DOCSIS 3.0

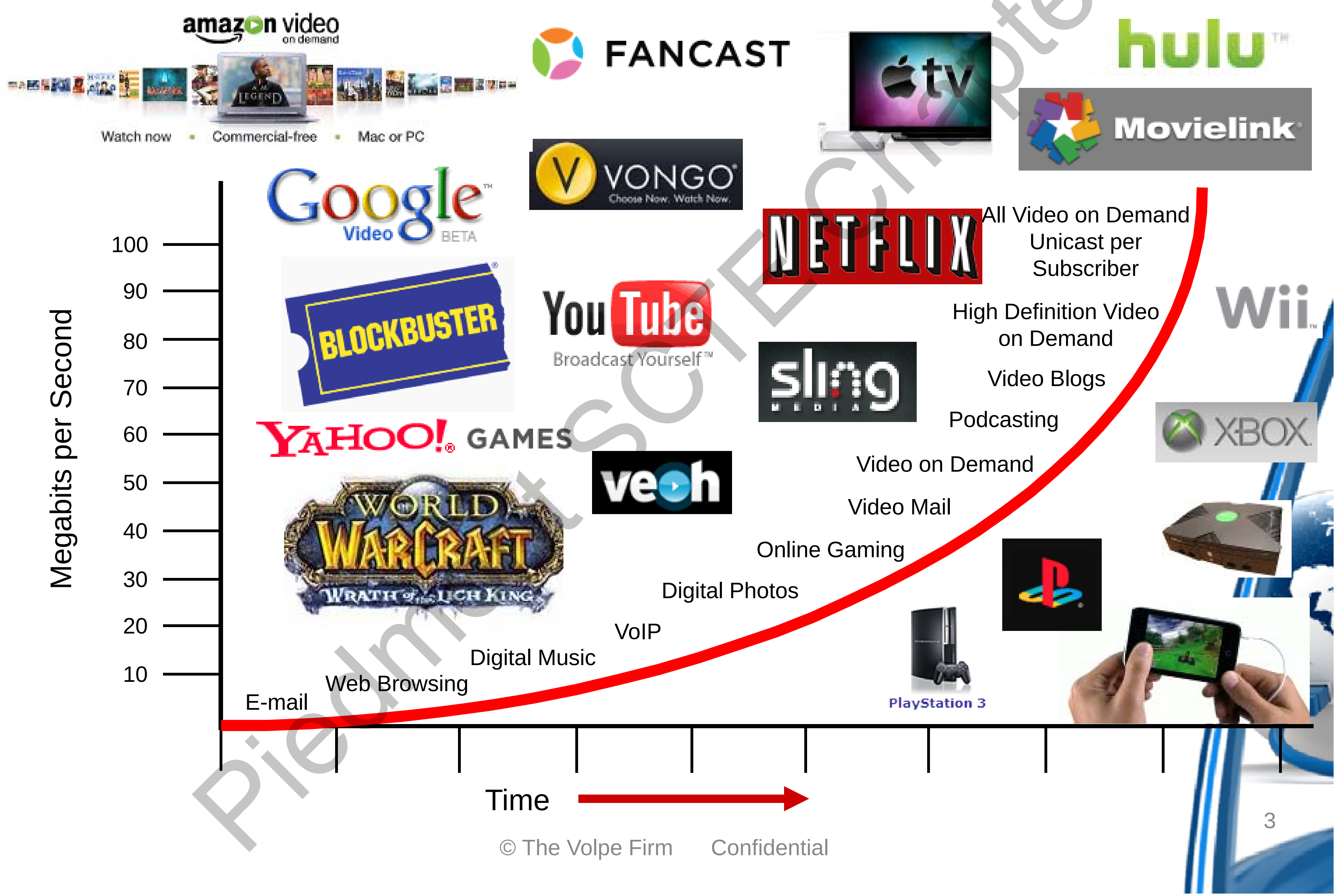
Terminology, Features and Troubleshooting

