Implementing ADSL and Deploying Dial Access for IPv6

This module describes the implementation of prefix pools and per-user Remote Access Dial-In User Service (RADIUS) attributes in IPv6. It also describes the deployment of IPv6 in Digital Subscriber Line (DSL) and dial-access environments. Asymmetric Digital Subscriber Line (ADSL) and dial deployment provide the extensions that make large-scale access possible for IPv6 environments, including IPv6 RADIUS attributes, stateless address configuration on Point-to-Point Protocol (PPP) links, per-user static routes, and Access Control Lists (ACLs).

Contents

Restrictions for Implementing ADSL and Deploying Dial Access for IPv6

ADSL and Dial Deployment is available for interfaces with PPP encapsulation enabled, including PPP over ATM (PPPoA), PPP over Ethernet (PPPoE), PPP over async, and PPP over ISDN.

Information About Implementing ADSL and Deploying Dial Access for IPv6

Address Assignment for IPv6

A Cisco router configured with IPv6 will advertise its IPv6 prefix(es) on one or more interfaces, allowing IPv6 clients to automatically configure their address(es). In IPv6, address assignment is performed at the network layer, in contrast to IPv4 where a number of functions are handled in the PPP layer. The only function handled in IPV6CP is the negotiation of a unique interface identifier. Everything else, including DNS server discovery, is done within the IPv6 protocol itself.

Contrary to IPv4 address assignment, an IPv6 user will be assigned a prefix, not a single address. Typically the Internet Service Provider (ISP) assigns a 64- or 48-bit prefix.

In the IPv6 world, Internet service providers (ISPs) assign long-lived prefixes to users, which has some impact on the routing system. In typical IPv4 environments, each NAS has a pool of 24-bit addresses and users get addresses from this pool when dialling in. If a user dials another POP or is connected to another NAS at the same POP, a different IPv4 address is assigned.

Addresses for IPv6 are assigned by two different methods.

Stateless Address Auto-configuration

Assigning addresses using the stateless address auto-configuration method can only be used to assign 64-bit prefixes. Each user is assigned a 64-bit prefix which is advertised to the user in a router advertisement (RA). All addresses are automatically configured based on the assigned prefix.

While a typical scenario is to assign a separate 64-bit prefix per user, users can also be assigned a prefix out of a shared pool of addresses. Using the shared limits addresses to only one address per user.

This solution works best for the cases where the customer provider edge router (CPE) is a single PC or is limited to only one subnet. If the user has multiple subnets, Layer 2 (L2) bridging, multi-link subnets or proxy RA can be used. The prefix advertised in the RA can come from an Authorization, Authentication, and Accounting (AAA) server, which also provides the prefix attribute, can be manually configured, or be allocated from a prefix pool.

The Framed-Interface-Id AAA attribute influences the choice of interface identifier for peers and, in combination with the prefix, the complete IPv6 address can be determined.

Prefix Delegation

Prefix Delegation is a new protocol that uses Dynamic Host Configuration Protocol (DHCP). Where the user requests a prefix from the prefix delegator, typically the NAS. The prefix is allocated as described for “Stateless Address Auto-configuration” section on page 2.

AAA Attributes for IPv6

New vendor-specific attributes (VSAs) have been developed to support Authorization, Authentication, and Accounting (AAA) for IPv6. The new Cisco VSAs are inacl, outacl, route, and prefix.

Prefix pools and pool names are configurable through AAA.

The RADIUS attributes as described in RFC 3162 are supported:

- Framed-Interface-Id
- Framed-IPv6-Prefix
- Login-IPv6-Host
- Framed-IPv6-Route
- Framed-IPv6-Pool
- Pool

The Framed-IPv6-Prefix and Framed-IPv6 route attributes perform the same functions as the Cisco VSAs. The Framed-Interface-Id attribute indicates the IPv6 interface identifier to be configured. It may be used in Access-Accept packets. If the Interface-Identifier IPv6CP option has been successfully negotiated, this attribute must be included in an Acc-0Request packet as a hint by the NAS to the server that it would prefer that value.

The Framed-IPv6-Prefix attribute is used for virtual access only and indicates an IPv6 prefix (and corresponding route) to be configured. It may be used in Access-Accept packets and can appear multiple times. The NAS will create a corresponding route for the prefix.

