PPP Configuration Options

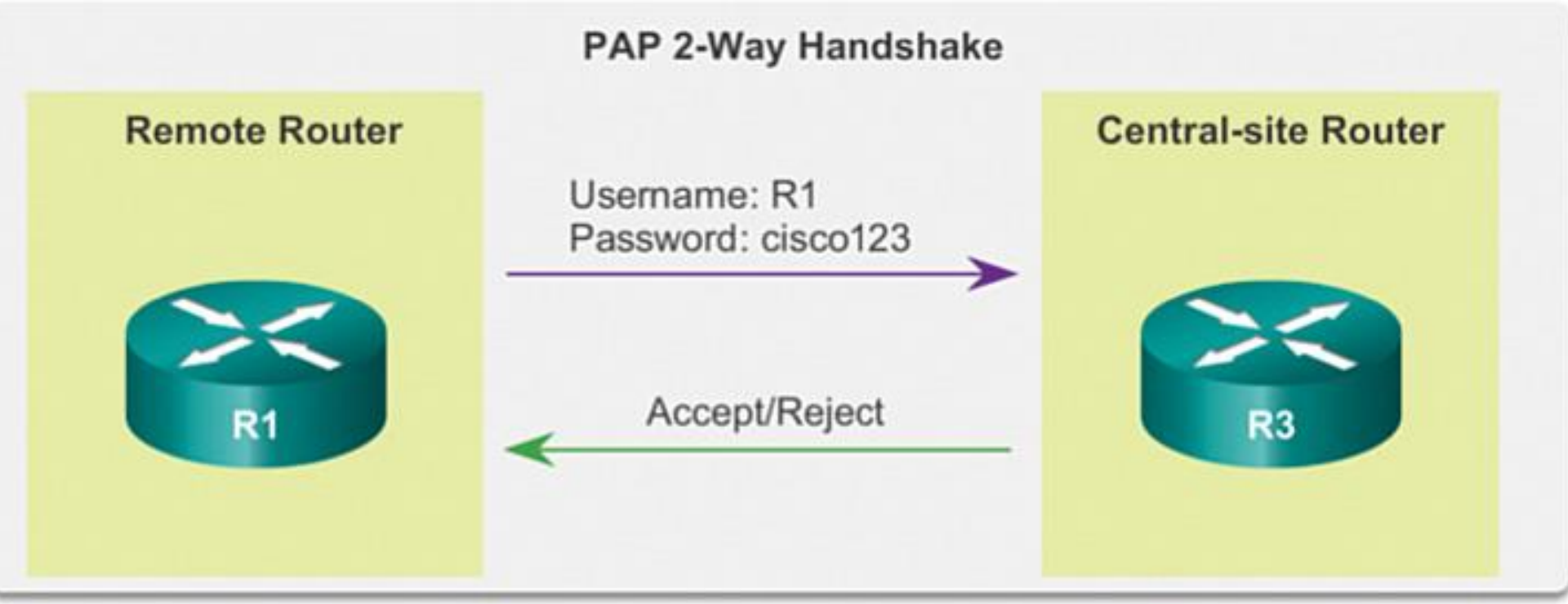
PPP Configuration Options

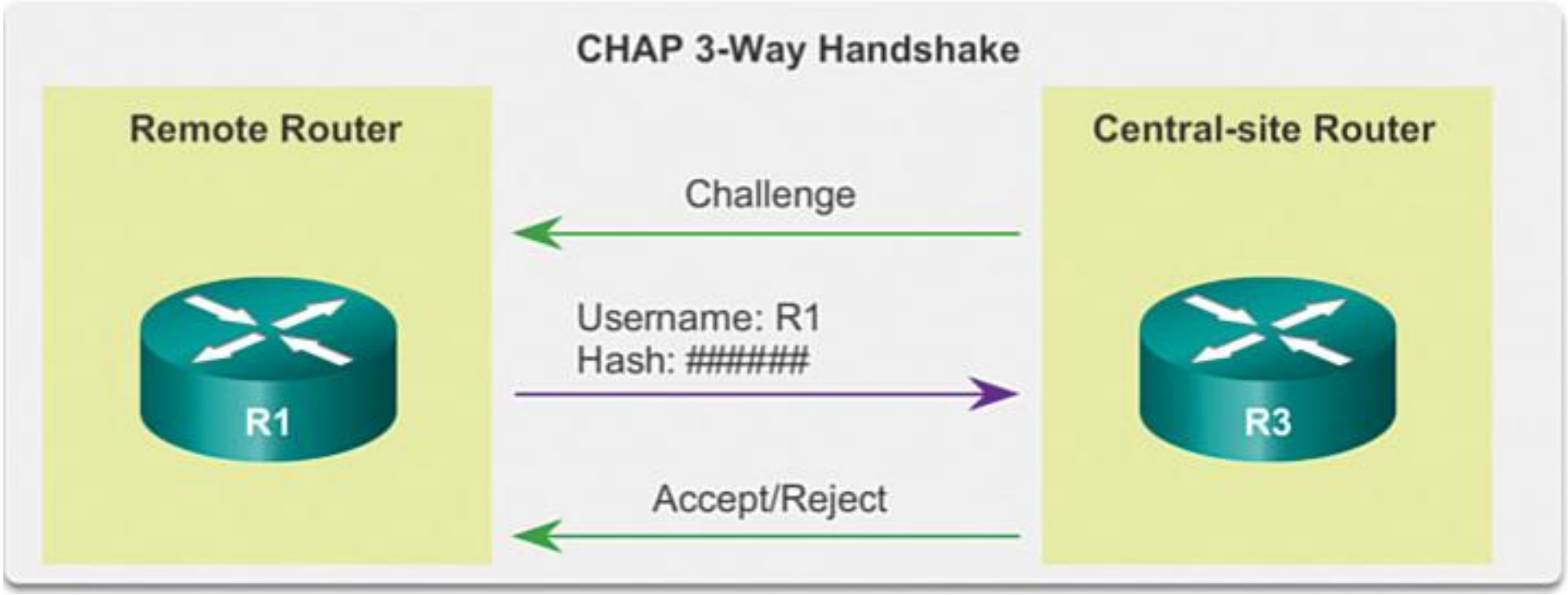
- PPP can be configured to support various functions including:

- Authentication using either PAP or CHAP
- Compression using either Stacker or Predictor
- Multilink which combines two or more channels to increase the WAN bandwidth.

PAP Authentication Protocol

- PPP defines an extensible LCP that allows negotiation of an authentication protocol for authenticating its peer before allowing Network layer protocols to transmit over the link. RFC 1334 defines two protocols for authentication, as shown in the figure.


PAP 2-Way Handshake
Remote Router
Central-site Router
Username: R1
Password: cisco123
R1
R3
Accept/Reject


CHAP 3-Way Handshake
Remote Router
Central-site Router
Challenge
Username: R1
Hash: #######
Accept/Reject
R1
R3

- **PAP** is a very basic two-way process. There is no encryption-the username and password are sent in plain text. If it is accepted, the connection is allowed.
- **CHAP** is more secure than PAP. It involves a three-way exchange of a shared secret.

- The authentication phase of a PPP session is optional. If used, you can authenticate the peer after the LCP establishes the link and choose the authentication protocol. If it is used, authentication takes place before the Network layer protocol configuration phase begins.

