



A RADIUS server (or daemon) can provide authentication and accounting services to one or more client NAS devices. RADIUS servers are responsible for receiving user connection requests, authenticating users, and then returning all configuration information necessary for the client to deliver service to the users. A RADIUS access server is generally a dedicated workstation connected to the network.

**RADIUS Servers**

RADIUS server software is available from several sources. Livingston Enterprises, Inc., and Merit (University of Michigan) offer RADIUS server C source code without use restrictions.

The Merit and Livingston distributions are available from their respective URLs:

```
ftp://RADIUS/releases/
RADIUS.2.4.16.tar.{z,gz}
ftp://ftp.livingston.com/pub/livingston/
RADIUS/
```

In addition to Merit and Livingston, other vendors have developed or adapted RADIUS server software to support their communications servers, and the software is usually available directly from the vendors. However, in most cases, the RADIUS servers distributed by these companies are not considered supported products, but are provided as a convenience to the user.

**CiscoSecure**

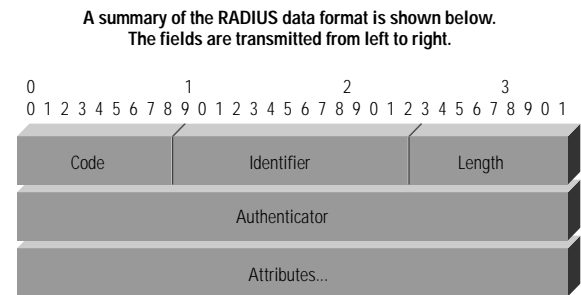
CiscoSecure™ software is a UNIX application program that provides AAA for dialup networks. It is the server portion of a distributed security solution using the TACACS+ protocol. Cisco will add RADIUS to CiscoSecure software in the near future. In addition to supporting all IETF attributes, CiscoSecure software will also support Cisco's RADIUS extensions and proprietary RADIUS extensions such as those used by Ascend. Users can also define their own extensions, creating a new RADIUS dictionary. A single database will be used to support both TACACS+ and RADIUS users, and all CiscoSecure V.2.0 features, such as token card support and the hypertext markup language (HTML)-based Web interface, will be supported in RADIUS.

**Protocol Operation**

Communication between a NAS and a RADIUS server is based on the User Datagram Protocol (UDP). Figure 1 shows the RADIUS packet format.

The authors of the RADIUS protocol selected UDP as the transport protocol for technical reasons. Generally, the RADIUS protocol is considered to be a connectionless service. Issues related to server availability, retransmission, and timeouts are handled by the RADIUS-enabled devices rather than the transmission protocol.

Figure 1 RADIUS Packet Format from RFC 2058



**Code**

The Code field is one octet, and identifies the type of RADIUS packet. When a packet is received with an invalid Code field, it is silently discarded. Radius Codes (decimal) are assigned as follows:

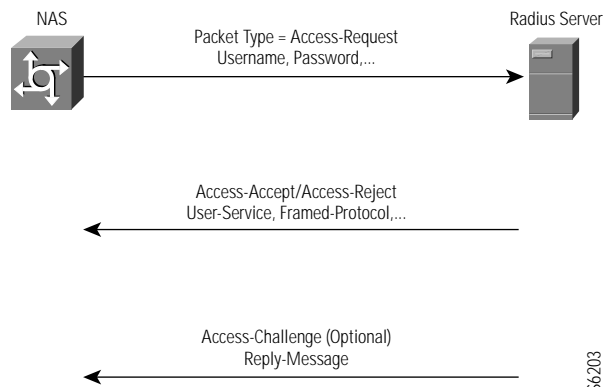
- 1 Access-Request
- 2 Access-Accept
- 3 Access-Reject
- 4 Accounting-Request
- 5 Accounting-Response
- 11 Access-Challenge
- 12 Status-Server (experimental)
- 13 Status-Client (experimental)
- 255 Reserved

Typically, a user login consists of a query (Access-Request) from the NAS to the RADIUS server and a corresponding response (Access-Accept or Access-Reject) from the server. The Access-Request packet contains the username, encrypted password, NAS IP address, and port. The format of the request also provides information on the type of session that the user wants to initiate. For example, if the query is presented in character mode, the inference is "Service-Type = Exec-User," but if the request is presented in Point-to-Point Protocol (PPP) packet mode, the inference is "Service-Type = Framed-User" and "Framed-Type = PPP."

