This tutorial explains following topics in detail with examples:-

- Overview of PPP Protocol
- Basic concepts of PPP Protocol
- PPP Framing (Encapsulation), LCP and NCP
- PPP Authentication PAP and CHAP
- Differences between PAP and CHAP
- Configure PPP Protocol on Cisco Router
- Configure PPP Authentication
- Configure Both CHAP and PAP in same link
- Verifying PPP Protocol implementation
- Debugging PPP Authentication

**Overview of PPP Protocol**

- PPP was built in 1990 as open standard protocol.
- Since it is based on open standard, it will run with all vendors.
- It works with Asynchronous serial connection, Synchronous serial connection, High-Speed Serial Interfaces (HSSI) and ISDN interfaces (BRI and PRI).
- It provides dynamic addressing, authentication, callback and compression facilities.
- It can encapsulate multiple network layer protocols to pass over the same link.
- It can perform error detection, correction and quality check of link.
- It can build single logical connection over multiple physical connections.

**Basic concepts of PPP Protocol**

PPP is built from three components; Framing, LCP and NCP. In this section we will take a closer look at these components.

**PPP Framing (Encapsulation)**

PPP Framing defines how network layer packets are encapsulated in PPP frame. As we know PPP can carry multiple Layer 3 protocols over a single link. To support multiple network layer protocols PPP uses *Protocol Type* filed in header. Following figure illustrates PPP framing

![PPP Framing Diagram](image)

**LCP (Link Control Protocol)**

This is the second component of PPP. PPP uses it to build and maintain data-link connections. It provides following options:-
**Authentication**:- LCP provides two types of authentication; PAP and CHAP. *(Explained shortly in next section)*

**Compression**:- Through compression LCP increases overall data transmission speed while saving bandwidth at the same time. It compresses data at sending end and decompresses data at receiving end.

**Error Detection**:- LCP uses LQM (Link Quality Monitoring) tool to detect the interface that exceeds threshold error percentage. Once faulty interface is identified, LCP will disable that interface and reroute the traffic from better route.

**Looped Link Detection**:- LCP uses magic number to detect looped link. Once looped link is detected LCP will disable that interface and reroute the traffic over the working link.

**Multilink**:- In this option multiple physical links are combined in a single logical connection at layer three. For example if we have two 64Kbps lines then this option can combine them in such a way that they appear as a single 128Kbps connection at layer 3.

**Call Back** :- In this option remote side router will call back to calling router. For example we have two routers; R1 and R2 with callback enabled. In this case, R1 will connect with R2 and authenticate itself. Once authentication process is completed, R2 will terminate the connection and then re-initiate the connection from its side. This way R1 will be charged only for the data that is used during the authentication process while R2 will be charged for remaining data transmission.

**NCP (Network Control Protocol)**

This is the third component of PPP. PPP uses NCP (Network Control Protocol) to allow multiple Network layer protocols (such as IPv4, IPv6, IPX) to be used in a single point to point connection.

**Exam Tips**

PPP is specified at the physical and Data Link layers only. Don’t confuse with NCP component. NCP component is only used to carry multiple Network Layer protocols simultaneously across the single point to point link. PPP is neither specified as layer 3 protocol nor it works as layer 3 (network layer) protocol.

This tutorial is the third part of our article “WAN Terminology Explained with Encapsulation Protocols and Methods”. You can read other parts of this article here.


This tutorial is the first part of article. This part explains basic wan concepts including terminology, encapsulation methods, switching concepts and encapsulation protocols in detail with example.


This tutorial is the second part of the article. This part explains HDLC (High-Level Data Link Control) protocol and encapsulation method in detail with examples including step by step configuration guide.
PPP Authentication

PPP Authentication is the method of identifying remote device. Through authentication we can find out whether remote party is genuine or imposter. For example there are two routers (R1 and R2) communicating over a serial link. Now R1 has some data for R2. But before sending this data, R1 want to be sure that remote device which is claiming itself as R2, is real R2. In this case R1 will initiate authentication process. In authentication process R2 will prove its identity. PPP supports two authentication protocols; PAP and CHAP.