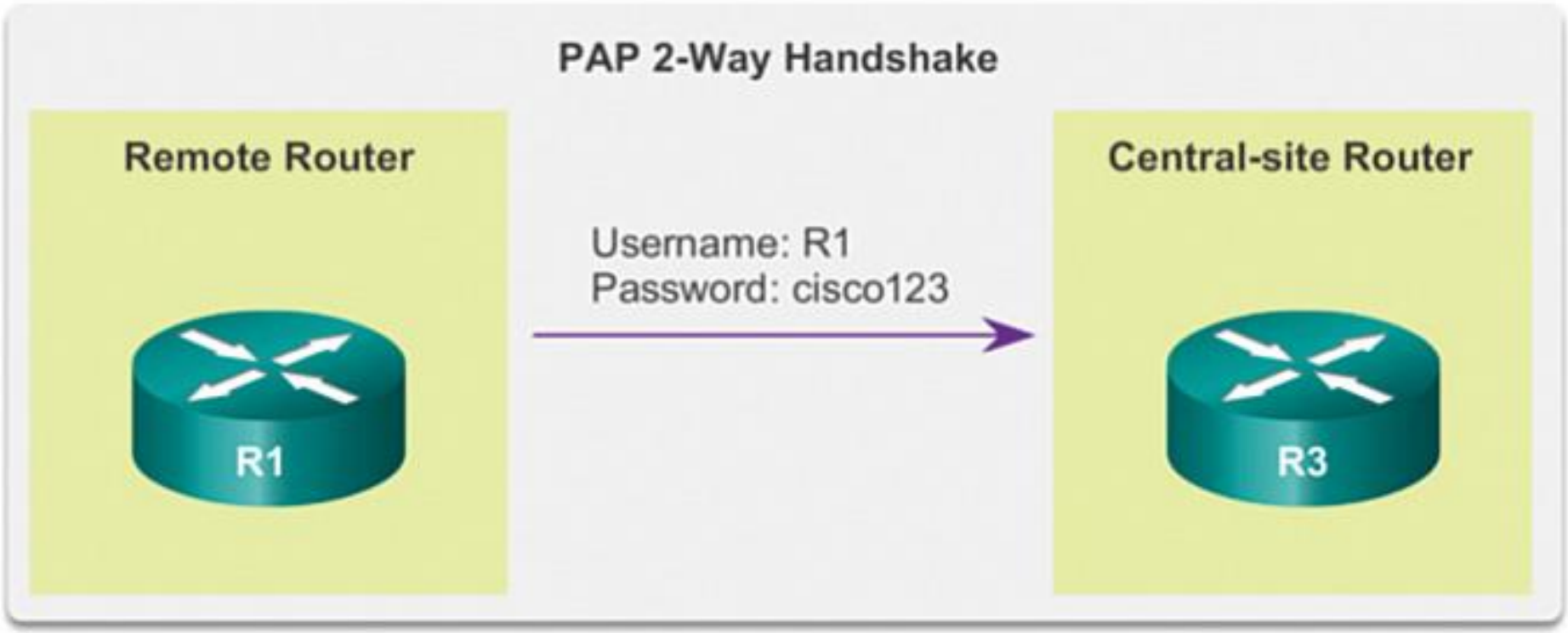
- The authentication options require that the calling side of the link enter authentication information. This helps to ensure that the user has the permission of the network administrator to make the call. Peer routers exchange authentication messages.

- One of the many features of PPP is that it performs Layer 2 authentication in addition to other layers of authentication, encryption, access control, and general security procedures.

