Password recovery .

Physical OFF and ON

CTR+SHIFT+PAUSE/BREAK (Pause/Break or equivalent command depends upon diff laptops)

Self decompressing the image :
####################################
monitor: command "boot" aborted due to user interrupt
rommon 1 > confreg 2142
rommon 2 > reset

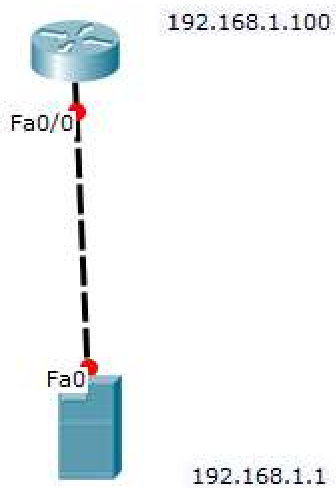
Continue with configuration dialog? [yes/no]:no

Router>enab
Router#conf t
Router(config)#no enable password
Router(config)#no enable secret
Router#show version
Configuration register is 0x2142
Router(config)#config-register 2102
Router#reload
This time it will not ask for the password.

ROUTER IOS RESTORE

IP_ADDRESS: The IP address for this unit – Router IP address
IP_SUBNET_MASK: The subnet mask for this unit – Subnet mask of the router

DEFAULT_GATEWAY: The default gateway for this unit - Router IP address
TFTP_SERVER: The IP address of the server to fetch from – Server IP address
TFTP_FILE: The filename to fetch – Image file



TFTPDNLD

IP_ADDRESS=192.168.1.100
IP_SUBNET_MASK=255.255.255.0
DEFAULT_GATEWAY=192.168.1.100
TFTP_SERVER=192.168.1.1
TFTP_FILE=pt1000-i-mz.122-28.bin
TFTPDNLD

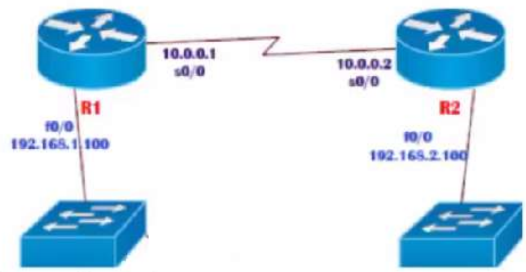
Do you wish to continue - Yes
Reset

<u>Troubleshooting connectivity.</u>

R-1#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.1.100	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0/0	10.0.0.1	YES	manual	up	up
Serial0/1	unassigned	YES	unset	administratively down	down

Troubleshooting Connectivity(contd)



1) Serial is up, line protocol is up

- Connectivity is fine.

2) Serial is down, line protocol is down

- remote device turned off
- remote port is in shutdown state
  - interface on the remote router has to be configured
- problem with connectivity

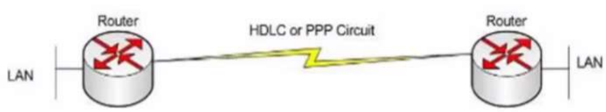
3) Serial is administratively down, line protocol is down

- local port is in shut down state
  - No Shutdown has to be given on the local router interface

4) Serial is up, line protocol is down

- Encapsulation mismatch
- clock rate command not given on serial interface (only applies in lab scenario)
- if using PPP , then authentication mismatch

WAN PROTOCOLS



HDLC	PPP
Higher level data link Control protocol	Point to Point Protocol
Cisco Proprietary	Standard Protocol
NO support Authentication, Compression & error correction	Supports Authentication, compression & error correction
Default on serial links	Change to PPP

R-1#sh interfaces s0/0

Serial0/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 10.0.0.1/8
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
***Encapsulation HDLC**, loopback not set, keepalive set (10 sec)*

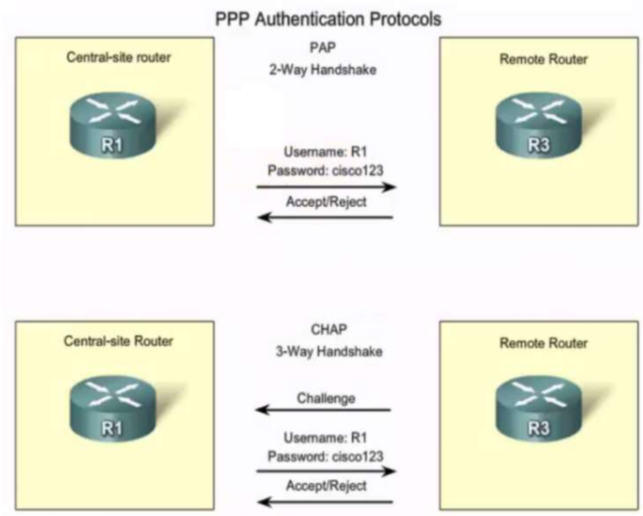
Configuration of PPP:

