Config Register Change:
```
config-register 0x2102
```

IPIA turn on NTP and Logging:
```
config t
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
clock timezone EST -5
clock summer-time EDT recurring
sntp server ntp.svc.us.xo.net
ntp server ntp.svc.us.xo.net
logging buffered debugging
logging buffered 8192
end
debug mgcp packets
copy run start
```

Ip Accounting:
router(config)# int (interface you want IA on)
router(config-f0)# ip accounting
router# sho ip accounting

Shows traffic inbound or outbound on port.

Cisco has updated their ping command to allow extended ping commands on one command line.

[71.5.208.161]#ping 65.106.1.196 data 0000 repeat 50 size 1500 source 67.93.15.33

Check for Null Routes in ERX:

CLR1.Seattle-WA#sho conf | i tag 9000

Forcing the Voice Port into Busyout State

To force the voice port into a busyout state, complete the following steps in configuration mode:

Step	Command	Purpose
1.	`router(config)# voice-port` *slot/port*	Enter voice-port configuration mode.
2.	`router(config-voiceport)#` **`busyout forced`**	Place the voice port into busyout state.
3.	`router#` **`show voice busyout`**	Verify the busyout status.

Enable Logging:
logging buffered debug

DNS SERVERS
65.106.1.196 & 65.106.7.196

PROXY SERVER
holycow.concentric.net Port - 3128

CHECKING THE ERX:
sho frame interface SERIAL4/0:10/1/2/3/1 – If connection is a Frame PVC (Escape PVC for Internet on a Frame)
sho config | b 4/0:10/1/2/3/1 - Shows the begging on the config on that interface (check for shut on int)
sh int Serial4/0:10
sho controllers oc12 4/0:10 details

sho ip int br | inc <WAN IP minus 1>
CLR1.Smyrna-ga#sho ip int br | inc 64.50.71.41 (one less than WAN IP)
serial1/0:2/23 64.50.71.41/30 down down
sho ppp int serial<cust serial info>
CLR1.Smyrna-ga#sho ppp int serial1/0:2/23
PPP interface serial 1/0:2/23 is passive (max configure exceeded)
CLR1.Phoenix-az#sho ip int serial 4/0:1/1/1/3/17
CLR1.Smyrna-ga#sho controller son 3/0:4/1/1/3/1
CLR1.Nashville-tn#sho controller sonet 3/0:8/1/2/4/1
CLR1.Washington-DC#sho ip int br | inc 4/0:2/1/4/3
SERIAL4/0:2/1/4/3/1 67.105.230.1/30 up up NA : 01-22163 :
SERIAL4/0:2/1/4/3/13 65.107.193.17/30 down down DM-EDB-CN2Z-000
sho ip int br | i SERIAL4/0:12/1/1/3
CLR1.NYC-NY#sho ip int serial 8/0:6/1/3/1/1
Multipath mode = round-robin<<<<<<<<<<<<<<<----------LOAD BALANCING
sho ppp int SERIAL3/0:9/1/5/1/1 full
sho ppp int | inc 4/0:9/1/4/1 <<<----------
sh ip bgp sum

UPGRADE CAC ROUTER
Load tftp 206.173.138.57 "tdm7_0_2_2_z_all.mgm"
load 6 tftp 206.173.138.57 "rtr_1_72_b_all.mgm"
set 6 "RemoteAdit" ip address <x.x.x.x> <x.x.x.x>
reset 6
reset if you say no the first time

SET CAC PSWD
set 6 password admin "free2bme" (router)
show users
add user "protohead"
set user "protohead" password
protohead
protohead

SHOW CAC CODE VER
02-08538>status equipment

TURN ON NAT
set 6:1 ip address <NAT LAN> <subnet> (This is the NON-routable LAN block used for NAT.)
add 6:1 secondary ip address <Public LAN> <subnet> (This is the routable LAN block)
add 6 "NEXT-XXX" nat bypass <lan network IP> <subnet>
add 6 "NEXT-XXX" firewall 1 pass incoming nolog Telnet <TDM IP>/32 0.0.0.0/0 (This allows access to the TDM)
add 6 "NEXT-XXX" firewall 1 pass incoming nolog Telnet <NAT LAN>/32 0.0.0.0/0 (Use the LAN NAT interface here. Still telnet and ping to WAN)
add 6 "NEXT-XXX" firewall 1 pass incoming nolog Ping <NAT LAN>/32 0.0.0.0/0 (Use the LAN NAT interface here. Still telnet and ping to WAN)
<TELNET 6> Change the WAN interface to reflect NAT
add 6 "NEXT-XXX" firewall 4 pass inout nolog protocol 0 0.0.0.0/0 0.0.0.0/0

