



Cramsession™ for Building Cisco Remote Access Networks

This study guide will help you to prepare for Cisco exam 640-505, Building Cisco Remote Access Networks. Exam topics include Bridging, Switching, Network and WAN Protocols, Network Management, Security (NAT), WAN Design, and Cisco and Networking Fundamentals.



Check for the newest version of this Cramsession
<http://cramsession.brainbuzz.com/checkversion.asp?V=2452019&FN=cisco/BCRAN.pdf>



Rate this Cramsession
<http://cramsession.brainbuzz.com/cramreviews/reviewCram.asp?cert=Cisco+BCRAN>



Feedback Forum for this Cramsession/Exam
<http://boards.brainbuzz.com/boards/vbt.asp?b=654>

More Cramsession Resources:



Search for Related Jobs
<http://jobs.brainbuzz.com/JobSearch.asp?R=&CSRE>



CramChallenge - practice questions
<http://www.cramsession.com/signup/default.asp#day>



IT Resources & Tech Library
<http://itresources.brainbuzz.com>



Certification & IT Newsletters
<http://www.cramsession.com/signup/>



SkillDrill - skills assessment
<http://skilldrill.brainbuzz.com>



Discounts, Freebies & Product Info
<http://www.cramsession.com/signup/prodinfo.asp>

Notice: While every precaution has been taken in the preparation of this material, neither the author nor BrainBuzz.com assumes any liability in the event of loss or damage directly or indirectly caused by any inaccuracies or incompleteness of the material contained in this document. The information in this document is provided and distributed "as-is", without any expressed or implied warranty. Your use of the information in this document is solely at your own risk, and Brainbuzz.com cannot be held liable for any damages incurred through the use of this material. The use of product names in this work is for information purposes only, and does not constitute an endorsement by, or affiliation with BrainBuzz.com. Product names used in this work may be registered trademarks of their manufacturers. This document is protected under US and international copyright laws and is intended for individual, personal use only. For more details, visit our [legal page](#).



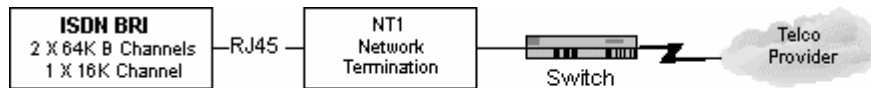
Contents:

Contents:	1
ISDN	2
Description and Interfaces	2
Logical Interfaces	3
RSTUV-Logical Reference Points	3
Configuring ISDN BRI.....	5
Dial on Demand Routing (DDR)	5
For OUTAGE Backup	7
For LOAD Backup.....	7
ISDN PRI	7
ISDN Physical Interfaces – SERIAL.....	9
X.25	10
Datagram Encapsulation	10
Frame Relay	12
Troubleshooting.....	14
Modems and Async.....	16
Dialer Profiles and Dialer Interfaces	18
Dialer Profiles.....	19
PPP.....	21
PPP Call Back Configuration	22
Multilink PPP	23
TroubleShooting PPP	23
Queuing and Compression	24
Dallas2(config)#priority-list 1 protocol ip high tcp telnet	24
Compression	24
AAA	25
NAT	26
Troubleshooting NAT	27
ROUTERS	27

ISDN

Description and Interfaces

ISDN BRI = Basic Rate Interface



DS0 = Digital Signal Level 0 = 64Kbps

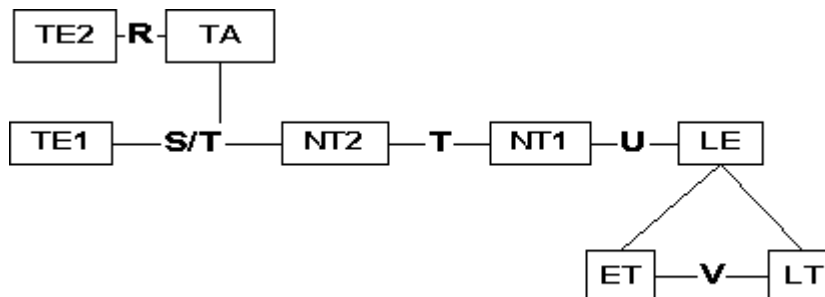
ISDN PRI US T1 = Primary Rate Interface -- Use of CSU/DSU requires different connectors. Uses DB15 and RJ48 connections.

DS1=1.54Mbps = 24 DS0's

ISDN PRI EUROPE E1 - 30 X DS0



In Europe, the ISDN service provider provides the NT1. In the US, the customer supplies the NT1.

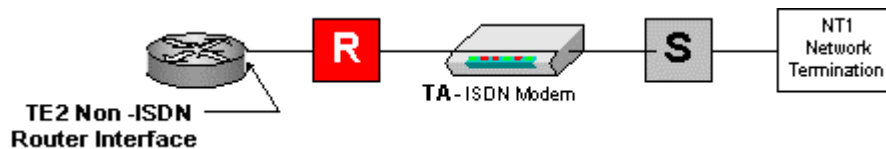


Logical Interfaces

Note: NT1 and NT2 can be combined into one device.

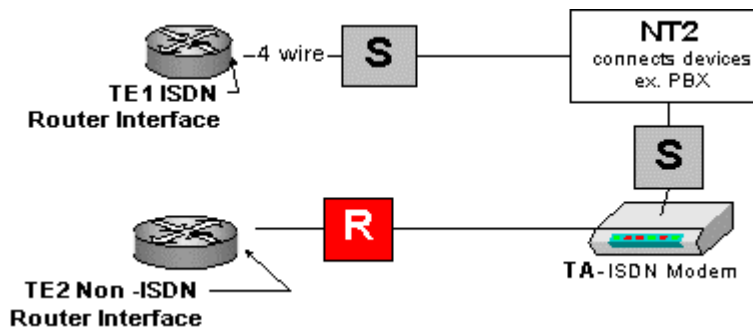
RSTUV-Logical Reference Points

Rate Reference Point - Located between the NON ISDN router interface and the Terminal Adapter (TA).