Brady Volpe

The Volpe Firm

Agenda

- DOCSIS 3.0 Overview
- DOCSIS 3.0 terminology
- DOCSIS modem registration
- IPv6 and what it means to you
- DOCSIS 3.0 security enhancements
- Advanced Troubleshooting
- Q&A


amazon video on demand
Watch now • Commercial-free • Mac or PC
FANCAST
hulu
Movielink
Google Video BETA
VONGO Choose Now. Watch Now.
NETFLIX
All Video on Demand
Unicast per
Subscriber
YouTube Broadcast Yourself
High Definition Video
on Demand
Wii
BLOCKBUSTER
sling MEDIA
Video Blogs
Podcasting
YAHOO! GAMES
veoh
XBOX
Video on Demand
Video Mail
WORLD WARCRAFT WRATH of the LICH KING
Online Gaming
Digital Photos
VoIP
Digital Music
Web Browsing
E-mail
PlayStation 3
Megabits per Second
100
90
80
70
60
50
40
30
20
10
Time

DOCSIS 3.0 Overview

- DOCSIS 3.0 Specification(s)
  - ✓ DOCSIS 3.0 Interface Specifications (Released December 2006)
  - ✓ Equipment readily available
- Downstream data rates of 160 Mbps or higher
  - ✓ Channel Bonding
  - ✓ 4 or more channels
- Upstream data rates of 120 Mbps or higher
  - ✓ Channel Bonding
  - ✓ 4 or more channels
- Internet Protocol version 6 (IPv6)
  - ✓ *Current System (IPv4) is limited to 4.3B numbers*
  - ✓ IPv6 greatly expands the number of IP addresses
    - Expands IP address size from 32 bits to 128 bits
    - IPv6 supports 3.4×10^{38} addresses;
    - Colon-Hexadecimal Format
- 100% backward compatible with DOCSIS 1.0/1.1/2.0

256QAM => ~40Mbps

8 x 256QAM => ~320 Mbps

64QAM => ~30Mbps

4 x 64QAM => ~120 Mbps

4923:2A1C:0DB8:04F3:AEB5:96F0:E08C:FFEC

DOCSIS Comparison

Version	Downstream						Upstream				
	Channel configuration						Channel configuration				
	Minimum selectable number of channels	Minimum number of channels that hardware must be able to support	Selected number of channels	Maximum number of channels	DOCSIS throughput	EuroDOCSIS throughput	Minimum selectable number of channels	Minimum number of channels that hardware must be able to support	Selected number of channels	Maximum number of channels	Throughput
1.x	1	1	1	1	42.88 (38) Mbit/s	55.62 (50) Mbit/s	1	1	1	1	10.24 (9) Mbit/s
2.0	1	1	1	1	42.88 (38) Mbit/s	55.62 (50) Mbit/s	1	1	1	1	30.72 (27) Mbit/s
3.0	1	4	*m*	No maximum defined	*m* × 42.88 (*m* × 38) Mbit/s	*m* × 55.62 (*m* × 50) Mbit/s	1	4	*n*	No maximum defined	*n* × 30.72 (*n* × 27) Mbit/s

(Source: Wikipedia)

Channel configuration		Downstream throughput		Upstream throughput
Number of downstream channels	Number of upstream channels	DOCSIS	EuroDOCSIS	
4	4	171.52 (152) Mbit/s	222.48 (200) Mbit/s	122.88 (108) Mbit/s
8	4	343.04 (304) Mbit/s	444.96 (400) Mbit/s	122.88 (108) Mbit/s

(Source: Wikipedia)