Router# ***configure terminal***
Router(config)# ***interface serial 0/0***
Router(config-if)# ***encapsulation ppp***

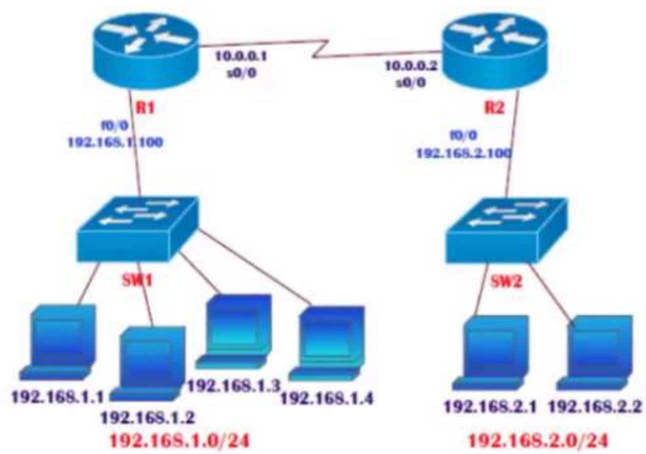
PPP Authentication

PAP	CHAP
Password Authentication Protocol	Challenge Handshake Authentication Protocol
PAP provides a simple method for a remote node to establish its identity using a two-way handshake.	After the PPP link establishment phase is complete, the local router sends a unique "challenge" message to the remote node.
PAP is done only upon initial link establishment	The remote node responds with a value (MD5)
PAP is not a strong authentication protocol.	The local router checks the response against its own calculation of the expected hash value.
Passwords are sent across the link in clear text.	If the values match, the authentication is acknowledged. Otherwise, the connection is terminated immediately.