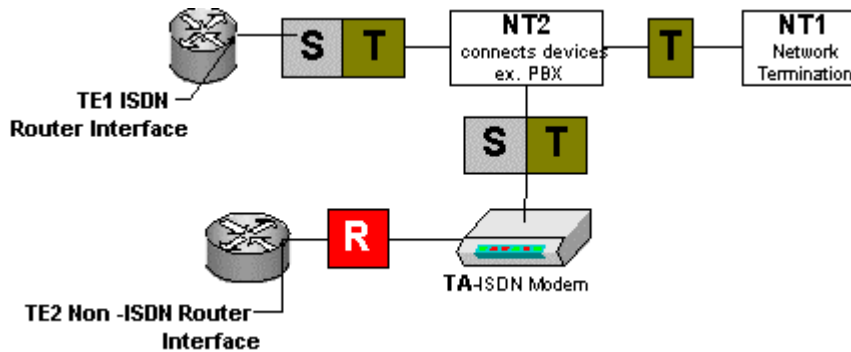
Example of TE2: Async/Sync Serial, non-ISDN phone

System Reference Point - Is the reference point between the ISDN user terminals and the NT2 or TA and NT2. Non-US demarcation.



Example of TE1: ISDN phone, Some teleconferencing Equipment

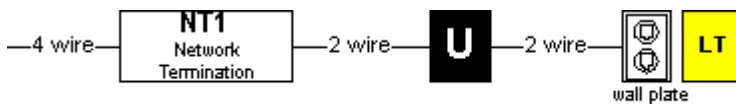
Terminal Reference Point - This is the reference point between the NT1 and NT2 (Customer Switching Equipment/PBX). This reference point is included in the NT1 as well. This point is NON-US demarcation.



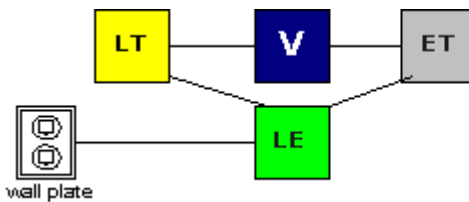
Example of NT2: PBX, multiplexer

User Reference Point - This reference point is a US demarcation. It references the point between the NT1 and the LT.

Example of NT1: ADTRAN ISU, 3Com TA



V Reference Point - Located between the LT and the ET. Also referred to as the local exchange.



ISDN Protocols - ITU-T groups the protocols, interfaces and addressing.

- **E-series** - describes **telephone network**; e.g., E.164=International addressing for ISDN.
- **I-series** - describes **Interfaces & Concepts**; e.g., I.430=BRI Interface.
- **Q-series** - describes switching and signaling. (e.g., Q.921=LAPD Link Access Procedure D channel, Q.931 DSS1 Digital Subscriber Signaling #1)

Configuring ISDN BRI

1. Select your switch type (provided by your carrier).

Router2(config)# isdn switch-type basic-dms100

Note: Before 11.3T, the IOS would support only one switch-type that was defined globally!

Router2(config-if)# isdn switch-type basic-dms100

2. Configure the appropriate interface on the router.

Router2(config)# interface bri X (x = the interface you are going to configure)

For a TE2 non-ISDN interface use the 'interface serial x' command -- but there is no need to define a switch-type or SPID in this case.

Router2(config)# interface serial X (x = the interface you are going to configure)

3. Set SPID's (Service Profile Identifiers). The service provider assigns these numbers.

Router2(config-if)# isdn spid1 512790203300 [local directory number]

Router2(config-if)# isdn spid2 512790203400 [local directory number]

4. Set the appropriate protocol for encapsulation and set the protocol for authentication. PPP or HDLC can be used for encapsulation. CHAP or PAP can be used for authentication. CHAP is encrypted; PAP sends information in plain text.

Router2(config-if)# encapsulation ppp

Router2(config-if)# ppp authentication chap

Dial on Demand Routing (DDR)

DDR for ISDN - Use DDR for connections that do not need to be connected for long periods of time. Determine what traffic is "interesting" and needs to bring up the link or reset the idle timeout. Use access lists to deny broadcasts such as SAP updates and permit traffic that needs to be interesting. You can also use the **passive interface** command to prevent the forwarding of routing updates; e.g., IGRP, OSPF, EIGRP

dialer-list [number] protocol [ip|ipx|bridge] [list|permit] is the global command used to define interesting traffic as all traffic of a certain protocol, or point to an access list that defines interesting traffic more specifically. There can be

multiple dialer-lists – one per protocol, including IP, IPX, NETBIOS, BRIDGE, DECNET, etc.

1. Define what traffic is interesting. An **access-list** command can be referred to from this **dialer-list** command to specify the appropriate traffic to raise the link or stop the idle-timer countdown.

