policy BRANCH-WAN-EDGE-CHILD
!
zone security inside
 description inside of branch
zone security outside
 description to internet
zone-pair security in-out source inside destination outside
 service-policy type inspect ZBP
zone-pair security out-in source outside destination inside
 service-policy type inspect FWIN
!
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
```

```
crypto isakmp key CISCO address 172.17.1.3
crypto isakmp key SYSTEMS address 172.18.1.4
crypto isakmp key SYSTEMS address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set brb esp-3des esp-sha-hmac
crypto ipsec transform-set brb-back esp-3des esp-sha-hmac
!
crypto ipsec profile dmvpn
 set security-association lifetime seconds 300
 set transform-set brb
!
crypto ipsec profile dmvpn-back
 set security-association lifetime seconds 300
 set transform-set brb-back
!
!
!
!
!
!
interface Loopback0
 ip address 10.122.1.1 255.255.255.254
 ipv6 address 2001:DB8:CAFE:1111::BAD1:A001/64
 ipv6 eigrp 1
!
interface Tunnel1
 description DMVPN to HQ Head-end 1
 ip address 10.126.1.2 255.255.255.0
 ip access-group INET in
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip mtu 1400
 ip pim sparse-dense-mode
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 ESE
 ip hold-time eigrp 10 35
 no ip next-hop-self eigrp 10
 ip flow ingress
 ip nhrp authentication secret
 ip nhrp map multicast dynamic
 ip nhrp map multicast 172.17.1.3
 ip nhrp map 10.126.1.1 172.17.1.3
 ip nhrp network-id 10203
 ip nhrp nhs 10.126.1.1
 ip virtual-reassembly in
 zone-member security outside
 no ip split-horizon eigrp 10
 load-interval 30
 delay 500
 ipv6 address 2001:DB8:CAFE:1261::BAD1:A001/64
 ipv6 mtu 1400
 no ipv6 redirects
 no ipv6 unreachables
 ipv6 eigrp 1
 ipv6 authentication mode eigrp 1 md5
 ipv6 authentication key-chain eigrp 1 ESE
 ipv6 hold-time eigrp 1 35
 no ipv6 split-horizon eigrp 1
 no ipv6 mfib forwarding input
 ipv6 nhrp authentication secret
 ipv6 nhrp map multicast dynamic
```

```
 ipv6 nhrp map multicast 172.17.1.3
 ipv6 nhrp map 2001:DB8:CAFE:1261::ACE1:F000/128 172.17.1.3
 ipv6 nhrp network-id 70809
 ipv6 nhrp nhs 2001:DB8:CAFE:1261::ACE1:F000
 ipv6 traffic-filter INET-WAN-v6 in
 keepalive 10 3
 tunnel source 172.16.1.2
 tunnel mode gre multipoint
 tunnel key 123
 tunnel protection ipsec profile dmvpn
 no clns route-cache
!
interface Tunnel2
 description DMVPN to HQ Head-end 2
 ip address 10.127.1.2 255.255.255.0
 ip access-group INET-BACK in
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip mtu 1400
 ip pim sparse-dense-mode
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 ESE
 ip hold-time eigrp 10 35
 no ip next-hop-self eigrp 10
 ip flow ingress
 ip nhrp authentication secret
 ip nhrp map multicast dynamic
 ip nhrp map 10.127.1.1 172.18.1.4
 ip nhrp map multicast 172.18.1.4
 ip nhrp network-id 30201
 ip nhrp nhs 10.127.1.1
 ip virtual-reassembly in
 zone-member security outside
 no ip split-horizon eigrp 10
 load-interval 30
 delay 500
 ipv6 address 2001:DB8:CAFE:1271::BAD1:A001/64
 ipv6 mtu 1400
 no ipv6 redirects
 no ipv6 unreachables
 ipv6 eigrp 1
 ipv6 authentication mode eigrp 1 md5
 ipv6 hold-time eigrp 1 35
 no ipv6 split-horizon eigrp 1
 ipv6 nhrp authentication secret
 ipv6 nhrp map multicast dynamic
 ipv6 nhrp map multicast 172.18.1.4
 ipv6 nhrp map 2001:DB8:CAFE:1271::ACE1:F000/128 172.18.1.4
 ipv6 nhrp network-id 90807
 ipv6 nhrp nhs 2001:DB8:CAFE:1271::ACE1:F000
 ipv6 traffic-filter INET-WAN-v6 in
 if-state nhrp
 tunnel source Serial0/0/0:1
 tunnel mode gre multipoint
 tunnel key 321
 tunnel protection ipsec profile dmvpn-back
 no clns route-cache
!