Initiating PAP

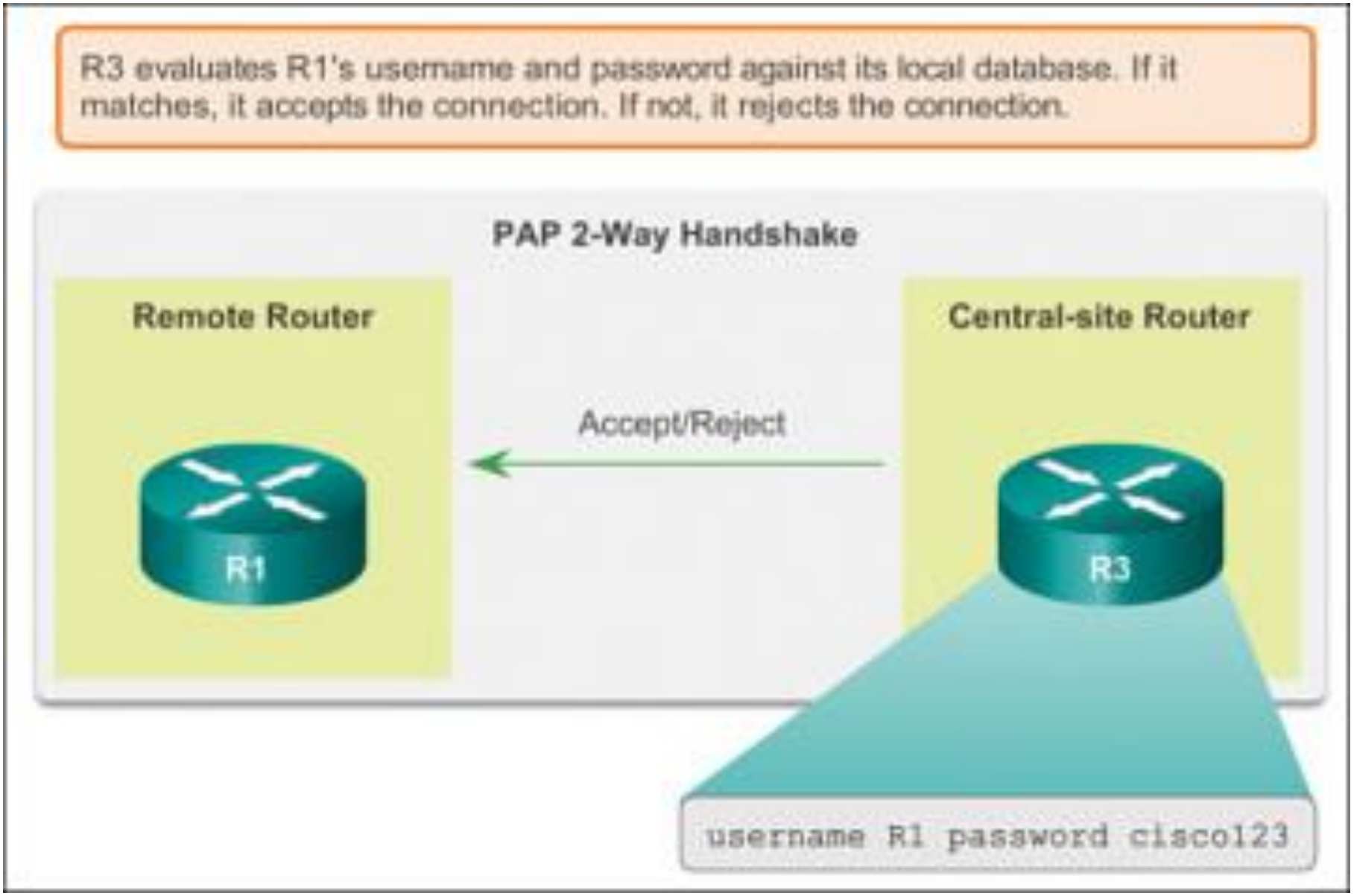
- PAP provides a simple method for a remote node to establish its identity using a two-way handshake. PAP is not interactive. When the ppp authentication pap command is used, the username and password are sent as one LCP data package, rather than the server sending a login prompt and waiting for a response.
- The figure shows that after PPP completes the link establishment phase, the remote node repeatedly sends a username-password pair across the link until the receiving node acknowledges it or terminates the connection.

R1 sends its PAP username and password to R3.



At the receiving node, the username-password is checked by an authentication server that either allows or denies the connection. An accept or reject message is returned to the requester.

R3 evaluates R1's username and password against its local database. If it matches, it accepts the connection. If not, it rejects the connection.



PAP is not a strong authentication protocol. Using PAP, you send passwords across the link in clear text and there is no protection from playback or repeated trial-and-error attacks. The remote node is in control of the frequency and timing of the login attempts.