PAP (Password Authentication Protocol)

In this protocol, password is sent in clear text format that makes it less secure in comparison with CHAP. PAP authentication is a two steps process. In step one, Router that want to be authenticate will send its user name and password to the Router that will authenticate it. In second step, if user name and password match, remote router will authenticate originating router otherwise authentication process will be failed. Following figure illustrate this process in detail

In step one, R1 sends user name and password in clear text format to R2 which will authenticate R1.
In step two, R2 will match received username and password with locally stored username and password. If both credential match, R2 will assume that R1 is real R1. R2 will send back an acknowledgment to R1 stating that it has passed authentication process and R2 is ready for data transmission.

**Key Points**

PAP authentication is only performed upon the initial link establishment. Once link is established, no more sequential authentication are done for that particular session. PAP sends user name and password in clear text format. Username and password are case sensitive.

**CHAP (Challenge Handshake Authentication Protocol)**

CHAP is used at initial startup and once link is established, sequential authentication are performed to make sure that router is still communicating with same host. If any sequential authentication is failed, connection will be terminated immediately. CHAP authentication is a three steps process.

**Step1**

In first step R1 (Source) sends its username (without password) to the R2 (Destination).

**Step2**

- Routers running CHAP need to maintain a local authentication database. This database contain a list of all allowed hosts with their login credential.
- R2 will scan this database to find out whether R1 is allowed to connect with it or not.
- If no entry for a particular host is found in database then that specific host is not allowed to connect with it. In such a case connection will be terminated at this point.
- A database entry for R1 (with password) will confirm that R1 is allowed to connect with it. R1’s password would be picked up for next process.
- At this moment a random key will be generated.
- This random key with password will be passed in MD5 hashing function.
- MD5 hashing function will produce a hashed value from given input (Random Key + Password).
- This hashed value is known as **Challenge**.
- R2 will send this **Challenge** with random key back to R1.

**Step3**

- R1 will receive hashed value (**Challenge**) and a random key.
- R1 will pass received random key and locally stored password in MD5 hashing function.
- MD5 hashing function will produce a hashed value from given input (Random Key + Password).
- Now R1 will compare this hashed value (generated from MD5 hashed function) with received hashed value from R2.
- If both hashed value do not match, process will be terminated and connection will be rejected.
If both hashed values (locally generated and received) match, R1 will assume that password used by remote router (R2) must have been same as password used by itself. Thus R2 is real R2 and permission for this connection can be granted.

R1 will update R2 about authentication result with Accepted or Rejected acknowledgement signal.
CHAP uses one way hash algorithm (MD5) to generate a hashed value. This hashed value is valid only for one time. So you need not to worry about those users who intentionally make a copy of this hashed value for later use. In CHAP authentication actual password is never sent across the link. So anybody tapping the wire will never be able to reverse the hash to know the original password.

**Key Points**

**CHAP uses three way handshake process to perform the authentication. In CHAP protocol actual password is never sent across the link. CHAP uses a hashed value for authentication that is generated from MD5 hashed function. MD5 uses locally store password and a random key to generate hashed value. This hashed value is valid only for one time.**

**Differences between PAP and CHAP authentication protocol**

<table>
<thead>
<tr>
<th>PAP</th>
<th>CHAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform authentication in two steps.</td>
<td>Perform authentication in three steps.</td>
</tr>
<tr>
<td>Username and password are sent across the link.</td>
<td>Only username is sent across the link.</td>
</tr>
<tr>
<td>Actual password is sent across the link.</td>
<td>Actual password is never sent across the link.</td>
</tr>
<tr>
<td>Password is sent in clear text format.</td>
<td>Password is hashed with a random key through the MD5 hashed function.</td>
</tr>
<tr>
<td>It is a less secure authentication protocol. Anyone tapping the wire can learn password.</td>
<td>It is a secure authentication protocol. Since actual password is never sent across the wire, no one can learn password from wire-tapping.</td>
</tr>
<tr>
<td>PAP authentication is performed only at initial link establishment.</td>
<td>CHAP authentication is performed at initial startup and if required, any time during the session.</td>
</tr>
</tbody>
</table>

**Configure PPP Protocol on Cisco Router**

Configuration of PPP encapsulation is simple and straightforward. Following command is used to configure the PPP encapsulation.

```
Router(config-if)# encapsulation ppp
```

Let’s understand this process in detail with following example.
In above network two routers are connected with each other via serial link. Serial interfaces are essentially configured with following configuration on both routers.