interface GigabitEthernet0/0
 ip address 10.123.1.1 255.255.255.0
 ip pim sparse-dense-mode
 ip igmp join-group 232.0.0.1 source 10.130.1.1
 duplex auto
```

```
 speed auto
!
interface GigabitEthernet0/1
 description Ethernet Handoff to ISP (PRIMARY)
 ip address 172.16.1.2 255.255.255.252
 ip access-group WAN-link in
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip nbar protocol-discovery
 ip flow ingress
 ip virtual-reassembly in
 ip verify unicast reverse-path
 load-interval 30
 duplex auto
 speed auto
 service-policy output BRANCH-WAN-EDGE-PARENT
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0:1
 ip address 172.15.1.2 255.255.255.252
 ip access-group WAN-link in
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip mtu 1400
 ip nbar protocol-discovery
 ip flow ingress
 ip virtual-reassembly in
 service-policy output BRANCH-WAN-EDGE-PARENT
!
interface Serial0/0/1:1
 no ip address
 shutdown
!
interface GigabitEthernet1/0
 description to INTERNAL SW-BR1-1
 ip address 1.1.1.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip pim sparse-mode
 ip flow ingress
 ip virtual-reassembly in
 ip policy route-map no_split
 ipv6 nd other-config-flag
 no ipv6 redirects
 no ipv6 unreachables
 ipv6 dhcp server DATA_VISTA
 ipv6 traffic-filter DATA_LAN-v6 in
 ipv6 virtual-reassembly in
 no snmp trap link-status
!
interface GigabitEthernet1/0.100
 description DATA VLAN for Computers
 encapsulation dot1Q 100
 ip address 10.124.1.1 255.255.255.128
 ip access-group LANout in
 no ip redirects
```

```
 no ip unreachables
 no ip proxy-arp
 ip pim sparse-dense-mode
 ip flow ingress
 ip virtual-reassembly in
 zone-member security inside
 ip policy route-map no_split
 ipv6 address 2001:DB8:CAFE:1100::BAD1:A001/64
 ipv6 nd other-config-flag
 no ipv6 redirects
 no ipv6 unreachables
 ipv6 dhcp server DATA_VISTA
 ipv6 eigrp 1
 ipv6 traffic-filter DATA_LAN-v6 in
 ipv6 virtual-reassembly in
 service-policy input BRANCH-LAN-EDGE-IN-PARENT
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet1/0.200
 description to Voice VLAN for IP Phones
 encapsulation dot1Q 200
 ip address 10.125.1.1 255.255.255.0
 ip access-group VOICEout in
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip pim sparse-dense-mode
 ip flow ingress
 ip virtual-reassembly in
 zone-member security inside
 ip policy route-map no_split
 ipv6 address 2001:DB8:CAFE:1200::BAD1:A001/64
 no ipv6 redirects
 no ipv6 unreachables
 ipv6 eigrp 1
 ipv6 traffic-filter VOICE_LAN-v6 in
 ipv6 virtual-reassembly in
 service-policy input BRANCH-LAN-EDGE-IN-PARENT
 service-policy output BRANCH-LAN-EDGE-OUT
!