PAP vs CHAP



CHAP configuration on R1/R2



R1/R2

*R-x(config)#**int s0/0***

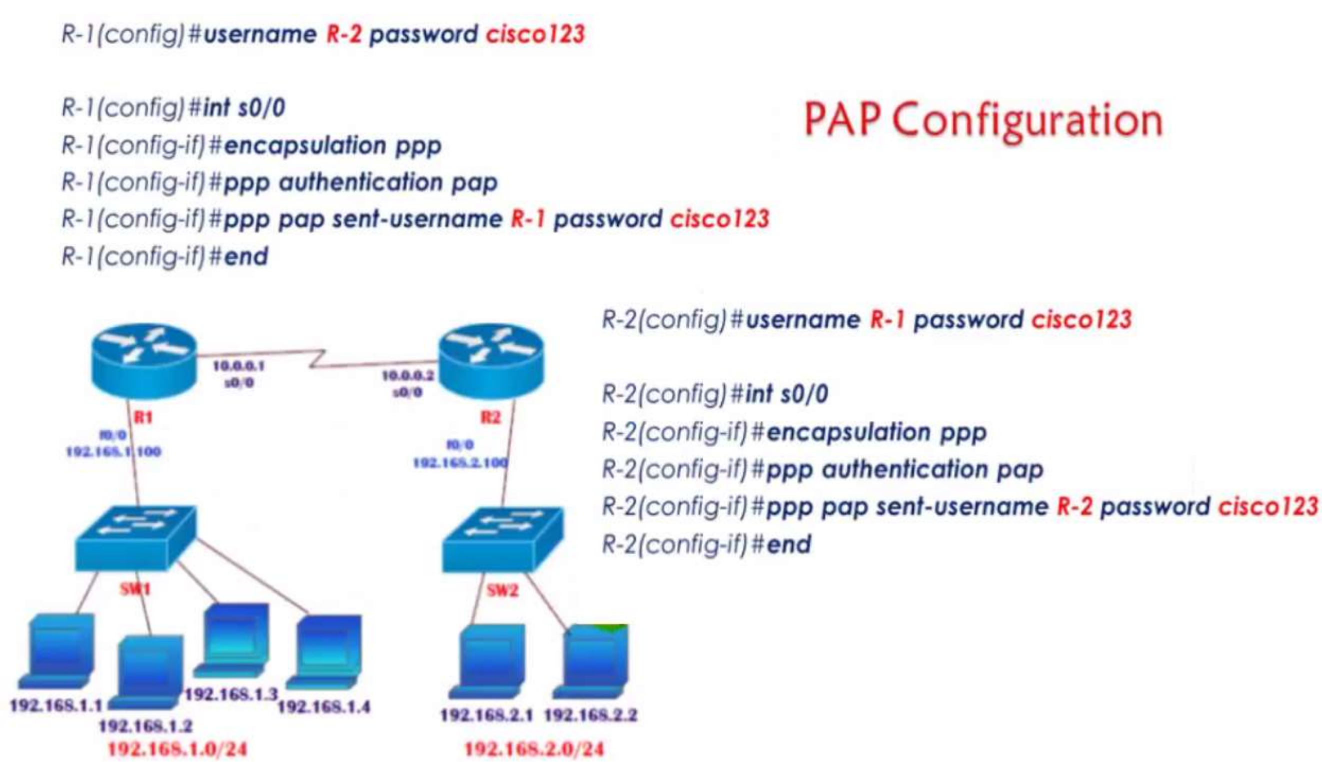
*R-x(config-if)# **encapsulation ppp***

*R-x(config-if)# **ppp authentication chap***

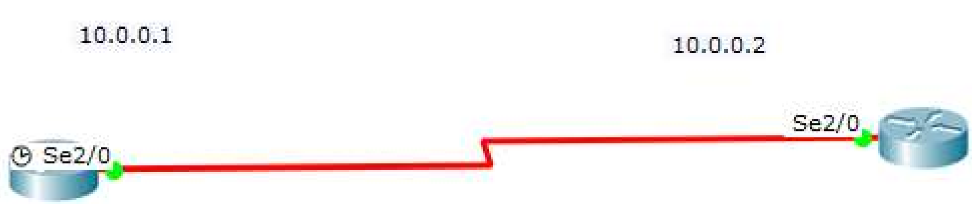
*R-x(config-if)# **exit***

*R-1(config)#**username R-2 password cisco123***

*R-2(config)#**username R-1 password cisco123***



PPP –



CHAP Configuration

Show interfaces serial 2/0

```
hostname R1
interface serial 2/0
ip address 10.0.0.1 255.0.0.0
no sh
exi

interface serial 2/0
encapsulation ppp
ppp authentication chap
exi
exi
username R2 password cisco

hostname R2
interface serial 2/0
ip address 10.0.0.2 255.0.0.0
no sh
exi

interface serial 2/0
encapsulation ppp
ppp authentication chap
exi
exi
username R1 password cisco
```

PAP Configuration

Show interfaces serial 2/0

interface serial 2/0
encapsulation ppp
ppp authentication pap
ppp pap sent-username R1 password cisco
exi
username R2 password cisco

interface serial 2/0
encapsulation ppp
ppp authentication pap
ppp pap sent-username R2 password cisco
exi
username R1 password cisco

Significance of Clock Rate

When you set the clock rate for a serial interface, you are setting the **speed of the interface**, in other words, the bandwidth (bandwidth meaning rate of data transfer). When using this command it's in the form of bits: 64000 bits = 64 kb

Router#show controllers serial 2/0
Interface Serial2/0
Hardware is PowerQUICC MPC860
DCE V.35, no clock

interface serial 2/0
clock rate 2400

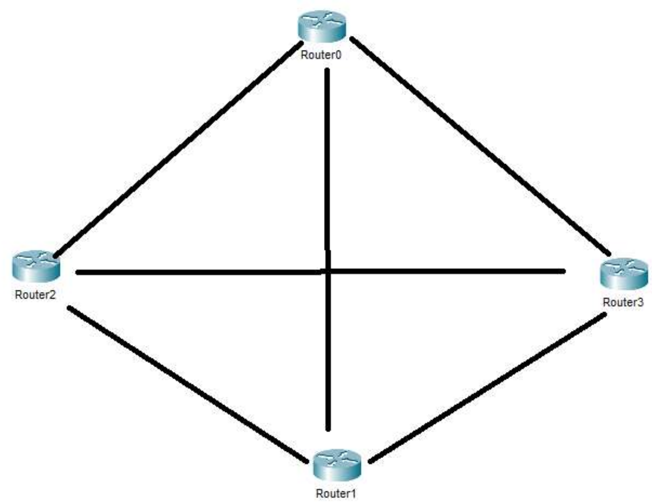
DTE (Router)& DCE (CSU/DSU)

DTE stands for Data Terminal Equipment, **and DCE stands for Data Communications Equipment**. DTE is typically either a dumb terminal or the serial port on a Router or Computer. DCE is typically a modem, DSU/CSU, or other piece of data communications equipment, hence the names.

A CSU/DSU (Channel Service Unit/Data Service Unit) is a hardware device about the size of an external modem that converts a digital data frame from the communications technology used on a local area network (LAN) into a frame appropriate to a wide-area network (WAN) and vice versa. For example, if you have a Web business from your own home and have leased a digital line (perhaps a T-1 or fractional T-1 line) to a phone company or a gateway at an Internet service provider, you have a CSU/DSU at your end and the phone company or gateway

Frame Relay

Frame Relay is one of the most popular WAN service deployed over the past decade. Even though several advanced technologies (such as VPN, Tunnelling) are available today, Frame Relay has many advantages due to its features, benefits and lower cost in comparison with other point to point wan services. For example have look on following figure that illustrates a network with simple point to point leased line connection.