When the RADIUS server receives the Access-Request from the NAS, it searches a database for the username listed. If the username does not exist in the database, either a default profile is loaded or the RADIUS server immediately sends an Access-Reject message. This Access-Reject message can be accompanied by an optional text message, which could indicate the reason for the refusal.

If the username is found and the password is correct, the RADIUS server returns an Access-Accept response, including a list of attribute-value pairs that describe the parameters to be used for this session. Typical parameters include service type (shell or framed), protocol type, IP address to assign the user (static or dynamic), access list to apply, or a static route to install in the NAS routing table. The configuration information in the RADIUS server defines what will be installed on the NAS. Figure 2 illustrates the RADIUS login and authentication process.

Figure 2 RADIUS Login and Authentication Process



## Authentication and Authorization Features

Authentication is the most troublesome aspect of remote security because of the difficulty associated with positively identifying a user. To ensure the identity of a remote user, the RADIUS protocol supports several methods of authentication, including Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and token cards. At present, all implementations of RADIUS require that the server of a token card vendor is run in addition to the RADIUS server. When CiscoSecure RADIUS support is released, it will include OEM support for CryptoCard token cards, and an additional server will not be necessary for these tokens.

### Enabling RADIUS Authentication

For every type of login that requires authentication, a command line must be entered. This line is the default list, which is used for login via RADIUS unless another list is configured:

```
aaa authentication login default radius local
```

Different login styles can be used, but each requires the creation of a separate method list.

For example:

```
aaa authentication ppp RADIUS tacacs+ local
aaa authentication login line RADIUS
aaa authentication login telnet RADIUS tacacs+
line
aaa authentication login physical RADIUS enable
```

```
BRI0
encapsulation ppp
ppp authentication chap ppp
line con 0
login authentication physical
line 1 8
login authentication line
modem InOut
flowcontrol hardware
line vty 0 4
password cisco
login authentication telnet
```

### Enabling RADIUS Authorization

RADIUS authorization is enabled with the AAA authorization command. The following command enables RADIUS authentication on exec sessions to the router:

```
aaa authorization exec radius
```

The same steps can be taken for PPP or Serial Line Internet Protocol (SLIP) access. The following command line is also required if RADIUS is to be used to help assign an IP address:

```
aaa authorization network radius
```

The following command authorizes commands to be used at different privilege levels:

```
aaa authorization command <level> radius
```

Of course, the RADIUS access control server must be configured with the appropriate permit or deny criteria. Customization of privilege levels on each NAS may also be appropriate.

## Accounting Features

The accounting features of the RADIUS protocol can be used independently of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of sessions, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session. An Internet Service Provider (ISP) might use RADIUS access control and accounting software to meet special security and billing needs.

### Enabling RADIUS Accounting

The **aaa accounting** command with the **radius** keyword are used to turn on RADIUS accounting for each Cisco IOS privilege level and network service. The accounting feature can be used for a variety of different actions that users might want to keep track of, including:

```
aaa accounting exec start-stop radius
aaa accounting network start-stop radius
```

These commands provide the starting and stopping time from a network and an exec session on the NAS.

RADIUS accounting can also be used to keep track of command levels accessed per user with the following:

```
aaa accounting command 5 stop-only radius
aaa accounting command 10 stop-only radius
```

This scenario provides accounting records for users who utilize commands set at level 5 and level 10 to the RADIUS daemon.

### RADIUS Support in Cisco IOS Software

#### Supported RADIUS Attributes

Cisco IOS software supports many of the RADIUS attributes specified in RFC 2058. Table 1 lists the RADIUS attributes supported in Cisco IOS software. These attributes are described in more detail in the “Configuring Network Access Security” section of the Cisco IOS Software Release Notes, which can be found at the following URL:

[http://www.cisco.com/univercd/data/doc/software/11\\_2/csecur/2caaa.htm](http://www.cisco.com/univercd/data/doc/software/11_2/csecur/2caaa.htm)

#### Interoperability

One of the goals of the RADIUS standard is to enable interoperability between the products of different vendors. There are, however, some caveats.