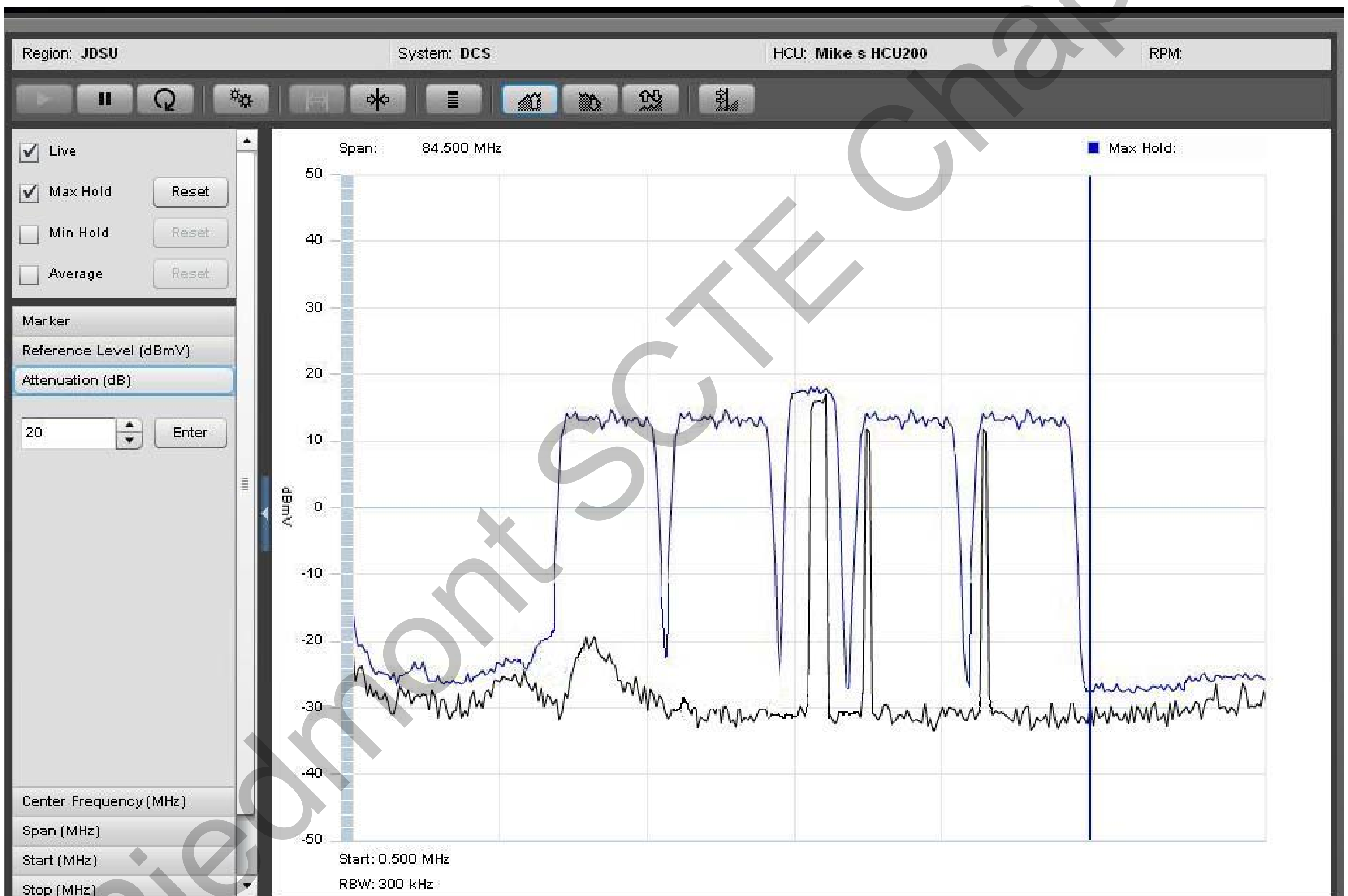
DOCSIS® 3.0 Assumed Downstream RF Channel Transmission Characteristics

