Deploying IPv6 in Branch Networks

Last Updated: April 8, 2011

Cisco Validated Design

Building Architectures to Solve Business Problems

About the Author

Shannon McFarland

Shannon McFarland, Corporate Consulting Engineer, Office of the CTO, Cisco Systems

Shannon McFarland, CCIE #5245, is a Corporate Consulting Engineer in the Office of the CTO and is focused on Enterprise IPv6 deployment, VDI, and Data Center technologies. Shannon has been responsible for the Enterprise IPv6 design and deployment effort at Cisco for the last 9 years. He has authored many technical papers and Cisco Validated Design guides, is a contributor to Cisco Press books, and is a frequent speaker at Cisco Live and other industry conferences. He co-authored a Cisco Press book, "IPv6 in Enterprise Networks". Prior to his time at Cisco corporate, Shannon was an SE in the Cisco Englewood, CO office. Shannon has been at Cisco for 11+ years.

About Cisco Validated Design (CVD) Program

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit http://www.cisco.com/go/designzone.

Deploying IPv6 in Branch Networks

Deploying IPv6 in Branch Networks

This document is intended to guide customers in planning or deploying IPv6 in 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*

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Branch/EnBrOver.html
- *Enterprise Branch Security Design Guide*

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Branch/E_B_SDC1.html

Introduction

This document requires a basic understanding of Cisco branch design, security, and the basics of IPv6. This prerequisite knowledge can be acquired through many documents and training opportunities that are available through Cisco Systems, Inc. and through the networking industry at large. References contains resources for these areas of interest.

Scope

This document provides a brief overview of the various branch IPv6 deployment profiles and general deployment considerations. This document also covers the implementation details for each branch profile individually.

This document focuses on the branch side of the WAN, but the basic configurations used on the head-end WAN routers are shown when appropriate. These configurations were used for testing only and are not necessarily the recommended WAN router configurations that customers should use. Updates to this document and new IPv6-related documents can be found at: http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Branch Deployment Overview

This section provides a high-level overview of the two mostly commonly deployed Cisco branch profiles to provide a basic understanding of how IPv6 can be integrated into these two branch profiles.

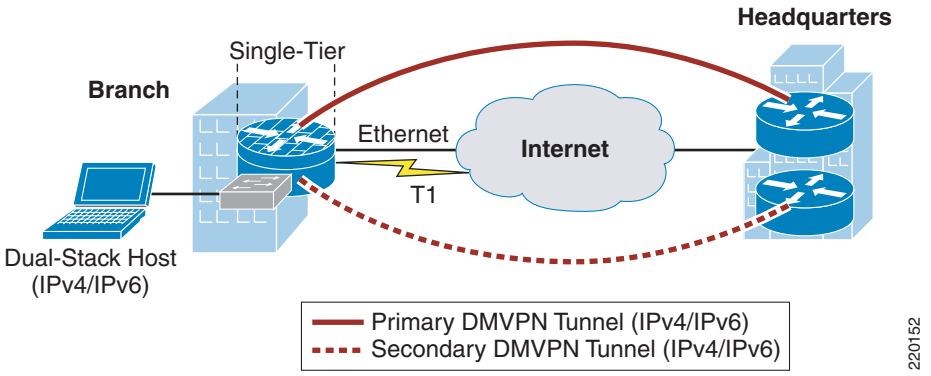
The branch IPv6 deployment profiles that are described in this section:

- Single-Tier Profile
- Multi-Tier Profile

Single-Tier Profile

The 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). Figure 1 shows a high-level view of the single-tier branch profile.

Figure 1 Single-Tier Profile



In the single-tier profile described in this document, a single ISR is used to provide WAN connectivity via an Ethernet hand-off from an Internet Service Provider (ISP). The Ethernet link is used as the primary link to the headquarters (HQ) site. For WAN redundancy, a backup connection is made via a T1/E1 circuit.

IPv4 and IPv6 connectivity to the HQ site is provided by IPv4 IPSec using Dynamic Multi-Point Virtual Private Network (DMVPN) technologies. The DMVPN tunnels traverse the Ethernet link as the primary path and establish backup tunnels over the T1/E1 link.

All traffic leaving the branch traverses the VPN connections to the HQ, including the Internet-bound traffic. Generally, Cisco does not recommend the use of split-tunneling at the branch site. If the customer requires split-tunneling, then Cisco recommends a careful analysis and testing of the routing and the security implications of such a deployment.

Note While it not covered in this document, it is also possible to establish native IPv6 IPSec tunnels from the ISR to the HQ site if the ISPs offers IPv6 support to the branch and HQ sites. In this document it is assumed that no IPv6 services are offered from the ISP to the branch site. More information on IPv6 IPSec configurations and support can be found at: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ipsec_ps10591_TSD_Products_Configuration_Guide_Chapter.html.

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 Zone-Based Firewall (an optional deployment). QoS for IPv4 and IPv6 is integrated into a single policy.

The obvious disadvantage of the single-tier profile is the lack of router and switch redundancy. There is redundancy for the link to the Internet and the VPN connections to HQ. However, because there is a single integrated switch and single router, if either component fails, then the site is completely disconnected from HQ. The multi-tier profile is the solution for customers requiring complete redundancy for all components (switches, routers, firewalls, and HQ connections).

Solution Requirements

The solution requirements for the single-tier profile are:

- IPv6 support on the operating system (OS) of the host machines in the branch
- IPv6/IPv4 dual-stack support on the Cisco ISR router
- MLD-snooping support on the LAN switch (required if using IPv6 multicast)
- IPv6 PIM on the Cisco ISR router (if using IPv6 multicast)
- Cisco IOS release and feature set that supports the Cisco Zone-Based Firewall
- Cisco IOS release and feature set that supports DMVPN

Tested Components

Table 1 lists the components that were used and tested in the single-tier profile.

Table 1 Single Tier Profile Components

Role	Hardware	Software
Router/firewall	Integrated Services router—2900 Series and 3900 Series	IOS 15.1(3)T
Switch	EtherSwitch Service Module—NME-16ES-1G-P	12.2(55)SE
Host devices	Various client devices	Microsoft Windows 7

Multi-Tier Profile

The multi-tier profile extends the single-tier profile by separating not only routing and switching, but also security. There is also a dedicated Access Tier that provides more scalability for sites with a larger number of hosts.

Figure 2 shows a high-level view of the multi-tier profile.

Figure 2 Multi-Tier Profile

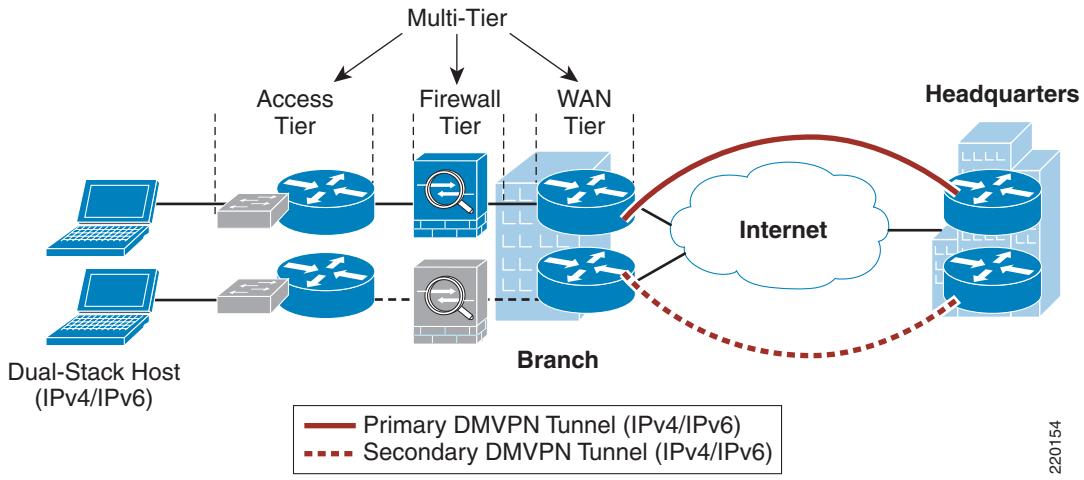


Figure 2 shows how the tiers or roles are distributed. Several changes are evident with the multi-tier vs. the single-tier:

- WAN tier—Connections to HQ are over DMVPN. Again, DMVPN is just one of many options for providing transport of IPv4 and IPv6 between the branch and the HQ WAN aggregation routers. MPLS, Frame Relay, and other methods are supported.
- Firewall tier—Firewall services are now separated from the WAN routers. This tier is optional as you may consider your private WAN/DMVPN connection to be trusted and therefore do not need comprehensive ACL or firewall services. The Cisco ASA 5500 series is shown here and is providing stateful firewall services for both IPv4 and IPv6. The second ASA (shown in Figure 2 as subdued grey) is in stateful failover mode. Both active/active and active/standby are supported on the Cisco ASA 5500.
- Access tier—The access tier is used for host network access and VLAN termination. The access tier is like a campus distribution and access layer.

Solution Requirements

The solution requirements for the multi-tier profile are:

- IPv6 support on the OS of the host machines in the branch
- IPv6/IPv4 dual-stack support on the Cisco ISR routers
- Cisco IOS release and feature set that supports DMVPN
- MLD-snooping support on the LAN switches (required if using IPv6 multicast)
- IPv6 PIM support on Cisco ISR routers (if using IPv6 multicast)
- Cisco ASA software version 8.3 and later

Tested Components

Table 2 lists the components that were used and tested in the multi-tier profile.

Table 2 Multi-Tier Profile Components

Role	Hardware	Software
Router	Integrated Services router—2900 Series and 3900 Series	IOS 15.1(3)T
Switch	EtherSwitch Service Module—NME-16ES-1G-P Catalyst 3750-E Series	12.2(55)SE
Firewall	Cisco ASA 5500 Series	8.3(1)
Host devices	Various client devices	Microsoft Windows 7

General Considerations

There are some general considerations that apply to all of the deployment profiles described in the implementation sections of this document. This section describes the general considerations to take into account when deploying IPv6 in a branch network, regardless of the deployment profile being used. If a specific consideration should be understood, then the specific profile is called out, along with the consideration for that profile. Also, the specific configurations for any profile-specific considerations can be found in that profile's implementation section.

All branch IPv6 profiles described in this document leverage the existing Cisco branch network design best practices as the foundation for all aspects of the deployment. The IPv6 components of the profiles are deployed in the same way as IPv4 whenever possible. When the same or similar features are not available for IPv6 as for IPv4, alternatives are used. In some cases, no alternatives are available and a reference for where to track feature support is given.

It is critical to understand the Cisco branch best practices recommendations before deploying the IPv6 in the branch profiles described in this document. The Cisco branch design best practice documents can be found under the "Branch Office" and "WAN" sections at: http://www.cisco.com/en/US/netsol/ns816/networking_solutions_program_home.html.