Router2(config)# dialer-list 3 protocol ip permit (all ip traffic is interesting)

Or

Router2(config)# dialer-list 3 protocol ip list 5 (use access-list 5 to define interesting traffic)

Router2(config)# access-list 5 permit 10.98.98.0 0.0.0.255 [all traffic sourced from the 10.98.98.0 network is interesting]

2. Assign the dialer-list to the appropriate interface.

Router2(config-if)# interface bri 2

Router2(config-if)#dialer-group 3 (use dialer list "3" to monitor for interesting traffic)

3. Assign the destination. Use the **dialer map** command to specify the destination parameters.

Router2(config-if)# dialer map ip 10.180.0.3 name router3 5125551092

4. Determine which call options to use. To use DDR successfully, you must specify the appropriate call values.

Router2(config-if)# dialer fast-idle 30 (if the interface is busy and another call needs to be placed, the 30 parameter specifies to disconnect the call if the line is idle for over 30 seconds; the default is 20 seconds)

Router2(config-if)# dialer idle-timeout 180 (tells the interface to disconnect after idle for 180 seconds; the default is 120 seconds)

Router2(config-if)# dialer load-threshold 128 [either|outbound|inbound] (numerical value 1 through 255 represents x/255 -- tells the router at what load to make another call)

Rate adaptation - The data speed of an ISDN line can be slowed down to 56K if necessary. Use the **speed** option with the **dialer map** command.

Router2(config-if)# dialer map ip 10.180.0.3 name router3 speed 56 broadcast 5125551038 (makes a 56K call to router3 at 5125551038, will pass multicasts and broadcasts to router3)

Backup Interfaces Load and Outage - This is important for fault tolerance and useful when interfaces exceed the expected load. Follow these simple steps to backup an interface:

For OUTAGE Backup

1. Select the interface you want to backup.

Router2(config)# interface serial 0

2. Define the interface you want to use as backup.

Router2(config-if)# backup interface bri2

3. Set when you want the backup line to come up. Set on/off parameters.

Router2(config-if)# backup delay 60 30 (the 60 parameter designates ON after bri2 is down for 60 seconds) (the 30 parameter designates OFF after serial0 is back online for 30 seconds)

For LOAD Backup

Use the **backup load** command to back up the primary line on a load basis rather than outage basis. Values are based on percentages.

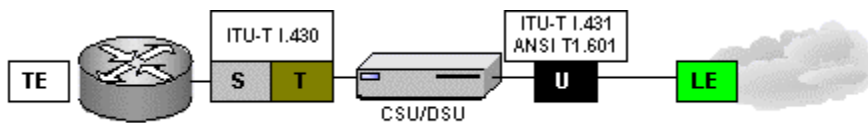
Set the bandwidth ON/OFF values for the backup interface.

Router2(config-if)# backup load 50 10 (50 designates ON when bri2 exceeds 50% of bandwidth) (10 designates OFF after the combined load reaches less than 10 percent of the primary line's bandwidth)

ISDN PRI

ISDN Protocols - ISDN uses several protocols; which protocol each channel uses is crucial to understanding how ISDN works.

Network Layers	B-Channel	D-Channel
Layer 3	IP IPX	DSS1 (Q.931)
Layer 2	LAPB HDLC PPP Frame Relay	LAPD (Q.931) Link Access Procedure D-channel
BRI Protocol	I.430 BRI used across S/T	I.430 BRI used to cross S/T interface
Layer 1	ANSI T1.601 BRI for U interface North American	ANSI T1.601 BRI for U interface North American
PRI Protocol	I.431 PRI for serial synch	I.431 PRI for serial synch



PRI Functional Groups and Reference Points - Since an ISDN PRI requires the use of a CSU/DSU the logical groups and reference points are much easier to identify. Note that the above diagram is for PRI and BRI.

ISDN PRI can be configured in five easy steps. SCFLC (Swami Can Fix Left-handed Clocks) can be used to remember the steps. For PRI you configure:

- Switch type
- Controller
- Frame type
- Linecode
- Clocksource

Syntax to configure ISDN PRI:

1. Select your switch type.
isdn switch-type primary-5ess
2. Choose the controller.

controller T1 slot/port

controller T1 2/1

3. Specify the frame type.

framing esf

4. Specify the linecode.

linecode b8zs

5. Specify clocksource

clock source line primary [internal | secondary]

Here are the common line coding and framing types. They will typically be seen together:

Framingtype	Line Coding
CRC4	HDB3
ESF	B8ZS
SF	AMI

ISDN PRI can accept incoming calls voice/speech calls by using the following command: (under the interface serial x:23, where x=the controller number)

isdn incoming-voice modem

ISDN Physical Interfaces – SERIAL

- EIA/TIA 232
- EIA/TIA -449
- EIA -530
- X.21

BOD Bandwidth on Demand - Can be used on BRI or PRI channels to supply additional bandwidth once a channel is connected. The traffic trigger can be set for inbound, outbound or either. The value metric is 0-255. (255 equals 100%)
Example:

Dallas2(config)# interface bri 0

Dallas2(config-if)# dialer load-threshold 128 either (specifies 50% load, either direction, and brings up additional line)

ISDN Caller ID Screening - ISDN can also be configured to only accept certain calls from certain numbers. X's can be used as wildcards. Example:

Dallas2(config-if)# isdn caller 555xxxx (allows any inbound call from 555 exchange)

X.25

X.25 is a packet switched protocol that operates at the Physical, Data Link and Network Layers of the OSI model. This protocol works by encapsulating the layer 3 protocols such as IP, IPX, decnet, PPP and Appletalk. The max speed for X.25 is 128K. X.25 was engineered for strong error checking and flow control at layers 2 and 3. X.25 uses LAPB, is very reliable, and also uses sliding windows (much like TCP/IP) for flow control. Options for flow control on the interface must match the remote router. X.25 uses SVC's (Switched Virtual Circuits) and PVC's (Permanent Virtual Circuits). PVC's are always connected. Use "show interface" to view configuration. X.25 is considered the predecessor to frame-relay.