interface GigabitEthernet1/0.300
 description to Printer VLAN
 encapsulation dot1Q 300
 ip address 10.124.1.129 255.255.255.128
 ip access-group PRINTERout in
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip pim sparse-dense-mode
 ip flow ingress
 ip virtual-reassembly in
 zone-member security inside
 ip policy route-map no_split
 ipv6 address 2001:DB8:CAFE:1300::BAD1:A001/64
 no ipv6 redirects
 no ipv6 unreachables
 ipv6 eigrp 1
 ipv6 traffic-filter PRINTER_LAN-v6 in
 ipv6 virtual-reassembly in
 service-policy input BRANCH-LAN-EDGE-IN-PARENT
 service-policy output BRANCH-LAN-EDGE-OUT
!
!
router eigrp 10
```

```
 network 10.0.0.0
 redistribute static
 passive-interface GigabitEthernet1/0
 passive-interface GigabitEthernet1/0.100
 passive-interface GigabitEthernet1/0.200
 passive-interface GigabitEthernet1/0.300
 eigrp stub connected summary
!
ip forward-protocol nd
!
ip pim ssm default
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
ip route 0.0.0.0 0.0.0.0 Serial0/0/0:1 200
ip route 223.255.248.115 255.255.255.255 GigabitEthernet0/0
!
ip access-list extended BULK-DATA-APPS
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 permit tcp any any eq pop3
 permit tcp any any eq 143
ip access-list extended INET
 permit igmp any any
 permit pim any any
 permit eigrp any any
 permit icmp any 10.126.1.0 0.0.0.255
 permit icmp any 10.126.1.0 0.0.0.255 packet-too-big
 permit icmp any 10.126.1.0 0.0.0.255 unreachable
 permit icmp any 10.126.1.0 0.0.0.255 echo-reply
 permit icmp any 10.126.1.0 0.0.0.255 time-exceeded
 permit icmp any 10.124.100.0 0.0.0.255
 permit icmp any 10.124.100.0 0.0.0.255 packet-too-big
 permit icmp any 10.124.100.0 0.0.0.255 unreachable
 permit icmp any 10.124.100.0 0.0.0.255 echo-reply
 permit icmp any 10.124.100.0 0.0.0.255 time-exceeded
 permit icmp any 10.124.1.0 0.0.0.255
 permit icmp any 10.124.1.0 0.0.0.255 packet-too-big
 permit icmp any 10.124.1.0 0.0.0.255 unreachable
 permit icmp any 10.124.1.0 0.0.0.255 echo-reply
 permit icmp any 10.124.1.0 0.0.0.255 time-exceeded
 permit icmp any 10.125.1.0 0.0.0.127
 permit icmp any 10.125.1.0 0.0.0.127 packet-too-big
 permit icmp any 10.125.1.0 0.0.0.127 unreachable
 permit icmp any 10.125.1.0 0.0.0.127 echo-reply
 permit icmp any 10.125.1.0 0.0.0.127 time-exceeded
 permit udp any host 10.124.100.1 eq ntp
 permit tcp any host 10.124.100.1 eq telnet
 permit tcp any host 10.124.100.1 eq 22
 permit ip any 10.125.1.0 0.0.0.255
 permit ip any 10.124.1.0 0.0.0.255
 permit ip any 10.126.1.0 0.0.0.255
 deny   ip host 255.255.255.255 any
 deny   ip any any log
ip access-list extended INET-BACK
 permit pim any any
 permit eigrp any any
 permit icmp any 10.127.1.0 0.0.0.255
 permit icmp any 10.127.1.0 0.0.0.255 packet-too-big
 permit icmp any 10.127.1.0 0.0.0.255 unreachable
 permit icmp any 10.127.1.0 0.0.0.255 echo-reply
 permit icmp any 10.127.1.0 0.0.0.255 time-exceeded
 permit icmp any 10.124.100.0 0.0.0.255
```

```
 permit icmp any 10.124.100.0 0.0.0.255 packet-too-big