Addressing

As previously mentioned, this document is not an introductory document and does not describe the basics of IPv6 addressing. However, it is important to describe a few addressing considerations for network devices.

There are several combinations of addressing for various link/interface types. In many cases, a customer will use a "64 everywhere" model where a /64 is used on links that have hosts as well as on point-to-point (P2P) links. It is also fine to use /64 on links with hosts and a /126 or /127 on P2P links. However, there are certain precautions that needed to be taken when using /127 on links. These precautions are documented in both RFC 3627 and a draft (at the time of writing this paper the draft was named: "Using 127-bit IPv6 Prefixes on Inter-Router Links") draft-kohno-ipv6-prefixlen-p2p. In all cases the use of /128 on Loopback interfaces is the recommendation.

The dynamic assignment of host IPv6 addresses can either be done by DHCPv6 or via RA-based (Router Advertisement) assignment from the VLAN or routed interface.

Physical Connectivity

Considerations for physical connectivity with IPv6 are the same as with IPv4 plus three additional elements:

- One important factor for deployment of any new technology, protocol, or application is to ensure that there is a sufficient amount of bandwidth for both existing and new traffic. This issue is especially true with the branch because in many cases the connections to the WAN are low-speed links and the reliance on QoS to solve bandwidth problems goes only so far. Bandwidth requirements for IPv6 are outside the scope of this document because there are many variables to account for and should therefore be considered in a case-by-case analysis.
- Understanding how IPv6 deals with Maximum Transmission Unit (MTU) on a link. This document is not meant to be an introductory document for basic IPv6 protocol operation or specifications, so Cisco recommends that you refer to the following links for more information on MTU and fragmentation in IPv6. A good starting point for understanding MTU and Path MTU Discovery (PMTUD) for IPv6 is with RFC 2460 and RFC 1981 at: http://www.ietf.org/rfc/rfc2460.txt, http://www.ietf.org/rfc/rfc1981.txt.

  Another aspect of MTU relates to the use of IPSec VPNs with GRE, manual tunnels, or DMVPN. When IPSec is used with these tunnels, it is important to account for the adjustment of the MTU value on the routers to ensure that the router is not forced to perform fragmentation of the IPv4 traffic due to the IPSec header and the additional tunnel overhead. More information on this can be found in any of the IPSec design guides at: http://www.cisco.com/en/US/tech/tk583/tk372/tech_design_guides_list.html.
- IPv6 over Wireless LANs—IPv6 should operate correctly over WLAN Access Points in much the same way as IPv6 operates over Layer 2 switches. However, there are considerations to IPv6 with WLAN environments such as managing WLAN devices (APs and controllers) via IPv6 and controlling IPv6 traffic via AP or controller-based QoS, VLANs and ACLs. IPv6 must be supported on the AP and/or controller devices in order to take advantage of these more intelligent services on the WLAN devices.

It is important to point out that Cisco supports the use of IPv6-enabled hosts that are directly attached to Cisco IP phone ports. These IP phone ports are switch ports and operate in much the same way as plugging the host directly into a Catalyst Layer 2 switch.

In addition to the previous considerations, Cisco recommends that a thorough analysis of the existing traffic profiles, memory, and CPU use on both the hosts and network equipment and also the Service Level Agreement (SLA) language be completed prior to implementing any of the IPv6 models described in this document.

VLANs

VLAN considerations for IPv6 are the same as for IPv4. When dual-stack configurations are used then both IPv4 and IPv6 traverse the same VLAN. The use of Private VLANs is not included in any of the deployment profiles described in this document and it was not tested.

The use of IPv6 on data VLANs that are trunked along with voice VLANs (behind IP phones) is fully supported. For the current VLAN design recommendations, refer to the Cisco branch-LAN design best practice documents at: http://www.cisco.com/en/US/netsol/ns816/networking_solutions_program_home.html.

Routing

Choosing an IGP to run in the campus network is based on a variety of factors—platform capabilities, IT staff expertise, and the size of network are just a few. In this document the IGP for both IPv4 and IPv6 is EIGRP. OSPFv2 for IPv4 and OSPFv3 for IPv6 can also be used.

EIGRP has been configured to provide authentication for both IPv4 and IPv6 adjacencies and updates.

High Availability

There are many aspects of High-Availability (HA) that are not applicable to or are outside the scope of this document. Many of the HA requirements and recommendations are met by leveraging the existing Cisco branch design best practices. The primary HA components described in this document are:

- Redundant WAN connections—In the single-tier profile, the primary WAN connection is an Ethernet hand-off from the ISP and the secondary is a T1/E1 connection to another ISP. However, both of these links come from only one ISR router (branch router). In the multi-tier profile, each of the two branch ISR routers has a connection to the ISP and, along with DMVPN, redundancy is achieved between the branch and HQ sites.
- Redundant routing and forwarding paths—This is accomplished by leveraging EIGRP for IPv4 and IPv6. In some cases, Equal Cost Multi-Path (ECMP) is used and in other cases, one path is preferred over another, but the secondary path is available for redundancy.
- High-availability of the first-hop gateways—This level of HA applies only to the multi-tier profile (single-tier has only one router). HSRPv2 for IPv4 and IPv6 is used to provide first-hop gateway redundancy in the multi-tier. Cisco also supports GLBP for IPv4 and IPv6.

QoS

Cisco recommends that QoS policies be implemented application- or service-dependent instead of protocol (IPv4 or IPv6)-dependent. Basically, if the existing QoS policy has specific classification, policing, and queuing for an application, then that policy should treat the IPv4 and IPv6 traffic for that application equally.

The key consideration as far as Modular QoS CLI (MQC) is concerned is the removal of the **ip** keyword in the QoS **match** and **set** statements when IPv6 QoS is required. Modification in the QoS syntax to support IPv6 and IPv4 allows for new configuration criteria (see Table 3).

Table 3 Qos Syntax Modifications

IPv4-Only QoS Syntax	IPv4/IPv6 QoS Syntax
match ip dscp	**match dscp**
match ip precedence	**match precedence**
set ip dscp	**set dscp**
set ip precedence	**set precedence**

There are QoS features that work for both IPv6 and IPv4 and require no modification to the CLI (such as WRED, policing, and WRR).

The implementation section for each profile does not go into great detail on QoS configuration as far as the definition of classes for certain applications, the associated mapping of DSCP values, and the bandwidth and queuing recommendations.

Cisco has an extensive collection of QoS recommendations for the branch and you are encouraged to seek guidance from the CCO documentation and also the Cisco Press book, *End-to-End QoS Network Design*.

Security

Many of the common threats and attacks on existing IPv4 campus networks also apply to IPv6. Unauthorized access, spoofing, routing attacks, viruses, worms, DoS, and man-in-the-middle attacks are just a few that plague both IPv4 and IPv6.

There are many new threats with IPv6 that do not exist with IPv4 or they operate differently than IPv4. There are inherent differences in how IPv6 handles neighbor and router advertisement and discovery, headers, and even fragmentation. Based on all of these variables and possibilities, IPv6 security is a very involved topic in general and detailed security recommendations and configurations are outside the scope of this document. There are numerous efforts both within Cisco and the industry to identify, understand, and resolve IPv6 security threats. This document points out some possible areas to address within the branch and gives basic examples of how to provide protection of IPv6 dual-stack and tunneled traffic.

Note The examples given in this document are not meant to be recommendations or guidelines, but rather points to stimulate a careful analysis of existent security policies and their extension to cover IPv6 in the branch.

General security considerations for network device protection that apply to both branch profiles are:

- Controlling management access to the branch routers and switches:
  - All of the branch routers and switches for each profile have configurations in place to provide management access protection to the devices. All routers have loopback interfaces configured for management and routing purposes along with access control to those interfaces.

```
interface Loopback0
 ipv6 address 2001:DB8:CAFE:1000::BAD1:A001/128
 no ipv6 redirects
```

    To more tightly restrict access to a particular switch/router via IPv6, an ACL is used to permit access to the management interface (line vty) by way of the loopback interface. The permitted source network is from the enterprise IPv6 prefix. To make ACL generation more scalable for a wide range of network devices, the ACL definition can permit the entire enterprise prefix as the primary method for controlling management access to the device instead of filtering to a specific interface on the device. The IPv6 prefix used in this enterprise site (for example only) is 2001:db8:cafe::/48.

```
ipv6 access-list MGMT-IN
 remark Permit MGMT only to Loopback0
 permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:1000::BAD1:A001
 deny ipv6 any any log-input
!
line vty 0 4
 session-timeout 3
 access-class MGMT-IN-v4 in
 password 7 08334D400E1C17
```

```
ipv6 access-class MGMT-IN in#Apply IPv6 ACL to restrict access
logging synchronous
login local
exec prompt timestamp
transport input ssh          #Accept access to VTY via SSH
```

  - Other protocol and service protection such as FTP, NTP, and SSH version 2 should be reviewed.

- Control Plane Policing (CoPP)—CoPP protects the router by preventing DoS or unnecessary traffic from negatively impacting CPU resources. Priority is given to important control plane/management traffic. The configuration of CoPP is based on a wide variety of factors and no single deployment recommendation can be made as the specifics of the policy are determined on a case-by-case basis.

  More information on CoPP can be found at: http://www.cisco.com/en/US/docs/ios/sec_control_plane/configuration/guide/15_1/cps_15_1_book.html.

- First-Hop Security—Features such as IPv6 Port-based ACL (PACL), Router Advertisement (RA) Guard, Neighbor Discovery (ND) Inspection, and SEcure Neighbor Discovery (SEND) are all mechanisms that can be deployed to protect the data and control plane of the first hop devices and attached hosts. The following shows an example of IPv6 PACL:

```
ipv6 access-list HOST_PACL
 remark Deny Rogue DHCP
 deny udp any eq 547 any eq 546
 remark Deny RA From Client
 deny icmp any any router-advertisement
 permit ipv6 any any
!
interface GigabitEthernet1/0/6
 ipv6 traffic-filter HOST_PACL in
```

  The following shows an example of RA Guard:

```
interface GigabitEthernet1/0/6
 ipv6 nd raguard
```

  You need to verify the Cisco platform and code version that supports these and other first hop security features. More information can be found at: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security_ps10592_TSD_Products_Configuration_Guide_Chapter.html.

- IPv6 Stateful Firewall Services—Firewalls provide a stateful security inspection for IPv6 traffic entering or leaving a branch network. Stateful firewall services can be deployed using the Cisco ASA and IOS Zone-Based Firewall.

- Disabling unused services—Many services, such as HTTP server, are supported for IPv4 and IPv6. Enabling or disabling these services generally applies to both protocols.