X.25 devices include DTE, DCE and PAD and uses LAPB (Link Access Procedure Balanced) as a Data Link Layer protocol.

Datagram Encapsulation

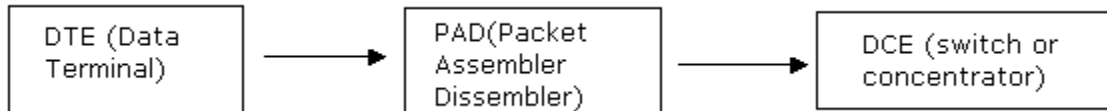


Network Function - X.25 is highly available and used worldwide.

PAD - Is a Packet Assembler Dissembler between the DTE and DCE device.

It collects the data transmissions from the terminals/DTE and gathers them into a X.25 data stream and vice versa. A Cisco router can act as a PAD. During

configuration of the X.25 you specify whether the interface will act as a DCE or DTE ('encapsulation x25 [dte|dce]'). When configured as a DCE the router behaves as an X.25 switch.



X.121 - Is the addressing standard. Static mappings must be made manually. X.25 does not support ARP or inverse-ARP. The addressing standard is a 3-digit country code followed by a 1-digit Service Provider code. The following 8 to 11 digits are assigned to the X.25 host.

To configure an X.25 interface for SVC - Define the encapsulation, assign the X.121 address and use map statements to link the X.121 logical address with the IP protocol or other addresses. Options for flow control must match on both sides.

Steps to configure X.25 on an interface:

SanAton2(config)# interface serial 2

SanAton2(config-if)# encapsulation x25

SanAton2(config-if)# x25 address 3167012345678 (316 country code, 7 is the service provider, the rest of the number specifies the x25 host address)

SanAton2(config-if)# ip address 10.98.98.25 255.255.255.0 (configures the IP address for the interface)

SanAton2(config-if)# x25 map ip 10.98.98.24 3160987654321 broadcast (maps the target IP address to the x121 address)

To configure an X.25 interface for PVC - Exactly the same as above except for the last step. You use the **pvc** command instead of the **map** command to establish the PVC.

SanAton2(config-if)# x25 pvc 6 ip 10.98.98.24 3160987654321 broadcast (maps the target IP address to the x121 address on virtual circuit #6)

Options for X.25 - Windows and packet sizes must match on both sides of the connection. Use the **x25 ips** command for incoming packet size and **x25 ops** for outgoing packet size. Window size uses a counter for when to send an

acknowledgement. **x25 win** and **x25 wout** commands are used. The modulo controls the size of the window; 8 or 128 is used to specify the number of packets.

<p>PACKET SIZES Bytes</p> <p>(config-if)#x25 ips 256 (config-if) x25 ops 256 specifies default packet size in and out</p>	<p>Window Parameters # of packets</p> <p>(config-if)# x25 win 7 (config-if)# x25 wout 7 window sends ack after 7 packets inbound or out</p>	<p>Packet numbering Modulus</p> <p>(config-if)# x25 modulo 8 Sets the window size</p>
---	---	--

Frame Relay

Physical Layer - Serial interfaces use DB-60 connectors. Frame relay requires the use of a CSU/DSU. Like X.25, frame relay uses SVC's and PVC's. PVC's are used for frequent and long connection times. SVC's are for sporadic infrequent traffic. List settings with **show interface** command or **show frame-relay map** command.

Example, EIA/TIA232 EIA/TIA449 .V35 X.21

Frame Relay Bandwidth - Max throughput is 2 Mbps to 56 Kbps. Frame relay is a layer 2 protocol. It uses the upper layer for error correction. It is faster than x.25.

LMI - Line Management Interface is the standard for signaling. There are three types:

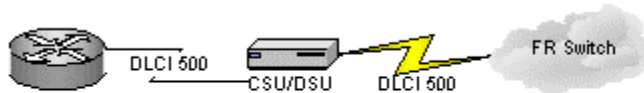
Cisco LMI	ANSI LMI	q.933a LMI
-----------	----------	------------

Cisco LMI is the default signaling. Service provider will specify the LMI in use.

- LMI's control data keep alive and verify the dataflow.
- Use multicast mechanism to provide network server to the DLCI.
- Use multicast addressing so DLCI has global significance.
- Verifies the DLCI's in use and the status to the local Frame relay switch.

LMI Autoconfigure - A router with IOS 11.2 and newer does not need to be configured for the LMI. The newer IOS will send all three to the FR switch until the switch responds.

DLCI - Data Link Connection Identifier verifies the logical circuits in use and the status from the CPE to the Frame Relay switch.



DLCIs have local significance only.

DLCI states are:

- **Deleted** - No LMI signal is being received from switch or no service is available from switch.
- **Active** - Lines are up; connections are active. Routers are exchanging data.
- **Inactive** - Frame relay switch to local connection is working. The remote routers' connection to the frame switch is not working.
- **Encapsulation Types** - Choices are Cisco and IETF. Cisco is the default. If the router is a non-Cisco router, use IETF. This designation can be made per DLCI. Even if all the routers are Cisco, you can communicate with a location with a non-Cisco router. Specify the IETF encapsulation and DLCI. You can use this with the **map** command. In short, encapsulation can be set per interface or per destination.