- Nonetheless, there are times when using PAP can be justified. For example, despite its shortcomings, PAP may be used in the following environments:

- A large installed base of client applications that do not support CHAP
- Incompatibilities between different vendor implementations of CHAP
- Situations where a plaintext password must be available to simulate a login at the remote host

Challenge Handshake Authentication Protocol (CHAP)

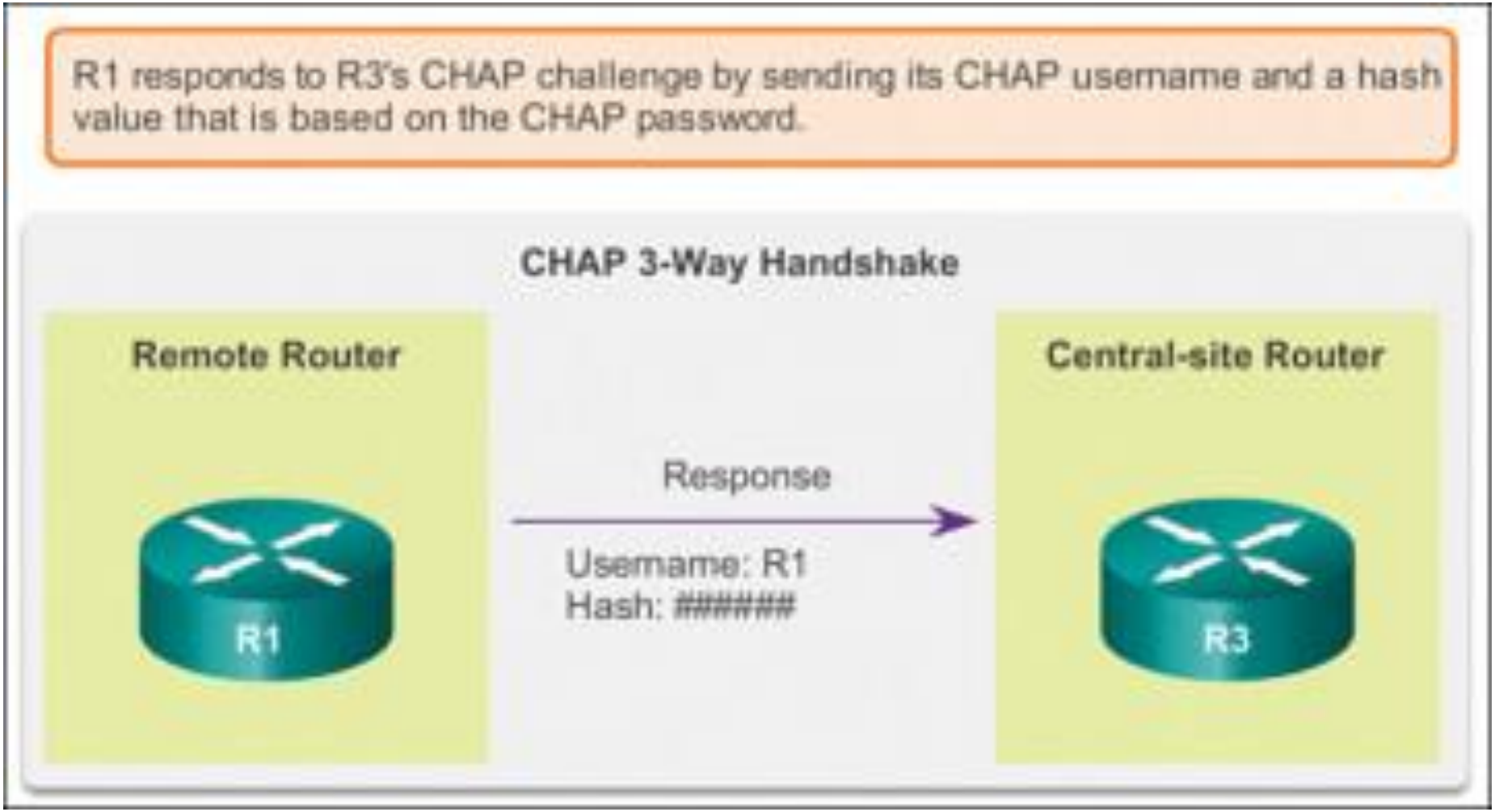
- Once authentication is established with PAP, it essentially stops working. This leaves the network vulnerable to attack. Unlike PAP, which only authenticates once, CHAP conducts periodic challenges to make sure that the remote node still has a valid password value.