- Ensure IPv6 source routing is disabled (it is disabled by default in IOS): `no ipv6 source-route`

- Increase IPv6 RA preference to “high” versus “medium”: `ipv6 nd router-preference High`

IPv6 ACL and firewall configuration details can be found at: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-sec_trfltr_fw_ps10592_TSD_Products_Configuration_Guide_Chapter.html.

Multicast

IPv6 multicast is an important service for any enterprise network design. One of the most important factors to IPv6 multicast deployment is to ensure that host/group control is handled properly in the branch LAN. Multicast Listener Discovery (MLD) in IPv6 is the equivalent to Internet Group Management Protocol (IGMP) in IPv4. Both are used for host multicast group membership control. MLD-snooping is the ability to control the distribution of multicast traffic only to the ports that have listeners. Without it, multicast traffic meant for only a single receiver (or group of receivers) would be flooded to all ports on the branch LAN switch belonging to the same VLAN. In the branch LAN it is important that the switches support MLD-snooping for MLD version 1 and/or version 2.

Today, Cisco IOS supports the following PIM implementations: PIM-SM, PIM-BSR, PIM-SSM, Bidirectional PIM, Embedded-RP, and Multiprotocol BGP for the IPv6 Multicast Address Family.

In this document, IPv6 multicast-enabled applications are supported in both branch profiles. The multicast-enabled applications tested in this design are: Windows Media Services and VLC (VideoLAN Media client) using PIM-SSM. The multicast sources are running on Microsoft Windows Server 2008 servers located in the HQ data center.

For more information, refer to the following:

- Cisco IPv6 Multicast: http://www.cisco.com/en/US/technologies/tk648/tk828/tk363/technologies_white_paper0900aecd8014d6dd.html.
- Cisco IOS IPv6 Multicast Configuration: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-multicast_ps10591_TSD_Products_Configuration_Guide_Chapter.html.

Management

Management for IPv6 is almost the same as for IPv4 with the exception of a specific Management Information Base (MIBs) used for IPv6. Many of the traditional management tools used today also support IPv6. In this document the only considerations for management of the branch network are related to basic control of management services (Telnet, SSH, FTP, and SNMP) and the feature IP Service Level Agreement (SLA). All of the IPv6-enabled devices in the two branch profiles described are manageable over IPv6.

The configuration and support of telnet, SSH, and FTP are the same as with IPv4. Commands such as **ip ftp source-interface** equally apply to IPv4 and IPv6. There is no special consideration to make other than ensuring the platform and code version you are running support these features with IPv6.

The deployment of SNMP for IPv6 is the same as with IPv4. In the branch profiles described in this paper, SNMPv3 (AuthNoPriv) is used to provide polling capabilities for the Cisco NMS servers located in the HQ data center. Here is an example of the SNMPv3 configuration used in the branch routers in this document:

```
snmp-server contact John Doe - ipv6rocks@cisco.com
snmp-server group IPv6-ADMIN v3 auth write v1default
snmp-server user jdoe IPv6-ADMIN v3 auth md5 cisco1234
```

If information needs to be sent to a Cisco NMS server, then an SNMP host can be defined. The host can be defined to send SNMP information over IPv4 and/or IPv6:

```
snmp-server host 2001:DB8:CAFE:11:2E0:81FF:FE2C:9332 version 3 auth jdoe
```

When using the IP SLA feature for IPv6, you can monitor the service levels of IPv6 applications in services. Various operations can be monitored over ICMP, TCP, UDP, and UDP jitter. In this document the routers are configured for IP SLA over IPv6 with object tracking. The following is a basic example configuration that can be used for monitoring an IPv6 host (2001:db8:cafe:1251:bad1:a002):

```
track 150 ip sla 150
…
ip sla 150
 icmp-echo 2001:DB8:CAFE:1251::BAD1:A002 source-ip 2001:DB8:CAFE:1250::ACE1:F000
ip sla schedule 150 life forever start-time now
```

Another area of management that you must thoroughly research is that of address management. Anyone who analyzed IPv6 even at an elementary level understands the size and potential complexity of deploying and managing the IPv6 address space. The process of assigning large hexadecimal addresses to many network devices should, at some point, be automated or at least made more user-friendly than it is today. Cisco is in the forefront of several efforts underway within the industry to provide recommendations and solutions to the address management issues.

Today, one way to help with the deployment of address prefixes on a Cisco ISR is through the use of the general prefix feature. The general prefix feature allows the customer to define a prefix or prefixes in the global configuration of the router with a user-friendly name. That user-friendly name can be used on a per-interface basis to replace the usual IPv6 prefix definition on the interface. The following is an example of how to use the general prefix feature:

Define the general prefix:

```
2900-br1-1(config)# ipv6 general-prefix ESE-BR-1 2001:DB8:CAFE::/48

Configure the general prefix named "ESE-BR-1" on a per-interface basis:
2900-br1-1(config-if)# ipv6 address ESE-BR-1 ::1100:0:0:BAD1:A001/64
```

Verify that the general prefix was correctly assigned to the interface:

```
2900-br1-1# show ipv6 interface g1/0.100
GigabitEthernet1/0.100 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::217:94FF:FE90:2829
  No Virtual link-local address(es):
  Description: DATA VLAN for Computers
  Global unicast address(es):
    2001:DB8:CAFE:1100::BAD1:A001, subnet is 2001:DB8:CAFE:1100::/64
```

More information on the general prefix feature can be found at the Cisco IOS IPv6 documentation page at:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-addrg_bsc_con_ps10591_TSD_Products_Configuration_Guide_Chapter.html#wp1132473.

Cisco supports the management of IPv6-enabled network devices via a variety of Network Management Products to include DNS, DHCPv6, device management and monitoring, and also network management, troubleshooting, and reporting. More information on the various Cisco Network Management solutions can be found at: http://www.cisco.com/en/US/products/sw/netmgtsw/index.html.

Scalability and Performance

This document is not meant to analyze scalability and performance information for the various platforms tested. The coverage of scale and performance is more focused on general considerations when planning and deploying IPv6 in the branch versus a platform-specific view.

In general, you should understand the link, memory, and CPU use of the existing branch network devices. If any of these aspects are already stressed, then adding IPv6 or any new technology, feature, or protocol into the design is a recipe for disaster.

Scalability and performance considerations for branch network devices include:

- It is common to see in IPv6 implementations a change in traffic utilization ratios on the branch network links. As IPv6 is deployed, IPv4 traffic utilization is very often reduced as users leverage IPv6 as the transport for applications that were historically IPv4-only. There is often a slight increase in overall network utilization which usually derives from control traffic for routing and also tunnel overhead.
- ARP/Neighbor cache—One of the primary scalability considerations is that of running two protocols on the router. The branch LAN router has to track both IPv4 and IPv6 neighbor information. Similar to ARP in IPv4, neighbor cache exists for IPv6. The primary consideration here is that with IPv4 there is usually a 1-to-1 mapping of IPv4 address-to-MAC address, but with IPv6 the host can have several mappings for multiple IPv6 addresses, such as link-local, unique-local, and multiple Global addresses, to a single MAC address in the routers neighbor cache. The following is an example of ARP and neighbor cache entries on a Cisco ISR located in the branch for a host with the MAC address of 0014.c2e1.e679.

  ARP entry for the host in the branch:

  ```
  Internet  10.124.2.4           2   0014.c2e1.e679  ARPA   FastEthernet0/0.100
  ```

  IPv6 Neighbor Cache entry for the host in the branch:

  ```
  IPv6 Address Age Link-layer Addr State Interface
  2001:DB8:CAFE:2100:DDD6:5CC5:3178:F038      0 0014.c2e1.e679  REACH Fa0/0.100
  FE80::D48A:B1B6:8861:812C                   0 0014.c2e1.e679  DELAY Fa0/0.100
  ```

  The IPv6 neighbor cache shows that there are two entries listed for the host. The first address is a global IPv6 address (optional) that is assigned by DHCP for IPv6 (could also be statically defined or assigned via stateless autoconfiguration) and the second address is the link-local address (mandatory) generated by the host. The number of entries can decrease to a minimum of one (link-local address) to a multitude of entries for a single host depending on the address types used on the host.

  It is important to understand the neighbor table capabilities of the branch network devices being used to ensure that the tables are not being filled during regular network operation.

  Another consideration is with IPv6 multicast. As previously mentioned, it is important to ensure that MLD-Snooping is supported in the branch LAN switch when IPv6 multicast is used to ensure that IPv6 multicast frames at Layer 2 are not flooded to all of the ports.
- Routing/forwarding—It is very important to understand the routing and forwarding capabilities of the branch routers. If the existing branch router is already running at high CPU and memory utilization rates for the handling of IPv4 routing tables and updates, then it is a bad idea to add IPv6 to the existing router.
- ACL processing—It is imperative that the deployment of ACLs be carefully planned. IPv6 ACLs in the branch routers are used for QoS (classification and marking of ingress packets from the access layer), for security (controlling DoS, snooping and unauthorized access for ingress traffic in the access layer), and for a combination of QoS and security to protect the control plane of the router from attack. The router can also provide Cisco IOS firewalling services, IDS/IPS, and voice services for IPv4 and new services for IPv6. Advanced services that are added to the branch router should support both IPv4 and IPv6. Performance will be impacted with all of these added services plus the newly-enabled IPv6 configuration.