ADTRAN 4303
Login = PASSWORD

ADTRAN 600'S
Download (show config in terminal)

CISCO COMMANDS
clear service-module s0
service-module t1 timeslots 13-24
sho serv
sho int

sno ver
clear counters
clear log
ip address 207.155.15.15 255.255.255.252
encap ppp
erase start (then reload)
no shutdown
ip accounting out
no ip accounting out
LOGGING
int s0
fair-queue
ip route-cache
int f0
ip route-cache
logging buffered
logging history debug
SET DUPLEX
half
full
no half
no full
LOAD BALANCING
Ip cef
Ip load-share per packet (run on int s0/0 and s0/1)

VOIP
Ip cef
fair-queue (on both interfaces)
mgcp dtmf-relay voip codec all mode disabled
Sho voice call sum
sho mgcp connection
sho rtp stat
866-836-8378
echo-cancel coverage <24 32 48 64>
echo-cancel erl worst-case 0
no comfort-noise
debug mgcp packets
disconnect-ack
no battery-reversal
idle-voltage high
disc_pi_off
echo-cancel coverage 24
echo-cancel erl worst-case 0
timing hookflash-in 100
caller-id enable

PORT MAP
ip nat inside source static <proto> <private ip> <port> <public ip> <port>
ip nat inside source static tcp 192.168.2.2 21 66.238.135.161 21
TURN OFF NAT
Int f0
ip address 65.104.2.225 255.255.255.240
no ip nat inside
int s0
no ip nat outside
no ip nat inside source list 1 interface Serial0 overload
no access-list 1

UPGRADE ROUTER
copy tftp flash
206.173.138.57
IOS/c1700-y-mz.121-8.bin
Copy run start
cop ftp://c2430x:protohead@206.173.117.132/c2430-is-mz.123-7.T10.bin flash:
config t
boot system flash c2430-is-mz.123-7.T10.bin
exit
copy run start

2431 IAD IOS UPDATES

---

cop ftp://ftp%seaofwires.cnchost.com:protohead@ftp.cnchost.com/files/c2430-is-mz.123-7.T10.bin flash:

cop ftp://c2430x:protohead@206.173.117.132/c2430-is-mz.123-7.T7.bin flash:

cop ftp://c2430x:protohead@206.173.117.132/c2430-is-mz.123-7.T10.bin flash:

config t
boot system flash c2430-is-mz.123-7.T10.bin
end
copy run start

config t
mgcp dtmf-relay voip codec all mode disabled
end
cop ru sta

PASSWORD RECOVERY ON CISCO
turn off
turn on
ctrl break
(boots to rom on mode)
confreg 0x2142
reset
initial configuration = no
en
copy start run
config t
enable secret install
line vty 0 4
password install
line con 0
password install
int S0
no shut
int F0
no shut
exit
config-register 0x2102 (enable mode)
<ctrl>-C
copy run start
reload

one of the CSU/DSU's have to be a timing source... one has to be internal one has to be set to line

TURN ON NAT
config t
int f0/0
ip address 192.168.1.1 255.255.255.0 sec
ip nat inside
int s1/0:0
ip nat outside
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 int s1/0:0 overload
NXT1
Int s1/0:0
Ip nat outside
int s1/1:0
ip nat outside
exit
ip nat pool XO 67.88.32.189 67.88.32.190 netmask 255.255.255.240
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 pool XO overload