 permit icmp any 10.124.100.0 0.0.0.255 unreachable
 permit icmp any 10.124.100.0 0.0.0.255 echo-reply
 permit icmp any 10.124.100.0 0.0.0.255 time-exceeded
 permit icmp any 10.124.1.0 0.0.0.255
 permit icmp any 10.124.1.0 0.0.0.255 packet-too-big
 permit icmp any 10.124.1.0 0.0.0.255 unreachable
 permit icmp any 10.124.1.0 0.0.0.255 echo-reply
 permit icmp any 10.124.1.0 0.0.0.255 time-exceeded
 permit icmp any 10.125.1.0 0.0.0.127
 permit icmp any 10.125.1.0 0.0.0.127 packet-too-big
 permit icmp any 10.125.1.0 0.0.0.127 unreachable
 permit icmp any 10.125.1.0 0.0.0.127 echo-reply
 permit icmp any 10.125.1.0 0.0.0.127 time-exceeded
 permit udp any host 10.124.100.1 eq ntp
 permit tcp any host 10.124.100.1 eq telnet
 permit tcp any host 10.124.100.1 eq 22
 permit ip any 10.125.1.0 0.0.0.255
 permit ip any 10.124.1.0 0.0.0.255
 permit ip any 10.127.1.0 0.0.0.255
 deny   ip host 255.255.255.255 any
 deny   ip any any log
ip access-list extended LANout
 permit udp host 0.0.0.0 host 255.255.255.255
 permit ip 10.124.1.0 0.0.0.127 any
 deny   ip any any log
ip access-list extended MGMT-IN-v4
 permit tcp 10.120.0.0 0.0.255.255 any
 permit tcp 10.126.0.0 0.0.255.255 any
 permit tcp 10.121.0.0 0.0.255.255 any
 permit tcp 10.122.0.0 0.0.255.255 any
 deny   ip any any log-input
ip access-list extended MISSION-CRITICAL-SERVERS
 permit ip any 10.121.10.0 0.0.0.255
 permit ip any 10.121.11.0 0.0.0.255
 permit ip any 10.121.12.0 0.0.0.255
ip access-list extended PRINTERout
 permit udp host 0.0.0.0 host 255.255.255.255
 permit ip 10.124.1.128 0.0.0.127 any
 deny   ip any any
ip access-list extended VOICEout
 permit udp host 0.0.0.0 host 255.255.255.255
 permit ip 10.125.1.0 0.0.0.127 any
 deny   ip any any
ip access-list extended WAN-link
 permit esp any any
 permit gre any any
 permit udp any host 172.16.1.2 eq isakmp
 permit icmp any host 172.16.1.2
 permit icmp any host 172.16.1.2 packet-too-big
 permit icmp any host 172.16.1.2 unreachable
 permit udp any host 10.124.100.1 eq isakmp
 permit icmp any host 10.124.100.1
 permit icmp any host 10.124.100.1 packet-too-big
 permit icmp any host 10.124.100.1 unreachable
 permit icmp any any echo-reply
 permit icmp any any time-exceeded
 deny   tcp any any
 deny   udp any any
 deny   ip host 255.255.255.255 any
 deny   ip any any
ip access-list extended WAN_TRAFFIC
 deny   ip any 10.124.1.0 0.0.0.255
 deny   ip any 10.125.1.0 0.0.0.127
```

```
 permit ip any any
ip access-list extended ZBFW-in
 permit esp any any
 permit udp any any eq isakmp
ip access-list extended v4-route
 permit ospf any any
 permit eigrp any any
!
access-list 10 permit 10.126.1.0
access-list 10 permit 172.16.1.0
access-list 99 permit 10.129.1.1
access-list 180 permit ip host 10.129.1.1 host 10.124.1.2
ipv6 router eigrp 1
 passive-interface GigabitEthernet1/0.100
 passive-interface GigabitEthernet1/0.200
 passive-interface GigabitEthernet1/0.300
 eigrp router-id 10.124.100.1
 eigrp stub connected summary
!