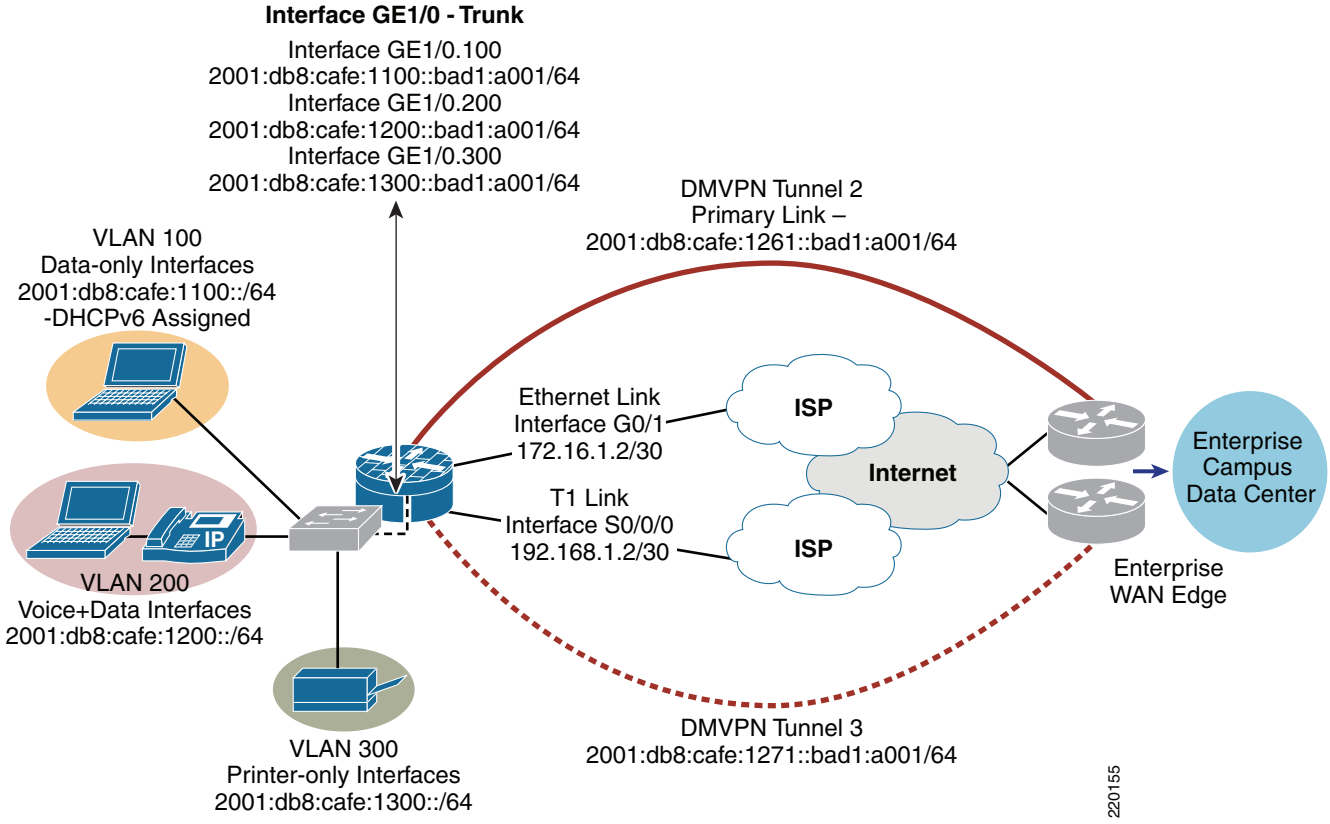
Single-Tier Implementation

This section focuses on the configuration of a single-tier deployment profile. The configurations are broken down into specific areas, such as WAN and LAN connectivity, DMVPN, routing, and security. IPv4 configurations are shown when the deployment of IPv6 is dependent upon IPv4 for access, such as with DMVPN.

Network Topology

Figure 3 serves as a reference for all of the configurations for the single-tier profile. Figure 3 shows the interface and addressing layout for the branch router and integrated switch. IPv4 addressing is shown only when IPv4 is required for connectivity by IPv6 (DMVPN).

Figure 3 Single-Tier Profile—Interface/Addressing Layout



A single router (2900-br1-1) is used with an integrated switch (sw-br1-1) to provide WAN and LAN connectivity for the three VLANs in the branch.

- WAN—The WAN consists of two connections—an Ethernet hand-off is used as the primary link and a T1/E1 is used as the backup link. The tunnels used for connectivity over the Internet to the HQ site are:
  - Tunnel 2 is used as the primary DMVPN tunnel for both IPv4 and IPv6 traffic and terminates on one of the HQ WAN aggregation router.

  - Tunnel 3 is used as the backup DMVPN tunnel for both IPv4 and IPv6 traffic and terminates on a different HQ WAN aggregation router.

  All of the tunnels use IPv4 IPSec with DMVPN for tunnel protection.

- LAN—The LAN portion of the single-tier uses an EtherSwitch Service Module. There are three VLANs in use in the single-tier profile:
  - VLAN 100—Used as the PC data VLAN. IPv4 addressing is provided by a local DHCP pool on the router. IPv6 addressing is also provided by a local DHCP pool for IPv6.
  - VLAN 200—Used as the voice VLAN. IPv4 addressing is provided by a local DHCP pool on the router to include any voice-specific options (TFTP server). IPv6 addressing is provided by a local DHCP pool on the router.
  - VLAN 300—Used as the printer VLAN. IPv4 addressing is provided by a local DHCP pool on the router. The Hewlett Packard Jet Direct cards located in the branch automatically receives an IPv6 address from the router interface via stateless autoconfiguration.

WAN Configuration

The WAN configurations are not specific to IPv6, but are used to provide the underlying transport for the DMVPN tunnels between the branch and HQ routers.

2900-br1-1

```
interface GigabitEthernet0/1
 description Ethernet Handoff to ISP (PRIMARY)
 ip address 172.16.1.2 255.255.255.252
!
interface Serial0/0/0
 description T1 Backup Link (Secondary)
 ip address 192.168.1.2 255.255.255.252
```

LAN Configuration

The LAN IPv6 configurations for 2900-br1-1 and sw-br1-1 follow. The configurations show the internal switch links between the router and the EtherSwitch module and also the interface and VLAN configurations on the switch itself.

There are many ways to provide address assignment to hosts to include DHCP in local pools (shown below), DHCP at a central site with the local router/switch acting as a "relay", SLAAC/RA-based assignment, or static.

Note On the Cisco Catalyst 3750, 3560, and EtherSwitch platforms it is required to enable the correct Switch Database Management (SDM) template to allow the TCAM to be used for different purposes. The sw-br1-1 switch has been configured (reload required) with the “dual-ipv4-and-ipv6” SDM template using the **sdm prefer dual-ipv4-and-ipv6 default** command.

For more information about the SDM **prefer** command and associated templates, refer to: http://www.cisco.com/en/US/docs/switches/lan/catalyst3750e_3560e/software/release/12.2_55_se/configuration/guide/swsdm.html.

2900-br1-1

```
ipv6 unicast-routing                                  #Globally enable IPv6 Unicast Routing
ipv6 cef                                              #Globally enable IPv6 CEF
!
ipv6 dhcp pool DATA_CLIENTS                          #DHCP for IPv6 pool name
 address prefix 2001:DB8:CAFE:1100::/64              #DHCP address prefix
 dns-server 2001:DB8:CAFE:10:20D:9DFF:FE93:B25D      #Primary IPv6 DNS server at HQ
 dns-server 2001:DB8:CAFE:10:51A1:5B1:4A85:B3DA      #Secondary IPv6 DNS server at HQ
 domain-name cisco.com
#DNS domain name passed to client
!
ipv6 dhcp pool IP_PHONES                             #DHCP pool for IP Phones (options below)
 address prefix 2001:DB8:CAFE:1200::/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
 vendor-specific 9                                   #Vendor ID (Cisco is "9")
  suboption 1 address 2001:DB8:CAFE:10::11AA         #TFTP server address (suboption 1)
!
interface GigabitEthernet1/0
 description to INTERNAL SW-BR1-1
 ip address 1.1.1.1 255.255.255.0
!
interface GigabitEthernet1/0.100
 description DATA VLAN for Computers
 encapsulation dot1Q 100
 ipv6 address 2001:DB8:CAFE:1100::BAD1:A001/64       #Define the router IPv6 address
                                                      #for VLAN100.
 ipv6 nd managed-config-flag                         #Set flag in RA to instruct host
                                                      #to use DHCPv6
 ipv6 dhcp server DATA_CLIENTS                       #Enables DHCP for IPv6 on this interface
 ipv6 nd router-preference High                      #Make RAs from this interface the highest

!
interface GigabitEthernet1/0.200
 description to Voice VLAN for IP Phones
 encapsulation dot1Q 200
 ipv6 address 2001:DB8:CAFE:1200::BAD1:A001/64
 ipv6 nd managed-config-flag
 ipv6 dhcp server IP_PHONES
 ipv6 nd router-preference High
!
interface GigabitEthernet1/0.300
 description to Printer VLAN
 encapsulation dot1Q 300
 ipv6 address 2001:DB8:CAFE:1300::BAD1:A001/64
 ipv6 nd router-preference High
!
```

sw-br1-1

```
vtp domain ce_branch
vtp mode transparent
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 100
 name DATA
```

```
!
vlan 200
 name VOICE
!
vlan 300
 name PRINTERS
!
interface GigabitEthernet1/0/2
 description TRUNK to 2900-br1-1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,200,300
 switchport mode trunk
!
interface FastEthernet1/0/3
 description PHONE + PC
 switchport access vlan 100
 switchport mode access
 switchport voice vlan 200
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface Vlan100
 description VLAN100 for PCs and Switch management
 ip address 10.124.1.126 255.255.255.128
 ipv6 address 2001:DB8:CAFE:1100::BAD2:F126/64
```

More information regarding IPv6 with DHCP and how to properly configure the network to support IPv6-enabled IP phones can be found at: http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/ipv6/netstruc.html#wp1052756.

Also, there may be times when RA messages are sent to the voice VLAN from the router and "bleed" over to the data VLAN and impact hosts attached to the data port of an IP phone. This may happen if the host attached to the data port of the IP phone has 802.1q tagging intelligence and processes the voice VLAN tag. Normally, the host should drop any packet with a tag set (i.e., from the voice VLAN). You can resolve this issue on the network side by one of two methods:

- Set the IP phone's PC Voice VLAN Access setting to disabled.
- Set the prefix lifetime of RAs from the router on the voice VLAN to a much shorter lifetime than the RAs for the data VLAN. Hosts in the data VLAN will use RFC3484 (default address selection) and pick the prefix with the longest lifetime.

DMVPN

The single-tier profile uses DMVPN for both IPv4 and IPv6. The design and configuration is basically just a dual stack deployment where both protocols are enabled on the DMVPN tunnel interface.

Both sides of the tunnel (branch and HQ) have statically-defined public IPv4 addresses that are used for tunnel sources. Only one of the two tunnels is shown in the configuration. The second tunnel has a nearly identical configuration as the first, with the exception of a tuned IGP that lowers the priority of the secondary tunnel and that the tunnel is sourced to the serial interface for the T1/E1 link.

Refer to the Cisco IOS IPv6 DMVPN for more information regarding DMVPN: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-dmvpn_ps10591_TSD_Products_Configuration_Guide_Chapter.html.

