Type text to search here...

Home > Point to Point Protocol (PPP) Tutorial

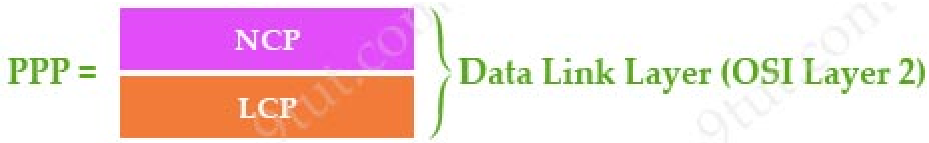
Point to Point Protocol (PPP) Tutorial

March 11th, 2016 Go to comments

Note: The Point-to-Point Protocol is not a topic in CCNA 200-301 so if you are preparing for this exam you can ignore this tutorial.

Point-to-Point Protocol (PPP) is an open standard protocol that is mostly used to provide connections over point-to-point serial links. The main purpose of PPP is to transport Layer 3 packets over a Data Link layer point-to-point link. PPP can be configured on:
+ Asynchronous serial connection like Plain old telephone service (POTS) dial-up
+ Synchronous serial connection like Integrated Services for Digital Network (ISDN) or point-to-point leased lines.

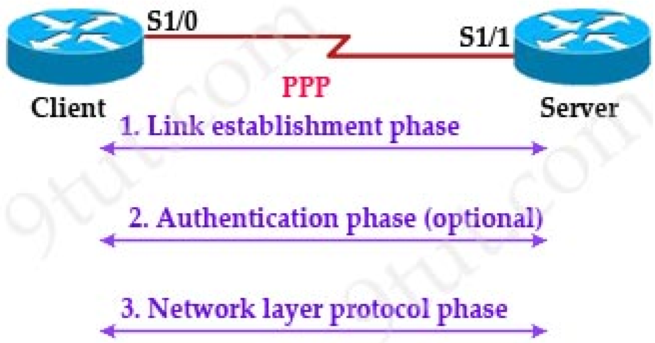
PPP consists of two sub-protocols:
+ **Link Control Protocol** (LCP): set up and negotiate control options on the Data Link Layer (OSI Layer 2). After finishing setting up the link, it uses NCP.
+ **Network control Protocol** (NCP): negotiate optional configuration parameters and facilitate for the Network Layer (OSI Layer 3). In other words, it makes sure IP and other protocols can operate correctly on PPP link



Establish a PPP session

Before a PPP connection is established, the link must go through three phases of session establishment:

1. **Link establishment phase**: In this phase, each PPP device sends LCP packets to configure and test the data link
2. **Authentication phase** (optional): If authentication is enabled, either PAP or CHAP will be used. PAP and CHAP are two authentication protocols used in PPP
3. **Network layer protocol phase**: PPP sends NCP packets to choose and configure Network Layer protocol (OSI Layer 3) to be encapsulated and sent over the PPP data link


S1/0
S1/1
PPP
Client
Server
1. Link establishment phase
2. Authentication phase (optional)
3. Network layer protocol phase

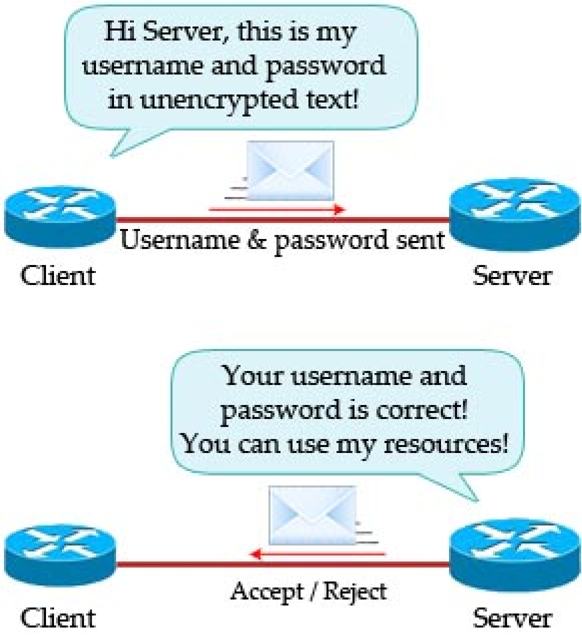
Note: The default serial encapsulation on Cisco routers is HDLC so if you want to use PPP you have to configure it. Unlike HDLC which is a Cisco proprietary protocol, PPP is an open standard protocol so you should use it to connect a Cisco router to a non-Cisco router

PPP Authentication Methods

In this part we will learn more about two authentication methods used in Authentication Phase of PPP.