!
!
!
!
!
!
ipv6 access-list INET-WAN-v6
 remark PERMIT EIGRP for IPv6
 permit 88 any any
 remark PERMIT PIM for IPv6
 permit 103 any any
 remark PERMIT ALL ICMPv6 PACKETS SOURCED USING THE LINK-LOCAL PREFIX
 permit icmp FE80::/10 any
 remark PERMIT SSH TO LOCAL LOOPBACK
 permit tcp any host 2001:DB8:CAFE:1000::BAD1:A001 eq 22
 remark PERMIT ALL ICMPv6 PACKETS TO LOCAL LOOPBACK
 permit icmp any host 2001:DB8:CAFE:1000::BAD1:A001
 remark PERMIT ALL ICMPv6 PACKETS TO TUNNEL3
 permit icmp any host 2001:DB8:CAFE:1261::BAD1:A001
 remark PERMIT ALL ICMPv6 PACKETS TO TUNNEL4
 permit icmp any host 2001:DB8:CAFE:1271::BAD1:A001
 remark PERMIT ALL ICMPv6 PACKETS TO DATA VLAN
 permit icmp any 2001:DB8:CAFE:1100::/64
 remark PERMIT ALL ICMPv6 PACKETS TO VOICE VLAN
 permit icmp any 2001:DB8:CAFE:1200::/64
 remark PERMIT ALL ICMPv6 PACKETS TO PRINTER VLAN
 permit icmp any 2001:DB8:CAFE:1300::/64
 remark PERMIT ALL IPv6 PACKETS TO DATA VLAN
 permit ipv6 any 2001:DB8:CAFE:1100::/64
 remark PERMIT ALL IPv6 PACKETS TO VOICE VLAN
 permit ipv6 any 2001:DB8:CAFE:1200::/64
 remark PERMIT ALL IPv6 PACKETS TO PRINTER VLAN
 permit ipv6 any 2001:DB8:CAFE:1300::/64
 deny ipv6 any any log
!
ipv6 access-list DATA_LAN-v6
 remark PERMIT ICMPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:1100::/64
 permit icmp 2001:DB8:CAFE:1100::/64 any
 remark PERMIT IPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:1100::64
 permit ipv6 2001:DB8:CAFE:1100::/64 any
 remark PERMIT ALL ICMPv6 PACKETS SOURCED BY HOSTS USING THE LINK-LOCAL PREFIX
 permit icmp FE80::/10 any
 remark PERMIT DHCPv6 ALL-DHCP-AGENTS REQUESTS FROM HOSTS
 permit udp any eq 546 any eq 547
 remark DENY ALL OTHER IPv6 PACKETS AND LOG
```

```
 deny ipv6 any any log-input
!
ipv6 access-list VOICE_LAN-v6
 remark PERMIT ICMPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:1200::/64
 permit icmp 2001:DB8:CAFE:1200::/64 any
 remark PERMIT IPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:1200::64
 permit ipv6 2001:DB8:CAFE:1200::/64 any
 remark PERMIT ALL ICMPv6 PACKETS SOURCED BY HOSTS USING THE LINK-LOCAL PREFIX
 permit icmp FE80::/10 any
 remark PERMIT DHCPv6 ALL-DHCP-AGENTS REQUESTS FROM HOSTS
 permit udp any eq 546 any eq 547
 remark DENY ALL OTHER IPv6 PACKETS AND LOG
 deny ipv6 any any log-input
!