2900-br1-1

```
crypto isakmp policy 1                              #Create ISAKMP policy
 encr aes 256                                          #Encryption method
```

```
 authentication pre-share                              #Pre-shared keys (passwords) used
 group 2
crypto isakmp key CISCO address 0.0.0.0 0.0.0.0      #Pre-shared key of "CISCO" used with
any IPv4 peer
crypto isakmp keepalive 10                        #Dead Peer Detection (DPD) enabled
!
crypto ipsec transform-set SPOKETrans esp-aes 256 esp-sha-hmac
crypto ipsec transform-set SPOKE-BUTrans esp-aes 256 esp-sha-hmac

!
crypto ipsec profile DMVPNProf
 set transform-set SPOKETrans
crypto ipsec profile BACKUPProf
 set transform-set SPOKEBUTran

interface Tunnel2                #If PIMv6 is used, tunnel 0 and 1 are used by default
                                                    #It is recommended to start at "2"
 description DMVPN to HQ Head-end 1
 ipv6 address 2001:DB8:CAFE:1261::BAD1:A001/64   #Only IPv6 portion of interface is shown
 ipv6 mtu 1416                                       #Lower MTU to account for tunnel
                                                     #and IPSec overhead - Neither are
                                                     #detected when host performs
                                                     #PMTUD for IPv6
 ipv6 nhrp authentication SECRET
 ipv6 nhrp map multicast dynamic
 ipv6 nhrp map multicast 172.16.2.3
 ipv6 nhrp map 2001:DB8:CAFE:1261::ACE1:F000/128 172.16.2.3   #Static address mapping
                                                              #v6-to-NBMA
 ipv6 nhrp network-id 70809
 ipv6 nhrp nhs 2001:DB8:CAFE:1261::ACE1:F000     #NHRP Server address is HQ router
 ipv6 nhrp holdtime 600
 ipv6 nhrp shortcut
 tunnel source 172.16.1.2
 tunnel mode gre multipoint
 tunnel key 123
 tunnel protection ipsec profile DMVPNProf
```

HQ Router

```
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key CISCO address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
crypto ipsec transform-set HUBTrans esp-aes 256 esp-sha-hmac
!
crypto ipsec profile DMVPNProf
 set transform-set HUBTrans

interface Tunnel2
 description DMVPN to Spoke
 ipv6 address 2001:DB8:CAFE:1261::ACE1:F000/64
 ipv6 mtu 1416
 ipv6 nhrp authentication SECRET
 ipv6 nhrp map multicast dynamic
 ipv6 nhrp network-id 70809
 ipv6 nhrp holdtime 600
 ipv6 nhrp redirect
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel key 123
```

```
 tunnel protection ipsec profile DMVPNProf
```

Routing

The IPv6 routing configuration for the single-tier profile is straightforward. There is a default route for IPv4 that points to ISP. EIGRP for IPv4 and IPv6 is used within the DMVPN tunnels and also the LAN interfaces to provide routing information to/from the HQ site and within the branch. The branch router is configured as an EIGRP stub router.

For more information on configuring EIGRP for IPv6, refer to the Cisco IOS IPv6 EIGRP routing configuration page at: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-eigrp_ps10591_TSD_Products_.onfiguration_Guide_Chapter.html.

2900-br1-1

```
ipv6 unicast-routing
!
key chain CISCO                                    #Enable EIGRP Authentication key chain
 key 1
  key-string 7 111B180B101719
!
interface Loopback0
 ipv6 address 2001:DB8:CAFE:1000::BAD1:A001/128
 ipv6 eigrp 1

interface Tunnel2
 ipv6 eigrp 1                                             #Enable EIGRP for IPv6 on tunnel
 ipv6 hold-time eigrp 1 35                          #Adjust the hold time for EIGRP
 ipv6 authentication mode eigrp 1 md5                     #Authentication type of MD5
 ipv6 authentication key-chain eigrp 1 CISCO              #Enables authentication of EIGRP
 no ipv6 split-horizon eigrp 1    #Disable EIGRP split-horizon for this multi-point intf.
!
interface GigabitEthernet1/0.100
 description DATA VLAN for Computers
 encapsulation dot1Q 100
 ipv6 eigrp 1
!
interface GigabitEthernet1/0.200
 description to Voice VLAN for IP Phones
 encapsulation dot1Q 200
 ipv6 eigrp 1
!
interface GigabitEthernet1/0.300
 description to Printer VLAN
 encapsulation dot1Q 300
 ipv6 eigrp 1
!
ipv6 router eigrp 1                                   #Router configuration mode - process 1
 router-id 10.124.100.1
 stub connected summary                               #This branch is a stub
 no shutdown
 passive-interface GigabitEthernet1/0.100
 passive-interface GigabitEthernet1/0.200
 passive-interface GigabitEthernet1/0.300
 passive-interface Loopback0
!
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1      #Primary IPv4 static route used for WAN
ip route 0.0.0.0 0.0.0.0 Serial0/0/0 200                 #Backup IPv4 static route

sw-1-br1
```

```
ipv6 route ::/0 Vlan100 FE80::217:94FF:FE90:2829        #Default route out VLAN100 to the
                                                        #link-local address of the 2900
VLAN100 interface
```

Security

The security configurations for IPv6 in the single-tier profile are very similar to the IPv4 configurations. In an "untrusted model" where the private WAN between the branch and the HQ site is not considered to be "trusted", additional security measures can be deployed. This is rare as most deployments consider a private WAN or VPN-based deployment to be trusted and therefore ACLs or a dedicated firewall at the branch site are unnecessary (except for protecting the site on the Internet-facing port).

The focus of the security configuration for IPv6 is to protect the infrastructure (router and switch) and optionally offer an additional line of defense for the branch site via either ACLs or an IPv6 stateful firewall. In a "trusted" model, the security is much less in-depth at the branch site as the central security policies at the HQ are considered to be good enough and no additional protection such as stateful firewalls are needed at each branch site.

The profiles described in this document are protected by a comprehensive security policy and design at the HQ site. However, the single-tier does use the Internet as a means of WAN connectivity and it is important to provide basic security at the local branch router in case of an Internet-based attack via the branch ISP links.

Note As previously mentioned, in this document there are no IPv6-enabled links directly to the ISP from the branch. All IPv6 connectivity is provided by the HQ site via the IPv4 IPSec tunnels. Future branch and WAN documents will describe native IPv6 IPSec connectivity in environments where the ISP offers IPv6 access services to the branch.

ACL policies can be applied to various interfaces in the single-tier profile. The ACL placement is summarized here:

- The Ethernet hand-off link and T1 link use IPv4-based ACLs to permit packets used to establish the IPSec VPN tunnels between the enterprise HQ and the branch router and ICMP packets used for troubleshooting.
- The DMVPN tunnels can have ACLs that allow traffic such as routing, PIM, access to the router's loopback interface, and various other permits. If you presume that your DMVPN tunnels between the spoke and hub are "trusted", then these ACLs or firewall configurations are unnecessary. The policies shown in this document are for example only and not meant to be a best practice recommendation.
- Branch LAN interfaces can have ingress ACLs to permit traffic from the VLAN interfaces based on source prefix or even specific applications (this is optional). The LAN ACL configuration shown is the same one discussed earlier in the document and is for providing basic PACL-based filtering to protect against rogue DHCP and rogue RAs coming from the hosts in the branch.
- Control access to the management plane of the branch router and switch. Narrow the access type to SSH and also create an ACL to allow management of the router and switch only from IPv6 prefixes within the HQ. The ACL can be more tightly defined to allow access only for a specific management prefix.

As was stated earlier, if you consider the WAN links to the HQ site to be trusted, then ACLs and/or stateful firewall are not really needed. However, if you consider the WAN links to the HQ site to be untrusted, then ACLs or a stateful firewall (both shown below) may be used.

The following single-tier profile configurations are for the 2900-br1-1 router and sw-br1-1 switch.

2900-br1-1—PACL

```
ipv6 access-list HOST_PACL
 remark Deny Rogue DHCP
 deny udp any eq 547 any eq 546
 remark Deny RA From Client
 deny icmp any any router-advertisement
 permit ipv6 any any
!
interface GigabitEthernet1/0.100
 ipv6 traffic-filter HOST_PACL in
!
interface GigabitEthernet1/0.200
 ipv6 traffic-filter HOST_PACL in
!
interface GigabitEthernet1/0.300
 ipv6 traffic-filter HOST_PACL in
```

2900-br1-1—Infrastructure ACLs (only relevant IPv4 and IPv6 configurations are shown)

```
interface Tunnel2
 description DMVPN to HQ Head-end 1
 ipv6 traffic-filter INET-WAN-v6 in
!
interface GigabitEthernet0/1
 description Ethernet Handoff to ISP (PRIMARY)
 ip access-group WAN-link in
!
interface Serial0/0/0
 ip access-group WAN-link in
!
ip access-list extended WAN-link          #IPv4 ACL on ISP facing link - permit for DMVPN
 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 192.168.1.2 eq isakmp
 permit icmp any host 192.168.1.2
 permit icmp any host 192.168.1.2 packet-too-big
 permit icmp any host 192.168.1.2 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
!
ipv6 access-list INET-WAN-v6      #IPv6 ACL for internal WAN/Application traffic from HQ
 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 TUNNEL2
 permit icmp any host 2001:DB8:CAFE:1261::BAD1:A001
```

```
 remark PERMIT ALL ICMPv6 PACKETS TO TUNNEL3
 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
```

2900-br1-1 - Management

```
banner login ^C
Unauthorized access to this device and/or network is prohibited.
^C

ipv6 access-list MGMT-IN
 remark Permit MGMT only to Loopback0
 permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:1000::BAD1:A001
 deny ipv6 any any log-input

line vty 0 4
 ipv6 access-class MGMT-IN in
 transport input ssh
```

2900-br1-1 - Zone-Based Firewall

As an alternative to basic ACLs, you can use the Cisco IOS Zone-Based Firewall that supports both IPv4 and IPv6. There are many ways to configure the Cisco IOS Zone-Based IPv6 firewall inspection policies. A very basic example is given here just to show the syntax, but the policy shown is by no means a recommended configuration. The example basically shows the same inspection policy in both directions (in/out), but uses a combination of protocol matching and ACL-based matching. More information about the Zone-Based Firewall can be found at: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-sec_trfltr_fw_ps10591_TSD_Products_Configuration_Guide_Chapter.html#wp1078659 and http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml.

```
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
!
class-map type inspect match-any v6-class                  #Protocol matching outbound
 match protocol tcp
 match protocol udp
 match protocol icmp
 match protocol ftp
!
class-map type inspect match-all v6-map-in           #Protocol and ACL matching inbound
 match protocol icmp
 match access-group name v6-FWIN
```

```
!
class-map type inspect match-any EIGRP-v6                    #ACL match just for EIGRP
 match access-group name v6-route
!
policy-map type inspect FWIN                        #Inbound policy with class
maps/inspection applied
class type inspect v6-map-in
  inspect
class type inspect EIGRP-v6
  pass
class class-default
  drop
!
policy-map type inspect FWOUT                       #Outbound policy with class
maps/inspection applied
class type inspect v6-class
  inspect
class type inspect EIGRP-v6
  pass
class class-default
  drop
!
zone security inside                                #Security zones created
 description inside of branch
zone security outside
 description to WAN
zone-pair security in-out source inside destination outside#Zone pairs applied based on
                                                           #direction
 service-policy type inspect FWOUT                               #Policy applied
zone-pair security out-in source outside destination inside
 service-policy type inspect FWIN
!
ipv6 access-list v6-route                   #EIGRP ACL
 permit 88 any any
!
ipv6 access-list v6-FWIN                    #IPv6 ACL (basically same as v6-class)
 permit ipv6 any any
```

sw-br1-1

```
interface Vlan100
 ipv6 address 2001:DB8:CAFE:1100::BAD2:F126/64
!
 ipv6 access-list MGMT-IN                    #Management ACL - Permit management access
                                             #for cafe::/48 prefix only to the switch
                                             #VLAN100 interface
 permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:1100::BAD2:F126
 deny ipv6 any any log-input
!
banner login ^C
Unauthorized access to this device and/or network is prohibited.
^C
!
line vty 0 4
 ipv6 access-class MGMT-IN in
 transport input ssh
```

QoS

The QoS configurations for the single-tier profile are almost the same for IPv4 and IPv6. In the configuration shown below, there are Network Based Application Recognition (NBAR) functions for IPv4. Because of the lack of NBAR awareness of IPv6, ACLs are used to statically define the application type and map the ACL match to a class-map used for setting the appropriate DCSP value.