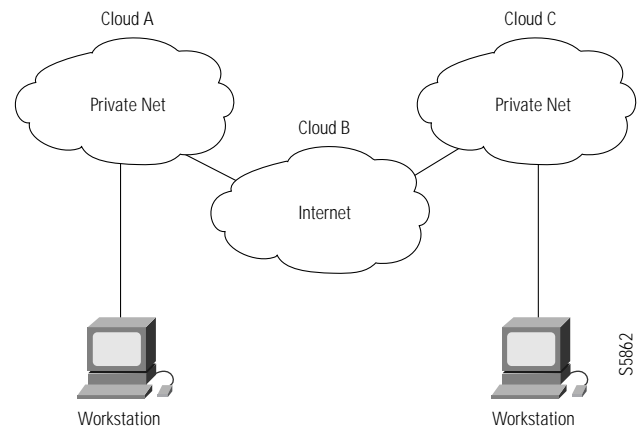
Although several vendors implement RADIUS clients, the products from all vendors are not always interoperable. Approximately 45 attributes are defined in the IETF RADIUS draft standard. Currently, Cisco’s NAS products support more than 30 IETF variables through Cisco IOS software. Cisco will continue to expand support for these variables in future software releases. (Generally, as long as customers use products that support the standard RADIUS attributes in their networks, these products will interoperate.) The RADIUS implementation in Cisco IOS software has been extensively tested to ensure interoperability with other RADIUS clients and access control servers that conform to the IETF RADIUS draft standard.

Unfortunately, some vendors, rather than following the RADIUS specification, have implemented proprietary extensions, for example, extended attributes, to the RADIUS protocol. If customers use these proprietary vendor-specific extended attributes, interoperability might be sacrificed.

### RADIUS and L2F

Layer 2 Forwarding (L2F) is a generic tunneling technique that encapsulates PPP frames so that devices in Cloud A believe that they have direct PPP connections with devices in Cloud B. (See Figure 3.)

Figure 3 Connecting Private Networks across an Untrusted Link

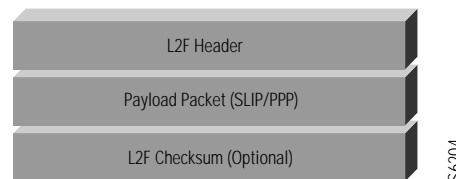


Advantages of encapsulating PPP frames include:

- L2F is insensitive to the protocol carried within the PPP frames and, therefore, can support multiple protocols
- The end systems communicating via the L2F tunnel can employ the same authentication procedures as if they were directly connected and, therefore, can be assured with a high level of confidence that the end systems have been authenticated

The specific details of the L2F protocol can be obtained from the draft RFC. In summary, L2F describes a series of messages that are exchanged between the tunnel endpoints, a format for the exchange of messages, and user data. Figure 4 shows the structure on an L2F packet.

