This was a customer's Frame-Relay traffic issue, which turned out to be a Cisco IOS bug using Frame Relay DLCI extenede addresses. This is an example of how Applied Methodlogies works with your staff and the vendor to resolve technical issues.

Here is the emailed analysis conversation between the customer's support team and Applied Methodologies.

From: Applied Methodologies, Inc.

Folks,

The Clinton DLCI 110 issue that affected 26 General Officess earlier this week was a result of an AT&T Frame POP switch card that malfunctioned over the weekend of 1/9 thus resulting in the GO running over our ISDN backup circuits on Monday and Tuesday this week. This card was replaced on Tuesday evening and the GOs have been operating normally since.

(Question??? Since this was an AT&T caused outage, do we get billing credit for the 2 days we were on ISDN???)

However, during the outage, AT&T noticed that packets with illegal headers were being sent from our Router(RTRCNJ_4 Se0). These packets are being sent to the AT&T pop and then discarded due to an invalid Frame-Relay header.

We do not know what these packets are nor do they pose an immediate or future threat to the operation of this circuit.

AT&T has stated that these packets are not causing a problem on the Frame-Relay. These packets, based on what I understand, may be taking some of the T-1 access bandwidth.

NY INSURANCE CO. routers are configured to use the RFC 1490 Multiprotocol over Frame-Relay encapsulation (this is induced with the Frame-Relay DLCI xxx IETF command).

We have traced the Se0 T-1 circuit and cannot see anything that remotely resembles what AT&T sees. Also, we checked the router and cannot find anything either. AT&T has checked DLCIs 210-910 as a control and those DLCIs and T-1 circuits do not see any packets with illegal headers.

AT&T has given me two different types of characterization of this activity. On Tuesday evening they stated that only 4/5 packets with illegal headers are transmitted every 60 seconds. We did some traffic tests to see if the questionable packets increase with traffic and they did not.

On Wednesday AT&T then tells me that the illegal header packets do increase with traffic activity.

Which is it? After working with AT&T to work with us on identifying this traffic the following will occur over the next couple of days:

NYI team will replace the CSU this evening to eliminate another variable. Even though the nature of the problem does not suggest a CSU, and if it did we would see CRCs, BPVs and error seconds errors, which we do not, we are doing this to satisfy AT&T.

1).NYI team will send a trace from the sniffer to Cisco for review. A Cisco TAC case has been opened.

2).AT&T will be on site at the Clinton Facility on Monday 1/18 at 10:am to trace the vaunted illegal header packets. Applied Methodologies will be there too with their trusty HP Internet Advisor to keep them honest for AT&T uses the same analyzer as AMI does.

3).If AT&T does not find anything on the trace they will them move their trace from our premise to their pop.

4). If we do see that the packets are coming from our router and can determine the type I will try to stop that operation.

5).If we do see that the packets are coming from our router but cannot determine what they are to turn off, I will then cut-over the config to Se3 on the same router and have AT&T monitor.

6).If I cut-over to Se3 and AT&T still sees the illegal headers we will have to push this issue back to AT&T and wait to see the results from Cisco.

7).If Cisco's results are positive, meaning the traffic comes from the router, we will then either turn off the function(if we can) or switch routers(if applicable).

8).If Cisco's results are negative, meaning the traffic is not coming from the router or cannot be identified, then we push to AT&T.

Any questions please contact me...

Thanks...

Applied Methodologies, Inc.

This is a result of what Applied Methodologies, Inc. found during the protocol analysis that was sent to the client and AT&T Frame Relay support.

To: **NY Insurance Co. team**
Subject: **DLCI 110 illegal headers**
From: **Applied Methodologies, inc.**

NYI team,

After meeting with AT&T yesterday and tracing these packets with my analyzer, it is conclusive that the packets with illegal headers do originate from our equipment.

Below is the information from the traces. NYI team and AMI tried some tests but were unable to stop this action and we were running out of time. This may be a Cisco bug. Please forward this information along to Cisco for further review under the TAC case you opened last week.

After looking at several LMI status report frames from AT&T, DLCI 128 is not listed as an active PCV. AT&T also has 128 deleted in their system. My analyzer may be just interpreting these EA frames as DLCI 128, but this is anyone's guess.

You may not see these frames with the sniffer, for these frames have a valid FCS. You may have to have the sniffer's filter set to look at frames with the DE bit set or all DLCI 128 frames.

These frames do not seem to pose any problems/threat at the moment. However, we should get some confirmation from Cisco. We do not want a problem to occur in the future that could have been prevented if this action is some indication of another problem...

Thanks...
Applied Methodologies, Inc.

There are two different traces from two different Advisor applications to support the condition that has been observed.