The following configurations are meant to show where the QoS policies are applied for IPv6 and any specific match/set modifications. The Cisco QoS Design Guide can be found at: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.html.

For the sake of completeness, the QoS policy configuration is shown for both IPv4 and IPv6. This policy is an example used in the lab and your policy may vary.

2900-br1-1

```
class-map match-any BRANCH-BULK-DATA
 match access-group name BULK-DATA-APPS
 match access-group name BULK-DATA-APPS-V6       #Match IPv6 ACL in from branch hosts
class-map match-all SQL-SLAMMER
 match protocol custom-02
 match packet length min 404 max 404
class-map match-all BULK-DATA              #Match previously set value or "trusted" value
 match  dscp af11  af12
class-map match-all INTERACTIVE-VIDEO
 match  dscp af41  af42
class-map match-any CALL-SIGNALLING
 match  dscp cs3
 match  dscp af31
class-map match-any BRANCH-TRANSACTIONAL-DATA
 match protocol citrix
 match protocol ldap
 match protocol sqlnet
 match protocol http url "*cisco.com"
 match access-group name BRANCH-TRANSACTIONAL-V6 #Match IPv6 ACL in from branch hosts
 match protocol sap
class-map match-any BRANCH-MISSION-CRITICAL
 match access-group name MISSION-CRITICAL-SERVERS
 match access-group name MISSION-CRITICAL-V6     #Match IPv6 ACL in from branch hosts
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 netbios
 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      #Match IPv6 ACL in from branch hosts
```

```
class-map match-all ROUTING
 match  dscp cs6
class-map match-all SCAVENGER
 match  dscp cs1
class-map match-all NET-MGMT
 match  dscp cs2
class-map match-any BRANCH-SCAVENGER
 match protocol gnutella
 match protocol fasttrack
 match protocol kazaa2
 match access-group name BRANCH-SCAVENGER-V6     #Match IPv6 ACL in from branch hosts
class-map match-all TRANSACTIONAL-DATA
 match  dscp af21  af22
!
policy-map BRANCH-LAN-EDGE-IN-CHILD
 class WORMS
   drop
 class class-default
  set dscp default
policy-map BRANCH-WAN-EDGE-CHILD                 #Apply queuing/bandwidth policy egress
 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 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 SCAVENGER
    bandwidth percent 1
 class class-default
    bandwidth percent 25
     random-detect
policy-map BRANCH-LAN-EDGE-OUT              #Copy DSCP value to COS for local branch LAN
 class class-default
  set cos dscp
policy-map BRANCH-LAN-EDGE-IN-PARENT        #Set DSCP values based on ingress NBAR/ACL
 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 BRANCH-WAN-EDGE-PARENT             #Class-based shaping & egress policy applied
 class class-default
```

```
    shape average percent 90
  service-policy BRANCH-WAN-EDGE-CHILD
!
interface GigabitEthernet0/1
 service-policy output BRANCH-WAN-EDGE-PARENT           #Apply policy
!
interface Serial0/0/0
 service-policy output BRANCH-WAN-EDGE-PARENT           #Apply policy
!
interface GigabitEthernet1/0.100                        #Data VLAN
 service-policy input BRANCH-LAN-EDGE-IN-PARENT #Apply ingress classification policy
 service-policy output BRANCH-LAN-EDGE-OUT      #Apply egress classification policy
!
interface GigabitEthernet1/0.200                        #Voice VLAN
 service-policy output BRANCH-LAN-EDGE-OUT      #Apply egress classification policy
!
interface GigabitEthernet1/0.300                        #Printer VLAN
 service-policy input BRANCH-LAN-EDGE-IN-PARENT
 service-policy output BRANCH-LAN-EDGE-OUT

ipv6 access-list BULK-DATA-APPS-V6                      #IPv6 ACL for bulk 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
!
ipv6 access-list MISSION-CRITICAL-V6                   #IPv6 ACL for dst prefix of servers
 remark Data-Center traffic-mark dscp 25
 permit ipv6 any 2001:DB8:CAFE:10::/64
 permit ipv6 any 2001:DB8:CAFE:11::/64
!
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
```

Multicast

The configuration for IPv6 multicast in the single-tier profile is quite simple. IPv6 multicast design is outside the scope of this document and there are many options that can be selected for PIM, multicast availability, and security. In this document, only basic configurations are shown for IPv6 multicast on the 2900-br1-1 router and sw-br1-1 switch. The configurations allow for PIM-SSM or Embedded-RP to be used. The IPv6 multicast streams originate in the data center at the HQ site.

sw-br1-1

```
ipv6 mld snooping                    #Globally enable MLD snooping (see following note)
```

2900-br1-1

```
ipv6 multicast-routing               #Globally enable IPv6 multicast routing
```

The first thing to be aware of is the lack of CLI input required to enable IPv6 multicast when using PIM-SSM or Embedded-RP. If PIM-SSM is used exclusively, then the only thing required to enable is **ipv6 multicast-routing** globally, which automatically enables PIM on all IPv6-enabled interfaces. This is a dramatic difference from what is required with IPv4 multicast.

Note If PIM-SSM is used, then the host is required to use MLDv2 and the branch switch should support MLDv2-Snooping. If the host or switch do not support MLDv2, a feature within Cisco IOS can be used to map MLDv1 reports to MLDv2 reports at the branch router. This is called SSM-Mapping. For more information, see the following URL: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-multicast_ps10591_TSD_Products_Configuration_Guide_Chapter.html#wp1058805.

SSM-Mapping is not required in this document because the switches fully support MLDv2-Snooping.

In the previous example, the Layer 2 switch (sw-br1-1) needs to have IPv6 multicast awareness in order to control the distribution of multicast traffic only on ports that are actively listening. This is accomplished by enabling MLD-Snooping. With MLD-Snooping enabled on the switch and with IPv6 multicast routing enabled on the branch router, it can be seen that sw-br1-1 can see 2900-br1-1as a locally-attached multicast router.

```
sw-br1-1# show ipv6 mld snooping mrouter
Vlan    ports
----    -----
 100    Gi1/0/2(dynamic)
 200    Gi1/0/2(dynamic)
 300    Gi1/0/2(dynamic)
```

When a group is active on the branch switch, information about the group can be displayed:

```
sw-br1-1# show ipv6 mld snooping address
Vlan      Group          Type        Version     Port List
------------------------------------------------------------
100       FF35::1111      mld         v2         Gi1/0/2
```

On 2900-br1-1, information about PIM, multicast route, RPF, and groups can be viewed in much the same way as with IPv4. Here is the output of an active group using PIM-SSM (FF35::1111). This stream is coming in from the HQ data center and going out the VLAN100 (2900-br1-1 G1/0.100) interface:

```
2900-br1-1# show ipv6 mroute                    #show ipv6 pim topology can also be used

Multicast Routing Table
```

```
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(2001:DB8:CAFE:11:2E0:81FF:FE2C:9332, FF35::1111), 00:01:28/00:03:10, flags: sTI
  Incoming interface: Tunnel3
  RPF nbr: FE80::230:F2FF:FE15:9C1B
  Immediate Outgoing interface list:
    GigabitEthernet1/0.100, Forward, 00:01:28/00:03:02
```

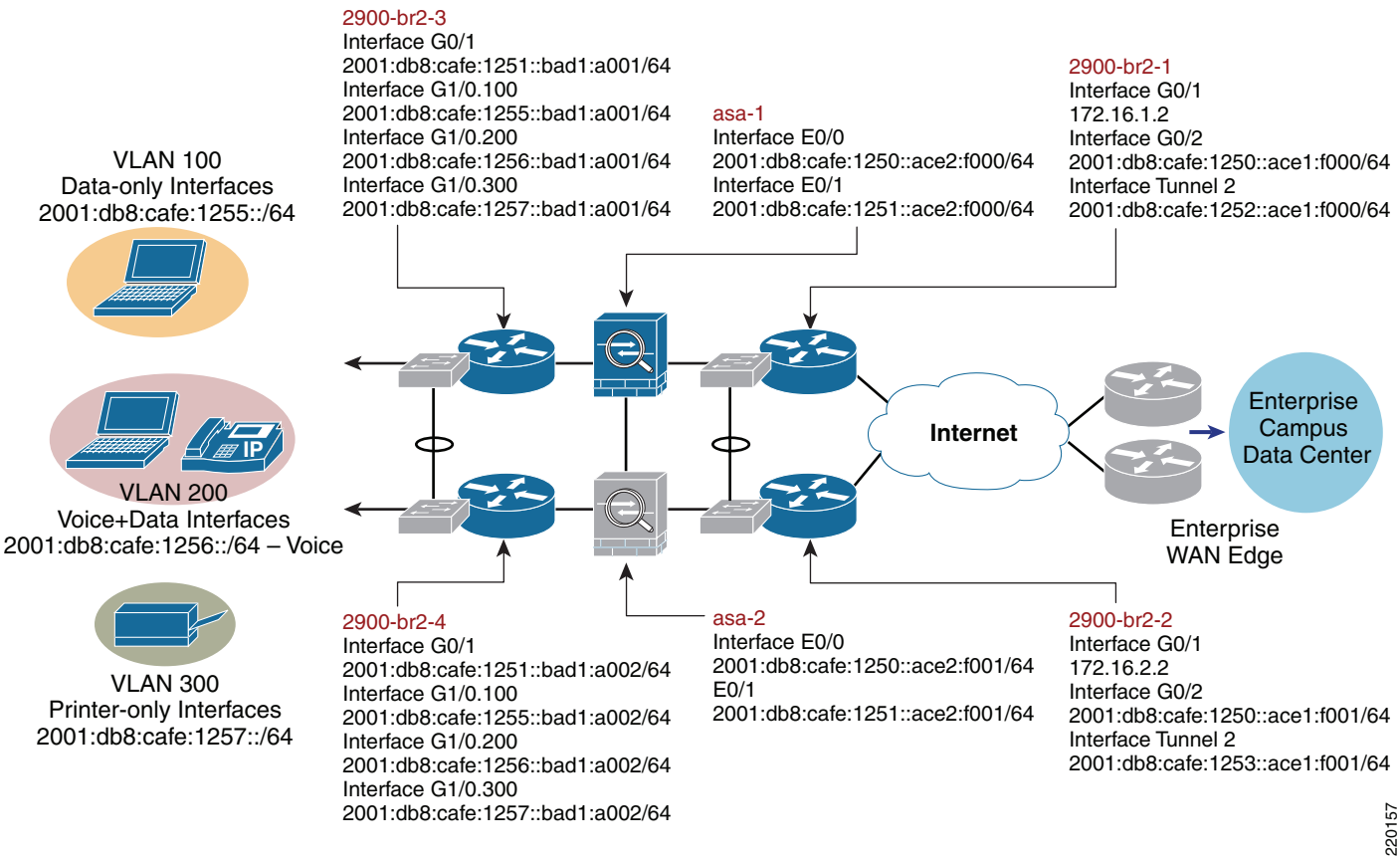
Multi-Tier Implementation

This section focuses on the configuration of the multi-tier profile.