AAA attributes are described in the following sections:

- RADIUS Per User Attributes for Virtual Access in IPv6 Environments, page 3
- IPv6 prefix pools, page 4

RADIUS Per User Attributes for Virtual Access in IPv6 Environments

The following new IPv6 attributes for RADIUS AV pairs are supported for virtual access:

- IPv6 route Attribute, page 3
- IPv6 ACL Attributes, page 3
- IPv6 Prefix Attribute, page 4
- IPv6 Pool Attribute, page 4

Apart from the new **prefix** and **pool** attributes, these are all existing cisco VSAs extended to support the IPv6 protocol.

IPv6 route Attribute

TheIPv6 route# attribute allows you to specify a per-user static route. A static route is appropriate when the Cisco IOS software cannot dynamically build a route to the destination. See the description of the **ipv6 route** command for more information about building static routes This example shows the ipv6 route# attribute used to define a static route.

Example:

```
cisco-avpair = "ipv6:route#1=3ffe:c00:1::/48",
cisco-avpair = "ipv6:route#2=3ffe:c00:2::/48",
```

IPv6 ACL Attributes

You can specify a complete IPv6 access list. The unique name of the access list is generated automatically. The access list is removed when its user logs out. The previous access list on the interface is reapplied.

The "inacl" and "outacl" attributes allow you to a specific existing access-list configured on the router. The following example shows ACL number 1 specified as the access list:

Example:

```
cisco-avpair = "ipv6:inacl#1=permit 3ffe:c00:1::/48",
cisco-avpair = "ipv6:outacl#1=deny fec0::/10",
```

IPv6 Prefix Attribute

The Ipv6 prefix# attribute lets you indicate which prefixes to advertise in Neighbor Discovery Router Advertisement messages. When the “prefix#” attribute is used, a corresponding route (marked as a per-user static route) is installed in the Routing Information Base (RIB) tables for the given prefix.

Example:Example:

```
cisco-avpair = "ipv6:prefix#1=3000::/64",
cisco-avpair = "ipv6:prefix#2=3001::/64",
```

IPv6 Pool Attribute

For RADIUS authentication, the IPv6 pool attribute extends the IPv4 address pool attributed to support the IPv6 protocol. It specifies the name of a local pool on the network access server (NAS) from which to get the prefix, and is used whenever the service is configured as PPP and whenever the protocol is specified as IPv6. Note that the address pool works in conjunction with local pooling. It specifies the name of the local pool which has been preconfigured on the NAS.

IPv6 prefix pools

The function of prefix pools in IPv6 is similar to that of address pools in IPv4. The main difference is that IPv6 assigns prefixes rather than single addresses.

As for IPv4, a pool or a pool definition can be configured locally or it can be retrieved from an AAA server. Overlapping membership between pools is not permitted.

Once a pool is configured it cannot be changed. If you change the configuration, the pool will be removed and recreated. All prefixes previously allocated will be freed.

Prefix pools can be defined so that each user is allocated a 64-bit prefix or so that a single prefix is shared among several users. In a shared prefix pool, each user may receive only one address from the pool.

How to Configure ADSL and Deploy Dial Access in IPv6

The configuration guidelines contained in this section show how to configure ADSL and dial access in IPv6 environments.

- Configuring the NAS, page 5 (Required)
- Configuring the Remote CE Router, page 7 (Required)
- Setting Up the RADIUS Profile for Preauthentication Enhancements for Callback, page 9 (Required)

Configuring the NAS

The first step in setting up dial access is to configure the network access server (NAS). All of the dialer groups, access lists, and routes are known to the NAS. This task shows how to configure the NAS to implement ADSL and deploy dial access for IPv6 environments.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **hostname** *name*
4. **aaa new-model**
5. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
6. **aaa authorization configuration default** [**radius** | **tacacs+**]
7. **show ipv6 route**
8. **virtual-profile virtual-template** *number*
9. **interface serial** *controller-number*:*timeslot*
10. **encapsulation** *encapsulation-type*
11. **dialer-group** *group-number*
12. **ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**]
13. **interface virtual-template** *number*
14. **ipv6 enable**
15. **dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*}
16. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias**{*hostname* | *ip-address*}]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure** {**terminal**	**memory**	**network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**hostname** *name* **Example:** `Router(config)# hostname cust1-53a`	Specifies the host name for the network server.