**R1**

```
Router>enable
Router#configure terminal
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.252
Router(config-if)#clock rate 64000
Router(config-if)#bandwidth 64
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

**R2**

```
Router>enable
Router#configure terminal
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 192.168.1.2 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

At this time both routers are running default encapsulation in serial interface. HDLC is the default encapsulation protocol in Cisco routers. I have already explained HDLC in detail with example in second part of this article.

Okay lets change default encapsulation to PPP with following command.

**R1**

```
Router(config)#interface serial 0/0/0
Router(config-if)# encapsulation ppp
Router(config-if)#exit
Router(config)#
```

**R2**

```
Router(config)#interface serial 0/0/0
Router(config-if)# encapsulation ppp
Router(config-if)#exit
Router(config)#
```
Router(config)#interface serial 0/0/0: This command is used to enter in serial interface. Encapsulation is interface specific. We can use different encapsulation protocols in different interfaces. For example we can use PPP in serial 0/0/0 and HDLC in serial 0/0/1.

Router(config-if)#encapsulation ppp: This command would set encapsulation protocol to PPP.

Router(config-if)#exit: This command is used to return back in global configuration mode.

Router(config): This command prompt indicates that we are in global configuration mode.

**Configure PPP Authentication**

PPP authentication requires two essential parameters:

1. Unique hostname of local router
2. Username and password of remote router

**Hostname of local router**

To set hostname we can use `hostname` global configuration command. Let’s assign unique hostname to our routers

**R1**

Router(config)#hostname R1
R1(config)#

**R2**

Router(config)#hostname R2
R2(config)#

**Username and password of remote router**

To set username and password for remote router following global configuration mode command is used

```
Router(config)#username remote_hostname password matching_password
```

Username is the hostname of remote router that will connect with this router. Hostname and password is case sensitive. Router stores password in clear text format that can be viewed with `show running-config` command.
Let's set username and password in our example

**R1**

R1(config)#username R2 password test
R1(config)#

**R2**

R2(config)#username R1 password test
R2(config)#

**Key Points**

Passwords assigned through the `username [hostname of remote device] password [password]` command would be save in running configuration as clear text format and could be viewed via `show run` command. To encrypt it use `service password-encryption` command from global configuration mode. Username and password is case sensitive. Username is the hostname of remote router that will connect with this router. Remote routers must also be configured with username and password. Password must be same on both routers.

**PPP Protocol PAP Authentication**

To configure PAP authentication use following commands on both routers

**R1**

R1(config)#interface serial 0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication pap
R1(config-if)#exit
R1(config)#

**R2**

R2(config)#interface serial 0/0/0
R2(config-if)#encapsulation ppp
PPP Protocol CHAP Authentication

To configure CHAP authentication use following commands on both routers

**R1**

```
R1(config)#interface serial 0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication chap
R1(config-if)#exit
R1(config)#
```

**R2**

```
R2(config)#interface serial 0/0/0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication chap
R2(config-if)#exit
R2(config)#
```

Configure Both CHAP and PAP in same link

To configure both CHAP and PAP in same link use following commands on both routers

**R1**

```
R1(config)#interface serial 0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication chap ppp
R1(config-if)#exit
R1(config)#
```

**R2**

```
R2(config)#interface serial 0/0/0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication chap ppp
R2(config-if)#exit
R2(config)#
```
If we use both methods on the same link as shown above then only the first method will be used in authentication process. Second method will be used only if first method fails. Thus second method will work as backup method.

**Verifying PPP Protocol implementation**

We can use `show interface [interface]` command to verify the PPP implementation.

```
R1#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
    Hardware is HD64570
    Internet address is 192.168.1.1/30
    MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation PPP, loopback not set, keepalive set
[Output omitted]
```

As output indicates encapsulation is set to PPP in this interface.

**Troubleshooting / Debugging PPP Authentication**

In this last section I will discuss some essential troubleshooting steps for PPP. When something went wrong, we should start debugging from the output of `show interface [interface]` command.

First line from output provides some clues about possible issue.