Parameter	Value
Frequency range	108 to 1002 MHz edge to edge
RF channel spacing (design bandwidth)	6 MHz
Transit delay from head-end to most distant customer	≤ 0.800 ms (typically much less)
Carrier-to-noise ratio in a 6 MHz band	Not less than 35 dB
Carrier-to- CTB, CSO, X-MOD, Ingress	Not less than 41 dB
Amplitude ripple	3 dB within the design bandwidth
Group delay ripple in the spectrum occupied by the CMTS	75 ns within the design bandwidth
Micro-reflections bound for dominant echo	-10 dBc@ <= 0.5 µsec -20 dBc@ <= 1.5 µsec -30 dBc@ > 1.5 µsec
Maximum analog video carrier level at the CM input	17 dBmV

DOCSIS® 3.0 Assumed Upstream RF Channel Transmission Characteristics

Parameter	Value
Frequency range	5 to 85 MHz edge to edge
Carrier-to-interference plus ingress ratio	Not less than 25 dB
Carrier hum modulation	Not greater than –23 dBc (7%)
Burst noise	Not longer than 10 µsec at a 1 kHz average rate for most cases
Amplitude ripple 5-42 MHz	0.5 dB/MHz
Group delay ripple 5-42 MHz	200 ns/MHz
Micro-reflections—single echo	-10 dBc@ <= 0.5 µsec -20 dBc@ <= 1.0 µsec -30 dBc@ > 1.0 µsec
Seasonal and diurnal reverse gain (loss) variation	Not greater than 14 dB min to max

The Bonded Upstream



Power Variance – 6dB Bonded vs. Unbonded

DOCSIS 3.0 Cable Modem 1 Channel Transmit Power Levels

Constellation	Constellation Gain G_{const} Relative to 64 QAM (dB)	P_{min} (dBmV)			P_{max} (dBmV) TDMA	P_{max} (dBmV) S-CDMA	P_{min} - G_{const} (dBmV)	P_{max} - G_{const} (dBmV) TDMA	P_{max} - G_{const} (dBmV) S-CDMA
		L	M	H					
QPSK	-1.18	17	20	23	61	56	18.18	62.18	57.18
8 QAM	-0.21	17	20	23	58	56	17.21	58.21	56.21
16 QAM	-0.21	17	20	23	58	56	17.21	58.21	56.21
32 QAM	0.00	17	20	23	57	56	17.00	57.00	56.00
64 QAM	0.00	17	20	23	57	56	17.00	57.00	56.00
128 QAM	0.05	17	20	23	N/A	56	16.95	N/A	55.95

(P_{min} is a function of Modulation Rate, with L = 1280 kHz, M = 2560 kHz, and H = 5120 kHz.)