PPP has two built-in security mechanisms which are **Password Authentication Protocol** (PAP) and **Challenge Handshake Authentication Protocol** (CHAP).

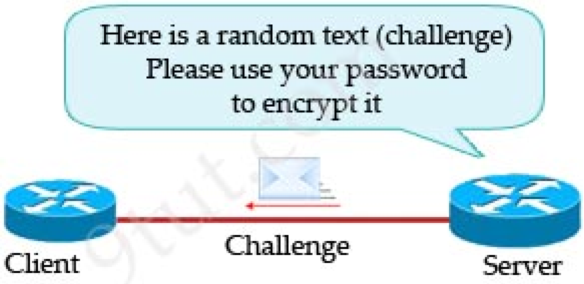
Password Authentication Protocol (PAP) is a very simple authentication protocol. The client who wants to access a server sends its username and password in clear text. The server checks the validity of the username and password and either accepts or denies connection. This is called two-way handshake. In PAP two-way handshake process, the username and password are sent in the first message.


Hi Server, this is my username and password in unencrypted text!
Client
Username & password sent
Server
Your username and password is correct! You can use my resources!
Client
Accept / Reject
Server

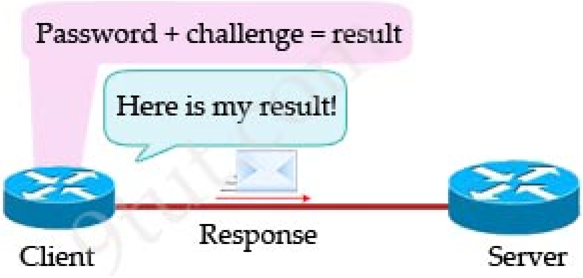
PAP two-way handshake

For those systems that require greater security, PAP is not enough as a third party with access to the link can easily pick up the password and access the system resources. In this case CHAP can save our life!

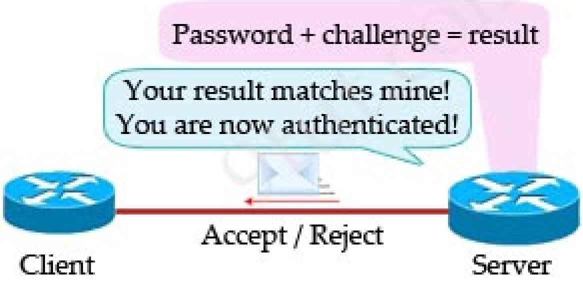
Challenge Handshake Authentication Protocol (CHAP) is an PPP authentication protocol which is far more secure than PAP. Let’s see how CHAP three-way handshake works:


Here is a random text (challenge) Please use your password to encrypt it
Client
Challenge
Server

With CHAP, the protocol begins (after the LCP phase is complete) with a random text (called a challenge) sent from the Server, which asks the Client to authenticate.



After receiving the challenge, the Client uses its password to perform a one-way hash algorithm (MD5) to encrypt the random text received from the server. The result is then sent back to the Server. Therefore even if someone can capture the messages between client and server, he cannot know what the password is.


Password + challenge = result
Your result matches mine!
You are now authenticated!
Client
Accept / Reject
Server

At the Server side, the same algorithm is used to generate its own result. If the two results match, the passwords must match too.

The main difference between PAP and CHAP is PAP sends username and password in clear text to the server while CHAP does not. Notice that in CHAP authentication process, the password itself is never sent across the link.

Another difference between these two authentication protocols is PAP performs authentication at the initial link establishment only while CHAP performs authentication at the initial link establishment and periodically after that. The challenge text is random and unique so the "result" is also unique from time to time. This prevents playback attack (in which a hacker tries to copy the "result" text sent from Client to reuse).

CHAP Summary:
+ CHAP is defined as a one-way authentication method. However, you use CHAP in both directions to create a two-way authentication. Hence, with two-way CHAP, a separate three-way handshake is initiated by each side.
+ In the Cisco CHAP implementation, by default, the called party must authenticate the calling party. The protocol begins with a random text (called a challenge) sent from the Server, which asks the Client to authenticate

In the next part we will learn how to configure PAP and CHAP for PPP.