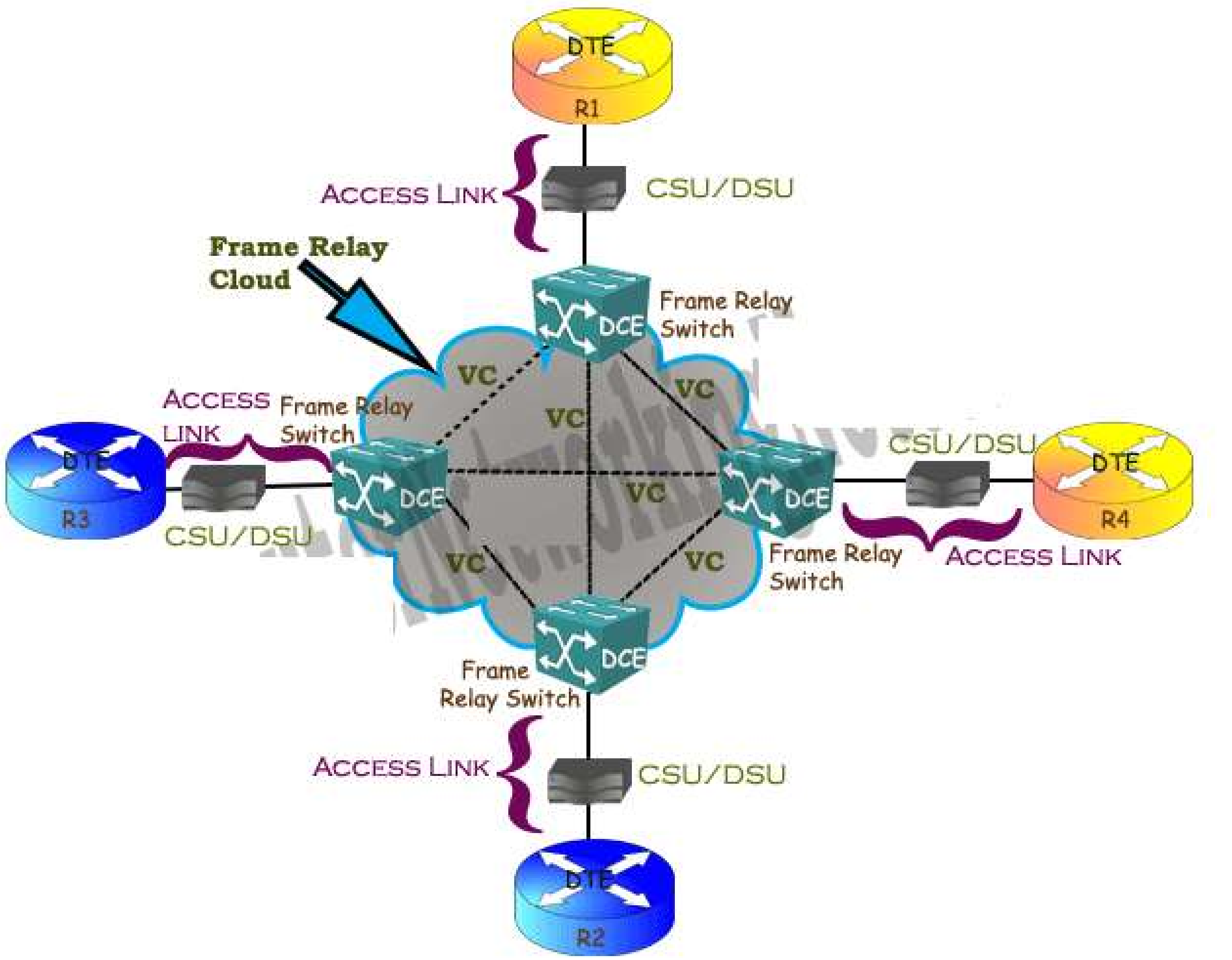
There are four routers in this network. To connect these routers with each other, total six leased lines and three serial interfaces on each router are used. We can use following formula to figure out how many connections are required:-

(N × (N – 1)) / 2 [Here N is the number of routers]

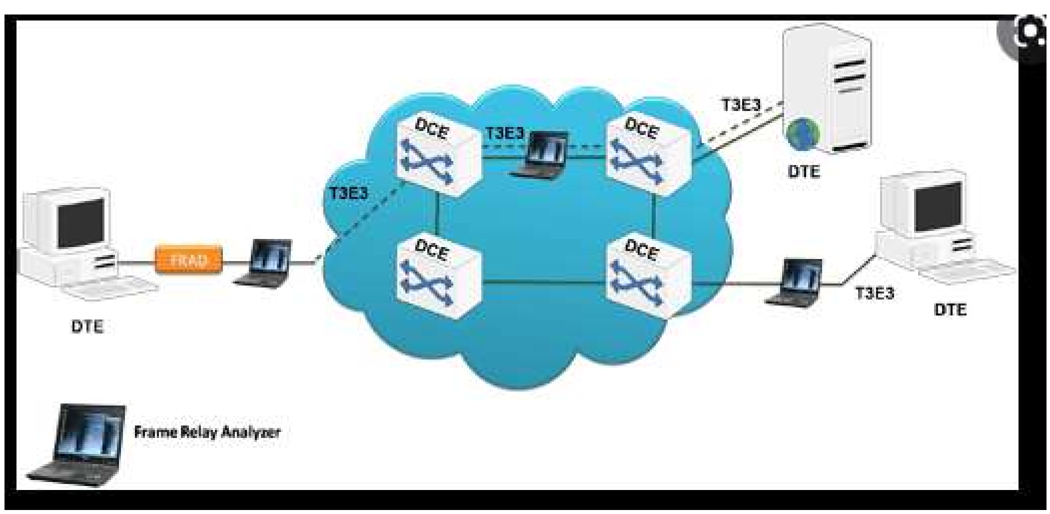
In our example we have four routers so we need (4 x (4-1)) /2 = 6 leased lines.

If we have 100 routers then we need (100 x (100-1)) /2 = 4950 lease lines and 99 serial interfaces on each router. Forget about low end routers, even a 7700 series router does not have sufficient physical interfaces to handle this requirement.

Here comes Frame Relay. Frame Relay turns physical interface in virtual interfaces. With virtual interface Frame Relay can effectively handle this network or even bigger network with single serial interface. Have a look on following figure that illustrate above network with Frame Relay


DTE
R1
Access Link
CSU/DSU
Frame Relay
Cloud
DCE
Frame Relay
Switch
VC
VC
VC
Access
Link
Frame Relay
Switch
DTE
R3
DCE
VC
DCE
CSU/DSU
DTE
R4
CSU/DSU
VC
VC
Frame Relay
Switch
Access Link
DCE
Frame
Relay Switch
Access Link
CSU/DSU
DTE
R2

b


DCE
T3E3
DCE
T3E3
DTE
T3E3
FRAD
DCE
DCE
DTE
T3E3
DTE
Frame Relay Analyzer

With Frame Relay implementation, we still need 6 connections to connect all these routers with each other. But instead of physical lines, Frame Relay uses virtual lines to connect all these locations. The biggest benefit of these virtual lines is that we do not need equal physical interfaces on router to connect them. We can connect multiple virtual lines with single interface

DTE

DTE (*Data Terminal Equipment*) is a device (usually a router or PC) that converts data frame into signals and reconvert received signals in data frame. DTE device communicates with DCE device.

CSU/DSU

A **CSU/DSU (*Channel Service Unit/Data Service Unit*)** is a device that converts data signal between LAN network and WAN network. LAN network and WAN network uses separate communication technology. A CSU/DSU understands both technologies. DSL and cable modems are the example of CSU/DSU.

DCE

DCE (*Data circuit terminating equipment*) is a device (usually modem, CSU/DSU or Frame Relay switch) that provides clock rate and synchronization.

Access Link

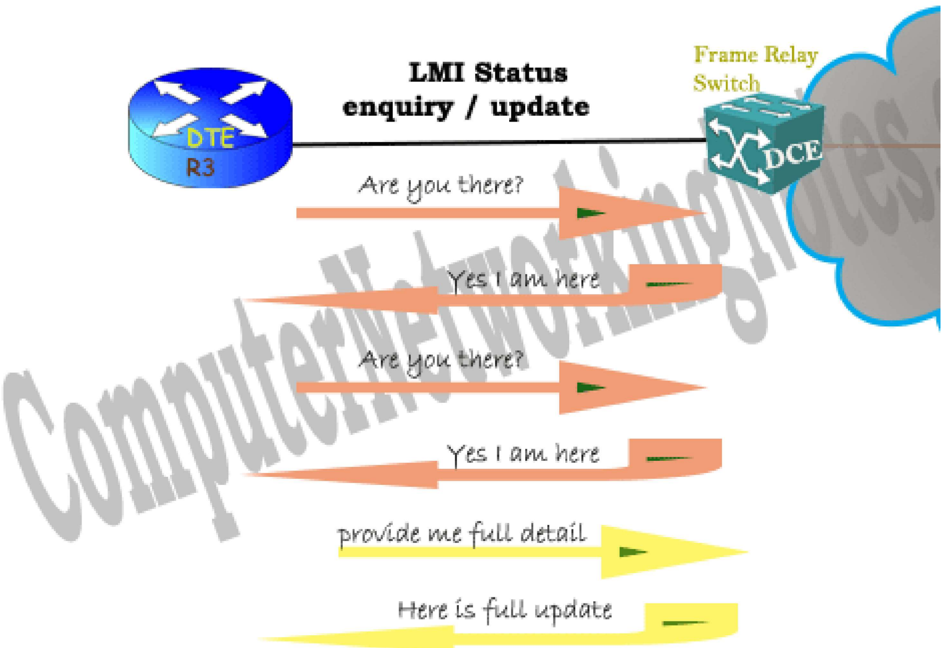
Connection line between DTE and DCE.

Frame Relay LMI (Local Management Interface) protocol

Before data transmission DTE confirms the status of remote end. It sends data only if remote end is up. To know the status of each other's, devices exchange *Keepalive* messages. If one end does not receive a *Keepalive* message from other end in specified time then it would assume that remote end is down. *Keepalive* messages are exchanged between directly connected devices. For example in leased line where two devices connect with each other via direct link, will exchange *Keepalive* messages. But in Frame Relay devices connect with each other via the **Frame Relay switches**, so they will exchange *Keepalive* message with Frame Relay switches.

Frame Relay uses LMI protocol to exchange the *Keepalive* messages between DTE (*connection end point*) and DCE (*last frame relay switch that is directly connected with the end point*). DTE (Routers) send LMI ***status enquiry messages*** to the connected DCE (Frame Relay switch). If DCE (Frame Relay) is up then it will respond with ***LMI status reply message***. If DTE does not get response form DCE then it will assume that either access link or frame relay switch is down.

Besides LMI status enquiry DTE also asks for full status updates. In response DCE respond with all information that is related to DTE. This information includes the status of VCs which are connected to the DTE and their configuration values (CIR, B_C, B_E and DLCIs).



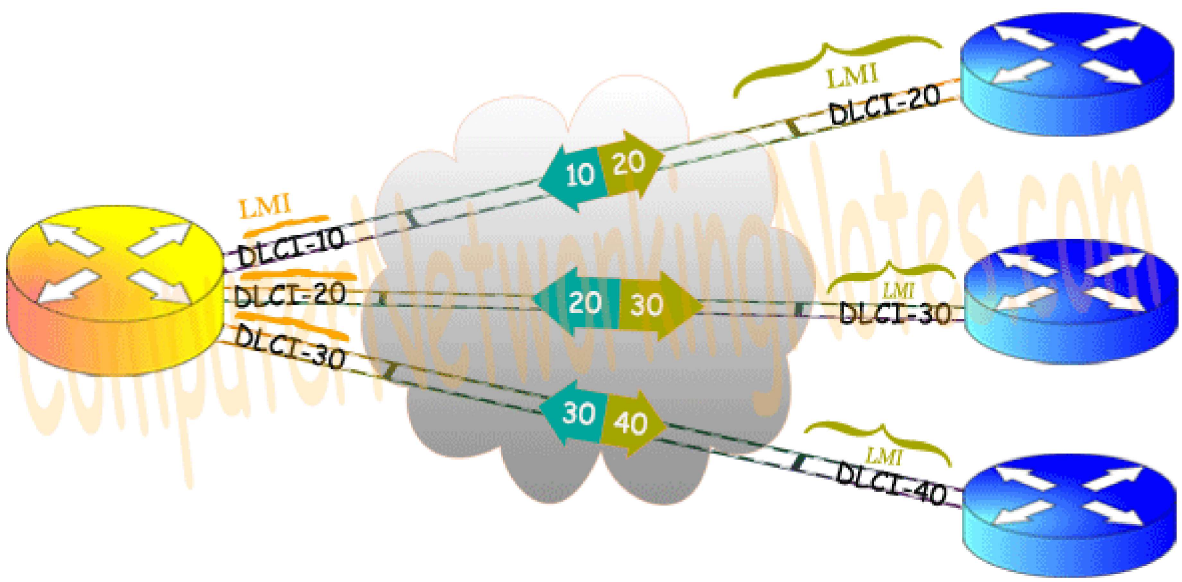
LMI status enquiry :- A simple query asking simple question "*Are you there*". Response of this query is also simple "*Yes I am here*".

LMI full status enquiry :- A complete query seeking full information "*Tell me everything that is related to me*". Response of this query contains all information that is related to DTE "*Here is all information which is related to you*".

Frame Relay DLCI (data link connection identifiers) explained

Frame Relay allows us to connect multiple VCs with single physical access link. In first example of this tutorial, we connected six VCs with single physical link (serial interface). Basically we divided a serial interface in six sub-interfaces and assigned one VC with each sub interface. Frame Relay must need to know which sub-interface is connected with which VC before it can transmit the data. Frame Relay uses DLCI (data link connection identifiers) number to map the interface with VC.

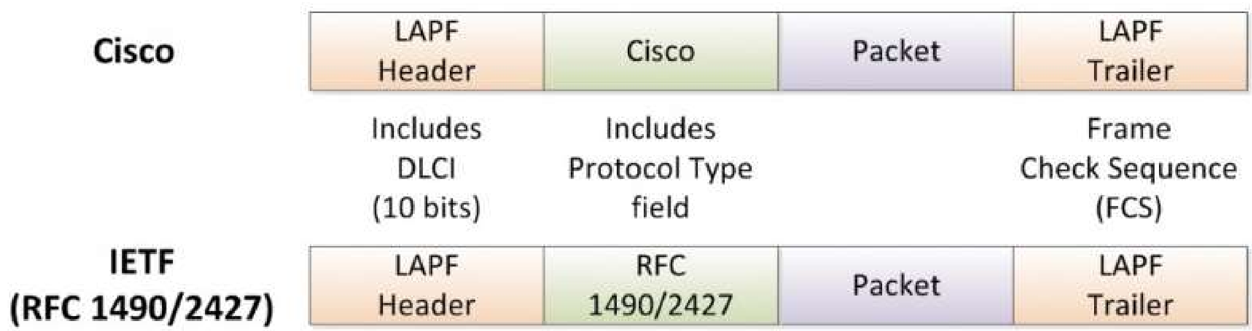
Since a VC has two ends it need two DLCI number, one for each end. DLCI value is provided by Telco. Probably we may get same or different DLCI number for both ends. DLCI number need to be unique only between Frame Relay switch and DTE router. If we received different DLCI number for both end then Frame Relay would convert DLCI number in midway.



- Cisco created a proprietary additional header, which appears between the LAPF header and the Layer 3 packet It includes a separate 2-byte Protocol Type field with values exactly matching the ones used in the same field Cisco uses for HDLC, as discussed earlier in the chapter.
- Internet Engineering Task Force (IETF) defined the second solution via RFC standards 1490 and later 2427. This solution is known as Multiprotocol Interconnect over Frame Relay and it

defines a header similar to the Cisco propreitary solution placed between the LAPF header and Layer 3 packet. The additional header includes a Protocol Type field as well as several other options.

Figure 12-11 Cisco and IETF Framing



In wide area network computing, **Link Access Procedure for Frame Relay** (or LAPF) is part of the network's communications protocol which ensures that frames are error free and executed in the right sequence. LAPF is formally defined in the International Telecommunication Union standard

Inverse Address Resolution Protocol (InARP) –

Instead of using Layer-3 address (IP address) to find MAC address, Inverse ARP uses MAC address to find IP address. As the name suggests, InARP is just inverse of ARP. InARP is used to find Layer-3 address from Layer-2 address (DLCI in frame relay). Inverse ARP dynamically maps local DLCIs to remote IP addresses when you configure Frame Relay. When using inverse ARP, we know the DLCI of remote router but don't know its IP address. InARP sends a request to obtain that IP address and map it to the Layer-2 frame-relay DLCI.

<u>Synchoronous (UDP)and Asynchronous communication(TCP)</u>

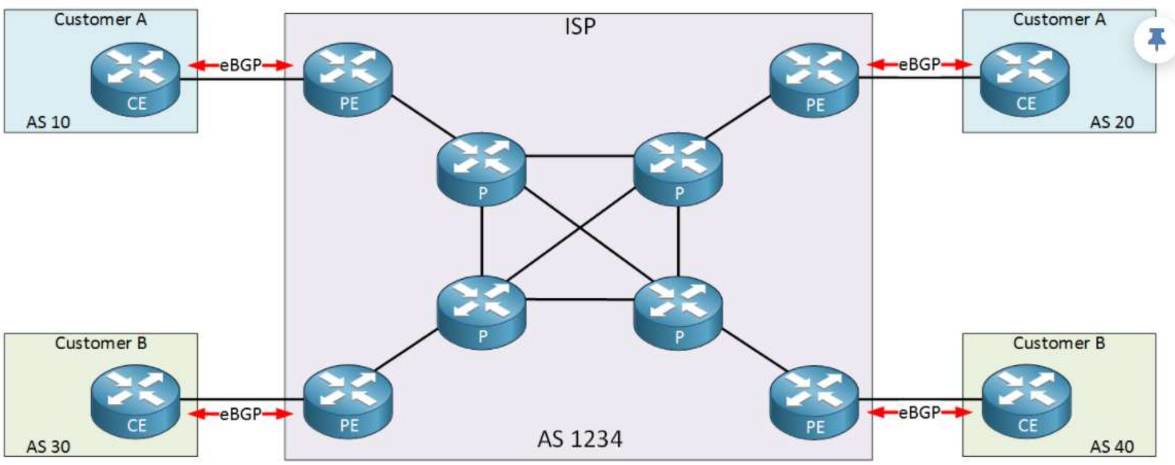
let’s see the difference between Synchronous (Continuous flow of data , travelling in a single path)and Asynchronous Transmission:

S.NO	Synchronous Transmission	Asynchronous Transmission
1.	In Synchronous transmission, Data is sent in form of blocks or frames.	In asynchronous transmission, Data is sent in form of byte or character.
2.	Synchronous transmission is fast.	Asynchronous transmission is slow.
3.	Synchronous transmission is costly.	Asynchronous transmission is economical.
4.	In Synchronous transmission, time interval of transmission is constant.	In asynchronous transmission, time interval of transmission is not constant, it is random.
5.	In Synchronous transmission, There is no gap present between data.	In asynchronous transmission, There is present gap between data.