Network Topology

Figure 4 serves as a reference for all of the configurations described in the dual-tier profile. It shows the interface and IPv6 addressing layout for the two branch routers and Catalyst switch.

Figure 4 Multi-Tier Profile—Interface/Addressing Layout



Two WAN tier branch routers (2900-br2-1 and 2900-br2-2) are used with internal network switch modules (or can be an external switch) to provide WAN and LAN connectivity.

- WAN—The WAN consists of an Ethernet hand-off connection to the ISP from each of the two branch routers. As in the single tier profile, DMVPN is used over the Internet for private WAN communications. Again, other WAN connection types can be used.
- LAN—The LAN-facing branch connection is used to connect each WAN tier router to the two Cisco ASA firewalls. Internal EtherSwitch modules are used to create a Layer 2 connection between each router and ASA firewall so that they are all on the same network (easier for redundancy/high availability).

Two firewall tier branch firewalls (asa-1 and asa-2) are connected via EtherSwitch modules to the WAN tier as well as inward facing via EtherSwitch modules at the access tier. The ASAs are configured for a primary (asa-1) and secondary (asa-2) role. As was mentioned in the single tier profile, this tier and configuration is optional. If the DMVPN or other private WAN deployment is considered to be a trusted link, then no additional firewall services are needed except for the native Internet-facing link and/or if a split-tunneling deployment is used. The firewall tier is shown in this document for the sake of completeness.

Two access tier routers (2900-br2-3 and 2900-br2-4) with integrated EtherSwitch modules are acting as distribution\access layer devices, as you would find in a campus network. They simply aggregate the Layer 2 access switches and provide routing and first-hop redundancy for the access VLANs. The access tier routers use the internal EtherSwitch modules for connections to the firewall tier and the branch hosts.

In the single-tier profile we looked at configurations based on role or technology (i.e., routing, security, QoS). In the multi-tier profile the configurations are broken down by the tier in the network (i.e., WAN tier, firewall tier).

WAN Tier

The following configurations are for the WAN tier devices. Only the IPv6 and generic network portion of the configuration are shown and only one side of the device pair is shown (i.e., 2900-br2-1<>EtherSwitch). The other device pair (i.e., 2900-br2-2<>EtherSwitch) are identically configured with the exception of addressing, HSRP priority, and routing preference. Also, there are many different options in this arrangement. The EtherSwitch module can be doing routing instead of doing it via the sub-interfaces of the router. Also, there could be a dedicated pair of external switches instead of the EtherSwitch module. The design and configuration shown is just one of many ways to do this.

Most of the configurations are not explained as they mirror very closely what was discussed in the single-tier profile. Because of this the QoS configuration is not shown here for the sake of brevity. The QoS configuration in the multi-tier is the exact same as the single-tier.

2900-br2-1

```
ipv6 unicast-routing
ipv6 cef
ipv6 multicast-routing
!
key chain CISCO
 key 1
  key-string 7 111B180B101719
!
track 150 ip sla 150                                  #Enable IP SLA
!
crypto ipsec
crypto isakmp policy 1
 encr aes 256
```

```
 authentication pre-share
 group 2
crypto isakmp key CISCO address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
crypto ipsec transform-set SPOKETrans esp-aes 256 esp-sha-hmac
!
crypto ipsec profile DMVPNProf
 set transform-set SPOKETrans
!
interface Tunnel2
 description DMVPN to HQ Head-end 1
 ipv6 address 2001:DB8:CAFE:1252::ACE1:F000/64
 ipv6 mtu 1416
 no ipv6 redirects
 no ipv6 unreachables
 ipv6 eigrp 1
 ipv6 authentication mode eigrp 1 md5
 ipv6 authentication key-chain eigrp 1 CISCO
 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 172.16.3.3
 ipv6 nhrp map 2001:DB8:CAFE:1252::ACE3:F003/128 172.16.3.3
 ipv6 nhrp network-id 10
 ipv6 nhrp nhs 2001:DB8:CAFE:1252::ACE3:F003
 ipv6 nhrp holdtime 600
 ipv6 nhrp shortcut
 tunnel source 172.16.1.2
 tunnel mode gre multipoint
 tunnel key 123
 tunnel protection ipsec profile DMVPNProf
!
track 2 interface GigabitEthernet0/1 line-protocol          #HSRP Interface Tracking
!
interface GigabitEthernet0/1
 description Ethernet-Handoff to ISP
 ip address 172.16.1.2 255.255.255.0
!
interface GigabitEthernet1/0
 description Internal EtherSwitch Link
 ip address 1.1.1.1 255.255.255.0
!
interface GigabitEthernet1/0.10
 description L2 Network for RTR-ASA
 encapsulation dot1Q 10
 ipv6 address 2001:DB8:CAFE:1250::ACE1:F000/64
 standby version 2
 standby 2 ipv6 FE80::5:73FF:FEA0:2  #Statically defined HSRP address (can be autoconfig)
 standby 2 priority 105
 standby 2 preempt
 standby 2 authentication CISCO
 standby 2 track 2 decrement 10                     #Link to tracking interface
 ipv6 eigrp 1
 ipv6 authentication mode eigrp 1 md5
 ipv6 authentication key-chain eigrp 1 CISCO
 ipv6 hold-time eigrp 1 35
!
ip route 172.16.3.3 255.255.255.255 172.16.1.1      #Static route for HQ WAN address
!
ip sla 150
 icmp-echo 2001:DB8:CAFE:10::15 source-ip 2001:DB8:CAFE:1250::ACE1:F000#Probe server at HQ
ip sla schedule 150 life forever start-time now
```

```
!
ipv6 route 2001:DB8:CAFE:1251::/64 2001:DB8:CAFE:1250::ACE2:F000#Static routes to ASA
                                                                #outside interface
ipv6 route 2001:DB8:CAFE:1255::/64 2001:DB8:CAFE:1250::ACE2:F000
ipv6 route 2001:DB8:CAFE:1256::/64 2001:DB8:CAFE:1250::ACE2:F000
ipv6 route 2001:DB8:CAFE:1257::/64 2001:DB8:CAFE:1250::ACE2:F000
!
ipv6 router eigrp 1                          #EIGRP for Tunnel and redist of local routes
 eigrp router-id 10.122.1.1
 redistribute static
 passive-interface Loopback0
```

wan-tier-switch-br2-1

```
ipv6 mld snooping
!
vlan 10
 name ASA
!
interface GigabitEthernet1/0/1                    #Interface to other EtherSwitch
 description TRUNK to 2900-br2-2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10
 switchport mode trunk
!
interface GigabitEthernet1/0/2                    #Internal interface to 2900-br2-1
 description TRUNK to 2900-br2-1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10
 switchport mode trunk
!
interface FastEthernet1/0/1                       #Connecting to ASA-1
 description ASA-1
 switchport access vlan 10
```

Firewall Tier

This tier is optional and used only when the connections to the HQ site are not considered to be fully trusted or if you use a split-tunneling deployment and need comprehensive security facing the Internet.

The following Cisco ASA configuration is for the primary unit only (with a special note on the failover configuration for the secondary unit). Only the relevant IPv6 configurations are shown.

ASA-1

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ipv6 address 2001:db8:cafe:1250::ace2:f000/64 standby 2001:db8:cafe:1250::ace2:f001
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ipv6 address 2001:db8:cafe:1251::ace2:f000/64 standby 2001:db8:cafe:1251::ace2:f001
!
ipv6 route inside 2001:db8:cafe:1255::/64 fe80::5:73ff:fea0:1    #Static routes to Access
                                                                 #tier HSRP
ipv6 route inside 2001:db8:cafe:1256::/64 fe80::5:73ff:fea0:1
ipv6 route inside 2001:db8:cafe:1257::/64 fe80::5:73ff:fea0:1
ipv6 route outside ::/0 fe80::5:73ff:fea0:2     #Default route to WAN tier HSRP address
!
failover
failover lan unit primary
```

```
failover lan interface FO GigabitEthernet0/2
failover key ****
failover link FO-LINK GigabitEthernet0/3
failover interface ip FO 2001:db8:cafe:bad::ace2:f000/64 standby
2001:db8:cafe:bad::ace2:f001
failover interface ip FO-LINK 2001:db8:cafe:bad1::ace2:f000/64 standby
2001:db8:cafe:bad1::ace2::f001
!
ipv6 access-list v6-ALLOW permit icmp6 any any echo            #Basic ACL example
ipv6 access-list v6-ALLOW permit icmp6 any any echo-reply
ipv6 access-list v6-ALLOW permit tcp any any eq ftp
ipv6 access-list v6-ALLOW permit tcp any any eq ftp-data
ipv6 access-list v6-ALLOW permit tcp any any eq telnet
ipv6 access-list v6-ALLOW permit tcp any any eq smtp
ipv6 access-list v6-ALLOW permit tcp any any eq www
ipv6 access-list v6-ALLOW permit udp any any eq domain
ipv6 access-list v6-ALLOW permit tcp any any eq https
ipv6 access-list v6-ALLOW permit tcp any any eq ssh
ipv6 access-list v6-ALLOW deny ip any any log
!
access-group v6-ALLOW in interface outside
!
ssh 2001:db8:cafe::/48 inside
```

The following configuration is specific to the ASA-2 (standby) for the failover configuration.

ASA-2