Trace #1 Advisor WAN Frame-Relay:

Summary Detailed Hex ASCII EBCDIC Filter... Search... Repeat
11:23:59.9837075ord #2796 (EQ) Captured on 01.18.99 at 11:23:59.9837075

Frame Relay: DLCI = 0118; CR = 0; DE = 0; FECN = 0; BECN = 0; FCS = Good
IP 220.12.19.211 -> 220.1.1.216 Id=9c87 >> UDP >> LMX_DG >> SMB
Summary of: Record #2797 (EQ) Captured on 01.18.99 at 11:23:59.9936579
Frame Relay: DLCI = 0118; CR = 0; DE = 0; FECN = 0; BECN = 0; FCS = Good

IP 220.12.19.211 -> 220.11.45.216 Id=9c87 >> UDP >> LMX_DG >> SMB
Summary of: Record #2798 (LN) Captured on 01.18.99 at 11:24:00.0591856
Frame Relay: DLCI = 0974; CR = 0; DE = 0; FECN = 0; BECN = 0; FCS = Good
Summary of: Record #2799 (LN) Captured on 01.18.99 at 11:24:00.0608080
Frame Relay: DLCI = 0128; CR = 0; DE = 1; FECN = 0; BECN = 0; FCS = Good
Frame Relay: >>> ERROR >>> Extended Address Bit EA1 Does Not Equal One
Summary of: Record #2800 (LN) Captured on 01.18.99 at 11:24:00.0623319
Frame Relay: DLCI = 0128; CR = 0; DE = 1; FECN = 0; BECN = 0; FCS = Good
Frame Relay: >>> ERROR >>> Extended Address Bit EA1 Does Not Equal One
Summary of: Record #2801 (EQ) Captured on 01.18.99 at 11:24:00.0891692
Frame Relay: DLCI = 0113; CR = 0; DE = 0; FECN = 0; BECN = 0; FCS = Good
Summary of: Record #2802 (LN) Captured on 01.18.99 at 11:24:00.1591605
Frame Relay: DLCI = 0270; CR = 0; DE = 0; FECN = 0; BECN = 0; FCS = Good
Summary of: Record #2803 (LN) Captured on 01.18.99 at 11:24:00.1608126
Frame Relay: DLCI = 0128; CR = 0; DE = 1; FECN = 0; BECN = 0; FCS = Good
Frame Relay: >>> ERROR >>> Extended Address Bit EA1 Does Not Equal One
Summary of: Record #2804 (LN) Captured on 01.18.99 at 11:24:00.1623378
Frame Relay: DLCI = 0128; CR = 0; DE = 1; FECN = 0; BECN = 0; FCS = Good
Frame Relay: >>> ERROR >>> Extended Address Bit EA1 Does Not Equal One
Summary of: Record #2805 (EQ) Captured on 01.18.99 at 11:24:00.2292217
Frame Relay: DLCI = 0146; CR = 0; DE = 0; FECN = 0; BECN = 0; FCS = Good
IP 220.9.46.2 -> 224.0.0.10 Id=0000 >> EIGRP
Summary of: Record #2806 (LN) Captured on 01.18.99 at 11:24:00.2597707
Frame Relay: DLCI = 0145; CR = 0; DE = 0; FECN = 0; BECN = 0; FCS = Good
Summary of: Record #2807 (LN) Captured on 01.18.99 at 11:24:00.2612720
Frame Relay: DLCI = 0160; CR = 0; DE = 0; FECN = 0; BECN = 0; FCS = Good

Here is a detail view of a frame from above:

Summary Detailed Hex ASCII EBCDIC Filter... Search... Repeat
11:24:00.0623319ord #2800 (LN) Captured on 01.18.99 at 11:24:00.0623319

Frame Relay:
DLCI = 0128
Command/Response = 0 (Command)
Discard Eligibility = 1 (Discardable)
Forward Congestion = 0
Backward Congestion = 0
FCS = 0xb8-fb (Good)
Frame Relay: >>> ERROR >>> Extended Address Bit EA1 Does Not Equal One

Trace #2 Advisor Decodes utility:
This trace shows the extended address

Frame	Len	Channel	DLCI	Prot	Description
1759	66	DCE	130	FRELAY	fecn=0 becn=0 de=0 IP 220.9.203.
1760	172	DCE		LN_STAT	T1
1761	57	DTE	176	FRELAY	fecn=0 becn=0 de=0
1762	57	DTE	174	FRELAY	fecn=0 becn=0 de=0
1763	172	DCE		LN_STAT	T1
1764	172	DTE		LN_STAT	T1
1765	172	DTE		LN_STAT	T1
1766	289	DTE	**1049600**	FRELAY	fecn=0 becn=0 de=1
1767	309	DTE	974	FRELAY	fecn=0 becn=0 de=0
1768	289	DTE	**1049600**	FRELAY	fecn=0 becn=0 de=1
1769	172	DTE		LN_STAT	T1
1770	172	DTE		LN_STAT	T1
1771	289	DTE	**1049600**	FRELAY	fecn=0 becn=0 de=1
1772	289	DTE	**1049600**	FRELAY	fecn=0 becn=0 de=1
1773	289	DTE	**1049600**	FRELAY	fecn=0 becn=0 de=1
1774	172	DTE		LN_STAT	T1
1775	172	DTE		LN_STAT	T1
1776	289	DTE	**1049600**	FRELAY	fecn=0 becn=0 de=1
1777	285	DTE	145	FRELAY	fecn=0 becn=0 de=0
1778	285	DTE	160	FRELAY	fecn=0 becn=0 de=0
1779	172	DTE		LN_STAT	T1
1780	172	DTE		LN_STAT	T1
1781	284	DTE	165	FRELAY	fecn=0 becn=0 de=0
1782	284	DTE	175	FRELAY	fecn=0 becn=0 de=0
1783	284	DTE	113	FRELAY	fecn=0 becn=0 de=0
1784	172	DTE		LN_STAT	T1
1785	172	DTE		LN_STAT	T1
1786	285	DTE	131	FRELAY	fecn=0 becn=0 de=0
1787	285	DTE	146	FRELAY	fecn=0 becn=0 de=0

