CHAPTER 14

Virtual Private Networks "VPNs"

This chapter describes the level of support that Cisco ANA provides for VPNs, as follows:

Technology Description

VPN

BGP/MPLS VPNs, as defined in RFC 2547 and related drafts and standards, provide a Layer 3 VPN. With Layer 3 VPNs, each Provider Edge (PE) device acts like a set of virtual routers, one per VPN. The network provider configures the VPN membership of each PE router interface. In most cases, one port is used for multiple interfaces where each is associated with different VPNs. The port's view of the network is restricted to the VPNs of which it is a member, and it cannot address devices outside that environment. Either static routes are provisioned on both the Customer Edge (CE) and PE, or, for more complex scenarios, a routing protocol (such as RIP, OSPF or BGP) is run between CE and PE. So the interface between the CE and PE devices is conventional IP routing.

The network provider also establishes a suitable mesh of MPLS Label Switched Paths (LSPs) between all the PE routers that need to communicate. The PE devices qualify each external IP address that they learn with a per VPN identifier, and broadcast them to all other PE routers using an extended form of BGP depending on BGP connectivity. They also include an MPLS label that is specific to the destination route (or, in some implementations, the destination port). Through this process, the PE devices build up a complete map of the VPNs and destination labels.

The PE routers then use this information to route the packets across the backbone network to the correct destination within the relevant VPN.

Inventory and Information Model Objects (IMOs)

This section includes the following tables:

- Equivalent Routing Entry (IRoutingEntries)
- Virtual Routing Entry (IVrfEntry)
- Multi Protocol BGP Entity (IMpBgp)
- Equivalent Cross Virtual Routing Entry (ICrossVrf)
- Cross Virtual Routing Entry (ICrossVrfRoutingEntry)

Virtual Routing Forwarding (VRF) Entity

The following Virtual Routing Forwarding (VRF) Entity object describes the routing and address resolution protocols independent forwarding component of a MPLS-BGP based VPN router, which is bound by its Logical Sons attribute to all Network layer IP Interface objects, which IP Packets are being routed between, by this Virtual Routing Forwarding Entity.

Table 14-1 Virtual Routing Forwarding (VRF) Entity (IVrf)

Attribute Name	Attribute Description
Virtual Routing Table	Array of Equivalent Routing Entries
Exported Route Targets	Array of route target identifiers
Imported Route Targets	Array of route target identifiers
Route Distinguisher	Route distinguisher
ARP Entity	Address Resolution Entity (ARP Entity) (see Internet Protocol "IP")
Name	VRF name
Logical Sons	Array of all IP Interfaces, which IP packets are being routed between, by this Virtual Routing Forwarding (VRF) Entity

Equivalent Routing Entry

The following Equivalent Routing Entry and Virtual Routing Entry objects describe a routing table's entries, each as an array of Virtual Routing Entries sharing a single IP Subnetwork destination.

Table 14-2 Equivalent Routing Entry (IRoutingEntries)

Attribute Name	Attribute Description
Routing Entries	Array of Virtual Routing Entries (sharing a single destination)

Virtual Routing Entry

Table 14-3 Virtual Routing Entry (IVrfEntry)

Attribute Name	Attribute Description
Next Hop BGP Address	Next hop BGP IP address
Incoming and Outgoing Inner Label	Incoming and outgoing inner MPLS label

Table 14-3 Virtual Routing Entry (IVrfEntry) (continued)

Attribute Name	Attribute Description
Outer Label	Outer MPLS label
Destination IP Subnet	Final destination IP subnet
Next Hop IP Address	Next hop IP address
Type	Route entry type (*Null, Other, Invalid, Direct, Indirect, Static*)
Routing Protocol Type	Routing protocol type (*Null, Other, "Local, Network Managed, ICMP, EGP, GGP, Hello, RIP, IS-IS, ES-IS, Cisco IGRP, BBN SPF IGP, OSPF, BGP, EIGRP*)
Outgoing Interface Name	Outgoing IP interface name

Multi Protocol BGP Entity

The following Multi Protocol BGP Entity object describes the BGP component of a MPLS-BGP based VPN router, which is bound by its Logical Sons attribute to all Virtual Routing Forwarding (VRF) Entity objects, which IP Packets are being routed between by this Multi Protocol BGP Entity.

Table 14-4 Multi Protocol BGP Entity (IMpBgp)

Attribute Name	Attribute Description
BGP Identifier	Border Gateway Protocol (BGP) identifier
Local Autonomous System	Local peer autonomous system
Cross Virtual Routing Table	Array of Equivalent Cross Virtual Routing Entry
BGP Neighbors	Array of BGP neighbor entries (see Routing Protocols "BGP/OSPF")
Logical Sons	Array of all Virtual Routing Entries, which IP packets are being routed between, by this Multi Protocol BGP Entity

Equivalent Cross Virtual Routing Entry

The following Equivalent Cross Virtual Routing Entry and Cross Virtual Routing Entry objects describe the first dimension of a cross virtual routing table, as an array of Cross Virtual Routing Entries sharing a single Virtual Routing Forwarding (VRF) Entity destination.

Table 14-5 Equivalent Cross Virtual Routing Entry (ICrossVrf)

Attribute Name	Attribute Description
Virtual Routing Entries	Array of Cross Virtual Routing Entries (sharing a single destination)
Virtual Routing Entity Name	Virtual Routing Entity (VRF) name

Cross Virtual Routing Entry

Table 14-6 Cross Virtual Routing Entry (ICrossVrfRoutingEntry)

Attribute Name	Attribute Description
Outgoing Virtual Routing Entity Identifier	Outgoing virtual routing entity Object Identifier (OID)
Incoming and Outgoing Virtual Routing Tags	Incoming and outgoing virtual routing tags
Destination IP Subnet	Final destination IP subnet
Next Hop IP Address	Next hop IP address
Type	Route entry type (*Null, Other, Invalid, Direct, Indirect, Static*)
Routing Protocol Type	Routing protocol type (*Null, Other, "Local, Network Managed, ICMP, EGP, GGP, Hello, RIP, IS-IS, ES-IS, Cisco IGRP, BBN SPF IGP, OSPF, BGP, EIGRP*)
Outgoing Interface Name	Outgoing IP interface name

Network Topology

The discovery of MPLS-BGP based Virtual Private (VPN) network topology is done by searching for the existence of the local Virtual Routing Forwarding (VRF) Entity's imported route targets in any remote side's VRF entity exported route targets.

Service Alarms

The following alarm is supported for this technology:

- Duplicate IP on VPN Found/Duplicate IP on VPN Fixed

Note This alarm is disabled by default.

Note For a detailed description of these alarms and for information about correlation see the *Cisco Active Network Abstraction Fault Management User Guide, 3.6.*