<table>
<thead>
<tr>
<th>Line Status</th>
<th>Protocol Status</th>
<th>Possible Reason</th>
<th>Possible solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administratively Down</td>
<td>Down</td>
<td>Interface is shutdown</td>
<td>Use <code>no shutdown</code> command from sub-interface mode</td>
</tr>
<tr>
<td>Down</td>
<td>Down</td>
<td>Physical layer issue.</td>
<td>Check cable, connector and other connecting devices.</td>
</tr>
<tr>
<td>UP</td>
<td>Down</td>
<td>Data Link Layer issue.</td>
<td>Check configuration.</td>
</tr>
</tbody>
</table>

In above example its “Serial 0/0/0 is up, line protocol is down” which indicates that physical layer is working properly but there is some issue in data link layer configuration.
Next, notice the states of LCP, IPCP and CDPCP. A Closed state for these indicates that something is wrong with LCP setup process, causing data link layer to fail. In rest of this tutorial I will explain some common causes for data link failure.

**Mismatched WAN Encapsulation**

In point to point link, encapsulation method at both ends must be same otherwise link will never come up. This problem is easy to find and fix. The `show interfaces [interface]` command will list the encapsulation type. Once you identify the problem, it can be fixed easily. Simply reconfigure the one end’s interface to match with other end’s encapsulation method.

Once you identify the problem, it can be fixed easily. Simply reconfigure the one end’s interface to match with other end’s encapsulation method.

**Mismatched IP configuration**

This problem is not directly associated with PPP configuration but can be tricky one question in exam. This problem cannot be spotted from `show interface [interface]` command as the output of this command will show “Serial 0/0/0 is up, line protocol is up” that makes you assume that everything is fine and operational at interface level. But when you try to ping remote router it gets fail. This is because PPP, HDLC and Frame Relay are layer 2 protocols and they don’t care about layer 3 configuration (IP Configuration). So even link is up, you cannot transfer the IP packets.
To fix this problem configure IP addresses in both ends from same subnet.

**Debug PPP Authentication**

To determine whether issue is related with PPP authentication or not, we can use `debug ppp authentication` command. If PPP encapsulation and authentication are setup correctly then this command will display output like this:

```
R1# debug ppp authentication
PPP authentication debugging is on
R1#
R1: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up
R1: Seo/0/0 PPP: Using default call direction
R1: Seo/0/0 PPP: Treating connection as a dedicated line
R1: Seo/0/0 PPP: Session handle[45004] Session id[12]
R1: Seo/0/0 CHAP: O CHALLENGE id 5 len 23 from "R1"
R1: Seo/0/0 CHAP: I CHALLENGE id 5 len 23 from "R2"
R1: Seo/0/0 PPP: Sent CHAP SENDAUTH Request
R1: Seo/0/0 CHAP: I RESPONSE id 5 len 23 from "R2"
R1: Seo/0/0 PPP: Received SENDAUTH Response PASS
R1: Seo/0/0 CHAP: Using hostname from configured hostname
R1: Seo/0/0 CHAP: Using password from AAA
R1: Seo/0/0 CHAP: O RESPONSE id 5 len 23 from "R1"
R1: Seo/0/0 PPP: Sent CHAP LOGIN Request
R1: Seo/0/0 PPP: Received LOGIN Response PASS
R1: Seo/0/0 CHAP: O SUCCESS id 5 len 4
R1: Seo/0/0 CHAP: I SUCCESS id 5 len 4
```

But if something wrong during authentication process output would look like this:-

```
R1# debug ppp authentication
```
PPP authentication debugging is on
! Lines omitted for brevity
R1: Se0/0/0 CHAP: O CHALLENGE id 1 len 23 from "R1"
R1: Se0/0/0 CHAP: I RESPONSE id 1 len 23 from "R2"
R1: Se0/0/0 CHAP: O FAILURE id 1 len 25 msg is "Authentication failed"

If username and password are not configure exactly as they should be then authentication will be failed.

To fix this problem configure username and password in proper way. Remember that username and password are case sensitive.

Another thing that you should notice is authentication type that must be same in both ends. If you configure one end to use PAP while another end to use CHAP then that link would never work.
To fix this problem change authentication type in one end to match with other end.

That’s all for this part. In next part I will explain basic concepts of frame really in detail with examples.

For more articles please visit our site

ComputerNetworkingNotes.com