Example:

```
Dallas2(config-if)# frame-relay map ip 10.98.98.24 25 broadcast IETF (25 = the DLCI#)
```

Steps to configure frame relay:

1. Select the interface.

```
Dallas2(config)# interface serial 3
```

2. Is the interface a DTE or DCE?

```
Dallas2(config-if)#frame-relay intf-type ?
```

```
dce Configure a FR DCE
```

dte Configure a FR DTE

nni Configure a FR NNI

3. Assign an IP address to the interface.

Dallas2(config-if)# ip address 10.98.98.25 255.255.255.0

4. Select the encapsulation mode.

Dallas2(config-if)# encapsulation frame-relay cisco (this is an example of setting the encapsulation per interface. All traffic leaving interface will be Cisco.)

5. Set the LMI (not necessary with IOS 11.2 and up).

Dallas2(config-if)# frame-relay lmi-type cisco

6. Map protocol.

Dallas2(config-if)# frame-relay map ip 10.98.98.24 25 broadcast cisco

Troubleshooting

Dallas2#show frame-relay ?

ip	show frame relay IP statistics
lmi	show frame relay lmi statistics
map	Frame-Relay map table
pvc	show frame relay pvc statistics
qos-autosense	show frame relay qos-autosense information
route	show frame relay route
rtp	show frame relay RTP statistics
traffic	Frame-Relay protocol statistics

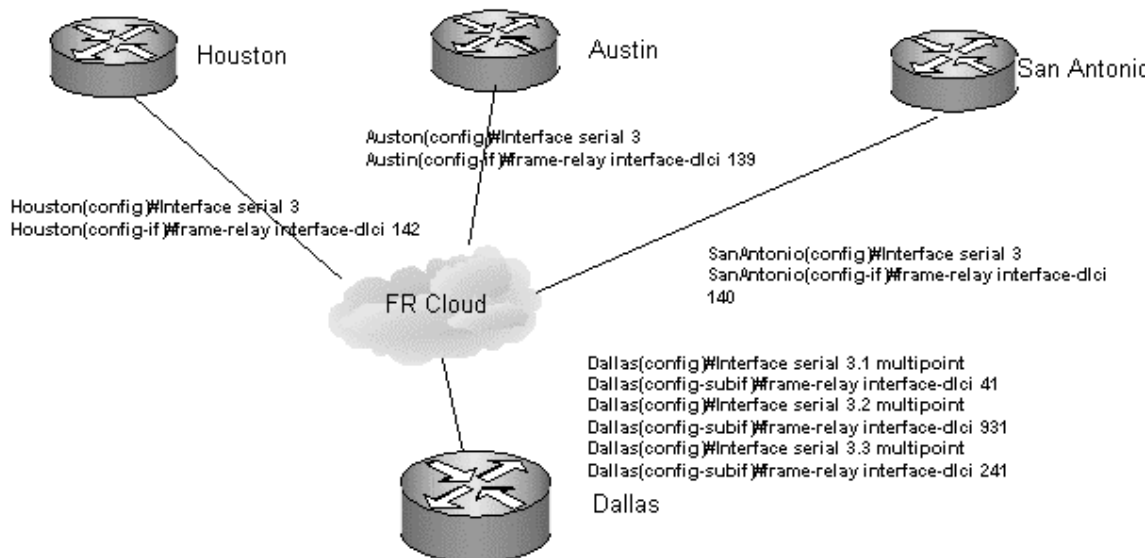
Dallas#show interfaces serial ?

<0-1> Serial interface number

2501#debug frame-relay ?

events	Important Frame Relay packet events
Ip	Frame Relay Internet Protocol
Llc2	Frame Relay llc2
lmi	LMI packet exchanges with service provider
packet	Frame Relay packets

Split Horizon and Routing Updates - Since routing updates should not be sent out the same interface you learned the update from (this causes routing loops), the solution to fixing this problem is creating subinterfaces with different DLCI's.
Example:



Each subinterface has its own DLCI enabled multipoint connection. Routing updates will now work properly.

Traffic Shaping - Since the speed of the frame relay circuits can vary, it is important to control how much and which traffic is sent or received on an interface.

Queuing - Priority, weighted, fair and custom queuing allow for specialized control of the traffic.

Rate Enforcement - You can configure the maximum amount of traffic to pass out the interface by setting the transmission rate. Usually determined by the CIR (Committed Information Rate)

BECN/FECN Support - Dynamic monitoring of the congestion of the frame relay network. Requires Cisco IOS 11.2 or higher to support BECN monitoring.

FECN - (Forward Explicit Congestion Notification) When the frame relay switch becomes congested, it sends a FECN to the destination.

BECN - (Backward Explicit Congestion Notification) When the frame relay switch becomes congested, it sends a BECN to the source.

To use traffic shaping with the BECN support, use the following commands: *Note uses map classes.

Dallas2(config)# map-class frame-relay foo

Dallas2(config-map-class)# frame-relay adaptive-shaping BECN

Enable rate adjustment in response to BECN (enabled by default)

Dallas2(config-map-class)# frame-relay traffic-rate 56000 128000 (9600 specifies the average, 33600 specifies the peak rate)

Dallas2(config-if)# frame-relay traffic-shaping

Dallas2(config-if)# frame-relay class foo

Modems and Async

There is no clock (hence the term) and must maintain in-band timing.

Physical Interfaces - (RJ11 or DB25) The connection from the router is a DB60 connection.

Use DTE lock to avoid speed mismatch. Modem often tries to match the inbound transfer rate of the modem to the DTE. Set speed under TTY line and at modem with AT commands.