Figure 4 Structure of an L2F Packet



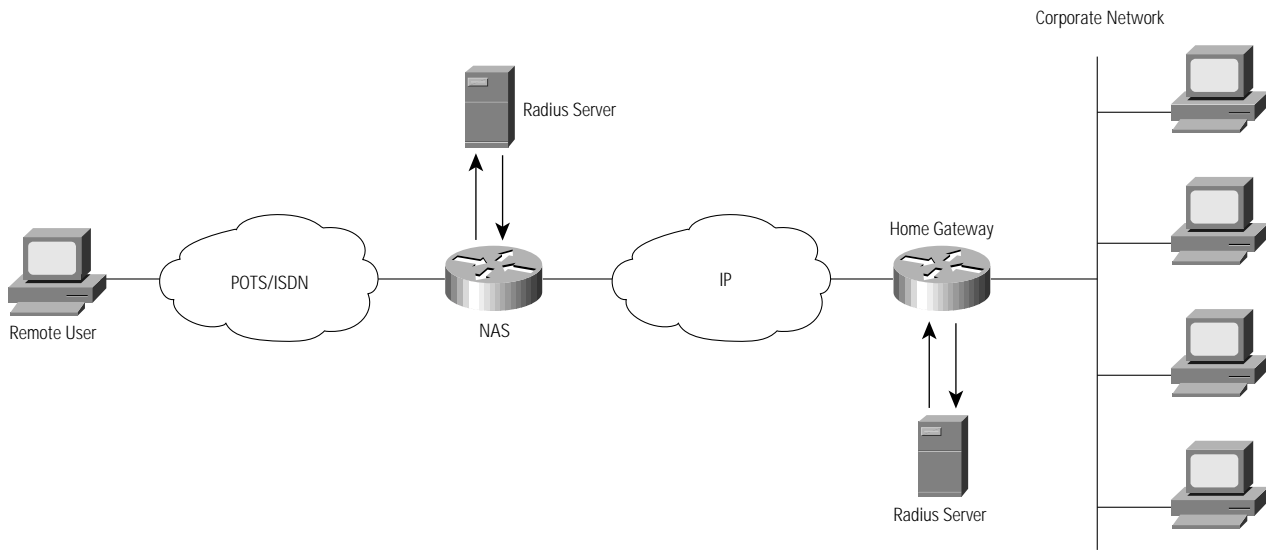
### RADIUS and L2F Interaction

In the vernacular used to describe L2F, the remote user (client or router) dials into a NAS. The NAS establishes a tunnel (or uses an existing tunnel) to communicate with the home gateway. For example, the home gateway is the router located at the corporate headquarters. The remote user now effectively has a PPP session with the home gateway as shown in Figure 5.

RADIUS and L2F overlap because:

- The home gateway must authenticate the remote user by applying the techniques provided by PPP, namely PAP or CHAP.
- The NAS must identify the appropriate tunnel for the particular remote user.
- The NAS and the home gateway (the two endpoints of the tunnel) must authenticate each other.

Figure 5 Client, NAS, Cloud, and Home Gateway



55861

As described previously, RADIUS is a client/server protocol that is used to obtain information that in turn can be used to authenticate (and authorize) a user wanting to gain access to network resources. In the L2F scenario described herein, the home gateway can query a RADIUS server (located deeper within the corporate network, for example) to determine whether user = user@bigcompany can be authenticated (via CHAP or PAP) and can be authorized to start a PPP session with the appropriate Network Control Programs (NCPs) (for example, an IP control point [CP] and an IPX CP). This scenario describes the normal use of the RADIUS protocol. In summary, the home gateway captures the remote user's name (user@bigcompany) and, in the case of CHAP, the response (from the remote user) to the CHAP challenge. This information (using an Access-Request) is sent to the RADIUS server. The server responds with an Access-Reject or an Access-Accept, along with a series of attribute/value pairs that allow the NAS to determine which services are authorized for that user.

To identify the appropriate tunnel for the remote user, the NAS queries the RADIUS server with the "name user = bigcompany" query. (In other words, the NAS strips off "user" before passing the username to the RADIUS server.) This RADIUS server is typically located in a telco or ISP network and is not the same as the RADIUS server within the corporate network. The RADIUS server uses the vendor-specific attribute (attribute 26) to convey the authorization to start a tunnel as well as the information describing the endpoint of the tunnel (cisco-avpair="vpdn:ip addresses=a.b.c.d" in RADIUS-speak), the name to be used when authenticating the tunnel (cisco-avpair="vpdn:tunnel-id=nas-name"), and information to authenticate the tunnel (cisco-avpair="vpdn:nas-password =mumble" and cisco-avpair="vpdn:gw-password =grumble"). Attribute 26 is used so that the L2F information can be communicated to the NAS in a syntax that a Cisco router will understand. User = bigcompany is used rather than user = user@bigcompany so that all users associated with bigcompany can establish

tunnels with the home gateway without the telco's (or ISP's) RADIUS server needing distinct entries for every user at bigcompany.

To support the NAS and home gateway mutual authentication, the NAS uses the information it received when it queried the RADIUS server with user = bigcompany to authenticate its side of the tunnel. The tunnel is authenticated using the same procedures that are used when using CHAP with PPP. In other words, the NAS must issue a challenge to the home gateway and verify the response that the home gateway sends. This scenario represents normal use of RADIUS and does not pose any particular challenge for RADIUS. In addition, the NAS must respond correctly to the challenge issued by the home gateway. This part poses a severe problem when using RADIUS because the NAS needs access to the clear text version of the password associated with the home gateway. Because RADIUS packets are not encrypted, the RADIUS protocol is not well suited as a means to pass clear text passwords around. However, the use of the Cisco-specific attributes (vpdn:nas-password and vpdn:gw-password) provides a workaround for the NAS.