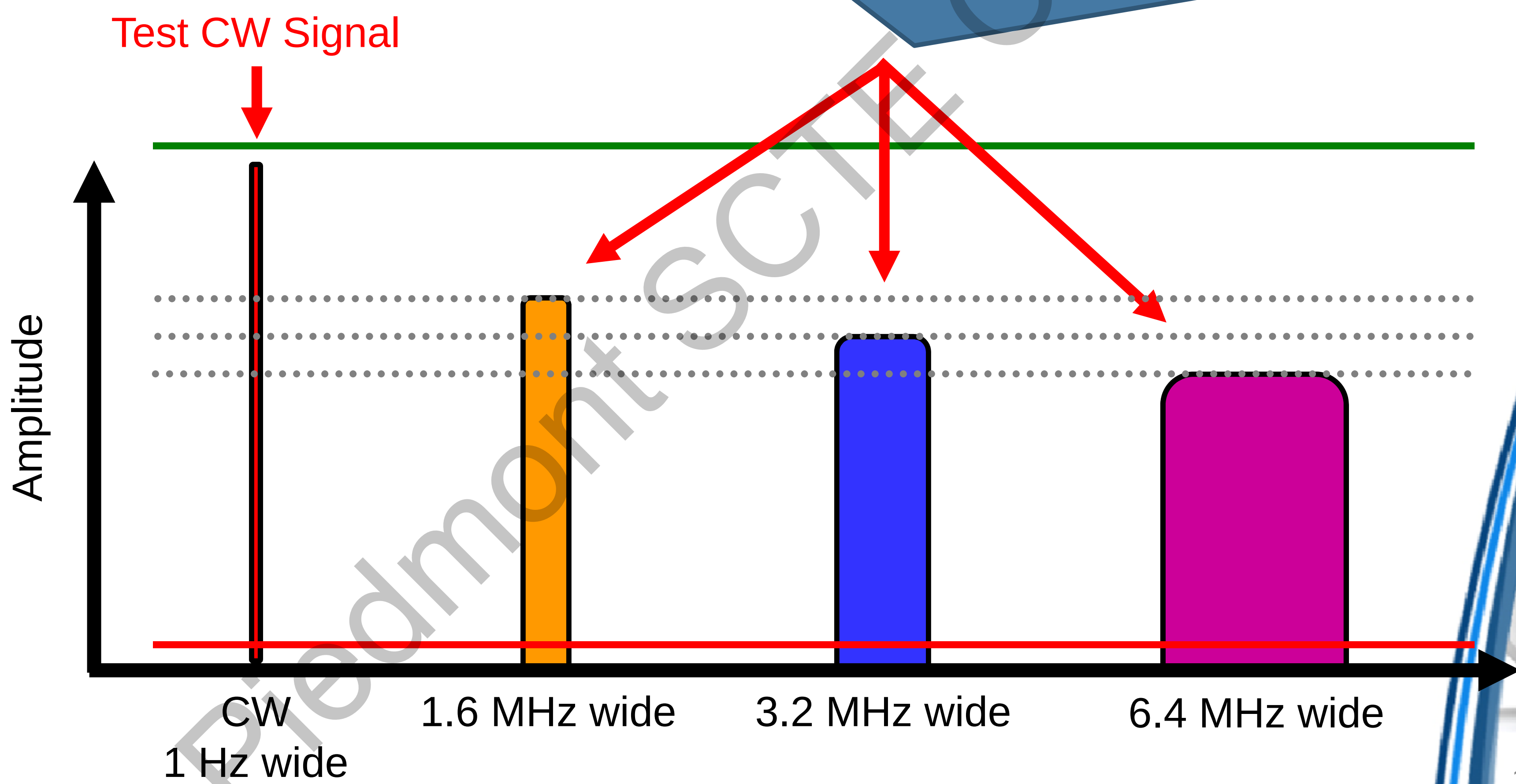
DOCSIS 3.0 Cable Modem 4 Channel Transmit Power Levels