Here is a decoded view of one of the above frames:

---------- FRELAY Header ----------
FRELAY: **Data Link Connection Identifier (DLCI): 1049600** (In channel layer 2 management)
FRELAY: Forward Explicit Congestion Notification (FECN): 0 (Unset)
FRELAY: Backward Explicit Congestion Notification (BECN): 0 (Unset)
FRELAY: Discard Eligibility: 1 (Set)

Here is a copy of the LMI report packet sent to us:

Summary Detailed Hex ASCII EBCDIC Filter... Search... Repeat
11:54:13.1743292ord #190 (LN) Captured on 01.18.99 at 11:54:13.1743292

Original LMI:
Message Type = 0x07d (Status)
--- Information Elements ---
Report type = 0x000 (Full Status Report)

Keep Alive Sequence
Send sequence num = 154
Recv sequence num = 058
PVC Status

DLCI = 0113 old active
Reserved/Bandwidth = 0x00-7d-00/32000 bps
PVC Status
DLCI = 0115 old active

Reserved/Bandwidth = 0x00-7d-00/32000 bps
PVC Status
DLCI = 0116 old active
Reserved/Bandwidth = 0x01-f4-00/128000 bps

PVC Status
DLCI = 0117 old active
Reserved/Bandwidth = 0x01-f4-00/128000 bps
PVC Status

DLCI = 0118 old active
Reserved/Bandwidth = 0x01-f4-00/128000 bps
PVC Status
DLCI = 0119 old active

Reserved/Bandwidth = 0x01-f4-00/128000 bps
PVC Status
DLCI = 0126 old active
Reserved/Bandwidth = 0x00-7d-00/32000 bps

PVC Status
DLCI = 0130 old active
Reserved/Bandwidth = 0x00-7d-00/32000 bps
PVC Status
DLCI = 0130 old active
Reserved/Bandwidth = 0x00-7d-00/32000 bps
PVC Status
DLCI = 0131 old active

Reserved/Bandwidth = 0x00-7d-00/32000 bps
PVC Status
DLCI = 0134 old inactive
Reserved/Bandwidth = 0x00-7d-00/32000 bps

PVC Status

```
  DLCI            = 0135  old active
Reserved/Bandwidth  = 0x00-7d-00/32000 bps
PVC Status

  DLCI            = 0145  old active
Reserved/Bandwidth  = 0x00-7d-00/32000 bps
PVC Status
  DLCI            = 0146  old active

Reserved/Bandwidth  = 0x00-7d-00/32000 bps
PVC Status
  DLCI            = 0147  old inactive
Reserved/Bandwidth  = 0x01-f4-00/128000 bps

PVC Status
  DLCI            = 0149  old active
Reserved/Bandwidth  = 0x01-f4-00/128000 bps
PVC Status

  DLCI            = 0151  old active
Reserved/Bandwidth  = 0x01-f4-00/128000 bps
PVC Status
  DLCI            = 0153  old active

Reserved/Bandwidth  = 0x01-f4-00/128000 bps
PVC Status
  DLCI            = 0160  old active
Reserved/Bandwidth  = 0x00-7d-00/32000 bps

DLCI            = 0163  old active
Reserved/Bandwidth  = 0x01-f4-00/128000 bps
PVC Status
  DLCI            = 0165  old active

Reserved/Bandwidth  = 0x00-7d-00/32000 bps
PVC Status
  DLCI            = 0168  old active
Reserved/Bandwidth  = 0x01-f4-00/128000 bps

PVC Status
  DLCI            = 0174  old active
Reserved/Bandwidth  = 0x01-f4-00/128000 bps
PVC Status

  DLCI            = 0175  old active
Reserved/Bandwidth  = 0x00-7d-00/32000 bps
PVC Status
  DLCI            = 0176  old active

Reserved/Bandwidth  = 0x01-f4-00/128000 bps
PVC Status
  DLCI            = 0180  old inactive
Reserved/Bandwidth  = 0x00-7d-00/32000 bps

PVC Status
  DLCI            = 0270  old active
```

Reserved/Bandwidth = 0x00-7d-00/32000 bps
PVC Status

  DLCI   = 0275 old active
Reserved/Bandwidth = 0x00-7d-00/32000 bps
PVC Status
  DLCI   = 0974 old active

Reserved/Bandwidth = 0x00-7d-00/32000 bps