Signal	Pin	Meaning
TD	2	Transmit from DTE to DCE
RD	3	Receive from DCE to DTE
RTS	4	Ready to send from DTE to DCE (DTE ready to receive)

CTS	5	Clear to send from DCE to DTE (DCE ready to send)
DSR	6	Data set ready (DCE ready)
GND	7	Ground
CD	8	Carrier detect (DCE has carrier signal)
DTR	20	Data terminal ready (DTE ready)

Interface Async/TTY Line Configuration Commands:

Below is the configuration necessary to configure a modem on an asynchronous interface such as AUX port or internal modem. This will allow EXEC prompt access to the router.

Dallas2 # show line (to see the numbering of all asynchronous interfaces)

Dallas2(config)# line 65 (AUX port of 2600 series)

Dallas2(config-line)# speed 115200 (DTE to DCE - not connect rate)

Dallas2(config-line)#modem inout (enables modem control)

Dallas2(config-line)#transport input all (allows reverse-telnet and others)

This is configuration to allow PPP access to the modem on line 65:

Dallas2(config)# interface asynchronous 65 (must match TTY line number)

Dallas2(config-if)# ip address 192.168.1.1 255.255.255.0

Dallas2(config-if)# encapsulation ppp

Dallas2(config-if)# ppp authentication [pap | chap | ms-chap]

The following commands are optional:

Dallas2(config-if)# peer default ip address 192.168.100.1 (assigns this address to ppp client)

Dallas2(config-if)#dialer in-band (enables v25bis on sync and chat-scripts on async)

Adding Modems to Router - The router has a built-in modem compatibility database (modemcap) to issue the correct initialization strings. Use the following command to have the router search and configure the new modem:

Dallas2(config-line)# modemcap autoconfigure discovery



You can also use a preset or user defined modem database.

Dallas2(config-line)# modemcap autoconfigure type <modemcap>

Dallas2 #show modemcap (displays modems in database)

Edit the database to add a new entry or modify an existing entry.

Dallas2(config)#modemcap edit <new modemcap> <attribute> <string>

Example - Dallas2(config)#modemcap edit newmodem autoanswer 1

This command is used to debug the modem auto configuration:

Dallas2 # debug confmodem

Chat Scripts/System Scripts - Can be triggered for DDR, on startup, on connection, line activation and to reset modems. Chat scripts are useful because they can reset modem configurations, dial and remotely login to a host and detect line failure. They can be used to initialize a modem attached to a router, automatically dial out on a modem, login and execute commands on another system or router.

Modem troubleshooting commands:

show line <line-number optional>(shows the modems physical config) as noted above, the line command is for physical attributes.

clear line <line-number> (returns the interface to idle state)

show modem (shows internal modem states)

debug modem (shows async communications between DTE and DCE)

debug chat (shows process of chat script expect-send sequence)

debug confmodem

Dialer Profiles and Dialer Interfaces

Dialer Interfaces are virtual interfaces that hold the logical configuration for one or more physical interface (Sync, async, ISDN)

You create and configure them with the '**interface dialer <0-255>**' command.

Dallas2(config-if)#dialer map protocol next-hop-address [name hostname] [spc] [speed 56 | 64] [broadcast]

[modem-script modem-regexp] [system-script system-regexp] [dial-string-] this command can be used to support a point-to-multipoint configuration under a dialer or physical interface. You can specify rate adaptation and use this map to pass multicasts or broadcasts (such as routing protocols).

Dialer rotary-group - allows you to apply a logical interface to multiple physical interfaces.

The following example shows how to configure multiple physical BRI interfaces to participate in a rotary group configuration.

```
Dallas2(config)# interface bri 0
Dallas2(config-if)# dialer rotary-group 2
Dallas2(config)# interface bri 1
Dallas2(config-if)# dialer rotary-group 2
Dallas2(config)# interface bri 2
Dallas2(config-if)# dialer rotary-group 2
Dallas2(config)# interface dialer 1
Dallas2(config-if)# ip address x.x.x.x
```

Under the interface dialer is where you would apply your settings for these interfaces such as encapsulation, layer 3 addressing, authentication and timers.

Dallas2(config-if)# dialer idle-timeout x (x= the number of seconds, 120 is default)

Analog lines take longer to make a connection, so use the **wait-for-carrier-time** command to tell the analog line to wait until a proper connection is made. Example:

Dallas2(config-if)# dialer wait-for carrier-time x (x=the number of seconds, default is 30)

Dallas2(config-if)# dialer fast-idle timeout x (x=number of seconds, 20 is default)

Dialer Profiles

Dialer Profiles - Are logical interfaces that can be used to control encapsulation, access list, and control features per call. The key to Dialer profiles is they can take a physical interface and make connections to a specific destination with specific call parameters.

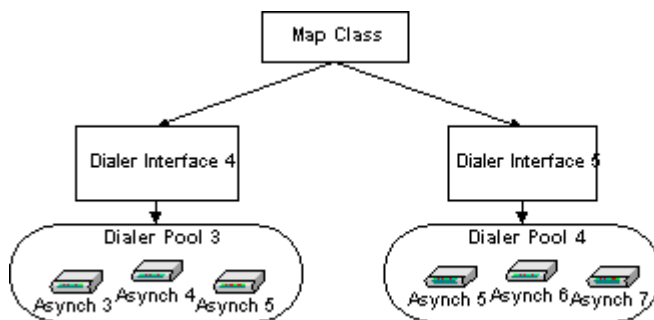
Dialer Profile Components:

- Dialer Interfaces (uses a per destination dialer profile)
- Dialer Map Classes
- Dialer Pools

The Advantages of Using Dialer Profiles:

- ISDN channels can be split.
- Different DDR settings can be made for each B-Channel.
- BRI and PRI b-channels, as well as asynch and synch interfaces, can be added to multiple dialing pools.
- B-Channels can be configured to call different locales with different IP addresses and subnets.
- An Interface can belong to multiple pools.