INTRO to MPLS

When you want to learn MPLS, you need to be very familiar with the following topics before you continue:

- IGPs (like OSPF and EIGRP)
- Tunneling (GRE)
- CEF (Cisco Express Forwarding)
- BGP (Border Gateway Protocol)

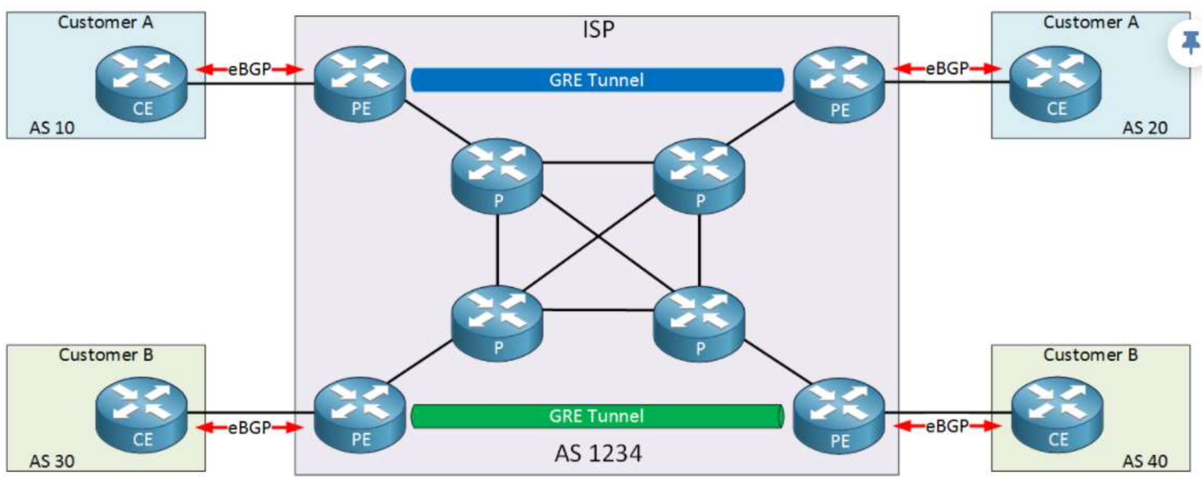


Multiprotocol Label Switching is a routing technique in telecommunications networks that directs data from one node to the next based on labels rather than network addresses. Whereas network addresses identify endpoints the labels identify established paths between endpoints.

Above we have an example of an ISP with two customers called “A” and “B”. The ISP only offers Internet connectivity and no other services. Each customer uses the ISP to have connectivity between their sites.

To accomplish our goal, the ISP is running eBGP between the CE (Customer Edge) and PE (Provider Edge) to exchange prefixes. This means all internal (P) routers of the ISP have to run iBGP or they don't know where to forward their packets to until and unless they learn about all the routes in the internet We can reduce this learning of routes by using route reflectors or a confederation. All routers have to do lookups in the routing table for any possible destination.

Now here's something to think about…when our goal is to have connectivity between two customer sites, why should all internal P routers know about this? The only routers that need to know how to reach the customer sites are the PE routers of the provider. Why not build a tunnel between the PE routers? Take a look at the picture below:



In the picture above I added two GRE tunnels:

- The two PE routers at the top will use a GRE tunnel for the customer A sites.
- The two PE routers at the bottom will use a GRE tunnel for the customer B sites.

Another issue with traditional networking is that there are multiple types of traffic passing through the internet Voice traffic, vedio traffic, multicast traffic so the ISP has to maintain all these traffic separately using different technologies based on the preference and many other parameters

MPLS overcomes all these disadvantages by using a single technology.

What does multi protocol label switching mean?

- **Multi protocol**: besides IP you can tunnel pretty much anything…IP, IPv6, Ethernet, PPP, frame-relay, etc.
- **Label switching**: forwarding is done based on labels, not by looking up the destination in the routing table.

PE1#**show mpls forwarding-table**

Local Label	Outgoing Label	Prefix or Tunnel Id	Bytes Label Switched	Outgoing interface	Next Hop
16	17	4.4.4.4/32	0	Gi0/2	192.168.23.3
17	Pop Label	192.168.34.0/24	0	Gi0/2	192.168.23.3
18	Pop Label	3.3.3.3/32	0	Gi0/2	192.168.23.3

Above you can see the labels that this router uses to reach certain prefixes.. To reach 4.4.4.4, this router will add label 17 to the IP packet and forwards it on GigabitEthernet 0/2 (towards the P router). A quicker method to see what labels are used for different prefixes is by checking the CEF table:

https://networklessons.com/mpls/introduction-to-mpls