ADD HOSTMAPPING
ip nat inside source static 192.168.1.2 66.88.74.66
ip nat inside source static 192.168.1.6 66.88.74.69
ip nat inside source static 192.168.1.12 66.88.74.71
ip nat inside source static 192.168.1.13 66.88.74.70

ip nat inside source static tcp 192.168.1.4 3389 66.88.74.85 3389

TURN ON DHCP

```
ip dhcp pool XO
network 192.168.1.0 255.255.255.0
dns-server 65.106.1.196 65.106.7.196
default-route 192.168.1.1
ip dhcp excluded-address 192.168.1.1 192.168.1.29
ip dhcp excluded-address 192.168.1.81 192.168.1.255
```

ADD TACX TO CISCO

```
no access-list 10
no access-list 98
!
no tacacs-server host 65.106.2.30sd
no tacacs-server host 65.106.2.62
no tacacs-server host 65.106.2.90
no tacacs-server host 65.106.2.162
tacacs-server host 65.106.2.94
tacacs-server host 65.106.2.62
tacacs-server host 65.106.2.30
tacacs-server host 65.106.2.126
tacacs-server key inter7panthgrate89
aaa new-model
aaa authentication login default tacacs+ line
enable secret free2bme
access-list 10 permit 205.158.207.205
access-list 10 permit 208.234.218.0 0.0.1.255
access-list 10 permit 206.117.160.0 0.0.0.31
access-list 10 permit 206.173.117.0 0.0.0.255
access-list 10 permit 206.173.135.0 0.0.0.255
access-list 10 permit 206.173.138.0 0.0.0.255
access-list 10 permit 206.83.90.0 0.0.0.255
access-list 10 permit 199.2.12.0 0.0.3.255
access-list 10 permit 208.234.218.0 0.0.1.255
access-list 10 permit 206.117.160.0 0.0.0.31
access-list 10 permit 206.173.117.0 0.0.0.255
access-list 10 permit 206.173.135.0 0.0.0.255
access-list 10 permit 206.173.138.0 0.0.0.255
access-list 10 permit 206.83.90.0 0.0.0.255
access-list 10 permit 199.2.12.0 0.0.3.255
access-list 10 permit 205.158.160.208 0.0.0.7
access-list 10 permit host 66.89.55.81
access-list 10 permit host 206.173.127.98
access-list 10 permit host 64.35.0.252
access-list 10 permit host 205.158.72.5
access-list 10 permit host 206.83.90.107
access-list 10 permit host 206.173.136.10
access-list 98 permit 207.88.4.130
access-list 98 permit 207.88.123.17
access-list 98 permit 206.117.160.0 0.0.0.31
access-list 98 permit 206.173.117.0 0.0.0.255
access-list 98 permit 206.173.135.0 0.0.0.255
access-list 98 permit 206.173.138.0 0.0.0.255
access-list 98 permit 206.83.90.0 0.0.0.255
access-list 98 permit 199.2.12.0 0.0.3.255
access-list 98 permit 64.50.71.200 0.0.0.7
access-list 98 permit 64.50.67.96 0.0.0.7
access-list 98 permit 64.50.38.72 0.0.0.7
access-list 98 permit 216.250.90.24 0.0.0.7
access-list 98 permit 216.250.90.176 0.0.0.7
access-list 98 permit 64.50.30.216 0.0.0.7
access-list 98 permit 64.50.41.24 0.0.0.7
access-list 98 permit 216.250.69.200 0.0.0.7
access-list 98 permit 64.50.68.8 0.0.0.7
access-list 98 permit 64.50.32.168 0.0.0.7
access-list 98 permit 64.50.28.48 0.0.0.7
access-list 98 permit 64.50.6.232 0.0.0.7
access-list 98 permit 64.50.36.160 0.0.0.7
access-list 98 permit 64.50.26.176 0.0.0.7
access-list 98 permit 64.50.29.48 0.0.0.7
access-list 98 permit 64.50.66.224 0.0.0.7
```