A dialer map (sets configuration) can be applied to several dialer interfaces:



*Note Asynch5 belongs to both dialer pools

Adding physical interfaces to a dialer pool - Use the following command:

Dallas2(config-if)# dialer pool member x (x= can equal a number 0-255)

Adding logical interfaces to a dialer pool - Use the following command:

Dallas2(config-if)# dialer pool x (x= can equal a number 0-255)

PPP

PPP - Is an encapsulation standard used over Async serial, Synch serial, and ISDN.

NCP - Is a layer protocol of PPP; encapsulates multiple protocols.

<u>NCP</u> <u>Layer2</u>	Apple Talk
	TCP/IP
	IPX

LCP - Another component of PPP is responsible for authentication, multilink, callback and compression.

<u>NCP</u> <u>Layer 2</u>	Authentication
	Multilink
	Compression
	Call Back

Setting the interface configuration to ***async mode dedicated*** dial in session is forced to use the encapsulation specified. ***Async mode interactive*** allows exec prompt access

Dallas2(config-if)#async mode [interactive | dedicated]

Setting the TTY line configuration to ***autoselect*** allows login to adapt to encapsulation in use. (SLIP or PPP)

Dallas2(config-line)#autoselect [ppp | slip]

Authentication – (CHAP or PAP) CHAP is encrypted, while PAP login and password information are sent in plain text.

Dallas2(config-if)#ppp authentication [pap | chap]

IP Addressing with PPP - A router can be used to assign a static IP address, assign an address from a local pool, use DHCP or have the dial-in user specify an IP address. The router can also be used as a DHCP server.

To use the router as a DHCP relay agent:

Dallas2(config-if)# peer default ip address [ip address | dhcp]

To allow the user or client dialing in to specify an address:

Dallas2(config-if)#async dynamic address

Static mapping on an interface:

Dallas2(config-if)#dial map ip 10.98.98.24 name dialup(forces user dialup to use 10.98.98.24 as an IP address)

Define and use locally defined address pool named async.

Dallas2(config)#ip local pool async192.168.1.0 192.168.1.100

Dallas2(config-if)#peer default ip local pool async

PPP Call Back Configuration

The configuration of the hold queue timer is vital to the success of a PPP call back configuration. Hold queue time out must be long enough to allow the call back server to make the return call before the timeout limit is hit.

Dallas2(config-if)#dialer hold-queue 300 (specifies that 300 packets are held in the queue)

Call back configuration sample:

Dallas2(config)#username hackmi password giforgot callback-dialstring 2145551234 callback-line 1 callback-rotary 2 (callback-dialstring = the number to call back, callback-line = specifies the line to call back on)

Dallas2(config)# interface s1 (select interface)

Dallas2(config-if)# 10.98.98.1 255.255.255.0 (specifies the IP address)

Dallas2(config-if)# encapsulation ppp

Dallas2(config-if)# ppp callback accept

The **dialer callback-secure** command automatically disconnects any calls that are not explicitly authorized for callback.

Dallas2(config-if)# dialer callback-secure

Dallas2(config-if)# dialer map ip 10.98.98.2 name Austin1 class dial 1512555134 (configures the dialer map)

Dallas2(config-if)# dialer-group 2 (configures dialer group)

Dallas2(config-if)# ppp callback accept (sets PPP for callback)

Dallas2(config-if)# ppp authentication PAP

To configure the callback client - use the same basic configuration for callback and use the **PPP callback request** command.

Multilink PPP

Multilink PPP - also referred to as MP; allows additional calls or channels to connect to a host for additional bandwidth. Multilink is configured on the interface.

LCP controls multilink.

- Works on Cisco 700 series routers
- Works on routers running Cisco IOS
- RFC 1900 allows for vendor compatibility
- Allows packet fragmentation across channels
- Supports sequencing and interleaving of packets and performs load calculation on lines or channels

Troubleshooting PPP

debug ppp negotiation command is used to troubleshoot LCP and NCP issues.

debug ppp authentication

debug ppp multilink events

show dialer command shows the status of calls. Used to troubleshoot PAP and CHAP issues.

show interface xx - shows the state of LCP and components

Queuing and Compression

WEIGHTED FAIR
All traffic gets equal priority. FTP gets balanced access.
Default

PRIORITY QUEUEING

Critical traffic goes through and for low bandwidth connections.

Queues are High/Medium/Normal/Low.

CUSTOM QUEUEING

Bandwidth is allocated. Designed for higher speed connections.

Queues number from 0-16

Access List can also be used to filter traffic. Access lists are read from top to bottom. If a filter has been set to deny, you cannot set a permit statement lower in the list.

Priority Queuing - uses *priority-list* command. Example:

```
Dallas2(config)#priority-list 1 protocol ip high tcp telnet
```

This command defines a list number 3 where telnet traffic has high priority.

Now you bind the list to the interface.

```
Dallas2(config)#interface serial 3
```

```
Dallas2(config-if)#priority-group 1
```

Custom Queueing - uses the *queue-list* command

```
Dallas2(config)#queue-list 14 protocol ip 16 udp rip
```

Here we define all udp rip traffic to the lowest priority queue.

```
Dallas2(config)#interface serial 1/0
```

```
Dallas2(config-if)#custom-group 14
```

Compression

Link compression - Leased, ISDN; compresses payload and header information. Compresses all traffic on the interface. Example, Stacker Predictor.