The home gateway faces the same problem as the NAS when authenticating the tunnel; that is, the home gateway must formulate a challenge and check the validity of the responses, as well as respond to the challenge issued by the NAS. As discussed previously, the first part can be supported by the RADIUS protocol, and the second part is problematical. In current Cisco IOS implementations, the home gateway cannot use RADIUS to authenticate the tunnel. The home gateway must use TACACS+ or have access to the information locally (that is, manually

configured on the home gateway). Once the tunnel has been established, the home gateway can use RADIUS to authenticate the remote user (user@bigcompany).

### Support for Token Cards

Each token card vendor has developed its own method for interacting with RADIUS. Typically this scenario has taken the form of specifically modified versions of RADIUS that call the token card server when they encounter authentications with special keywords in the password field. For instance, Security Dynamics and Ascend created a version of the RADIUS server that recognizes a special password, "securid." If the server encounters a user with that password, it passes the authentication information off to the Security Dynamics server, and the response from that server back to the NAS<sup>1</sup>. Cisco can now interoperate with this and several other modified RADIUS servers to provide token card support. When CiscoSecure 2.0 RADIUS server support is released, it will interoperate with servers from Security Dynamics and Enigma Logics, as well as provide onboard support for CryptoCard, which Cisco will OEM.

### Future RADIUS Enhancements

Cisco continues to enhance support for RADIUS in Cisco IOS software. Some planned enhancements to the RADIUS support in Cisco IOS software include support for additional IETF standard attributes, as well as support for those vendor proprietary attributes that make sense in the context of Cisco NAS implementations. As these features are added to Cisco IOS software, information on their configuration and interoperability will be made available in the appropriate software configuration guides.

Also, as previously noted, Cisco will soon release an enhanced version of the CiscoSecure access control server that will support RADIUS. These two components will work together to offer a comprehensive solution to the problems presented by increasingly important and complex remote access challenges.

### Comparisons of RADIUS and TACACS+

RADIUS is just one protocol that provides authentication and accounting functions for dialin services. Another widely deployed protocol is TACACS+, which is the latest evolution

of the Cisco TACACS protocol. Although these protocols provide similar functionality, they have several key differences.

#### Transport Mechanism

The most fundamental difference between TACACS+ and RADIUS is the network transport protocol that each uses. The RADIUS protocol uses UDP to exchange information between the NAS and the access control server, whereas TACACS+ uses Transmission Control Protocol (TCP).

TCP is a connection-oriented transport protocol, whereas UDP offers best-effort delivery. RADIUS utilizes additional, programmable variables to control issues such as retransmit attempts and timeouts in order to compensate for the best-effort transport provided by UDP. TACACS+, using TCP transport, does not need these extra variables, because connection issues are handled transparently by the TCP protocol.

Using TCP provides a separate acknowledgment, via a TCP acknowledgment packet, that a request has been received by the access control server within an approximate network round-trip time. This acknowledgment occurs regardless of the congestion of the access control server.

TCP provides immediate indication of an unavailable server. Long-lived TCP connections will even reveal servers that go down and then come back up. UDP is unable to discriminate between a down server, a slow server, and a nonexistent server.

Using TCP keepalives, server crashes can be detected out of band with actual requests. Connections to multiple servers can be maintained simultaneously, and messages need to be sent only to servers that are known to be up and running. TCP provides a stable foundation that efficiently adapts to growing as well as congested networks.

#### Confidentiality

RADIUS encrypts only the password in the Access-Request packet from the client to the server. The remainder of the packet is in the clear. Other information such as username, authorized services, and accounting could be captured by a third party, making RADIUS networks potential targets of hackers using session capture and replay attacks. Because of this inherent openness, RADIUS networks must be carefully designed to minimize the opportunities for attack.

1. Because the RADIUS server stores its passwords in the clear, it will fail unexpectedly if a user with a clear text password sets it to "securid." The RADIUS server will attempt to authenticate the user via the token card server, and the authentication will fail.

TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header. Within the header is a field that indicates whether or not the body is encrypted. Normal operation fully encrypts the body of the packet for more secure communications.

#### **Distribution of Functionality**

The RADIUS protocol combines the processes of authentication and authorization. The Access-Accept packets sent by the RADIUS server to the client contain all the authorization information, making separation of the authentication and authorization functions difficult. The use of RADIUS is most appropriate when simple, single-step authentication and authorization is required, as with most service provider networks.

TACACS+ uses the AAA architecture, which separates authentication, authorization, and accounting. This setup allows separate authentication solutions that can still use TACACS+ for authorization and accounting. For example, using TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. After a network access server authenticates to a Kerberos server, it requests authorization information from a TACACS+ server without having to reauthenticate. The NAS informs the TACACS+ server that it has successfully authenticated on a Kerberos server, and the server then provides authorization information.

During a session, if additional authorization checking is needed, the access server checks with a TACACS+ server to determine if the user is granted permission to use a particular command. This feature provides greater control over the commands that can be executed on the access server while decoupling authorization from the authentication mechanism. TACACS+ is thus more appropriate to use when

multiple authentications in a complex network environment are anticipated. This scenario occurs, for example, inside most large corporate networks.

Because network security is exploding with many different competing solutions, the most scalable architecture must separate the AAA functionality and open the door to future options.

#### **Multiprotocol Support**

RADIUS has limited support for protocols other than TCP/IP. For example, RADIUS does not natively support the following protocols:

- AppleTalk Remote Access (ARA)
- NetBIOS frame protocol control
- Novell Asynchronous Services Interface (NASI)
- Packet assembler/disassembler (PAD) connection

These protocols are natively supported by TACACS+.

#### **Cisco IOS Software Provides Users the Choice of Which Protocols to Use**

Cisco has supported the RADIUS protocol since Cisco IOS Release 11.1 in February 1996. RADIUS support in Cisco IOS software continues to be enhanced with new features and capabilities. Cisco is committed to supporting RADIUS as a standard. Cisco's access servers are unique in that they implement both RADIUS and TACACS+.

#### **Configuring RADIUS to Use**

##### **TACACS+ Attribute/Value Pairs**

The RADIUS protocol specifies a method by which special information not specifically defined as an attribute by the RADIUS specification can be transmitted. The vendor-specific attribute, number 26, can be configured to exchange any desired string of characters. Through the use of this variable, all the TACACS+ attribute/value pairs can be exchanged in a RADIUS environment. The TACACS+ information is passed in the following format:

```
ciscoav = "attribute=value"
```

## The TACACS+ IETF Informational Internet Draft

Cisco is committed to open standards and continues to lead the industry in standards development. In October 1996, the IETF published Version 1.75 of the TACACS+ protocol specification as an informational Internet draft. The text of the IETF document can be found at the following URL:

```
ftp://ftp.ietf.cnri.reston.va.us/  
internet-drafts/draft-grant-tacacs-00.txt.
```



### Corporate Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
World Wide Web URL:  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

### European Headquarters

Cisco Systems Europe s.a.r.l.  
Parc Evolic-Batiment L1/L2  
16, Avenue du Quebec  
BP 706-Villebon  
91961 Courtaboeuf Cedex  
France  
Tel: 33 1 6918 61 00  
Fax: 33 1 6928 83 26

### Americas

**Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
Tel: 408 526-7660  
Fax: 408 526-4646

### Asia Headquarters

Nihon Cisco Systems K.K.  
Fuji Building  
3-2-3 Marunouchi  
Chiyoda-ku, Tokyo 100  
Japan  
Tel: 81 3 5219 6000  
Fax: 81 3 5219 6010

**Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco Connection Online Web site at <http://www.cisco.com>.**

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China (PRC) • Colombia • Costa Rica • Czech Republic • Denmark  
Finland • France • Germany • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Malaysia • Mexico  
The Netherlands • New Zealand • Norway • Philippines • Poland • Portugal • Russia • Singapore • South Africa • Spain • Sweden  
Switzerland • Taiwan, ROC • Thailand • United Arab Emirates • United Kingdom • Venezuela