- After the PPP link establishment phase is complete, the local router sends a challenge message to the remote node.


R3 initiates the 3-way handshake and sends a challenge message to R1.
CHAP 3-Way Handshake
Remote Router
Central-site Router
Challenge
R1
R3

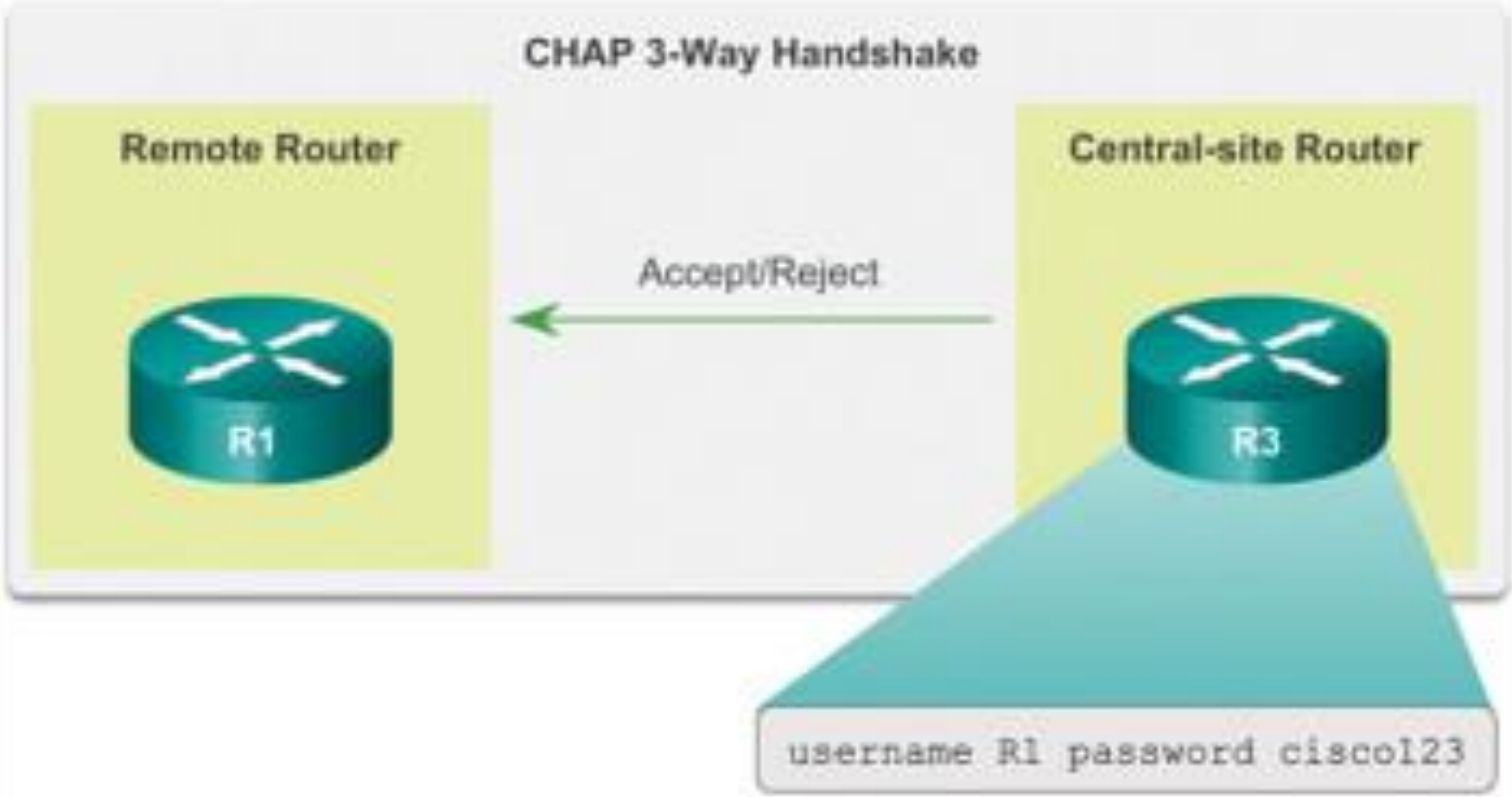
- The remote node responds with a value calculated using a one-way hash function, which is typically Message Digest 5 (MD5) based on the password and challenge message.