```
failover
failover lan unit secondary
failover lan interface FO GigabitEthernet0/2
failover key ****
failover link FO-LINK GigabitEthernet0/3
failover interface ip FO 2001:db8:cafe:bad::ace2:f000/64 standby
2001:db8:cafe:bad::ace2:f001
failover interface ip FO-LINK 2001:db8:cafe:bad1::ace2:f000/64 standby
2001:db8:cafe:bad1::ace2::f001
```

Access Tier

The following configuration is for the access tier devices. This tier can be deployed via a pair of Layer 2/Layer 3 switches, routers plus external switches, or as shown here with routers and internal EtherSwitch modules. There are many possible options for providing distribution layer functions within the branch.

In the access tier shown in this document, two 2900 series routers have internal EtherSwitch modules that have trunk connections between them for VLANs 100, 200, 300, which represent the data VLAN (100), voice VLAN (200), and printer VLAN (300).

In the single-tier profile, IPv6 addressing was assigned via a combination of local DHCPv6 pools and RA-based assignment. Those are fully supported in the multi-tier profile. However, to show a slightly different configuration, all hosts will obtain IPv6 addressing and options via a centralized DHCPv6 server located at the HQ.

As was stated before, Layer 3 functionality can be enabled on the EtherSwitch module that terminates the VLANs, but in this design the EtherSwitch module is performing basic Layer 2 functions and the router is terminating the VLANs on sub-interfaces. The EtherSwitch modules connects hosts in VLANs 100, 200, 300 as well as the ASAs in the firewall tier.

Also, configurations for QoS and local LAN security are identical to those configured in the single-tier profile and are not shown for the sake of brevity.

Note On the Catalyst 3750, 3560, and EtherSwitch platforms, it is required to enable the correct Switch Database Management (SDM) template to allow the TCAM to be used for different purposes. The 3560-br2-1 switch has been configured (reload required) with the "dual-ipv4-and-ipv6" SDM template using the **sdm prefer dual-ipv4-and-ipv6 default** command. For more information on the **sdm prefer** command and associated templates, see: http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst3750e_3560e/software/release/12.2_55_se/configuration/guide/swsdm.html.

2900-br2-3

```
ipv6 unicast-routing
ipv6 cef
ipv6 multicast-routing
!
key chain CISCO
 key 1
  key-string 7 111B180B101719
!
interface GigabitEthernet1/0
 description to INTERNAL SW-BR1-1
 ip address 1.1.1.1 255.255.255.0
!
interface GigabitEthernet1/0.20
 description L2 Network for RTR-ASA
 encapsulation dot1Q 20
 ipv6 address 2001:DB8:CAFE:1251::BAD1:A001/64
 standby version 2
 standby 2 ipv6 FE80::5:73FF:FEA0:1
 standby 2 priority 105
 standby 2 preempt
 standby 2 authentication CISCO
 no ipv6 redirects
 no ipv6 unreachables
 ipv6 eigrp 1
 ipv6 authentication mode eigrp 1 md5
 ipv6 authentication key-chain eigrp 1 CISCO
 ipv6 hold-time eigrp 1 35
!
interface GigabitEthernet1/0.100
 description DATA VLAN for Computers
 encapsulation dot1Q 100
 standby version 2
 standby 4 ipv6 autoconfig
 standby 4 preempt
 standby 4 authentication CISCO
 no ipv6 redirects
 no ipv6 unreachables
 ipv6 address 2001:DB8:CAFE:1255::BAD1:A001/64
 ipv6 nd managed-config-flag                        #Set flag in RA to instruct host
                                                    #how to use DHCPv6
 ipv6 dhcp relay destination 2001:DB8:CAFE:10::2    #DHCPv6 relay to server at HQ
 ipv6 eigrp 1
 ipv6 authentication mode eigrp 1 md5
 ipv6 authentication key-chain eigrp 1 CISCO
 ipv6 hold-time eigrp 1 35
!
interface GigabitEthernet1/0.200
 description to Voice VLAN for IP Phones
 encapsulation dot1Q 200
 standby version 2
```

```
 standby 6 ipv6 autoconfig
 standby 6 preempt
 standby 6 authentication CISCO
 no ipv6 redirects
 no ipv6 unreachables
 ipv6 address 2001:DB8:CAFE:1256::BAD1:A001/64
 ipv6 nd managed-config-flag
 ipv6 dhcp relay destination 2001:DB8:CAFE:10::2
 ipv6 eigrp 1
 ipv6 authentication mode eigrp 1 md5
 ipv6 authentication key-chain eigrp 1 CISCO
 ipv6 hold-time eigrp 1 35
!
interface GigabitEthernet1/0.300
 description to Printer VLAN
 encapsulation dot1Q 300
 standby version 2
 standby 8 ipv6 autoconfig
 standby 8 preempt
 standby 8 authentication CISCO
 no ipv6 redirects
 no ipv6 unreachables
 ipv6 address 2001:DB8:CAFE:1257::BAD1:A001/64
 ipv6 nd managed-config-flag
 ipv6 dhcp relay destination 2001:DB8:CAFE:10::2
 ipv6 eigrp 1
 ipv6 authentication mode eigrp 1 md5
 ipv6 authentication key-chain eigrp 1 CISCO
 ipv6 hold-time eigrp 1 35
!
ipv6 route ::/0 2001:DB8:CAFE:1251::ACE2:F000       #IPv6 default route to ASA interface
!
ipv6 router eigrp 1
 eigrp router-id 10.122.1.3
 redistribute static
 passive-interface GigabitEthernet1/0.100
 passive-interface GigabitEthernet1/0.200
 passive-interface GigabitEthernet1/0.300
 passive-interface Loopback0
```

accesss-tier-switch-br2-1

```
ipv6 mld snooping
!
vlan 20
 name ASA
!
vlan 100
 name DATA
!
vlan 200
 name VOICE
!
vlan 300
 name PRINTERS
!
interface GigabitEthernet1/0/1                    #Interface to other EtherSwitch
 description TRUNK to 2900-br2-4
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 20
 switchport mode trunk
!
interface GigabitEthernet1/0/2                    #Internal interface to 2900-br2-1
 description TRUNK to 2900-br2-3
```

```
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 20,100,200,300
 switchport mode trunk
!
interface FastEthernet1/0/1                          #Connecting to ASA-1
 description ASA-1
 switchport access vlan 20
!
interface FastEthernet1/0/3                        #Example of Data/Voice access interface
 description PHONE + PC
 switchport access vlan 100
 switchport mode access
 switchport voice vlan 200
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface Vlan100
 description VLAN100 for PCs and Switch management
 ipv6 address 2001:DB8:CAFE:1255::BAD1:F128/64
```

Multicast in the Multi-Tier Profile

One note to make regarding IPv6 multicast in the multi-tier profile concerns the Cisco ASA. At the time this document was published, the Cisco ASA did not support IPv6 multicast routing/forwarding. If you want IPv6 multicast support for the branch hosts in the access tier (acting as receivers) with IPv6 multicast sources in the HQ, then you must enable a manually-configured or GRE tunnel between the access tier routers and the WAN tier routers—through the Cisco ASA.

Careful testing needs to be completed when doing this as unicast routing between the dual stack Ethernet interfaces between the WAN tier, firewall tier, and access tier can cause issues with unicast routing over the tunnel interfaces.

A basic example of the tunnel configuration might look similar to this:

2900-br2-1

```
ipv6 multicast-routing
!
interface Tunnel4
 description Manual tunnel to Access Tier
 ipv6 address 2001:DB8:CAFE:1258::1/127
 tunnel source 10.124.10.1               #Tunnel source is 2900-br2-1 LAN intf (WAN tier)
 tunnel destination  10.124.100.1        #Tunnel destination is 2900-br2-3 LAN intf
(Access tier)
 tunnel mode ipv6ip                           #IPv6-in-IPv4 tunnel mode
```

2900-br2-3

```
ipv6 multicast-routing
!
interface Tunnel4
 description Manual tunnel to WAN Tier
 ipv6 address 2001:DB8:CAFE:1258::2/127
 tunnel source 10.124.100.1
 tunnel destination  10.124.10.1
 tunnel mode ipv6ip
```

You need to configure routing in such a way as to ensure that unicast traffic is traversing the dual stack Ethernet interfaces between the access tier and firewall tier, but multicast is traversing the tunnel. In order to do that, it is critical to configure a static multicast route to ensure proper Reverse Path Forwarding (RPF) behavior. If the access tier router attempts to perform an RPF check against the

Ethernet interface connecting towards the source at the HQ (via the ASA), it will fail as no multicast forwarding is supported. The command below enables a simple multicast route so that RPF checks for the multicast source network (at the HQ - 2001:DB8:CAFE:11::/64) are done against the tunnel (next hop is the address of the WAN tier tunnel interface address) instead of the Ethernet link facing the ASA.

```
ipv6 route 2001:DB8:CAFE:11::/64 2001:DB8:CAFE:1258::1 multicast
```

Finally, you need to configure the Cisco ASA to allow for the tunnel in the security policy.

```
access-list MCAST extended permit 41 host 10.124.10.1 host 10.124.100.1   #Protocol 41 is
                                                                          #for v6-in-v4 tunnel
access-group MCAST in interface outside
```

Conclusion

This document describes how to deploy IPv6 in the branch network. The branch profiles described were single-tier and multi-tier. The configurations were mostly based on the existing Cisco branch design best practices. The profiles described are certainly not the only ways to deploy IPv6 in this environment, but they provide options that can be leveraged based on the branch environment.

References

There are many notes and disclaimers in this document that describe the need to fully understand the technology and protocol aspects of IPv6. There are many design considerations associated with the implementation of IPv6, including security, QoS, availability, management, IT training, and application support.

This section provides additional resources for IPv6, Cisco design recommendations, products, and solutions, and industry activity.

Cisco-Specific References

- Cisco IPv6
  http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html
- Cisco Branch/WAN guides
  http://www.cisco.com/en/US/netsol/ns816/networking_solutions_program_home.html
- Cisco IOS IPv6 Configuration Guide
  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/15_0/ipv6_15_0_book.html
- Catalyst 3750-E and 3560-E Switch Software Configuration Guide
  http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst3750e_3560e/software/release/12.2_55_se/configuration/guide/3750escg.html
- Enterprise QoS SRND
  http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.html
- Cisco ASA 5500 Series Configuration Guide
  http://www.cisco.com/en/US/partner/docs/security/asa/asa84/configuration/guide/asa_84_cli_config.html

IPv6 Industry References

- *IPv6 in Enterprise Networks* by Shannon McFarland, Muninder Sambi, Nikhil Sharma, Sanjay Hooda (ISBN-10:1-58714-227-9; ISBN-13: 978-1-58714-227-7)
  http://www.ciscopress.com/bookstore/product.asp?isbn=1587142279
- *Deploying IPv6 Networks* by Ciprian P. Popoviciu, Eric Levy-Abegnoli, Patrick Grossetete (ISBN-10:1-58705-210-5; ISBN-13:978-1-58705-210-1)
  http://www.ciscopress.com/bookstore/product.asp?isbn=1587052105&rl=1
- *IPv6 Security* by Scott Hogg, Eric Vyncke (ISBN-10:1-58705-594-5; ISBN-13: 978-1-58705-594-2)
  http://www.ciscopress.com/bookstore/product.asp?isbn=1587055945