Pages: 1 2
Comments (2) Comments

1. Mat: question from Khanh
   January 8th, 2020

   Hi,

   "I am trying to cofigure PPP CHAP on Cisco Tracer, I got above errors, could you please tell me what was wrong? Thanks"
   you have got a problem with the above situation because you were using there an interface g0/0 not serial that is dedicated under PPP protocol.

BR,
Mat

2. abdikadir
   August 9th, 2020

   hi mat,
   interface g0/0 is an ethernet interface and ppp is used for serial interface only so if u want configure ppp on the router , u need to do that on serial interface.

Add a Comment

Name

Submit Comment

Subscribe to comments feed
Checking Lab Challenge 3 (VTP, STP, EtherChannel) WAN Tutorial

Premium Member Zone

Welcome Gurjeet singh!

- Welcome Premium Member
- CCNA – New Questions Part 5
- CCNA – New Questions Part 6
- CCNA – New Questions Part 7
- CCNA – New Questions Part 8
- CCNA – New Questions Part 9
- Composite Quizzes

- Logout

CCNA 200-301

- Basic Questions
- Topology Architecture Questions
- Cloud & Virtualization Questions
- CDP & LLDP Questions
- Switch Questions
- VLAN & Trunking Questions
- VLAN & Trunking Questions 2
- STP & VTP Questions
- EtherChannel Questions
- TCP & UDP Questions
- IP Address & Subnetting Questions
- IP Routing Questions

- IP Routing Questions 2
- OSPF Questions
- OSPF Questions 2
- EIGRP Questions
- NAT Questions
- NTP Questions
- Syslog Questions
- HSRP Questions
- Access-list Questions
- AAA Questions
- Security Questions
- Security Questions 2
- DAI Questions
- IPv6 Questions
- DNS Questions
- QoS Questions
- Port Security Questions
- Wireless Questions
- Wireless Questions 2
- SDN Questions
- DNA Center Questions
- Drag Drop Questions
- Drag Drop Questions 2
- Drag Drop Questions 3
- VPN Questions
- DHCP Questions
- Automation Questions
- Miscellaneous Questions
- CCNA FAQs & Tips
- Share your new CCNA Experience

CCNA Self-Study

- Practice CCNA GNS3 Labs
- CCNA Knowledge
- CCNA Lab Challenges
- Puppet Tutorial
- Chef Tutorial
- Ansible Tutorial
- JSON Tutorial
- Layer 2 Threats and Security Features
- AAA TACACS+ and RADIUS Tutorial
- STP Root Port Election Tutorial
- GRE Tunnel Tutorial
- Basic MPLS Tutorial
- TCP and UDP Tutorial
- Border Gateway Protocol BGP Tutorial
- Point to Point Protocol (PPP) Tutorial
- WAN Tutorial
- DHCP Tutorial
- Simple Network Management Protocol SNMP Tutorial
- Syslog Tutorial
- Gateway Load Balancing Protocol GLBP Tutorial
- EtherChannel Tutorial
- Hot Standby Router Protocol HSRP Tutorial
- InterVLAN Routing Tutorial
- Cisco Command Line Interface CLI

- Cisco Router Boot Sequence Tutorial
- OSI Model Tutorial
- Subnetting Tutorial – Subnetting Made Easy
- Frame Relay Tutorial
- Wireless Tutorial
- Virtual Local Area Network VLAN Tutorial
- VLAN Trunking Protocol VTP Tutorial
- IPv6 Tutorial
- Rapid Spanning Tree Protocol RSTP Tutorial
- Spanning Tree Protocol STP Tutorial
- Network Address Translation NAT Tutorial
- Access List Tutorial
- RIP Tutorial
- EIGRP Tutorial
- OSPF Tutorial

Network Resources

- Free Router Simulators
  - CCNA Website
  - ENCOR Website
  - ENSDWI Website
  - ENARSI Website
  - DevNet Website
  - CCIE R&S Website
  - Security Website
  - Wireless Website
  - Design Website
  - Data Center Website
  - Service Provider Website
  - Collaboration Website

Top

Site Privacy Policy. Valid XHTML 1.1 and CSS 3.H