Configurable CHAP Challenge Length

The Configurable Challenge Handshake Authentication Protocol (CHAP) Challenge Length feature allows you to configure the length of the CHAP challenge by specifying the minimum and maximum allowable challenge lengths in bytes.

Prerequisites for Configurable CHAP Challenge Length

The PPP encapsulation must be configured on the interface.

Information About Configurable CHAP Challenge Length

Configurable CHAP Challenge Length Overview

Challenge Handshake Authentication Protocol (CHAP) along with PPP is used to provide remote-device information to the central site. It verifies the identity of the peer by means of a three-way handshake.

When CHAP is enabled on any interface that supports PPP encapsulation, and a remote device attempts to connect to it, the local device or the access server sends a CHAP packet to the remote device. The CHAP packet requests or “challenges” the remote device to respond.

By default, the CHAP challenge is sent with a fixed 16-byte length to the peer. The Configurable CHAP Challenge Length feature allows the configuration of variable CHAP challenge lengths. A variable challenge length reduces the probability of an attacker predicting the challenge, thus optimizing the security.

Use the **ppp chap challenge-length** command to configure the CHAP challenge lengths.

How to Configure Configurable CHAP Challenge Length

Configuring Configurable CHAP Challenge Length

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **ppp authentication chap**
5. **ppp chap challenge-length** *min-length max-length*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **Example:** `Device(config)# interface virtual-template 1`	Creates a virtual template interface and enters interface configuration mode. The range is from 1 to 4095.
Step 4	**ppp authentication chap** **Example:** `Device(config-if)# ppp authentication chap`	Enables CHAP authentication.
Step 5	**ppp chap challenge-length** *min-length max-length* **Example:** `Device(config-if)# ppp chap challenge-length 20 30`	Configures the minimum and maximum CHAP challenge lengths in bytes. The range is from 16 to 63.
Step 6	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for Configurable CHAP Challenge Length

Example: Configuring Configurable CHAP Challenge Length

The following example shows how to configure the Challenge Handshake Authentication Protocol (CHAP) challenge lengths:

```
Device> enable
Device# configure terminal
Device(config)# interface virtual-template 1
Device(config-if)# ppp authentication chap
Device(config-if)# ppp chap challenge-length 20 30
Device(config-if)# end
```

Additional References for Configurable CHAP Challenge Length

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
PPP commands	Dial Technologies Command Reference
Wide-area networking commands	Wide-Area Networking Command Reference

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configurable CHAP Challenge Length

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Configurable CHAP Challenge Length

Feature Name	Releases	Feature Information
Configurable CHAP Challenge Length	Cisco IOS XE Release 3.12S	The Configurable Challenge Handshake Authentication Protocol (CHAP) feature allows you to configure the length of the CHAP challenge by specifying the minimum and maximum allowable challenge length in bytes. The following command was introduced: **ppp chap challenge-length**.