Payload compression - compresses the data section of the packet.

TCP Header Compression - RFC 1144. Works by compressing the header of TCP traffic. Most effective on slower links and with packet transaction intensive applications. Supported by WAN links such as FR, PPP, X25.

Both Predictor and Stacker can be used as link compression and are supported by PPP and LAPB.

Stacker (LZS)- compression based; repeated data replaced with token. Processor intensive.

Predictor - predicts the next sequence of characters. Memory intensive.

MPPC - Microsoft Point to Point Compression protocol allows compressed data from Microsoft clients.

Compression for WAN - Can use payload compression or TCP header compression, but you should not use both.

AAA

AAA - stands for Accounting, Authentication and Authorization. Both RADIUS and TACACS+ servers can be used.

Radius uses UDP, TACACS uses TCP sessions. TACACS can be configured for more security.

Use the command below to enable the aaa process and commands.

Dallas2(config)#aaa new-model

Cisco Secure is software used for security management and accounting. It uses three major components to accomplish this:

1. **AAA server** - interacts with RADIUS and TACACS+ servers
2. **Netscape Fastrack Server** - web browser
3. **RDBMS** - Relational Database Management System

Define the TACACS+ server with the command:

Dallas2(config)# tacacs-server host 10.98.98.1

To use AAA authentication, use TACACS first, then local authentication. If there is an error, use the following syntax:

Dallas2(config)# aaa authentication login default tacacs+ local

Here we enable accounting for when network services start and stop. We log to the TACACS server

Dallas2(config)#aaa accounting network start-stop tacacs+

Here we enable authorization to gain EXEC prompt access to the router. We will authenticate against TACACS first, and if there is an error, we will authorize against the local database.

Dallas2(config)#aaa authorization exec tacacs+ local

NAT

Network Address Translation - can be used to merge two large networks without having to re-address the whole network. Another function of NAT is overloading inside global addresses. This process consists of several inside addresses using a single IP address. NAT can also use a pool of addresses or multiple interfaces. NAT uses PAT and a NAT table to keep these translations.

Natrouter(config)#ip nat inside source list 5 interface bri0 overload

Natrouter(config)#access-list 5 permit ip 172.16.10.0 0.0.0.255

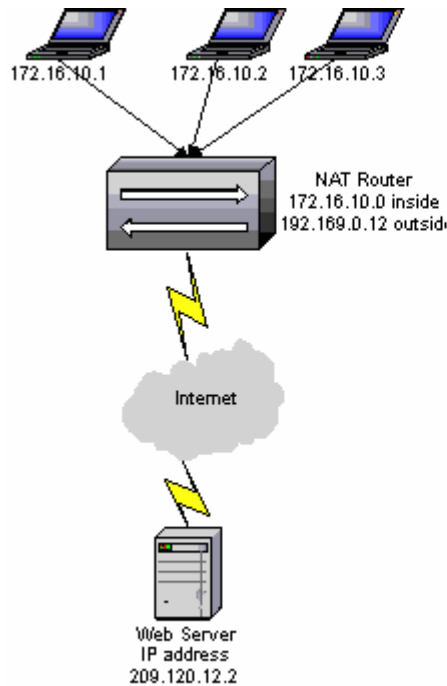
Natrouter(config)#interface ethernet 0

Natrouter(config-if)#ip address 172.16.10.0 255.255.255.0

Natrouter(config-if)#ip nat inside

Natrouter(config-if)#interface bri 0

Natrouter(config-if)#ip address 192.169 0.12 255.255.255.0



Troubleshooting NAT

show ip nat translations command displays current translations.

clear ip nat translations * command clears the entries in the NAT table.

debug ip nat command lists per packet output of translations.

show ip nat statistics command shows the values and timeout periods.

ROUTERS

AS5X00 - are access servers for multiple modems and ISDN interfaces. Considered central office equipment.

Cisco 700 - Odd numbered models have an S/T interface, even have a U interface. The 77x series have a 4pt hub built-in. The 76x series have a single ethernet port. They do not use the standard Cisco IOS, but set and reset commands. The command **upload** is the equivalent of a **show running-config**. There are 3 permanent profiles, 16 user profiles and 1 system(global) profile.

1600 Series - modular router.

1601 = 1 10baseT, 1 sync serial, 1 WIC slot.


1602 = 1 10baseT, 1 Frac T1 56Kcsu/dsu WIC, 1 WIC slot.

1603 = 1 10baseT, ISDN BRI S/T, 1 WIC slot.

1604 = 1 10baseT, ISDN BRI U, 1 WIC slot.


1605 = 2 10baseT interfaces, 1 WIC slot.

LED's - are located on the routers and can be used to check activity on an interface and to ensure the router has booted properly and hardware has been installed correctly. EN light LED is on when a module has been installed properly.




commuter
or home

Models
700 has ISDN
800 has ISDN
1000 has ISDN & WAN options



HQ
Central

Models
3000 2/4 LAN, WAN, asynch, synch ISI
4000 T1,E1 Modular
AS5000 Access Server asynch,ISDN
7200 Huge High Performance



Branch
Offices

Models
1600 has ISDN & WAN Options
1630 modular has ISDN & WAN Options
1640 modular has ISDN & WAN Options
1700 10/100 LAN to WAN, Internet and Intranet & VPI
2500 Ether, Token, synch serial, asynch, BRI, LAN
2600 2 WAN slots 2 LAN slots

Special thanks to
[Julian Laredo](#)
for contributing this
Cramsession, and [Joe Garcia](#) for
his revisions.