access-list 98 permit 64.50.64.96 0.0.0.7
access-list 98 permit 64.50.25.72 0.0.0.7
access-list 98 permit 64.50.34.128 0.0.0.7
access-list 98 permit 64.50.19.160 0.0.0.7
access-list 98 permit 64.50.11.168 0.0.0.7
access-list 98 permit 64.50.65.80 0.0.0.7
access-list 98 permit 64.50.8.144 0.0.0.7
access-list 98 permit 64.50.6.32 0.0.0.7
access-list 98 permit 64.50.69.48 0.0.0.7
access-list 98 permit 64.50.70.80 0.0.0.7
access-list 98 permit 209.31.251.136 0.0.0.7
access-list 98 permit 208.176.115.8 0.0.0.7
access-list 98 permit 216.112.125.152 0.0.0.7
access-list 98 permit 64.1.89.32 0.0.0.7
access-list 98 permit 216.112.78.48 0.0.0.7
access-list 98 permit 209.31.197.224 0.0.0.7
access-list 98 permit 64.220.202.80 0.0.0.7
access-list 98 permit 205.158.70.168 0.0.0.7
access-list 98 permit 208.176.45.72 0.0.0.7
access-list 98 permit 209.220.111.64 0.0.0.7
access-list 98 permit 208.176.66.120 0.0.0.7
access-list 10 permit <ERX IP>
no snmp-server community internex RW 98
no snmp-server host 208.234.219.83 brillian
no snmp-server host 208.234.219.84 brillian
!
line con 0
password yruhere
transport input none
!
line aux 0
password yruhere
!
line vty 0 4
access-class 10 in
password yruhere
exit

REMOVE AAA
config t
no aaa new-model
no access-list 10
no access-list 98
no tacacs-server host 65.106.2.90
no tacacs-server host 65.106.2.126
no tacacs-server key inter7panthgrate89
no snmp-server community ro1028 RO 98
no snmp-server community nxlkcncx RO 98
no snmp-server community brillian RO 10
no snmp-server location 3930 East Ray Road Phoenix AZ 85044
no snmp-server contact Richard Purscell 480-706-4800
no snmp-server chassis-id <Serial #>
no snmp-server enable traps syslog
no snmp-server host 206.173.117.190 nxlkcncx
no snmp-server host 206.173.138.104 nxlkcncx
no snmp-server host 206.173.138.68 nxlkcncx
no snmp-server host 206.173.117.189 ro1028
no snmp-server host 206.173.117.190 ro1028
no snmp-server host 206.173.138.61 ro1028
enable secret password
line con 0
password password
exit
line vty 0 4
password password
exit
exit
wr mem

MPLS ROUTING

PREM ROUTER

*** NON-LISTED IP'S MAY BE THE CUSTOMER FIREWALL ***

1. FIND OUT HOW MANY SITES THE CUSTOMER HAS.
2. WHICH SITE DO THEY WANT TO ROUTE TO - FROM WHAT SITE ARE THEY ROUTING FROM

*** MPLS INTERFACE IP'S BEGIN WITH ONE OF THE FOLLOWING PREFIXES ***

10.	172.	192.

COMMAND

3. TO SHOW MPLS & VPN ROUTES - SHOW CONFIG | IN IP ROUTE
4. THE PREM DEFAULT ROUTE ALWAYS ROUTES TO THE CLOSEST EDGE ROUTER...

EXAMPLE | IP ROUTE VRF VPN 0.0.0.0 | SUBNET MASK | EDGE ROUTER IP

EDGE ROUTER

5. CLR

ENTER THE VIRTUAL = V :(VRF NAME)

COMMAND

SHOW IP ROUTE = ROUTING TABLE

6. MCR

COMMAND

SHOW ROUTE TABLE (VRF NAME) = ROUTING TABLE

LEAD/LEVEL 3

*** INFORMATION NEEDED TO HAVE LEAD/LEVEL 3 ADD ROUTE TO EDGE ROUTER ***

- EDGE ROUTER NAME
- ROUTED SUBNET MASK
- CUSTOMER WAN IP
- VRF NAME
- ROUTE CUSTOMER WANTS TO ADD (IP ADDRESS)

PREM ROUTER

ADDING ROUTES

7. COMMANDS TO ADD ROUTE TO PREM ROUTER:

- CONFIG T
- IP ROUTE VRF VPN [A] 10.231.60.0 [B] 255.255.255.0 [C] 207.87.131.198

A) ROUTE CUSTOMER WOULD LIKE ADDED (CUSTOMER'S PRIVATE IP)

B) SUBNET MASK

C) SPECIFIED CUSTOMER'S IP/EDGE ROUTER ← DEPENDING ON INCOMMING OR OUTGOING TRAFFIC