	Command or Action	Purpose
Step 4	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA server.
Step 5	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication ppp default if-needed group radius`	Specifies one or more authentication, authorization, and accounting (AAA) authentication methods for use on serial interfaces that are running PPP
Step 6	**aaa authorization configuration default** [**radius** | **tacacs+**] **Example:** `Router(config)# aaa authorization network default group radius`	Downloads configuration information from the AAA server.
Step 7	**show ipv6 route** **Example:** `Router(config)# show ipv6 route`	Shows the routes installed by the previous commands.
Step 8	**virtual-profile virtual-template** *number* **Example:** `Router(config)# virtual-profile virtual-template 1`	Enables virtual profiles by virtual interface template.
Step 9	**interface serial** *controller-number*:*timeslot* **Example:** `Router(config)# interface Serial0:15`	Specifies a serial interface created on a channelized E1 or channelized T1 controller (for ISDN PRI, channel-associated signalling, or robbed-bit signalling).
Step 10	**encapsulation** *encapsulation-type* **Example:** `Router(config-if)# encapsulation ppp`	Sets the encapsulation method used by the interface.
Step 11	**exit**	Returns to global configuration mode.
Step 12	**dialer-group** *group-number* **Example:** `Router(config)# dialer-group 1`	Control access by configuring an interface to belong to a specific dialing group.
Step 13	**ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] **Example:** `Router(config)# ppp authentication chap`	Enables Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) or both and specifies the order in which CHAP and PAP authentication are selected on the interface.

	Command or Action	Purpose
Step 14	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template1`	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
Step 15	**ipv6 enable** **Example:** `Router(config)# ipv6 enable`	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
Step 16	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*} **Example:** `Router(config)# dialer-list 1 protocol ipv6 permit`	Defines a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list.
Step 17	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias**{*hostname* | *ip-address*}] **Example:** `Router(config)# radius-server host 172.17.250.8 auth-port 1812 acct-port 1813 key testing123`	Specifies a RADIUS server host.

Troubleshooting Tips

Verify that the access list is installed correctly before proceeding with the next task. Use the **show ipv6 access-list** and **show ipv6 interface** commands.

What to Do Next

Configure the remote CE router as described in the "Configuring the Remote CE Router" section on page 7

Configuring the Remote CE Router

After you have configured the NAS, configure each remote CE router as described in the following steps.

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **hostname** *name*
4. **interface bri** *number.subinterface-number* **[multipoint | point-to-point]**
5. **encapsulation** *encapsulation-type*

6. **ipv6 address autoconfig**
7. **isdn switch-type** *switch-type*
8. **ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**]
9. **ppp multilink** [**bap** | **required**]
10. **dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*}
11. **ipv6 route** *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [*administrative-distance*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**hostname** *name* **Example:** `Router(config)# hostname cust1-36a`	Specifies the host name for the network server.
Step 4	**interface bri** *number.subinterface-number* **[multipoint | point-to-point]** **Example:** `Router(config)# interface BRI1/0`	Configures a BRI interface and enters interface configuration mode.
Step 5	**encapsulation** *encapsulation-type* **Example:** `Router(config-if)# encapsulation ppp`	Sets the encapsulation method used by the interface.
Step 6	**ipv6 address autoconfig** **Example:** `Router(config-if)# ipv6 address autoconfig`	Indicates that the IPv6 address will be generated automaticaly.
Step 7	**isdn switch-type** *switch-type* **Example:** `Router(config-if)# isdn switch-type basic-net3`	Specifies the central office switch type on the ISDN interface.

	Command or Action	Purpose
Step 8	**ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] **Example:** `Router(config-if)# ppp authentication chap optional`	Enables Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
Step 9	**ppp multilink** [**bap** | **required**] **Example:** `Router(config-if)# ppp multilink`	Enables Multilink PPP (MLP) on an interface and, optionally, enables Bandwidth Allocation Control Protocol (BACP) and Bandwidth Allocation Protocol (BAP) for dynamic bandwidth allocation.
Step 10	**exit**	Exits interface configuration mode and returns to global configuration mode.
Step 11	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*} **Example:** `Router(config)# dialer-list 1 protocol ipv6 permit`	Defines a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list.
Step 12	**ipv6 route** *ipv6-prefix/prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [*administrative-distance*] **Example:** `Router(config)# ipv6 route 2001::1/128 BRI1/0`	Establishes static IPv6 routes. Use one command for each route.

Setting Up the RADIUS Profile for Preauthentication Enhancements for Callback

Configure RADIUS to establish the AV pairs for callback. Callback allows remote network users such as telecommuters to dial in to the NAS without being charged. When callback is required, the NAS hangs up the current call and dials the caller back. When the NAS performs the callback, only information for the outgoing connection is applied. The rest of the attributes from the preauthentication access-accept message are discarded.