ipv6 access-list PRINTER_LAN-v6
 remark PERMIT ICMPv6 PACKETS FROM HOSTS WITH PREFIX CAFE:1300::/64
 permit icmp 2001:DB8:CAFE:1300::/64 any
 remark PERMIT IPv6 PACKETS FROM HOSTS WITH PREFIX CAFE:1300::64
 permit ipv6 2001:DB8:CAFE:1300::/64 any
 remark PERMIT ALL ICMPv6 PACKETS SOURCED BY HOSTS USING THE LINK-LOCAL PREFIX
 permit icmp FE80::/10 any
 remark PERMIT DHCPv6 ALL-DHCP-AGENTS REQUESTS FROM HOSTS
 permit udp any eq 546 any eq 547
 remark DENY ALL OTHER IPv6 PACKETS AND LOG
 deny ipv6 any any log-input
!
ipv6 access-list ACCESS_port
 deny udp any eq 547 any eq 546
 deny icmp any any router-advertisement
 permit ipv6 any any
!
ipv6 access-list MGMT-IN
 remark permit mgmt only to loopback
 permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:1000::BAD1:A001
 deny ipv6 any any log-input
!
ipv6 access-list BULK-DATA-APPS-V6
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 permit tcp any any eq pop3
 permit tcp any any eq 143
!
ipv6 access-list BRANCH-SCAVENGER-V6
 remark Gnutella, Kazaa, Doom, iTunes traffic-mark dscp cs1
 permit tcp any any range 6346 6347
 permit udp any any range 6346 6347
 permit tcp any any eq 1214
 permit tcp any any eq 666
 permit udp any any eq 666
 permit tcp any any eq 3689
 permit udp any any eq 3689
!
ipv6 access-list BRANCH-NET-MGMT-V6
 remark Common management traffic plus vmware console-mark dscp cs2
 permit udp any any eq syslog
 permit udp any any eq snmp
 permit tcp any any eq telnet
 permit tcp any any eq 22
 permit tcp any any eq 2049
 permit udp any any eq 2049
 permit tcp any any eq domain
 permit udp any any eq tftp
 permit tcp any any eq 902
!
```

```
ipv6 access-list BRANCH-TRANSACTIONAL-V6
 remark Microsoft RDP traffic-mark dscp af21
 permit tcp any any eq 3389
 permit udp any any eq 3389
!
ipv6 access-list ipv6_only
 permit tcp 2001:400:1:1::/64 2001:400:2:1::/64
 permit udp 2001:400:1:1::/64 2001:400:2:1::/64
 permit icmp 2001:400:1:1::/64 2001:400:2:1::/64
 deny ipv6 any any
!
ipv6 access-list ZFWv6
 permit ipv6 any any
!
ipv6 access-list ZBFW-v6-in
 permit esp any any
 permit udp any any eq isakmp
!
ipv6 access-list v6-route
 permit 88 any any
!
ipv6 access-list FWIN
 permit ipv6 any any
!
ipv6 access-list MISSION-CRITICAL-V6
 remark Data-Center traffic-mark dscp 25
 permit ipv6 any 2001:DB8:CAFE:10::/64
 permit ipv6 any 2001:DB8:CAFE:11::/64
!
control-plane
!
!
!
!
mgcp profile default
!
!
!
!
!
gatekeeper
 shutdown
!
!
!
line con 0
 session-timeout 3
 exec-timeout 0 0
 password lab
 logging synchronous
 login local
 transport output all
line aux 0
 session-timeout 3
 login local
line 67
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
 session-timeout 3
 access-class MGMT-IN-v4 in
```

```
 privilege level 15
 password lab
 ipv6 access-class MGMT-IN in
 login local
 exec prompt timestamp
 transport input ssh
 transport output all
line vty 5 15
 session-timeout 3
 access-class MGMt-in-V4 in
 privilege level 15
 ipv6 access-class MGMT-IN in
 login local
 transport input ssh
!
no exception data-corruption buffer truncate
scheduler allocate 20000 1000
end
```

Related Information

Technical Support & Documentation - Cisco Systems