**WAN Connection lab**

Serial connection explanation and configuration in packet tracer

The Serial Connection is used to create a WAN connection with the help of a service provider who offers a dedicated leased line to its customers.

Business organizations buy leased lines to establish a WAN connection to connect with different offices and business sites that could physically be thousands of miles apart. Businesses have to pay for these leased lines according to the service availed. And accordingly, the service providers charge for this service i.e. based on the bandwidth they offer to their client organizations.

One of the connections used for a leased line is the Serial Connection in Cisco-based networks. If we have Cisco routers on both sides of the network then the default encapsulation known as HDLC will be used by the Cisco routers. However, this will not work with other brands’ routers (i.e. with the non-Cisco routers) because this protocol is solely a Cisco proprietary.

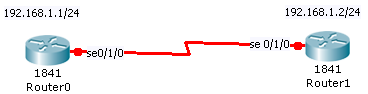
If we are configuring a new cisco router then by default the data link protocol would be HDLC however if we are configuring an old device then we should check the configuration and if there is a mismatch then we have to configure the same protocol on both routers.

Although HDLC works out of the box on all cisco routers however it is not widely used because of its proprietary nature and it does not provide much feature so PPP protocol is used by the most organization. Even on cisco routers, organizations prefer PPP protocol over HDLC protocol due to its advanced features and benefits.

In this lab, we will configure a Serial Connection between the routers. We will set up a clock rate at 56000, which will provide a speed of 56 Kbps. In the real world, the DCE side of the cable is configured by the service provider.

Generally, the clock speed is configured according to the availability of the bandwidth speed that the service provider is offering.

The following lab uses a serial cable that will simulate a service provider. We will configure the clock speed on the router that has the DCE (data carrier equipment) side connected.



**Lab Tasks**

1. Assign IP address to both routers and turn them on  
2. Set clocking on DCE side, which is router 0

**Lab Configuration**

**Task 1**

Router 0

Router(config)#interface serial 0/1/0

Router(config-if)# ip address 192.168.1.1 255.255.255.0

Router(config-if)# no shut

Router 1

Router(config)#interface serial 0/1/0

Router(config-if)# ip address 192.168.1.2 255.255.255.0

Router(config-if)# no shut

**Task 2**

Router 0

Router(config-if)# clock rate 56000

# PPP configuration in packet tracer

**In this lab, we will perform the PPP configuration in the packet tracer. Let’s check the steps to configure the PPP protocol to establish the WAN connection on the Cisco router.**

PPP encapsulation is used on the WAN connections, which are offered by the service providers through a leased line.

Point to Point Protocol is an industry-standard protocol. As a result, this protocol is supported by many vendors that produce the networking devices.

It has many features like data compression, authentication, and multi-link that make it very popular among companies.

PPP uses the following protocols to support a variety of features.

**Link Control Protocol (LCP) –**

**LCP protocol is used by the PPP to establish the connection.**

**PPP can use the following NCPs (Network control protocol)**

· Internet Protocol Control Protocol (IPCP)

· OSI Network Layer Control Protocol (OSINLCP)

· Applet talk control protocol (ATCP) and Internetwork Packet Exchange Control Protocol (IPXCP)

· Internetwork Packet Exchange Control Protocol (IPXCP)

· DECnet Phase IV Control Protocol (DNCP)

· NetBIOS Frames Control Protocol (NBFCP)

· IPv6 Control Protocol (IPV6CP)

PPP can use two following protocols for authentication.

· Password Authentication Protocol (PAP)

PAP provides password-based protection to the connection however sends the password in plain text over the network, which makes it a less secure protocol so this protocol should be avoided on highly secured networks as this vulnerability can be easily used by the hacker to break into the network.

· Challenge Handshake Authentication Protocol (CHAP)

This protocol uses a three-way handshake and uses MD5 hashing to encrypt the plain text. In this type of authentication, a peer sends the hash value to the authenticator instead of plain text and then the authenticator matches that value with its calculated hash value to establish the connection.

Authentication happens several times in the already established connection to enhance the security and make sure that the security is not compromised.

CHAP protocol is far better than PAP authentication as encryption makes the password highly secure and even if somebody is using the packet sniffer then the only hash value can be captured. Although MD5 does not provide complete protection as there are ways by which someone can reverse engineer the hash to receive the plain text however these techniques are highly complex to use.

In this lab, we will configure PPP protocols on the routers. PPP should be enabled on both the routers to work, as the routers are required to use the same protocol to establish a connection. Also, we will set up clocking on the router 0 that is connected with the DCE side of the cable.

## **PPP protocol configuration**



**Lab Tasks**

1. Assign IP address to both routers  
2. Set PPP encapsulation  
3. Set clocking

**Lab Configuration**

Task 1

Router 0

Router(config)#int se 2/0

Router(config-if)# ip address 192.168.1.1 255.255.255.0

Router(config-if)# no shut

Router 1

Router(config)# int se 2/0

Router(config-if)# ip address 192.168.1.2 255.255.255.0

Router(config-if)# no shut

Task 2

On both routers

Router(config)#in se 2/0

Router(config-if)#encapsulation ppp

n router 0

Router(config)#in se 2/0

Router(config-if)# clock rate 56000