The following example shows a RADIUS profile configuration for a local campus.

```
campus1 Auth-Type = Local, Password = "mypassword"
               User-Service-Type = Framed-User,
               Framed-Protocol = PPP,
               cisco-avpair = "ipv6:inacl#1=permit dead::/64 any",
               cisco-avpair = "ipv6:route=dead::/64",
               cisco-avpair = "ipv6:route=cafe::/64",
               cisco-avpair = "ipv6:prefix=dead::/64 0 0 onlink autoconfig",
               cisco-avpair = "ipv6:prefix=cafe::/64 0 0 onlink autoconfig",
               cisco-avpair = "ip:route=11.0.0.0 255.0.0.0",
```

Refer to the *Cisco IOS Security Configuration Guide* for detailed information about configuring RADIUS.

Configuration Examples for Implementing ADSL and Deploying Dial for IPv6

Implementing ADSL and Deploying Dial Access for IPv6 Example

This example shows a typical configuration for ADSL and Dial access. The following three separate configurations are required:

- NAS Configuration
- Remote CE Router Configuration
- RADIUS Configuration

NAS Configuration

This configuration for the ISP NAS shows the configuration that supports access from the remote customer edge router.

```
hostname cust1-53a
aaa new-model
aaa authentication ppp default if-needed group radius
aaa authorization network default group radius
virtual-profile virtual-template 1
interface Serial0:15
 encapsulation ppp
 dialer-group 1
 ppp authentication chap
!
interface Virtual-Template1
 ipv6 enable
!
dialer-list 1 protocol ipv6 permit
radius-server host 172.17.250.8 auth-port 1812 acct-port 1813 key testing123
```

Remote CE Router Configuration

This configuration for the remote customer edge router shows PPP encapsulation and IPv6 routes defined.

```
hostname cust-36a
interface BRI1/0
 encapsulation ppp
 ipv6 enable
 isdn switch-type basic-net3
 ppp authentication chap optional
 ppp multilink
!
dialer-list 1 protocol ipv6 permit
ipv6 route 2001::1/128 BRI1/0
ipv6 route ::/0 2001::1
```

RADIUS Configuration

This RADIUS configuration shows the definition of AV pairs to establish the static routes.

```
campus1 Auth-Type = Local, Password = "mypassword"
              User-Service-Type = Framed-User,
              Framed-Protocol = PPP,
              cisco-avpair = "ipv6:inacl#1=permit dead::/64 any",
              cisco-avpair = "ipv6:route=library::/64",
              cisco-avpair = "ipv6:route=cafe::/64",
              cisco-avpair = "ipv6:prefix=library::/64 0 0 onlink autoconfig",
              cisco-avpair = "ipv6:prefix=cafe::/64 0 0 onlink autoconfig",
              cisco-avpair = "ip:route=11.0.0.0 255.0.0.0",
```

Where to Go Next

For information about implementing routing protocols for IPv6, refer to the *Implementing RIP for IPv6*, *Implementing IS-IS for IPv6*, or the *Implementing Multiprotocol BGP for IPv6* module. For information about implementing security for IPv6 environments, refer to the *Implementing Security for IPv6* module.

Additional References

For additional information related to Implementing ADSL and Deploying Dial for IPv6, refer to the following references:

- Releated Documents
- Standards
- MIBs
- RFCs
- Technical Assistance

Releated Documents

Related Topic	Document Title
Certification authority and interoperability, Registration Authority (RA) proxy	The chapter "Configuring Certification Authority Interoperability " in the *Cisco IOS Security Configuration Guide*, Release 12.2 http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/index.htm
RADIUS server configuration	*Cisco IOS Security Configuration Guide*, Release 12.2 http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/index.htm and *Cisco IOS Dial Services Configuration Guide*, Release 12.2 http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fdial_c/index.htm
Per-user configuration (AAA, AV pairs table, IP address pooling, RADIUS server configuration), large-scale dial-out, virtual templates and virtual profiles	*Cisco IOS Dial Services Configuration Guide*, Release 12.2 http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fdial_c/index.htm
ADSL (asymmetric digital subscriber line), PPP	*Cisco IOS Wide Area Networking Configuration Guide*, Release 12.2 http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fwan_c/index.htm
Vendor-Specific Attributes (VSAs)	*Cisco Access Register Concepts and Reference Guide* *http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/3_0/concepts/vsa.htm*

Standards

Standards[1]	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

1. Not all supported standards are listed.

MIBs

MIBs[1]	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

1. Not all supported MIBs are listed.

RFCs

RFCs[1]	Title
RFC 3162	*RADIUS and IPv6*
RFC 3177	*IAB/IESG Recommendations on IPv6 Address*

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml