Chapter 12 Point to Point WAN   FROM SLIDES

Name	***Meaning or Reference***
Leased circuit, circuit	The words line and circuit are often used as synonyms in telco terminology; circuit makes reference to the electrical circuit between the two endpoints.
Serial link, serial line	The words link and line are also often used as synonyms. Serial in this case refers to the fact that the bits flow serially and that routers use serial interfaces.
point-to-point link, point-to-point line	Refers to the fact that the topology stretches between two points, and 2 points only. (Some older leased lines allowed more than 2 devices.)
T1	A specific type of leased line that transmits data at 1.544 megabits per second (1.544 Mbps).
WAN link, link	Both these terms are very general, with no reference to any specific technology.

slide added private line - data sent over line cant be copied by other telco customers
CPE telco equip in Demarc to CSU/DSU also from telco provide clocking
built into a router module
our config is not on CSUDSU but on serial to router from CSU/DSU

Serial speeds review

DS0	64 Kbps
Fractional T1	Multiples of 64 Kbps, up to 24X
DS1 (T1)	1.544 Mbps (24 DS0s, for 1.536 Mbps, plus 8 Kbps overhead)
Fractional T3	Multiples of 1.536 Mbps, up to 28X
DS3 (T3)	44.736 Mbps (28 DS1s, plus management overhead)

TDM - time division multiplexing - (remember clocking?) T1 is 24 "time slots"
DTE to DCE review.
Remember: DTE portion is straight-through serial cable, and DCE cable side is like crossover
Reminds us this DTE/DCE stuff is a "lab-ism" - not seen out in the role of engineer
does sh running config just list interface clock rate set/mentioned and no other? it is

re-encapsulation: HDLC
HDLC - open no type field in the frame.
I asked if there was a naming difference. Answer- anything in this is considered Cisco.
How does Cisco handle a Juniper frame without a type field? Answer- it is out of scope of this exam.
Ended up making up a "guess"

configuring hdlc
give IP address, no shutdown, ***encapsulation hdlc***, clock rate on DCE router (if applicable) optional bandwidth kps/ descriptions.

PPP
Link control protocol
network control protocol

- Definition of a header and trailer that allows delivery of a data frame over the link
- Support for both synchronous and asynchronous links
- A protocol Type field in the header, allowing multiple Layer 3 protocols to pass over the same link
- Built-in authentication tools: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP)

- Control protocols for each higher-layer protocol that rides over PPP, allowing easier integration and support of those protocols

- ***Link Control Protocol (LCP):*** This one protocol has several different individual functions, each focused on the data link itself, ignoring the Layer 3 protocol sent across the link.
- ***Network Control Protocols (NCP):*** This is a category of protocols, one per network layer protocol. Each protocol does functions specific to its related Layer 3 protocol.

- The PPP LCP implements the control functions that work the same regardless of the Layer3 protocol. For features related to any higher-layer protocols, usually Layer 3 protocols, PPP uses a series of PPP control protocols (CP), such as IP Control Protocol (IPCP). PPP uses one instance of LCP per link and one NCP for each Layer 3 protocol defined on the link. For example, on a PPP link using IPv4, IPv6, and Cisco Discovery Protocol (CDP), the link uses one instance of LCP plus IPCP (for IPv4), IPv6CP (for IPv6), and CDPCP (for CDP).

Function	***LCP Feature***	***Description***
Looped link detection	Magic number	Detects whether the link is looped, and disables the interface, allowing rerouting over a working route
Error detection	Link-quality monitoring (LQM)	Disables an interface that exceeds an error percentage threshold, allowing rerouting over better routes
Multilink support	Multilink PPP	Load balances traffic over multiple parallel links
Authentication	PAP and CHAP	Exchanges names and passwords so that each device can verify the identity of the device on the other end of the link

```
R1# show interfaces serial 0/0/0 Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Description: link to R2
  Internet address is 192.168.2.1/24
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
```

Configure the routers' hostnames using the ***hostname*** name global configura- tion command.
Configure the username for the other router, and the shared secret password, using the ***username*** name ***password*** password global configuration command or the ***username*** name secret password command.
Enable CHAP on the interface on each router using the ***ppp authentication chap*** interface subcommand.

Review:

Line Status	***Protocol Status***	***Likely General Reason/Layer***
Administratively down	Down	Interface shutdown
Down	Down	Layer 1
Up	Down	Layer 2
Up	Up	Layer 3

Line Status	***Protocol Status***	***Likely Reason***
Up	Down on both ends1	Mismatched ***encapsulation*** commands
Up	Down on one end, up on the other	Keepalive disabled on the end in an up state when using HDLC
Up	Down on both ends	PAP/CHAP authentication failure

mismatched subnets

From book:

Part IV: Wide-Area Networks 357

Chapter 12 Implementing Point-to-Point WANs 359

Leased Line WANs with HDLC

Works a lot like a long Ethernet crossover cable connecting two routers
Leased Line provides the physical layer bit transmission
Router supplies the data link protocol - *High-level Data Link Control*

The Physical Components of a Leased Line

Customer Premise Equipment (CPE) - Telco equipment that sits at the customer’s site
Channel Service Unit/Data Service Unit (CSU/DSU) - Provides *clocking*
WAN interface cards (WIC) to hook CSU/DSU to router with CSU cables; some WICS have CSU built-in

------------------------------

The CSU sits between the telco leased line and the router; it understands both worlds and their conventions at Layer 1. On the telco side, that means the CSU connects to the line from the telco, so it must understand all these details about the T-carrier system, TDM, and the speed used by the telco. The CSU must be configured to match the telco’s settings to run at the same speed. For instance, a CSU connected to a 256-Kbps fractional T1 requires differ- ent configuration from one connected to a full T1 (1.544 Mbps).

On the router side of the equation, the CSU connects to the router, with roles called the DCE and DTE, respectively. The CSU, acting as DCE (data circuit-terminating equipment), controls the speed of the router. The router, acting as DTE (data terminal equipment), is con- trolled by the clocking signals from CSU (DCE). That is, the CSU tells the router when to send and receive bits; the router attempts to send and receive bits only when the DCE creates the correct electrical impulses (called clocking) on the cable.

The DCE and DTE concept works a little like an overanxious child who is ready to throw balls to the parent as fast as possible. But the child must wait until each time his parent shouts “Now!” The parent sits there and shouts “Now! Now! Now! Now!” at a regular pace: the pace at which the parent is willing to catch the balls. Similarly, the CSU/DSU has a con- figuration that tells it the speed at which to clock the router, with the CSU shouting “Now!” by changing the electrical current on some wires (clock signals) in the serial cable.

------------------------------

Leased Lines and the T-Carrier System 365

DS0	64 Kbps
Fract T1	Multiples of 64 Kbps up to 24X
DS1 (T1)	1.544 Mbps
Fracti T3	Multiples of 1.536 Mbps up to 28X
DS3 (T3)	44.736 Mbps

Layer 2 Leased Lines with HDLC

- PC1 encapsulates IP packet in Ethernet frame
- R1 deencapsulates packet from frame and reencapses packet in HDLC frame to R2
- R2 deencapsulates packet and forwards Ethernet frame

In case you wonder why HDLC has an Address field at all, in years past the telcos offered multidrop circuits. These circuits included more than two devices, so there was more than one possible destination, requiring an Address field to identify the correct destination. [You may be asked if it supports layer 3 protocols with extensions- this is a trick question since PPP has NCP for multilink. HDLC of course (allows) using layer 3 protocols!]
Synchronous point to point, no authentication
Most HDLCs are proprietary like Cisco's is, so PPP is usually used so different equipment can talk

Configuring HDLC

Configure interface IP with ***ip address***

Following is required only when specific condition(s) are true

If an ***encapsulation*** *protocol* setting exists, enable HDLC with ***encapsulation hdlc***
(it is default, so you may not have to specify encapsulation unless another is set)

If interface is administratively down, enable with ***no shutdown***

If serial link is in a lab, use ***clock rate*** *speed* on DCE router
Optional steps:
Configure link's speed with ***bandwidth*** *speed-in-kbps*
Configure a description using ***description*** *text*

PPP Concepts

Support for both synchronous and asynchronous links
Protocol Type field in the header, allowing multiple Layer 3 protocols
Built-in authentication: PAP and CHAP
Control protocols for higher-layer protocols riding over PPP

PPP contains four main components:

Physical layer: EIA/TIA-232-C, V.24, V.35, and ISDN
Data-Link Layer:
HDLC - A method for encapsulating datagrams over serial links.
LCP - A method of establishing, configuring, maintaining, and terminating the point-to-point connection. It also provides features such as authentication
NCP(s) are a method of establishing and configuring different routed Network layer protocols for transport across the link -designed to allow the simultaneous use of multiple Network layer protocols. on a PPP link using IPv4, IPv6, and Cisco Discovery Protocol (CDP), the link uses one instance of LCP plus IPCP (for IPv4), IPv6CP (for IPv6), and CDPCP (for CDP).

Link Control Protocol (LCP) offers different PPP encapsulation options, including the following:

Function	***LCP Feature***	***Description***
Looped Link Detection	Magic number	Detects if link is looped and disables the interface
Error Detection	Link-quality monitoring (LQM)	Disable interface exceeding error percentage threshold
Multilink Support	Multilink PPP	Makes several separate physical paths appear as one logical path at layer 3 [two T1s running multilink PPP would show up as a single 3 Mbps path to a layer 3 routing protocol.]
Authentication	PAP and CHAP	Exchange names and passwords - verify identity of device at other end
Compression		Before transmission, frame payload is compressed and decompressed on the other end

PPP callback On a dial-up connection, PPP can be configured to call back after successful authentication. PPP callback can be a very good thing because it allows us to keep track of usage based upon access charges for accounting records and a bunch of other reasons. "With callback enabled, a calling router (client) will contact a remote router (server) and authenticate. Predictably, both routers have to be configured for the callback feature for this to work. Once authentication is completed, the remote router will terminate the connection and then reinitiate a connection to the calling router from the remote router.

PPP Session Establishment

When PPP connections are started, the links go through three phases of session establishment
1) Link-establishment phase LCP packets are sent by each PPP device to configure and test the link. These packets contain a field called Configuration Option that allows each device to see the size of the data, the compression, and authentication. If no Configuration Option field is present, then the default configurations will be used.

2) Authentication phase If required, either CHAP or PAP can be used to authenticate a link. Authentication takes place before Network layer protocol information is read, and it's also possible that link-quality determination will occur simultaneously.

3) Network layer protocol phase PPP uses the NCP to allow multiple Network layer protocols to be encapsulated and sent over a PPP data link. Each Network layer protocol (e.g., IP, IPv6, which are routed protocols) establishes a service with NCP.

CHAP Configuration and Verification

Configure hostname using ***hostname*** *name*

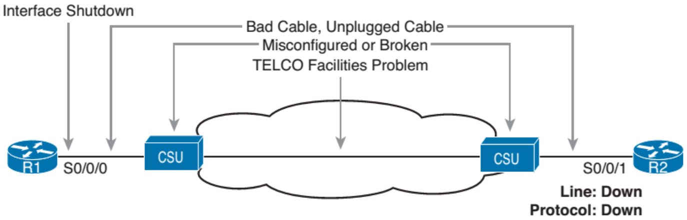
Configure username for other router and shared secret password - ***username*** *name* ***password*** *password*
Enable CHAP on the interface with ***ppp authentication chap***

Troubleshooting Serial Links

Step 1. From one router, ping the other router’s serial IP address.
Step 2. If the ping fails, check interface status on both routers and investigate likely problem areas listed below
Step 3. If the ping works, also verify that any routing protocols are exchanging routes over the link

Line Status	***Protocol Status***	***Likely Reason/Layer***
Administratively down	Down	Interface shutdown
Down	Down	Layer 1
Up	Down	Layer 2
Up	Up	Layer 3

Troubleshooting Layer 1 Problems (down/down)



Troubleshooting Layer 2 Problems

Line Status	***Protocol Status***	***Likely Reason***
Up	Down on both ends	Mismatched ***encapsulation*** commands
Up	Down on one end, Up on other	Keepalive disabled on the Up end when using HDLC
Up	Down on both ends	PAP/CHAP authentication failure

Show interfaces: (normal)

Encapsulation PPP, LCP Open
Open: IPCP, CDPCP, loopback not set

Keepalive Failure - re-enable keepalive on affected router- you will see "no keepalive set" on the interface
PAP and CHAP (MD5) Authentication Failure watch the process with ***debug ppp authentication***
Messages with O are output I are input

Troubleshooting Layer 3

Mismatched subnet is usually the culprit, but it differs with HDLC and PPP
HDLC - If interfaces are up/up and ping is successful, problem is mismatched subnet
PPP - Subnet mismatch will have a successful ping, but EIGRP and OSPF neighbor relationships will not form

Ch 13 Frame Relay FROM SLIDES

Frame Relay networks are multiaccess networks, which means that more than two devices can attach to the network, similar to LANs. Unlike with LANs, you cannot send a data link layer broad- cast over Frame Relay. Therefore, Frame Relay networks are called nonbroadcast multiaccess (NBMA) networks. Also, because Frame Relay is multiaccess, it requires the use of an address that identifies to which remote router each frame is addressed

Figure 13-1 shows the most basic components of a Frame Relay network. A leased line is installed between the router and a nearby Frame Relay switch; this link is called the access link. To ensure that the link is working, the device outside the Frame Relay network, called the data terminal equipment (DTE), exchanges regular messages with the Frame Relay switch. These keepalive messages, along with other messages, are defined by the Frame Relay Local Management Interface (LMI) protocol. The routers are considered DTE, and the Frame Relay switches are data communications equipment (DCE).

NOTE The terms DCE and DTE have different meanings in different contexts. Here, witha Frame Relay service, the roles are as described in the previous paragraph. On a physical leased line, the DCE provides Layer 1 clocking, and the DTE receives and reacts to the DCE's clock signal. These are two different (and accepted) uses of the same two terms.

Table 13-2 Frame Relay Terms and Concepts

Chapter 13: Understanding Frame Relay Concepts 393

Term	***Description***
Virtual circuit (VC)	A logical concept that represents the path that frames travel between DTEs. VCs are particularly useful when you compare Frame Relay to leased physical circuits.
Permanent virtual circuit (PVC)	A predefined VC. A PVC can be equated to a leased line in concept.
Switched virtual circuit (SVC)	A VC that is set up dynamically when needed. An SVC can be equated to a dial connection in concept.
Data terminal equipment (DTE)	DTEs are connected to a Frame Relay service from a telecommunications company. They usually reside at sites used by the company buying the Frame Relay service.
Data communications equipment (DCE)	Frame Relay switches are DCE devices. DCEs are also known as data circuit-terminating equipment. DCEs are usually in the service provider's network.
Access link	The leased line between the DTE and DCE.
Access rate (AR)	The speed at which the access link is clocked. This choice affects the connection's price.
Committed information rate (CIR)	The speed at which bits can be sent over a VC, according to the business contract between the customer and provider.
Data link connection identifier (DLCI)	A Frame Relay address used in Frame Relay headers to identify the VC.
Nonbroadcast multiaccess (NBMA)	A network in which broadcasts are not supported but more than two devices can be connected.
Local Management Interface (LMI)	The protocol used between a DCE and DTE to manage the connection. Signaling messages for SVCs, PVC status messages, and keepalives are all LMI messages.

CIR - you pay for a certain bandwidth, you get something else
You are gurantted to get CIR, but sometimes might get more.
airline ticket analogy - sell more seats than they have

Company A
Company B
Both t1's - pipes are bundled together... share "headroom" if one is using less and one needs more
if both need most, there is no "headroom"

LMI protocol between telco DCE (in it's cloud) and cusprem DTE router
DLCI to telco - unique - to one connection provided by service provider (in lab you pick (17-1000)
DLCI on the other end is different
DLCI to telco- both ends have same DLCI, other side ends have a different DLCI)

LAPF PVC info contains destination DLCI

Virtual Circuits

Frame Relay provides significant advantages over simply using point-to-point leased lines. The primary advantage has to do with VCs. Consider Figure 13-3, which shows a typical Frame Relay network with three sites.

The partial mesh has some advantages and disadvantages compared to a full mesh. Partial- mesh designs save money compared to full-mesh designs because the provider charges per VC. The downside is that traffic from R2's site to R3's site must go to R1 first and then be forwarded. If that is a small amount of traffic, it is a small price to pay. If it is a lot of traffic, a full mesh is probably worth the extra money because traffic going between two remote sites would have to cross R1's access link twice.

Frame Relay and other multiaccess WAN technologies have an even bigger cost advantage with larger enterprise WANs. For instance, imagine an organization with 100 sites, with one router at each site. To connect each pair of routers with a leased line, that company would need 4950 leased lines! And besides that, each router would need 99 serial interfaces. With Frame Relay, each router could use one serial interface and one access link into the Frame Relay cloud, for a total of 100 access links. Then, the Frame Relay provider could create a PVC between each pair of routers (a total of 4950 VCs). The Frame Relay solution requires a lot fewer actual physical links, and you would need only one serial interface on each router.

When the Frame Relay network is engineered, the design might not include a VC between each pair of sites. Figure 13-3 includes PVCs between each pair of sites; this is called a full- mesh Frame Relay network. When not all pairs have a direct PVC, it is called a partial-mesh network. Figure 13-4 shows the same network as Figure 13-3, but this time with a partial mesh and only two PVCs. This is typical when R1 is at the main site and R2 and R3 are at remote offices that rarely need to communicate directly.

The partial mesh has some advantages and disadvantages compared to a full mesh. Partial- mesh designs save money compared to full-mesh designs because the provider charges per VC. The downside is that traffic from R2's site to R3's site must go to R1 first and then be forwarded. If that is a small amount of traffic, it is a small price to pay. If it is a lot of traffic, a full mesh is probably worth the extra money because traffic going between two remote sites would have to cross R1's access link twice.

Full mesh FR has PVCs for each site pair
Partial mesh FR doesnt have PVCs for each site pair

LMI
The most important LMI message relating to topics on the exam is the LMI status inquiry message. LMI status messages perform two key functions:

- They perform a keepalive function between the DTE and DCE. If the access link has a problem, the absence of keepalive messages implies that the link is down.

- They signal whether a PVC is active or inactive. Even though each PVC is predefined, its status can change. An access link might be up, but one or more VCs could be down. The router needs to know which VCs are up and which are down. It learns that information from the switch using LMI status messages.

Name	*Document*	*IOS LMI-Type Parameter*
Cisco	Proprietary	***cisco***
ANSI	T1.617 Annex D	***ansi***
ITU	Q.933 Annex A	***q933a***

keyword used in the Cisco IOS software ***frame-relay lmi-type*** interface subcommand.
USE DEFAULT AUTOCONFIGURE

A Frame Relay-connected router encapsulates each Layer 3 packet inside a Frame Relay header and trailer before it is sent out an access link. The header and trailer are defined by Frame Relay (or more specifically, the Link Access Procedure Frame Bearer Services [LAPF] specification, ITU Q.922-A). The sparse LAPF framing provides error detection with an FCS in the trailer, a DLCI field (discussed in detail later in this chapter), plus a few other header fields. Figure 13-5 diagrams the frame.

However, routers actually use a longer header than just the standard LAPF header because the standard header does not provide all the fields usually needed by routers. In particular, Figure 13-5 does not show a Protocol Type field. Each data link header needs a field to define the type of packet that follows the data link header. If Frame Relay is using only the LAPF header, DTEs (including routers) cannot support multiprotocol traffic because there is no way to identify the type of protocol in the Information field.
Two solutions were created to compensate for the lack of a Protocol Type field in the stan- dard Frame Relay header:
■ Cisco and three other companies created an additional header, which comes between the LAPF header and the Layer 3 packet shown in Figure 13-5. It includes a 2-byte Protocol Type field, with values matching the same field Cisco uses for HDLC.

■ RFC 1490 (and later 2427), Multiprotocol Interconnect over Frame Relay, defined the second solution. RFC 1490 was written to ensure multivendor interoperability between Frame Relay DTEs. This RFC defines a similar header, also placed between the LAPF header and Layer 3 packet, and includes a Protocol Type field as well as many other options.

Layer 2 only error correction, layer 3 error correction (quote from class)
DLCI = DelSee

At a basic conceptual level, Frame Relay addresses, called data link connection identifi-ers (DLCI), have some similarity with the more familiar MAC and IP addresses. All these addresses exist as binary values, but they all have some more convenient format: hex for MAC addresses, dotted decimal for IP, and decimal for DLCIs. Frame Relay defines the DLCI as a 10-bit value, written in decimal, with the low- and high-end values usually reserved. (The specific range does not matter much because the service provider assigns the values, but they usually range from around 17 to a little less than 1000.)
When you dig deeper, particularly into how DLCIs impact the forwarding of Frame Relay frames, the similarities to MAC and IP addressing fades, and stark differences appear. This section focuses on that forwarding logic, first discussing the idea that Frame Relay ad- dresses actually identify one end of a PVC. Following that, the discussion turns to the for- warding logic used inside the Frame Relay cloud.

The service provider assigns each PVC two local DLCI values: one on one end of the PVC, and one for the other end. The term local DLCI has several different origins, but you can think of the word local as emphasizing the fact that from a router's perspective, the local DLCI is the DLCI used on the local end of the PVC where the router sits. Figure 13-7 shows the idea.

In this example, the PVC between routers A and B has two DLCIs assigned by the provider. Router A's end uses local DLCI 41 to identify the PVC, and router B's end uses DLCI 40 to identify the same PVC. Similarly, the PVC between routers A and C, as usual, has two local DLCIs assigned, one on each end. In this case, router A’s end uses 42, and router C’s end uses 40.

The service provider could have used any DLCI values within the range of legal values, with one exception: The local DLCIs on a single access link must be unique among all PVCs that use one physi- cal Frame Relay access link, because Frame Relay DLCIs are locally significant.

Network addressing with FR - pages 400-end was pretty quick but important stuff...

- One subnet containing all Frame Relay DTEs
- One subnet per VC
- A hybrid of the first two options

- This figure shows a fully meshed Frame Relay network because the single-subnet option is usually used when a full mesh of VCs exists. In a full mesh, each router has a VC to every other router, meaning that each router can send frames directly to every other router.

Network Layer Addressing with Frame Relay

Frame Relay networks have both similarities and differences as compared to LAN and point- to-point WAN links. These differences introduce some additional considerations for passing Layer 3 packets across a Frame Relay network. In particular, Frame Relay gives us three dif- ferent options for assigning subnets and IP addresses on Frame Relay interfaces:

- One subnet containing all Frame Relay DTEs
- One subnet per VC
- A hybrid of the first two options

- This figure shows a fully meshed Frame Relay network because the single-subnet option is usually used when a full mesh of VCs exists. In a full mesh, each router has a VC to every other router, meaning that each router can send frames directly to every other router.

=---------------

Chapter 7 - Virtual Private Networks

VPN Fundamentals

VPNs provide: Confidentiality (Privacy), Authentication, Data Integrity, Anti-replay

To accomplish these goals,

Two devices near the edge of network create a VPN/VPN tunnel, Adding headers to the original packet

The cost of a high-speed Internet connection is usually much less than that of many modern WAN options.

The Internet is seemingly everywhere, so is availability: intranet, extranet, and remote access connections.

The VPN devices also encrypt the original IP packet

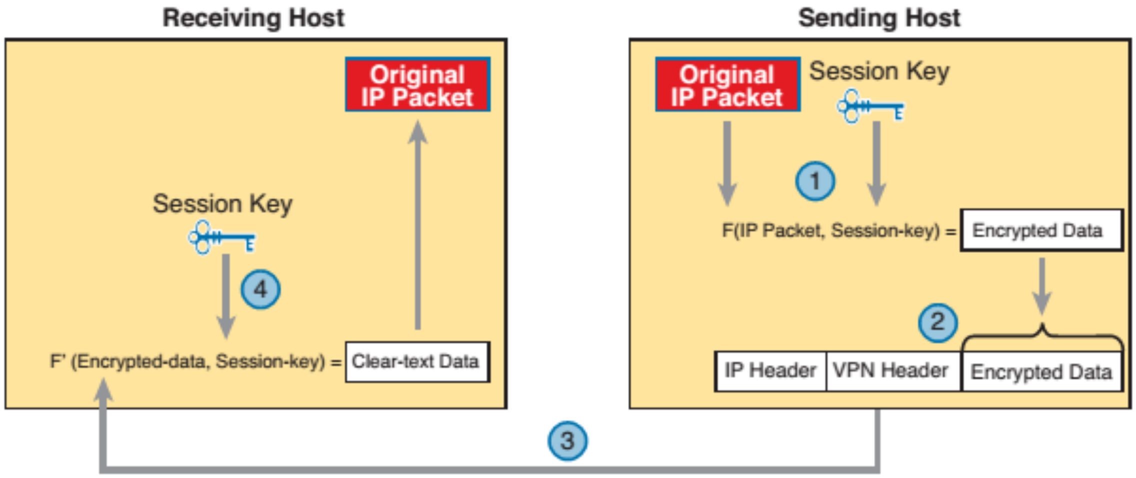
Types of VPNs
Intranet - Site-to-site VPN connecting all computers at two sites, usually one VPN device at each site
Extranet - Site-to-site VPN connecting computers at partnering organizations, usually one VPN device at each site
Remote Access   Connects individual Internet users to the enterprise

To build a VPN, the following hardware/software devices are needed:

Routers - Routing plus VPN functions through add-on cards
Adaptive Security Appliances (ASA) - Leading security appliance with VPN concentrator capabilities
VPN client - Software enabling remote access devices to connect

VPN Benefits

Cost - can be cheaper than private WAN options (leased-lines)
Security - can be as secure as private WAN connections
Scalability - scaled to many sites at a reasonable cost



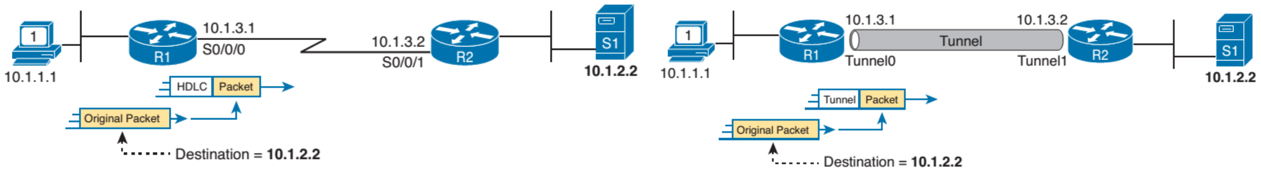
IPSec VPN The four steps highlighted in the figure are as follows:
1. The sending VPN device feeds the original packet and the session key into the encryption formula, calculating the encrypted data.
2. The sending device encapsulates the encrypted data into a packet, which includes the new IP header and VPN header.
3. The sending device sends this new packet to the destination VPN device
4. The receiving VPN device runs the corresponding decryption formula, using the encrypted data and session key- the same key value as was used on the sending VPN device-to decrypt the data

Encryption Algorithm	***Key Length (Bits)***	***Comments***
DES	56	Older and less secure than the other options
Triple DES (3DES)	56 x 3 (168)	3 different 56-bit DES keys in succession
AES	128 and 256	Stronger encryption and less

SSL VPNs
IPSec alternative- Web browser's SSL (port 443) is actually small tunnel itself!
The Cisco AnyConnect VPN client is PC software for a VPN remote-access tunnel.

GRE Tunnel Concepts
The endpoint first encrypts the packet, then encapsulates the packet in a new IP header. The new IP header uses addresses that allow the routers in the unsecured network between the two VPN tunnel end- points to forward the VPN IP packet. The original IP packet, including the original IP header, is encrypted and unreadable.

Tunnels, just like serial

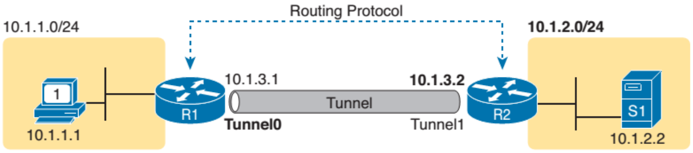


Tunnels exist between 2 routers and act like a serial link

Instead of serial interfaces with packets inside HDLC headers, tunnel interfaces use tunnel headers

Interfaces have IP addresses in the same subnet

Routers learn about interface addresses via routing protocols, even form neighborships.



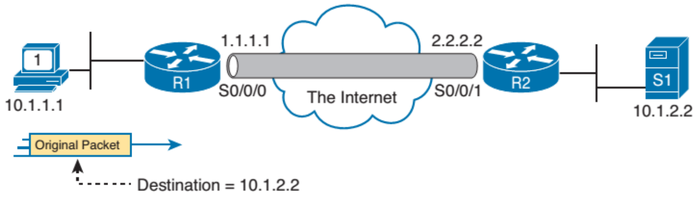
R1 Routing Table

Subnet	Interface	Next-hop
10.1.2.0/24	**Tunnel0**	**10.1.3.2**

R2 Routing Table

Subnet	Interface	Next-hop
10.1.1.0/24	Tunnel1	10.1.3.1

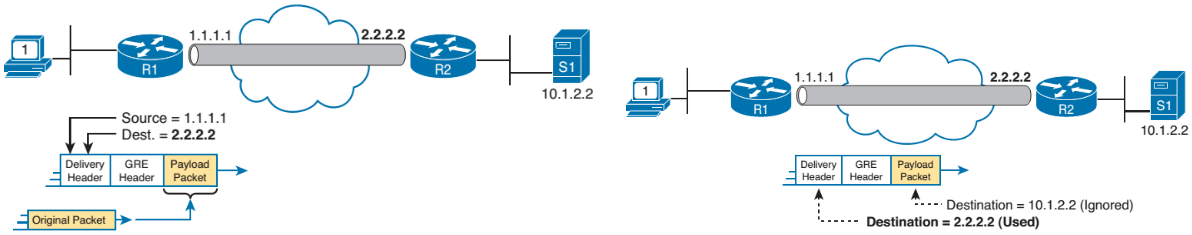
Routes learned by each router listed at the bottom.



Details that the engineer needs to know about the two routers before configuring the GRE tunnel on both ends:

Interfaces R1 and R2 each will use to connect to the Internet.

IP addresses each router uses on their Internet connections

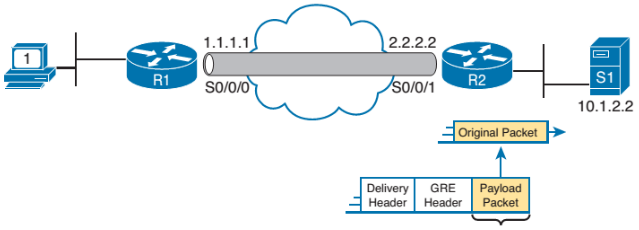


A packet coming into router R1 from PC1, needs to get to 10.1.2.2; when the router uses its IP routing logic R1 wants to send over the tunnel interface.

This figure shows the encapsulation done by R1

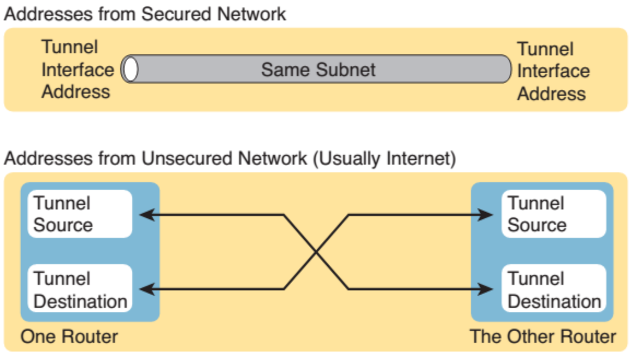
While this packet passes through the Internet, the routers on the Internet use this outer GRE delivery IP header to route the packet; they just forward the IP packet based on the 2.2.2.2 destination IP address.

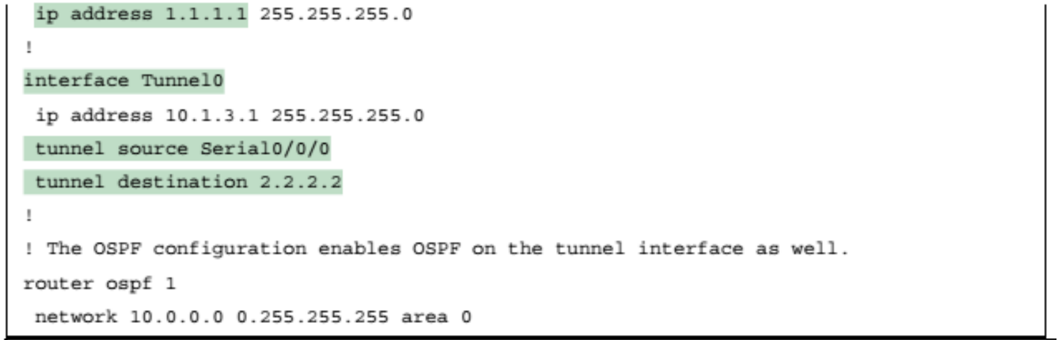
This packet may be routed by many routers in the Internet before arriving, then R2 needs to extract the original IP packet.



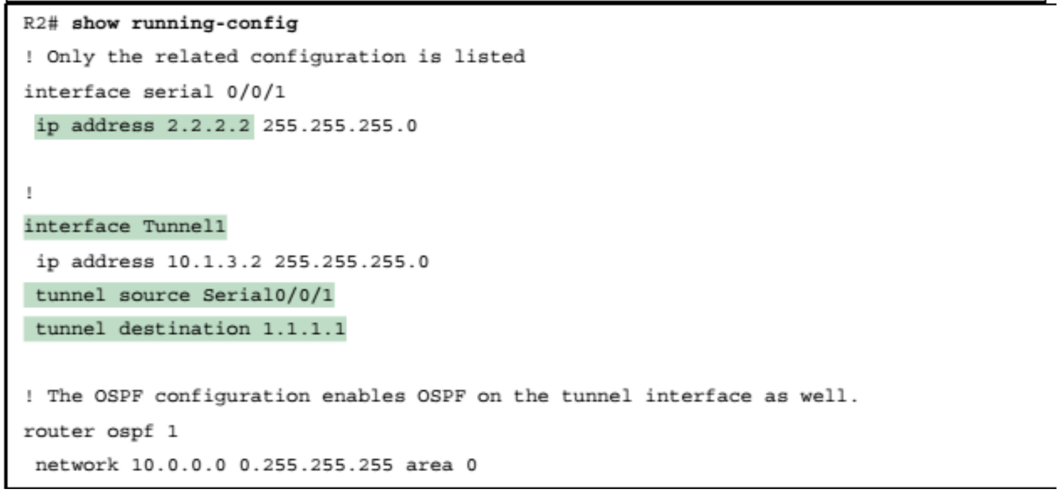
Configuring GRE Tunnels

1. Create a local tunnel interface with ***interface tunnel number*** (does not have to match between routers)
2. Assign an IP to the tunnel interface with ***ip address address mask***
   Use subnet from secure network's address range, both routers should use address from same subnet
3. Configure tunnel's source IP in the public network with ***tunnel source interface*** or ***tunnel source ip-address*** in interface mode. Value must match other router's tunnel destination
4. Configure tunnel's destination IP with ***tunnel-destination ip-address*** (must match source IP from Step 3)
5. Configure the routers to use the tunnel by enabling a dynamic routing protocol or configuring static routes





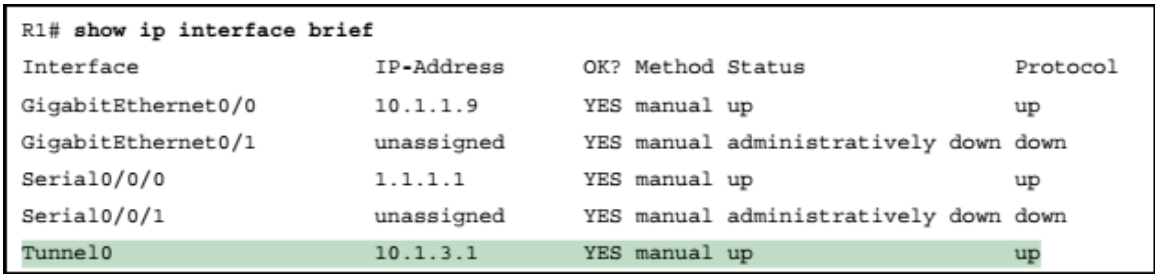
```
 ip address 1.1.1.1 255.255.255.0
!
interface Tunnel0
 ip address 10.1.3.1 255.255.255.0
 tunnel source Serial0/0/0
 tunnel destination 2.2.2.2
!
! The OSPF configuration enables OSPF on the tunnel interface as well.
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
```



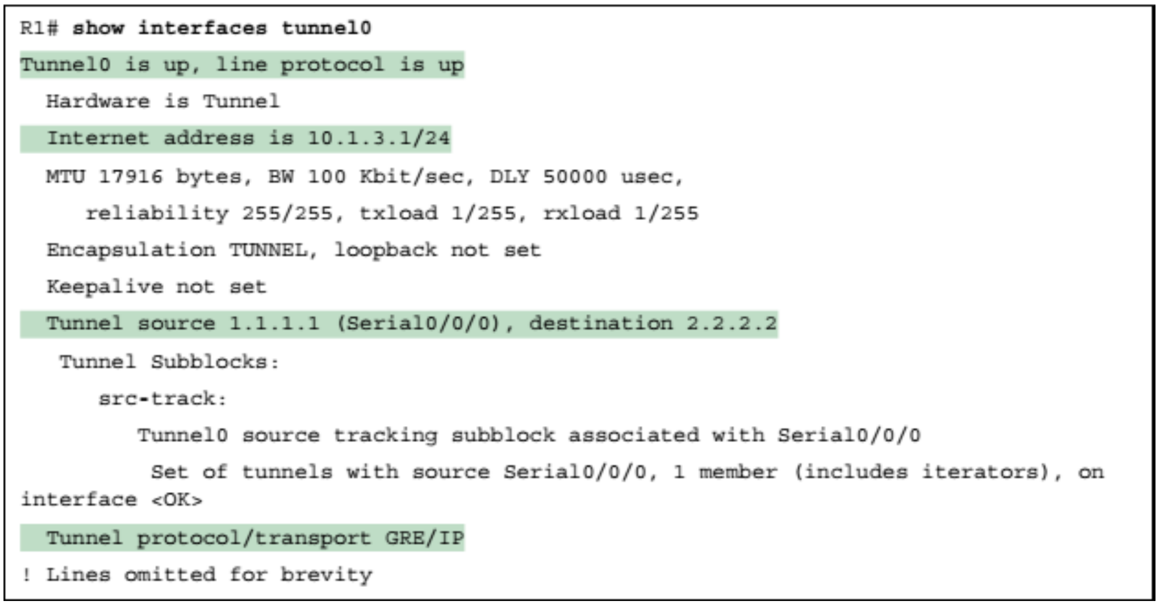
```
R2# show running-config
! Only the related configuration is listed
interface serial 0/0/1
 ip address 2.2.2.2 255.255.255.0

!
interface Tunnel1
 ip address 10.1.3.2 255.255.255.0
 tunnel source Serial0/0/1
 tunnel destination 1.1.1.1

! The OSPF configuration enables OSPF on the tunnel interface as well.
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
```

R1 and R2 form a tunnel using public addresses 1.1.1.1 and 2.2.2.2, respectively.
The tunnel uses subnet 10.1.3.0/24, with R1 and R2 using IP addresses 10.1.3.1 and 10.1.3.2, respectively.

Verifying a GRE Tunnel

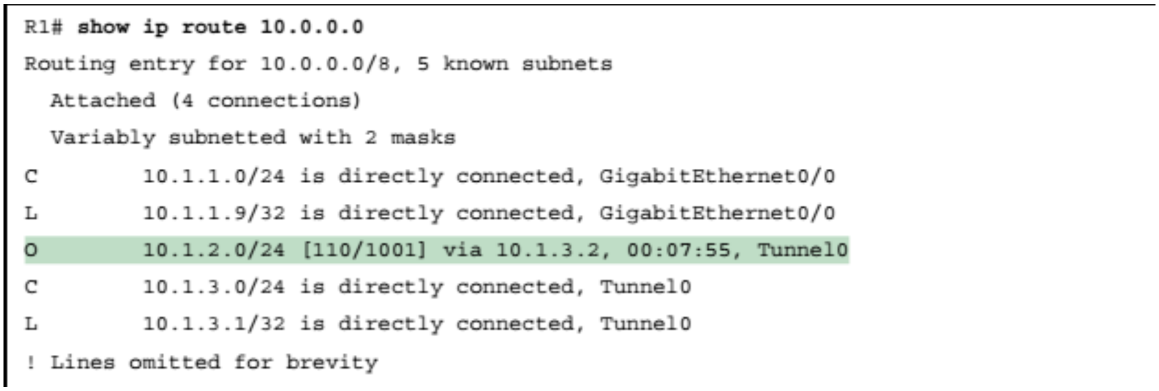


```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         10.1.1.9        YES manual up                    up
GigabitEthernet0/1         unassigned      YES manual administratively down down
Serial0/0/0                1.1.1.1         YES manual up                    up
Serial0/0/1                unassigned      YES manual administratively down down
Tunnel0                    10.1.3.1        YES manual up                    up
```



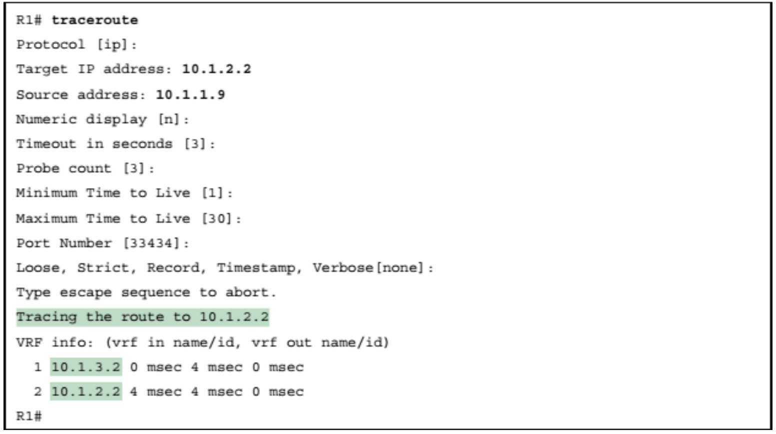
```
R1# show interfaces tunnel0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 10.1.3.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 1.1.1.1 (Serial0/0/0), destination 2.2.2.2
   Tunnel Subblocks:
      src-track:
         Tunnel0 source tracking subblock associated with Serial0/0/0
          Set of tunnels with source Serial0/0/0, 1 member (includes iterators), on
interface <OK>
  Tunnel protocol/transport GRE/IP
! Lines omitted for brevity
```

The familiar show ip interface brief command on R1, with R1's tunnel0 interface highlighted.
Output of sh interface for R1's Tunnel0 interface. Note that it lists the local router (R1) configuration of the source (1.1.1.1) and destination (2.2.2.2) IP addresses, and it confirms the use of GRE encapsulation

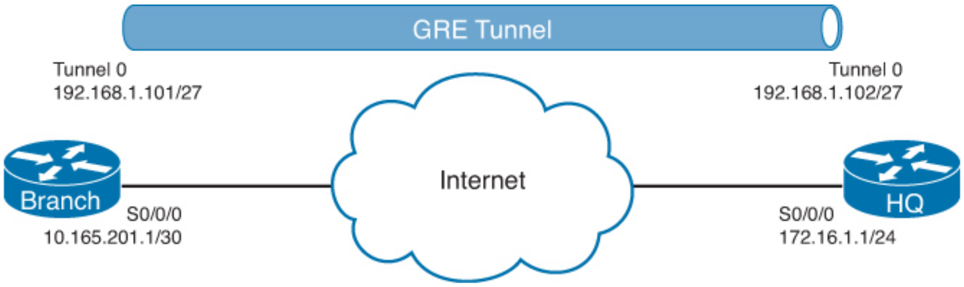


```
R1# show ip route 10.0.0.0
Routing entry for 10.0.0.0/8, 5 known subnets
  Attached (4 connections)
  Variably subnetted with 2 masks
C        10.1.1.0/24 is directly connected, GigabitEthernet0/0
L        10.1.1.9/32 is directly connected, GigabitEthernet0/0
O        10.1.2.0/24 [110/1001] via 10.1.3.2, 00:07:55, Tunnel0
C        10.1.3.0/24 is directly connected, Tunnel0
L        10.1.3.1/32 is directly connected, Tunnel0
! Lines omitted for brevity
```

R1 listing an OSPF-learned route to R2's LAN subnet of 10.1.2.0/24



```
R1# traceroute
Protocol [ip]:
Target IP address: 10.1.2.2
Source address: 10.1.1.9
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 10.1.2.2
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.3.2 0 msec 4 msec 0 msec
  2 10.1.2.2 4 msec 4 msec 0 msec
R1#
```



Branch Router

`Branch(config)#`**`interface tunnel0`**	Moves to interface configuration mode
`Branch(config-if)#`**`tunnel mode gre ip`**	Sets tunnel encapsulation method to GRE over IP
`Branch(config-if)#`**`ip address 192.168.1.101 255.255.255.224`**	Sets IP address and mask information for interface
`Branch(config-if)`**`#tunnel source 10.165.201.1`**	Maps tunnel source to Serial 0/0/0 interface
`Branch(config-if)#`**`tunnel destination 172.16.1.1`**	Maps tunnel destination to HQ router

HQ Router

`HQ(config)#`**`interface tunnel0`**	Moves to interface configuration mode
`HQ(config-if)#`**`tunnel mode gre ip`**	Sets tunnel encapsulation method to GRE over IP
`HQ(config-if)#`**`ip address 192.168.1.102 255.255.255.224`**	Sets IP address and mask information for interface
`HQ(config-if)#`**`tunnel source 172.16.1.1`**	Maps tunnel source to Serial 0/0/0 interface
`HQ(config-if)#`**`tunnel destination 10.165.201.1`**	Maps tunnel destination to Branch router

Verifying the Tunnel

`Router#`**`show interface tunnel0`**	Verifies GRE tunnel configuration.
`Router#`**`show ip interface brief`**	Shows brief summary of all interfaces, including tunnel interfaces.
`Router#`**`show ip interface brief | include tunnel`**	Shows summary of interfaces named tunnel.
`Router#`**`show ip route`**	Verifies a tunnel route between Branch and HQ routers. The path will be seen as directly connected (C) in the route table.

VPN FROM SLIDES

Mainly IPSEC
SSL variants
GRE tunnels, point to point, acts and looks like a basic serial link
(GRE tunnel instead of hdlc)
interfaces have IPAddresses in the same subnet
learns using routing protocols on both ends

Each end shows up int the routers on both ends - 10.1.3.1 Tunnel0 interface ====TUNNEL==== tunnel1 10.1.3.2 interface
Looks alot like etherchannel when implemented
10.1.3.1 is likely a virtual interface
NATs out - 10.1.3.x is a private address NAT to 2.2.2.2 send to other end 1.1.1.1 to unwrap tunnel with destination back onto 10.1.3x

```
int s0/0/0
        ip address 1.1.1.1 255.255.255.0

interface tunnel0
        ip address 10.1.3.1255.255.255.0
        tunnel source Serial 0/0/0
        tunnel destination 2.2.2.2
```

OSPF for 10.1.3.x

OTHER SIDE: ================================

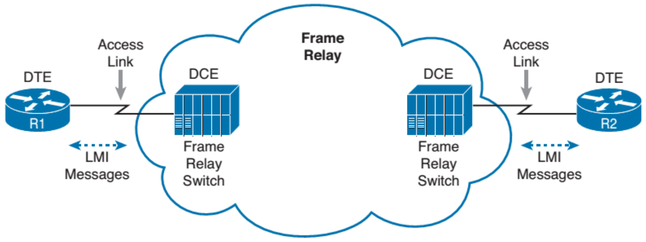
```
int s0/0/0
        ip address 2.2.2.2 255.255.255.0

interface tunnel2   <tunnel number here doesnt matter - is just a name  for the 'virtual port' device)
        ip address 10.1.3.2 255.255.255.0
        tunnel source Serial 0/0/0
        tunnell destination 1.1.1.1
```

OSPF with for 10.1.3.x

Chapter 13 - Understanding Frame Relay

Frame Relay Overview

Provide more features and benefits than a simple point-to-point WAN
Called Nonbroadcast Multiaccess (NBMA) networks
Basic physical topology and terminology

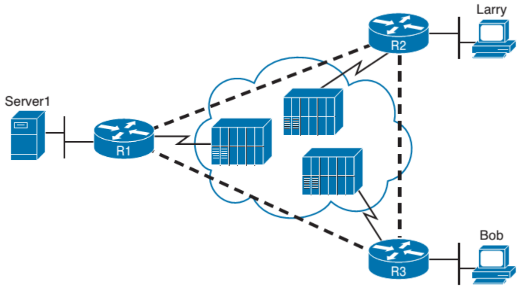


To ensure that the link is working, the router outside the Frame Relay network [data terminal equipment (DTE)], exchanges messages with the Frame Relay switch at the SP [data communications equipment (DCE)]. These keepalive messages, along with other messages, are defined by the Frame Relay Local Management Interface (LMI) protocol .

Virtual Circuit (VC)	Path that frames travel between DTEs - a “logical leased physical circuit”
Permanent VC (PVC)	Predefined (by service provider) VC
Switched VC (SVC)	VC set up dynamically when needed; similar to a dialup connection
Data Terminal Equipment (DTE)	Connected by telecom; usually reside at sites company (custprem)
Data Comm Equipment (DCE)	Frame Relay switches are DCE devices; usually in the SP's network
Access link	The leased line between DTE and DCE
Access Rate (AR)	Clocked speed for access link
Committed Information Rate (CIR)	VC bit speeds, according to provider contract
Data Link Connection ID (DLCI)	For non-broadcast-networks where 2+ devices can be connected
Local Management Interface (LMI)	Protocol used between DCE and DTE to manage the connection

Virtual Circuits

VCs define the logical path between two DTEs, acts like a point-to-point circuit
VCs share the access link and FR network. Many customer share the same FR network, and each VC has a CIR
Provides connectivity to each site with a single access link between them
Major advantage over leased lines, and requires fewer physical interfaces



Full-mesh Frame Relay has PVCs for each site pair
Partial-mesh Frame Relay does not have PVCs for each site pair

LMI and Encapsulation Types

LMI status messages perform two key functions:
Keepalive between DTE and DCE. Absence of these messages implies a down link
Signal whether a PVC is active or inactive - Access link may be up, but VC may be down

Name	***Document***	***IOS LMI-Type Parameter***
Cisco	Proprietary	cisco
ANSI	T1.617 Annex D	ansi
ITU	Q.933 Annex A	q933a

Use the default, it will auto sense what LMI to use

Frame Relay Encapsulation and Framing

- Router encapsulates packets inside Frame Relay header and trailer
- The Link Access Procedure Frame (LAPF) adds error detection and a DLCI field

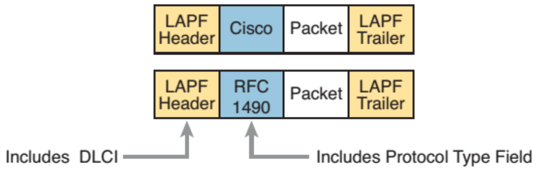
  However, routers use a longer header than the LAPF standard

  - Without it, multiprotocol traffic could not be supported

  Two solutions to LAPF header

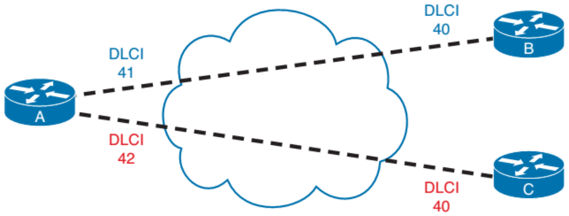
  -Cisco created an additional header

  -RFC 1490 (2427) Multiprotocol Interconnect over Frame Relay



Frame Relay Local Addressing

PVCs are assigned 2 Data Link Connection Identifier (DLCI) values



Service provider can use any DLCI values with one exception: local DLCIs on an access link must be unique
The local DLCIs on a single access link must be unique among all PVCs that use one physical Frame Relay access link, because Frame Relay DLCIs are locally significant

The Frame Relay header lists only one DLCI field, and it does not identify a source or a destination, but the PVC. considers the fact that the provider knows the local DLCI used on both ends of the PVC, plus the access links that connect to those routers.

First, router A sends a frame over the PVC connected to router B. For router A, it only knows it as the PVC with local DLCI 41, so it sends it with that in the header. The service provider looks at the info about this PVC, forwards the frame over toward router B with the new DLCI 40 header, so the frame arrives at router B.

Network Layer Addressing with Frame Relay

3 different options for assigning subnets/IPs on Frame Relay interfaces

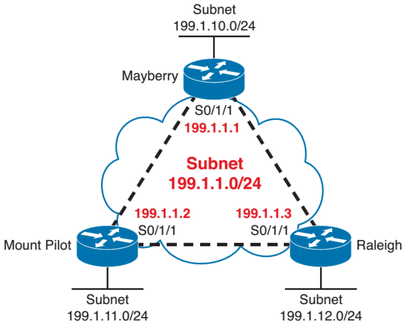
One subnet containing all Frame Relay DTEs; one subnet per VC; or a hybrid of the first two options

<u>Frame Relay Layer 3 Addressing Option 1</u>

One Subnet Containing All Frame Relay DTEs - No Partial Mesh

Straightforward and conserves IP address space

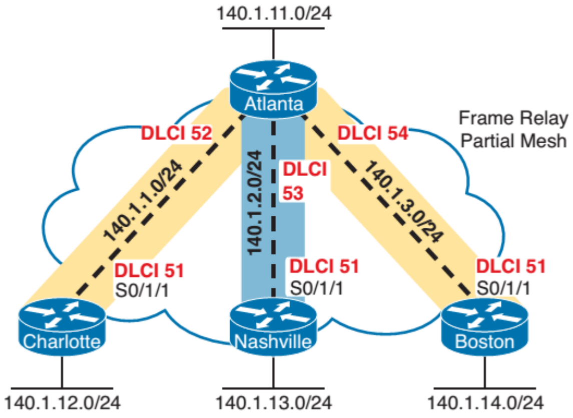
Unfortunately, most companies build partial-mesh Frame Relays



Frame Relay Layer 3 Addressing Option 2

One Subnet Per VC

Uses same logic as point-to-point links. Does waste some IPs, but works better with partial-mesh designs



Frame Relay Layer 3 Addressing Option 3

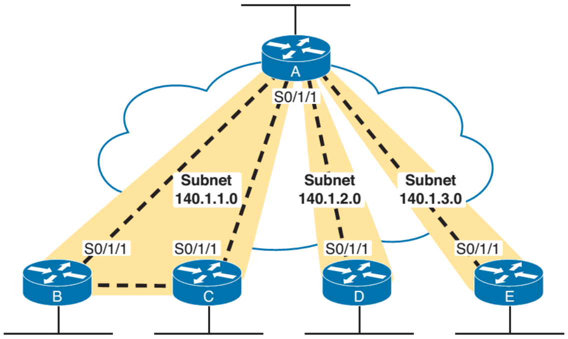
Hybrid Approach - Uses subinterfaces - a subnet for each fully meshed subset

Point-to-point subinterfaces are used when VC is all that is in a group

A to D and/or A to E

Multipoint interfaces are used when more than 2 routers are in a group

A, B, and C



Chapter 14 - Implementing Frame Relay- Configuration and Verification

You must consider the following when planning Frame Relay:

Define which physical sites need a FR access link installed, define the clock (access) rate for each link.

Define each VC by identifying the endpoints and setting the committed information rate (CIR).

Agree to an LMI type (usually dictated by the provider).

The network engineer who plans the Frame Relay configuration must also choose the following settings, independent of any settings of the Frame Relay provider:

Choose the IP subnetting scheme: one subnet for all virtual circuits (VC), one subnet for each VC, or a subnet for each fully meshed subset. (the Layer 3 options 1-3)

Pick whether to assign the IP addresses to physical, multipoint, or point-to-point subinterfaces.

Choose which VCs need to use IETF encapsulation instead of the default value of cisco. (IETF encapsulation is usually used when one router is not a Cisco router.)

Planning a Frame Relay Configuration

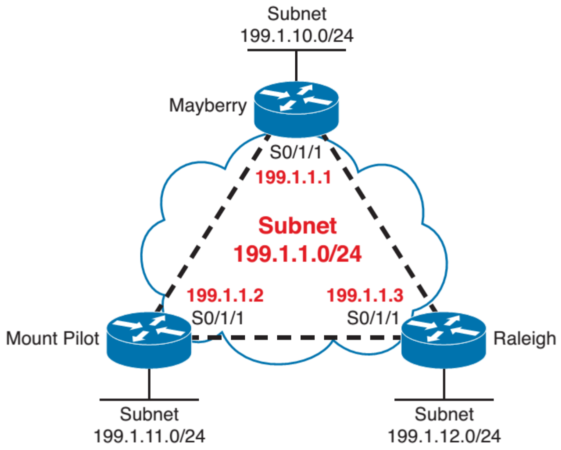
1. Configure interface to use Frame relay with ***encapsulation frame-relay*** *type*
2. Configure IP address on the interface (***ip address***)
3. (Optional) manually set LMI type (***frame-relay lmi type***)
4. (Optional) change default encapsulation (cisco) to ***ietf***
   - For all VCs add ***ietf*** to ***encapsulation frame-relay*** line
   - For a single VC add ***ietf*** to ***frame-relay interface-dlci*** line
5. (Optional) define static mapping using ***frame-relay map ip*** *address dlci* ***broadcast***

Do this if you are not using the (default) Inverse ARP to map the DLCI to the next-hop router's IP address

6. On subinterfaces, associate one DLCI (point-to-point) or multiple DLCIs (multipoint) with the subinterface:

For point-to-point: Use the ***frame-relay interface-dlci*** *dlci* command
For multipoint: Use the ***frame-relay map ip*** *ip-address dlci* ***broadcast***

Configuring Using Physical Interfaces and One IP Subnet



Full Mesh with IP Address

Install links into three routers, using physical interfaces, default settings for LMI, Inverse ARP, and encapsulation
Create a full mesh of PVCs using a single subnet (e.g., Class C network 199.1.1.0) in the Frame Relay network.

Steps One and Two of "Planning" list: Configuring Using Physical Interfaces and One IP Subnet
The first example (before other stuff is added) would work, but we need to configure the other settings on top.

Mayberry Configuration

```
interface serial0/1/1
 encapsulation frame-relay
 ip address 199.1.1.1 255.255.255.0
!
interface gigabitethernet 0/0
 ip address 199.1.10.1
255.255.255.0
!
router eigrp 1
 network 199.1.1.0
 network 199.1.10.0
```

Mount Pilot Configuration

```
interface serial0/1/1
encapsulation frame-relay
ip address 199.1.1.2 255.255.255.0
!
interface gigabitethernet 0/0
ip address 199.1.11.2
255.255.255.0
!
router eigrp 1
 network 199.1.1.0
 network 199.1.11.0
```

Raleigh Configuration

```
interface serial0/1/1
encapsulation frame-relay
ip address 199.1.1.3 255.255.255.0
!
interface gigabitethernet 0/0
ip address 199.1.12.3
255.255.255.0
!
router eigrp 1
 network 199.1.1.0
 network 199.1.12.0
```

The ***encapsulation frame-relay*** command tells the routers to use Frame Relay data link protocols instead of the default, which is High-Level Data Link Control (HDLC). Note that the IP addresses on the three routers' serial interfaces are all in the same Class C network. Also, this simple configuration takes advantage of the following IOS default settings:

The LMI type is automatically sensed; the (default) encapsulation is Cisco.

PVC DLCIs are learned via LMI status messages. Inverse ARP is enabled (by default) and is triggered when a router receives an LMI status message declaring that the VCs are up.

Configuring the Encapsulation and LMI

The defaults so far work just fine. To show an alternative configuration, let's add the following requirements: The Raleigh router needs IETF encapsulation on both VCs. Mayberry's LMI type should be ANSI, and LMI autosense should not be used.

Mayberry Configuration with New Requirements

Raleigh Configuration with New Requirements

```
interface serial0/1/1
 encapsulation frame-relay
 frame-relay lmi-type ansi
 frame-relay map ip 199.1.1.3 53 ietf
 ip address 199.1.1.1  255.255.255.0
```

```
interface serial0/1/1
 encapsulation frame-relay ietf
 ip address  199.1.1.3  255.255.255.0
```

Raleigh changed its encapsulation for both its PVCs with the ***ietf*** keyword. This applies to all VCs on the interface.
The two VCs terminating in Mayberry each need to use either IETF or Cisco encapsulation. So, it needs the ***frame-relay map*** command, separately addressing it's DLCI (53) for the VC to Raleigh with the ***ietf*** keyword. Mount Pilot needs to have this same configuration change, just not shown here for brevity.

The new requirements for Mayberry called for disabling autosensing of the LMI type. Specifying ***frame-relay lmi-type ansi***, specifies the LMI-type it would have used anyway, but also turns off autosensing.

Frame Relay Address Mapping
A Mapping Table is needed on multiaccess networks to correlate next-hop router's Layer 3 addresses to their matching Layer 2 DLCI address.

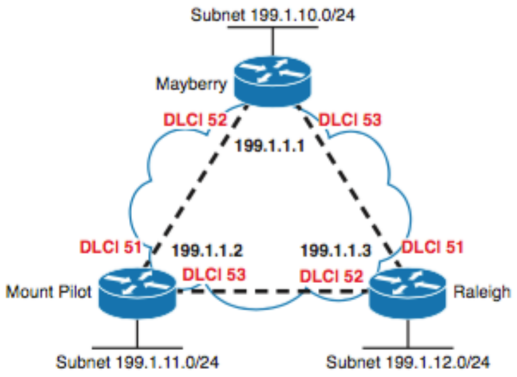
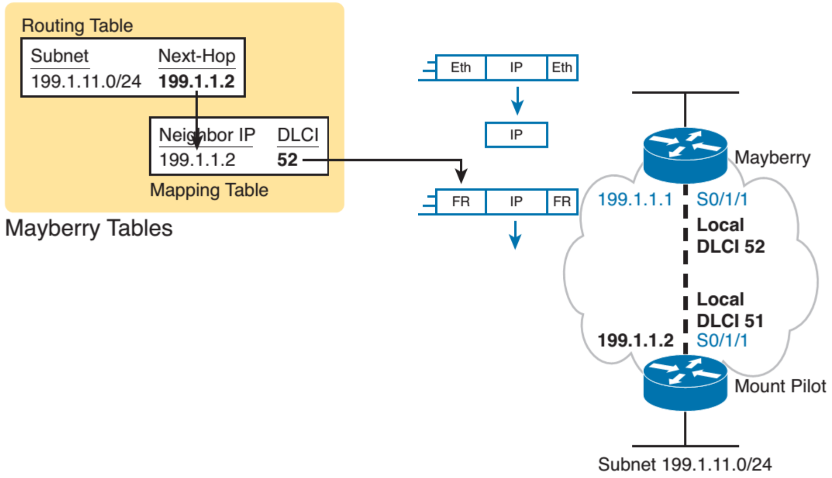


Figure 14-2 *Full Mesh with Local DLCIs Shown*



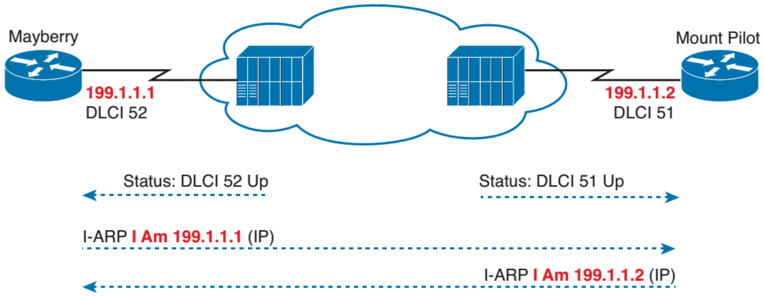
When a packet enters Mayberry's LAN interface and is destined for network 199.1.11.0/24, (Mount Pilot's LAN) it goes through normal routing steps, removing the packet from Ethernet header and trailer, choosing to route the packet out Mayberry's S0/1/1 interface to Mount Pilot. The Frame Relay Mapping table lists that same next-hop router IP address, along with the DLCI used to send frames to that address (the equivalent of an ARP table). The DLCI (52, Mayberry's local DLCI for the PVC connected to Mount Pilot) is put in the Frame Relay header.
The following lists the ***show frame-relay pvc*** and ***show frame-relay map*** which displays the mapping table.

```
Mayberry# show frame-relay pvc
PVC Statistics for interface Serial0/1/1 (Frame Relay DTE)
```

```
            Active      Inactive      Deleted      Static
Local       2           0             0            0
Switched    0           0             0            0
Unused      0           0             0            0
DLCI = 52, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/1/1

input pkts 37               output pkts 39              in bytes 2542
out bytes 2752              dropped pkts 0              in pkts dropped 0
out pkts dropped 0          out bytes dropped 0

in FECN pkts 0              in BECN pkts 0              out FECN pkts 0
out BECN pkts 0             in DE pkts 0                out DE pkts 0
out bcast pkts 26           out bcast bytes 1664
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 00:20:02, last time pvc status changed 00:20:02

DLCI = 53, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/1/1
input pkts 37               output pkts 37              in bytes 2618
out bytes 2746              dropped pkts 0              in pkts dropped 0
out pkts dropped 0          out bytes dropped 0
in FECN pkts 0              in BECN pkts 0              out FECN pkts 0
out BECN pkts 0             in DE pkts 0                out DE pkts 0
out bcast pkts 25           out bcast bytes 1630
5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:20:02, last time pvc status changed 00:20:02
```

```
Mayberry# show frame-relay map
Serial0/1/1 (up): ip 199.1.1.2 dlci 52(0x34,0xC40), dynamic,
          broadcast,, status defined, active
Serial0/1/1 (up): ip 199.1.1.3 dlci 53(0x35,0xC50), dynamic,
          broadcast,, status defined, active
```

The show frame-relay pvc command lists two DLCIs, 52 and 53, and both are active.
The show frame-relay map - “ip 199.1.1.2 dlci 52” - it's just like an ARP table. Point to point subinterfaces will not show the IP address. This is because the routing table is referenced instead for that Layer 3 info on subints.



Inverse ARP

The ARP process used by Inverse ARP differs for ARP on a LAN. After the VC is up, each router announces its network layer address by sending an Inverse ARP message over that VC. It's almost like a hello message- to get the other side to map the VC with to the IP address.

- Mayberry sends an InARP with 199.1.1.1; Mount Pilot receives the InARP with DLCI 51 in the header, so Mount Pilot’s mapping lists 199.1.1.1 and DLCI 51.

- Mount Pilot sends an InARP with 199.1.1.2; Mayberry receive the InARP with DLCI 52 in the header, so Mayberry’s mapping lists 199.1.1.2 and DLCI 52.

Static Frame Relay Mapping

You can statically configure the same mapping information instead of using Inverse ARP. In a production network, you probably would just go ahead and use Inverse ARP. You'd still need to know how to configure the static map command statements.

The broadcast keyword on the frame-relay map command is required when the router needs to send broadcasts or multicasts to the neighboring router- for example, to support routing protocol messages such as Hellos.

Mayberry

```
interface serial 0/0/0
 no frame-relay inverse-arp
 frame-relay map ip 199.1.1.2 52 broadcast
 frame-relay map ip 199.1.1.3 53 broadcast
```

Mount Pilot

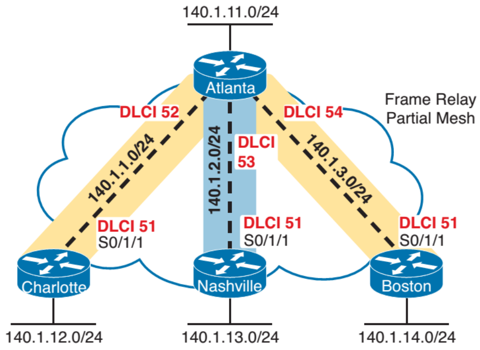
```
interface serial 0/0/0
 no frame-relay inverse-arp
 frame-relay map ip 199.1.1.1 51 broadcast
 frame-relay map ip 199.1.1.3 53 broadcast
```

Raleigh

```
interface serial 0/0/0
 no frame-relay inverse-arp
 frame-relay map ip 199.1.1.1 51 broadcast
 frame-relay map ip 199.1.1.2 52 broadcast
```

Configuring Point-to-Point Subinterfaces - Partial Mesh w/ Subnets and local DLCIs

. Point-to-point subinterfaces work well when the subnetting design calls for one subnet for each PVC. Examples that follow show four routers using only point-to-point subinterfaces. Pay close attention to the command prompts as they change when you configure subinterfaces.



<u>Atlanta Configuration</u>

```
Atlanta(config)# interface serial0/1/1
Atlanta(config-if)# encapsulation frame-relay

Atlanta(config-if)# interface serial 0/1/1.1 point-to-point
Atlanta(config-subif)# ip address 140.1.1.1 255.255.255.0
Atlanta(config-subif)# frame-relay interface-dlci 52
Atlanta(config-fr-dlci)# interface serial 0/1/1.2 point-to-point
Atlanta(config-subif)# ip address 140.1.2.1 255.255.255.0
Atlanta(config-subif)# frame-relay interface-dlci 53

Atlanta(config-fr-dlci)# interface serial 0/1/1.3 point-to-point
Atlanta(config-subif)# ip address 140.1.3.1 255.255.255.0
Atlanta(config-subif)# frame-relay interface-dlci 54

Atlanta(config-fr-dlci)# interface gigabitethernet 0/0
Atlanta(config-if)# ip address 140.1.11.1 255.255.255.0
```

Charlotte Configuration

```
interface serial0/1/1
 encapsulation frame-relay
!
interface serial 0/1/1.1 point-to-point
 ip address 140.1.1.2  255.255.255.0
 frame-relay interface-dlci 51
!
interface gigabitethernet 0/0
 ip address 140.1.12.2 255.255.255.0
```

Nashville Configuration

```
interface serial0/1/1
 encapsulation frame-relay
!
interface serial 0/1/1.2 point-to-point
 ip address 140.1.2.3 255.255.255.0
 frame-relay interface-dlci 51
!
interface gigabitethernet 0/0
 ip address 140.1.13.3 255.255.255.0
```

Boston Configuration

```
interface serial0/1/1
encapsulation frame-relay
!
interface serial 0/1/1.3 point-to-point
ip address 140.1.3.4 255.255.255.0
frame-relay interface-dlci 51
!
interface gigabitethernet 0/0
ip address 140.1.14.4  255.255.255.0
```

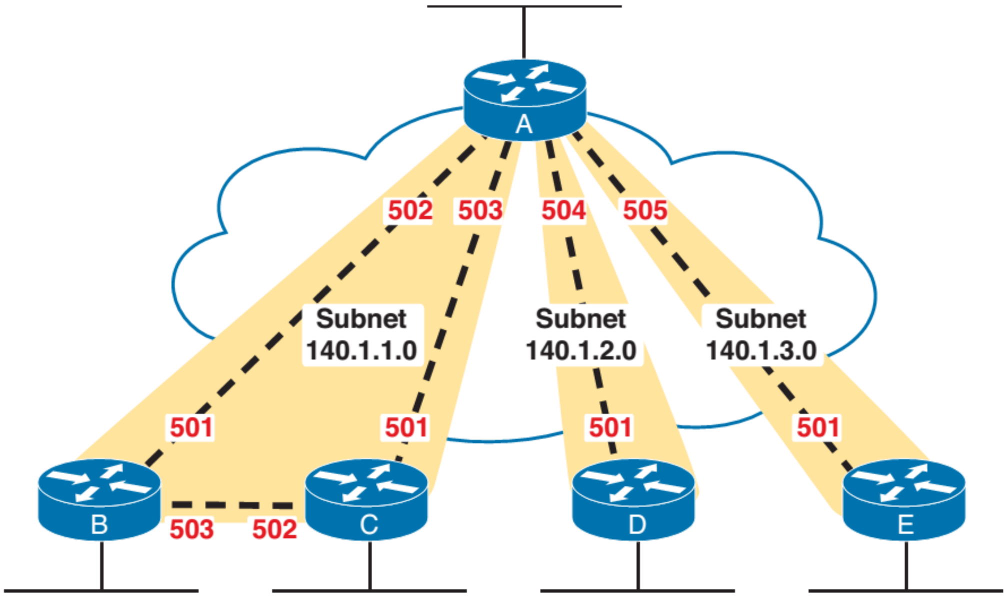
The LMI type is autosensed, and Cisco encapsulation is used, which is just like the fully meshed examples. Inverse ARP is not really needed on point-to-point subinterfaces, but it is enabled by default in case the router on the other end of the VC needs to use Inverse ARP

Two new commands create the configuration required with point-to-point subinterfaces. First, the ***interface serial 0/1/1.1 point-to-point*** command creates logical subinterface number 1 under physical interface serial 0/1/1. This command also defines the subinterface asa point-to-point subinterface instead of point-to-multipoint. Then, the configuration must associate one PVC with the subinterface; the ***frame-relay interface-dlci*** subinterface sub- command tells the router which single local DLCI is associated with that subinterface.

Verifying Point-to-Point Frame Relay

The ***show frame-relay pvc*** command lists useful management information. the output includes a variety of counters and rates for packets going over each PCV- good for troubleshooting .

The ***show frame-relay map*** command lists mapping information.
With the earlier example of a fully meshed network, in which the configuration did not use any subinterfaces, a Layer 3 address was listed with each DLCI. For subinterfaces the router looks to the routing table for IP addresses.
The ***debug frame-relay lmi*** output lists information for the sending and receiving of LMI inquiries.



Configuring with Multipoint Subinterfaces

Multipoint subinterfaces work best when you have a full mesh between a set of routers.
On routers A, B, and C, a multipoint subinterface is used for the configuration referencing the other two routers, because you can think of these three routers as forming a fully meshed subset of the network .

Router A

```
interface serial0/1/1
 encapsulation frame-relay
!
interface serial 0/1/1.1 multipoint
 ip address 140.1.1.1  255.255.255.0
 frame-relay interface-dlci 502
 frame-relay interface-dlci 503
!
interface serial 0/1/1.2 point-to-point
 ip address 140.1.2.1 255.255.255.0
 frame-relay interface-dlci 504
!
interface serial 0/1/1.3 point-to-point
 ip address 140.1.3.1 255.255.255.0
 frame-relay interface-dlci 505
```

Router B (

```
interface serial0/1/1
 encapsulation frame-relay
!
interface serial 0/1/1.1 multipoint
 ip address 140.1.1.2
255.255.255.0
```

Router C

```
interface serial0/1/1
 encapsulation frame-relay
!
interface serial 0/1/1.1 multipoint
 ip address 140.1.1.3
255.255.255.0
```

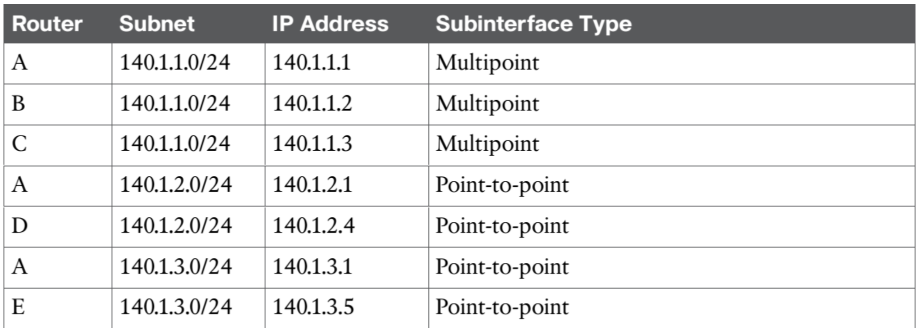
Router D (E is the same format)

```
interface serial0/0/0
encapsulation frame-relay
!
interface serial 0/1/1.1 point-to-
point
 ip address 140.1.2.4
```

```
frame-relay interface-dlci 501      frame-relay interface-dlci 501      255.255.255.0
frame-relay interface-dlci 503      frame-relay interface-dlci 502       frame-relay interface-dlci 501
```

Notice that there are two commands for each multipoint subinterface in this case, because each of the two PVCs associated with this subinterface must be identified as being used with that subinterface.

summarizes the addresses and subinterfaces used.



Router	Subnet	IP Address	Subinterface Type
A	140.1.1.0/24	140.1.1.1	Multipoint
B	140.1.1.0/24	140.1.1.2	Multipoint
C	140.1.1.0/24	140.1.1.3	Multipoint
A	140.1.2.0/24	140.1.2.1	Point-to-point
D	140.1.2.0/24	140.1.2.4	Point-to-point
A	140.1.3.0/24	140.1.3.1	Point-to-point
E	140.1.3.0/24	140.1.3.5	Point-to-point

OSPF Issues on Frame Relay Multipoint and Physical Interfaces 429
Frame Relay Troubleshooting 430

A Suggested Frame Relay Troubleshooting Process

If the Frame Relay router can ping some, but not all, of the other Frame Relay routers whose VCs share a single access link, jump to step 3. If a Frame Relay router's pings fail for all remote routers whose VCs share a single access link, do the following:

1. Check for Layer 1 problems on access link between router and Frame Relay switch
2. Check for Layer 2 problems on access link (encapsulation and LMI)
   LMI messages flow in both directions for two purposes:
      DCE to inform DTE about each VC's DLCI and its status and provide keepalive function
   Use s***how frame-relay lmi*** to check encaspsulation and LMI type***.*** ***show interfaces*** also lists encaps.
   Also make sure everything is on the expected interfaces.
3. Check for PVC problems based on PVC status and subinterface status
   Discover the IP and mask of each FR interface/subinterface, doublecheck subnets validity
   Compare IP address of the neighbor and pick the interface with the same subnet
   Discover the PVCs assigned to that interface/subinterface
   If multiple PVCs are assigned, determine which one is used to reach a neighbor
   [***show frame-relay map*** and ***pvc;show interfaces, show ip interfaces brief]***

Subinterface line and protocol status codes, just like physical interfaces, but different.
Down/down: Associated DLCIs are inactive or deleted, or underlying physical interface is not up/up
Up/up: At least one of the DLCIs associated with the subinterface is active or static.

*PVC Status (listed s**how frame-relay pvc**)*	*Active*	*Inactive*	*Deleted*	*Static*
The PVC is defined to the Frame Relay network.	Yes	Yes	No	Unknown
The router will attempt to send frames on a VC	Yes	No	No	Yes

4. Check for Layer 2/3 problems with static and dynamic (inverse ARP) mapping
   Point-to-Point
      Subinterfaces do not need Inverse ARP or static mapping
      IOS automatically maps IP addresses in same subnet as point-to-point
      show frame-relay map will show InARP learned in mapping
   Physical and Multipoint
      Need to use InARP or static mapping
      show frame-relay map shows router's FR IP and local DLCI for each PVC

If using static mapping, ***broadcast*** keyword is needed for routing protocols

5. Check for Layer 2/3 problems related to end-to-end encapsulation mismatch
6. Check for other Layer 3 issues, including mismatched subnets

encapsulation frame-relay [***ietf***]
Interface configuration mode command defines the FR encapsulation that is used rather than HDLC, PPP, and so on
frame-relay lmi-type {***ansi*** | ***q933a*** | ***cisco***}
Interface configuration mode command that defines the type of LMI messages sent to the switch
no frame-relay lmi-type
Interface configuration mode command that reverts back to the default LMI setting of autosensing the LMI type
bandwidth num
Interface subcommand that sets the router's perceived interface speed
frame-relay map {protocol protocol-address dlci} [***broadcast***] [***ietf*** | ***cisco***]
Interface configuration mode command that statically defines a mapping between a network layer address and a DLCI
frame-relay interface-dlci dlci [***ietf*** | ***cisco***]
Subinterface configuration mode command that links or correlates a DLCI to the subinterface
keepalive sec
Interface configuration mode command defines whether and how often LMI status messages are sent/expected
interface serial number.sub [***point-to-point*** | ***point-to-multipoint***]
Global configuration mode command that creates a subinterface or references a previously created subinterface
[***no***] ***frame-relay inverse-arp***
Physical and multipoint subcommand to disable Frame Relay Inverse ARP (***no inverse-arp***) or enable it

show frame-relay pvc [***interface*** interface][dlci] - Lists information about the PVC status
show frame-relay lmi [type number] - Lists LMI status information
show frame-relay map [type number] - Lists FR mapping info matching next-hop IP addresses to local DLCIs
show interfaces [type number] - Lists stats and details of interface configuration, including the encapsulation type
show ip interface brief - Lists one line of output per interface with IP address and interface status
debug frame-relay lmi - Displays the contents of LMI messages

Chapter 15** - **Identifying Other Types of WANs

Private WANs to Connect Enterprises

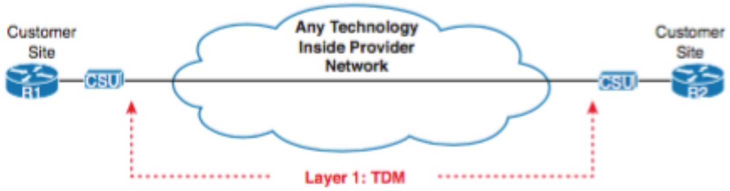
With a private service, one customer connects to the WAN service provider with connections from many sites. The provider promises to forward data between those sites. Later, when a second customer connects to that same WAN service, the WAN service keeps the two customer's data traffic private. While the data may flow through the same devices inside the provider's network, the provider never forwards data sent by customer 1 to customer 2, and vice versa, making the network private from the customer perspective.

Leased Lines

In figures, the generic version shows the crooked line that looks like a lightning bolt. Other figures show the channel service unit/ data service unit (CSU/DSU) that is needed for each router; note that the figure shows an external CSU/DSU.

As for other words, the technology used to create the line includes terms like T-carrier and time-division multiplexing (TDM), as well as the names for the common line speeds: DS1, T1, E1, T3, and E3.

As for protocols, leased lines provide a Layer 1 service, in that the provider promises to deliver bits to the other end of the line. The service provider lets the customer use any data link and higher-layer protocols that the customer wants to use.

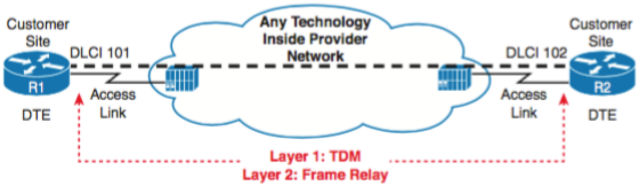


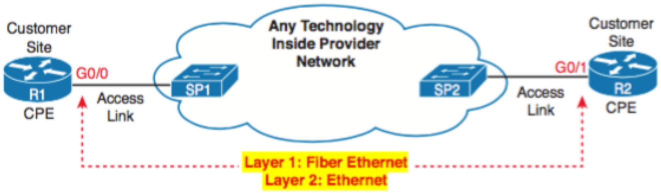
	Leased Line	***Frame Relay***	***Ethernet WAN***	***MPLS***
Physical links	TDM (T1, E1, and so on)	TDM (T1, E1, etc)	Ethernet (fiber)	Any supporting IP
Router int	Serial	Serial	Ethernet	Any supporting IP
Protocols	HDLC, PPP (not required)	Frame Relay	Ethernet	Any supporting IP
WAN service	Deliver individual bits to other end of leased line	Get FR frames through each PVC to endpoint	Get Ethernet frames to specific endpoints	Deliver IP packets

Frame Relay

What items should you watch for to notice Frame Relay WANs in the exam as opposed to other WAN technology?

- The access links- the link from the customer router to the Frame Relay network- typically use a leased line.
- The customer routers (DTE in Frame Relay) use Frame Relay data link protocols.
- The FR SP makes promise: to deliver FR frames to the correct other customer router (based on its PVC DLCI)
- The service is private, in that frames sent by customer A will not be sent to routers owned by customer B.
- usually uses no faster than the 44 Mbps or so of a T3 link





Ethernet WANs

- Access links use any Ethernet physical layer, but usually some fiber-optic standard for longer cable lengths.
- The customer routers (or LAN switches) will use some kind of Ethernet interface, not a serial interface.

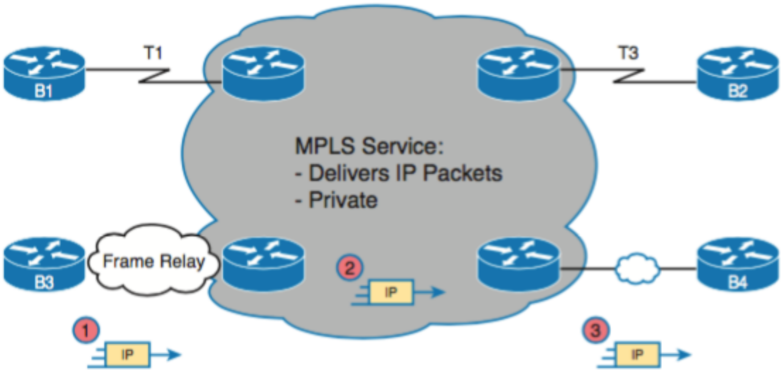
- The customer routers (or LAN switches) use Ethernet data link protocols.
- The figure will not show DLCIs, but may show MAC addresses on the WAN.
- The figure may show Ethernet switches inside the Provider's cloud.
- Private, for the same reasons as leased lines and Frame Relay.
- Ethernet WAN services usually support 100-Mbps or 1Gbps Ethernet

Names include Ethernet over MPLS (EoMPLS) and the more generic Ethernet WAN. Other terms include Metropolitan Ethernet (MetroE) and Virtual Private LAN Service (VPLS). Finally, Ethernet emulation emphasizes the fact that the provider emulates a big Ethernet network but that the provider can use any technology to create the service.

MPLS

Multiprotocol Label Switching (MPLS) follows some ideas similar to both Frame Relay and Ethernet WANs. Many types of MPLS WAN services exist, so here it's about one specific use of MPLS, called MPLS VPNs.

The biggest difference between MPLS VPN and other WAN services is that the service promises to deliver the customer's IP packets between sites, instead of delivering bits (leased lines) or delivering data link frames (Frame Relay and Ethernet WAN). Basically, to the customer, the MPLS network acts much like an IP network, routing the customers' IP packets between sites- much more flexibility than some other WAN services- can support any kind of access link that supports IP packets

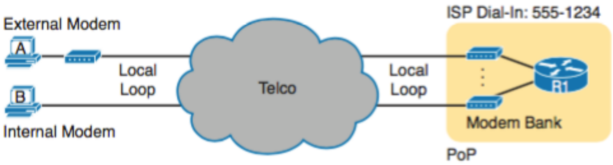


VSAT - Very Small Aperture Terminal

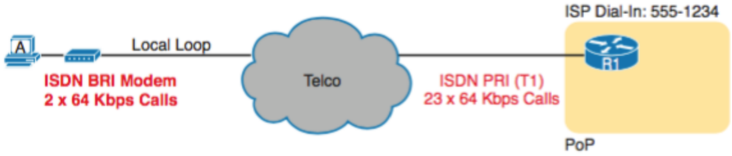
Using VSATs creates a private WAN somewhat like using leased lines while meeting an important need: connectivity to locations where connectivity is difficult. Dishes like satellite TV from the home, usually about 1 meter in width, cabled to a special router interface, with the router inside the building

Public WANs and Internet Access

Internet Access (WAN) Links
Dial Access with Modems and ISDN



I



Dialup using a telephone line, a phone call creates an electrical circuit that uses analog signals. Computers use digital signals; so to use an analog circuit, analog modems- one at the customer site, and one at the ISP- would modulate, or convert, the digital signal to an analog signal. The sending modem then transmits the analog signals to the receiving modem, which would then demodulate the analog back into the original digital. (The term modem comes from the squashing of those two terms together: modulate and demodulate)

The ISP purposefully puts a point of presence (PoP) in most local calling areas, so the phone call to connect to the Internet is free, rather than having a long-distance charge. Also the equipment cost fell pretty quickly over time, so the price to get started is relatively low. Telcos refer to the telephone cable that runs into a customer's home or business the local loop, and POTS lines (Plain Old Telephone Service). Dialup with modems tops out at 56Kbps.