R1 responds to R3's CHAP challenge by sending its CHAP username and a hash value that is based on the CHAP password.



- The local router checks the response against its own calculation of the expected hash value. If the values match, the initiating node acknowledges the authentication. Otherwise, it immediately terminates the connection.

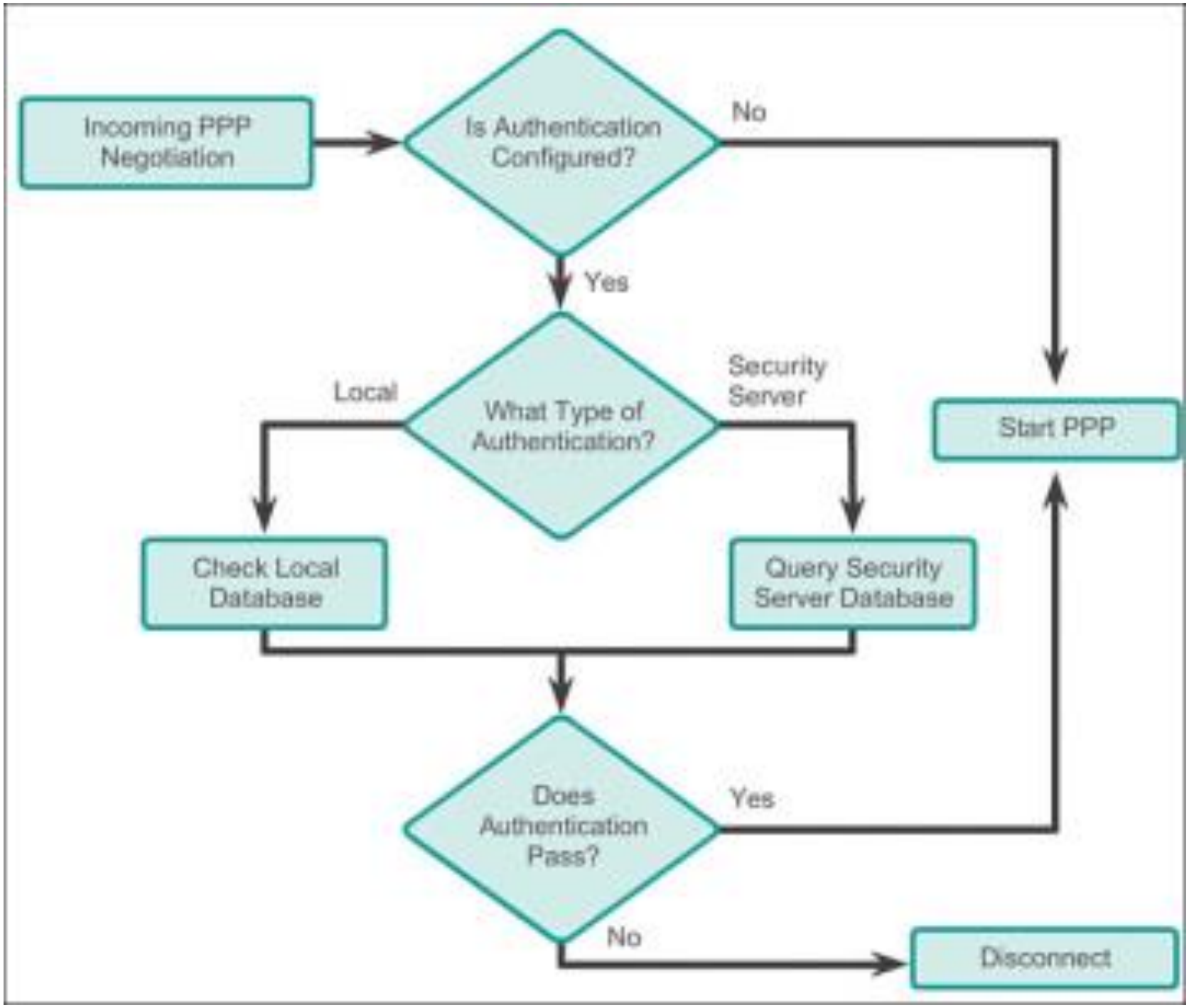
Using the username and password for R1 in it's local database, R3 compares its calculated hash value with the one sent from R1.



- CHAP provides protection against playback attack by using a variable challenge value that is unique and unpredictable. Because the challenge is unique and random, the resulting hash value is also unique and random. The use of repeated challenges limits the time of exposure to any single attack.

PPP Encapsulation and Authentication Process

- You can use a flowchart to help understand the PPP authentication process when configuring PPP. The flowchart provides a visual example of the logic decisions made by PPP.


Incoming PPP Negotiation
Is Authentication Configured?
No
Yes
Local
What Type of Authentication?
Security Server
Start PPP
Check Local Database
Query Security Server Database
Does Authentication Pass?
Yes
No
Disconnect

- For example, if an incoming PPP request requires no authentication, then PPP progresses to the next level. If an incoming PPP request requires authentication, then it can be authenticated using either the local database or a security server. As illustrated in the flowchart, successful authentication progresses to the next level, while an authentication failure will disconnect and drop the incoming PPP request.

Example

- Router R1 wishes to establish an authenticated PPP CHAP connection with Router R2.

- **Step 1**. R1 initially negotiates the link connection using LCP with router R2 and the two systems agree to use CHAP authentication during the PPP LCP negotiation.

- **Step 2**. Router R2 generates an **ID** and a **random number** and sends that plus its username as a CHAP challenge packet to R1.

- **Step 3**. R1 will use the username of the challenger (R2) and cross reference it with its local database to find its associated password. R1 will then generate a unique MD5 hash number using the ID, random number and the shared secret password.

- **Step 4**. Router R1 then sends the challenge ID, the hashed value, and its username (R1) to R2.

- **Step 5**. R2 generates it own hash value using the ID, the shared secret password, and the random number it originally sent to R1.

- **Step 6**. R2 compares its hash value with the hash value sent by R1. If the values are the same, R2 sends a link established response to R1.

- If the authentication failed, a CHAP failure packet is built from the following components:

- 04 = CHAP failure message type
- id = copied from the response packet
- "Authentication failure" or some such text message, which is meant to be a user-readable explanation

- Note that the shared secret password must be identical on R1 and R2.

Configuring PPP Authentication

- The figure is an example of a two-way PAP authentication configuration. Both routers authenticate and are authenticated, so the PAP authentication commands mirror each other. The PAP username and password that each router sends must match those specified with the **username** *name* **password** *password* command of the other router.

PAP Authentication Configuration


```
hostname R1
username R3 password samecne
!
interface serial 0/0/0
ip address 128.0.1.1 255.255.255.252
encapsulation ppp
ppp authentication PAP
ppp pap sent-username R1 password samecne
```

```
hostname R3
username R1 password samecne
!
interface serial 0/0/0
ip address 128.0.1.2 255.255.255.252
encapsulation ppp
ppp authentication PAP
ppp pap sent-username R3 password samecne
```

A sample PAP configuration.

- CHAP periodically verifies the identity of the remote node using a three-way handshake. The hostname on one router must match the username the other router has configured. The passwords must also match. This occurs on initial link establishment and can be repeated any time after the link has been established. The figure is an example of a CHAP configuration.

CHAP Authentication Configuration


```
hostname R1
username R3 password samecode
!
interface serial 0/0/0
ip address 128.0.1.1 255.255.255.252
encapsulation ppp
ppp authentication CHAP
```

```
hostname R3
username R1 password samecode
!
interface serial 0/0/0
ip address 128.0.1.2 255.255.255.252
encapsulation ppp
ppp authentication CHAP
```

A sample CHAP configuration.