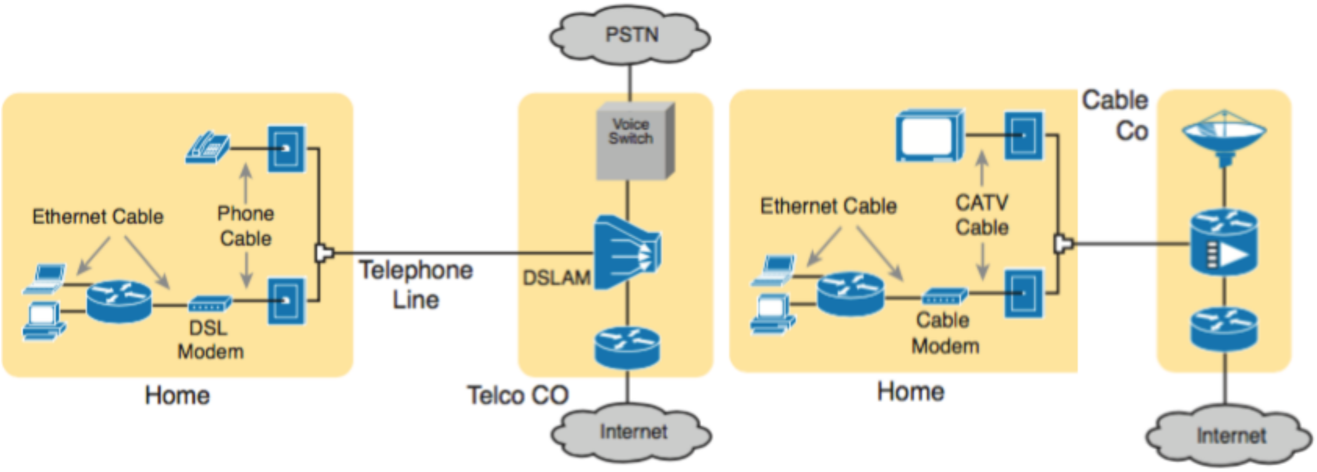
Integrated Services Digital Network (ISDN) used the same local loop (local phone line), also had a PoP in each local calling areas but used digital signals over the local loop, instead of analog. In addition, it supports two calls at the same time, each at 64 Kbps, over that one local loop phone line. Both calls (channels) could be dialed to the ISP, for a 128-Kbps Internet service, or the use could have one 64-Kbps Internet connection at the same time as an open voice line.

The consumer side of an ISDN used a Basic Rate Interface (BRI), which with two 64-Kbps channels and some type of ISDN-aware device, often referred to as an ISDN modem . The ISP side of the connection could use many different technologies including an ISDN technology called a Primary Rate Interface (PRI). This technology turned a T1 physical line into 23 ISDN channels ready to accept those ISDN calls

Digital Subscriber Line

For the data, a DSL modem connects to a spare phone outlet. The DSL modem sends and receives the data, as digital signals, at higher frequencies, over the same local loop, even at the same time as a telephone call. Because DSL uses analog (voice) and digital (data) signals on the line, the telco has to some- how split those signals on the telco side of the connection. To do so, the local loop must be connected to a DSL access multiplexer (DSLAM) located in the nearby telco central office (CO). The DSLAM splits out the digital data over to the router on the lower right, which completes the connection to the Internet. The DSLAM also splits out the analog voice signals over to the voice switch.

Asymmetric DSL (ADSL), which many of the consumer DSL offerings is based, routinely supports speeds in the 5-Mbps range, and up to 24 Mbps in ideal conditions. Also, ADSL supports asymmetric speeds, which better matches most consumer traffic models. Asymmetric speeds means that the transmission speed toward the home (down-stream) is much faster than the transmissions toward the ISP (upstream). Asymmetric speeds work better for consumer Internet access from the home because clicking a web page sends only a few hundred bytes upstream into the Internet but may trigger many megabytes of data to be delivered downstream to the home.



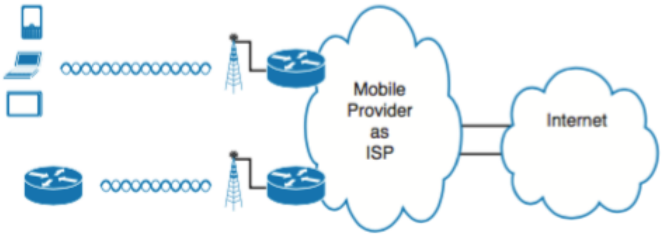
Cable Internet

The Internet service flows over one frequency, like yet another TV channel, just reserved for Internet service. The CATV company side of the connection must split out the data and video traffic. Data flows to the lower right, through a router, to the Internet. The video comes in from video dishes for distribution out to the TVs in people's homes. Cable Internet usually runs at faster speeds than DSL, with DSL providers often keeping their prices a little lower to compete. Both support asymmetric speeds, and both provide an "always on" service, in that you can communicate with the Internet without the need to first take some action to start the Internet connection.

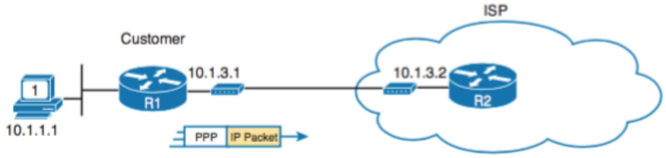
	Analog Modem	***ISDN***	***DSL***	***Cable***
Physical link	Phone line (local loop)	Phone line (local loop)	Phone line (local loop)	CATV cable
Always on?	No	No	Yes	Yes
Data service	Send bits to called party	Send bits to called party	Send data to ISP	Send data to ISP
Speed (general)	56 Kbps	128 Kbps	10s of Mbps	10s of Mbps
Asymmetric?	No	No	Yes	Yes

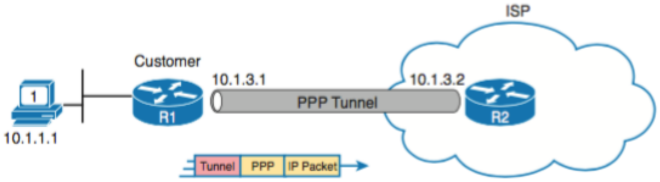
Mobile Phone Access with 3G/4G

Wireless Internet: A general term for Internet services from a mobile phone or from any device that uses the same technology. 3G/4G Wireless: Short for third generation and fourth generation, these terms refer to the major changes over time to the mobile phone companies' wireless networks. LTE: Long-Term Evolution, which is a newer and faster technology considered to be part of fourth generation (4G) technology.



PPPoE (PPP over Ethernet) Concepts





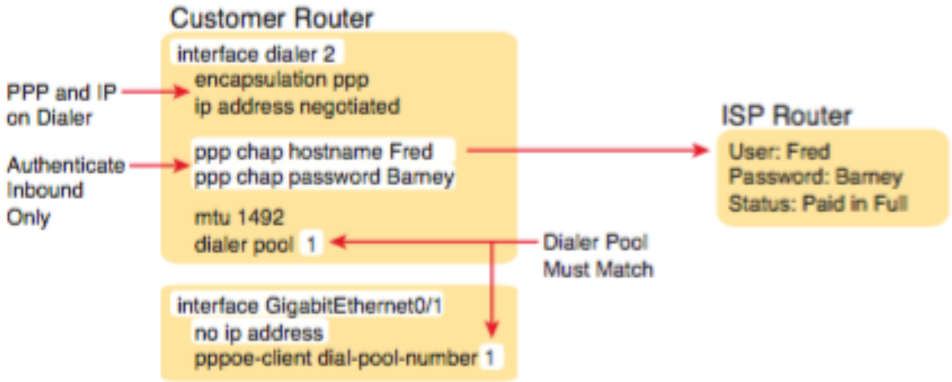
Overlaid on top of some DSL connections. PPP can be used on serial links, which includes those links created with dial-up analog and ISDN modems. For instance, the link from a dial user to an ISP, using analog modems, likely uses PPP today.

ISPs used PPP as the data link protocol for a couple of reasons. PPP supports a way to assign IP addresses to the other end of the PPP link- assign each customer one public IPv4 address to use. It supports CHAP to authenticate customers. Then, when using CHAP to authenticate, ISPs could check accounting records to determine whether the customer's bill was paid before letting the customer connect to the Internet.

Analog modems and ISDN for dial-up could use PPP and CHAP, but DSL which did not create a point-to-point link could not support PPP and CHAP. (the ethernet link only supported Ethernet data link protocols, and not PPP). New protocols were created- one that allowed the sending of PPP frames encapsulated inside Ethernet frames, and this is why PPPoE exists.

PPPoE basically creates a tunnel through the DSL connection, which does not create a single point-to-point link between the routers. Before sending the frames over any physical link, the routers encapsulate the frames inside various headers. The PPPoE tunnel header in this case has a typical Ethernet header (for PPPoE's use) and then the PPP frame (which includes the IP packet).

PPP over Ethernet Configuration



```
interface dialer 2
 encapsulation ppp
 ip address negotiated

 ppp chap hostname Fred
 ppp chap password Barney

 mtu 1492
 dialer pool 1

interface GigabitEthernet0/1
 no ip address
 pppoe-client dial-pool-number 1
```

The Official CCNA book only gives this customer configuration!

The PPP configuration sits on the dialer interface, not the Ethernet interface. Check the CHAP username and password, which must match the settings on the ISP. Make sure that the ***dialer interface*** is linked to the Ethernet interface with the ***dialer pool*** and ***pppoe-client*** commands, with the same number as noted in the figure. (The dialer interface number itself does not have to match.) And the maximum transmission unit (MTU) should be set down to 1492 (versus the default of 1500) to accommodate the PPPoE headers.

At the ISP end

- configure a Broadband Aggregation (BBA) group which will handle incoming PPPoE connection attempts
- name it ***MyGroup***, and bind it to a virtual template
- apply PPPoE session limits (limit # of sessions per client MAC address (setting to 2 allows a new session to be established immediately if the prior session was orphaned and is waiting to expire).

```
ISP(config)# bba-group pppoe MyGroup
ISP(config-bba-group)# virtual-template 1
ISP(config-bba-group)# sessions per-mac limit 2
```

Create the virtual template for the customer-facing interface. When client initiates session the router auto-spawns a virtual interface to represent the connection. At minimum, we'll need an IP address, and an address pool (like DHCP)

```
ISP(config)# interface virtual-template 1


ISP(config-if)# ip address 10.0.0.1 255.255.255.0
ISP(config-if)# peer default ip address pool MyPool
```

You'll have to define the pool in global config.

```
ISP(config)# ip local pool MyPool 10.0.0.2 10.0.0.254
```

Finally, enable our PPPoE group on the interface facing the customer network

```
ISP(config)# interface f0/0
ISP(config-if)# no ip address   <---- (the addressing is provided by our virtual template)
ISP(config-if)# pppoe enable group MyGroup
ISP(config-if)# no shutdown
```

Lock it down! Create a local user account name ***CPE*** and the password ***MyPassword,*** enforce CHAP authentication on our virtual template. In real practice, account creation is typically performed on a back-end server and referenced via RADIUS or TACACS+ rather than being stored locally

```
ISP(config)# username CPE password MyPassword
ISP(config)# interface virtual-template 1
ISP(config-if)# ppp authentication chap callin
```

```
!
! Server
!
username CPE password 0 MyPassword
!
bba-group pppoe MyGroup
 virtual-template 1
 sessions per-mac limit 2
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 pppoe enable group MyGroup
!
interface Virtual-Template1
 ip address 10.0.0.1 255.255.255.0
 peer default ip address pool MyPool
 ppp authentication chap callin
!
ip local pool MyPool 10.0.0.2 10.0.0.254


!
! Client
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 pppoe enable
 pppoe-client dial-pool-number 1
!
interface Dialer1
 mtu 1492
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 ppp chap password 0 MyPassword
```