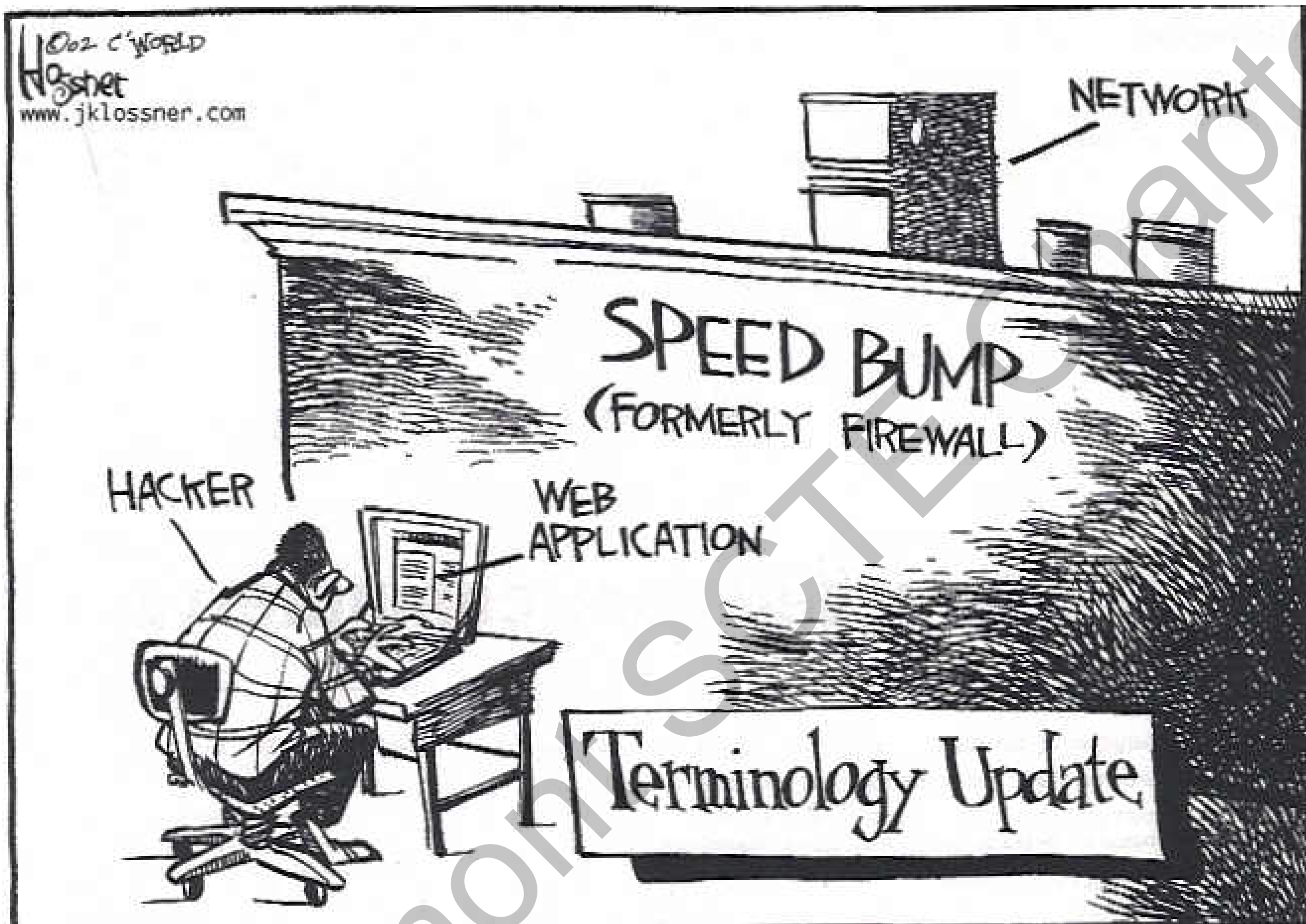
Constellation	Constellation Gain G_{const} Relative to 64 QAM (dB)	P_{min} (dBmV)			P_{max} (dBmV) TDMA	P_{max} (dBmV) S-CDMA	P_{min} - G_{const} (dBmV)	P_{max} - G_{const} (dBmV) TDMA	P_{max} - G_{const} (dBmV) S-CDMA
		L	M	H					
QPSK	-1.18	17	20	23	55	53	18.18	56.18	54.18
8 QAM	-0.21	17	20	23	52	53	17.21	52.21	53.21
16 QAM	-0.21	17	20	23	52	53	17.21	52.21	53.21
32 QAM	0.00	17	20	23	51	53	17.00	51.00	53.00
64 QAM	0.00	17	20	23	51	53	17.00	51.00	53.00
128 QAM	0.05	17	20	23	N/A	53	16.95	N/A	52.95

(P_{min} is a function of Modulation Rate, with L = 1280 kHz, M = 2560 kHz, and H = 5120 kHz.)

Measuring Upstream Carrier Amplitudes

These carriers will NOT have the same peak amplitude level when measured on a typical spectrum analyzer when they are each hitting the CMTS at "0 dBmV power per channel".





TERMINOLOGY & REGISTRATION

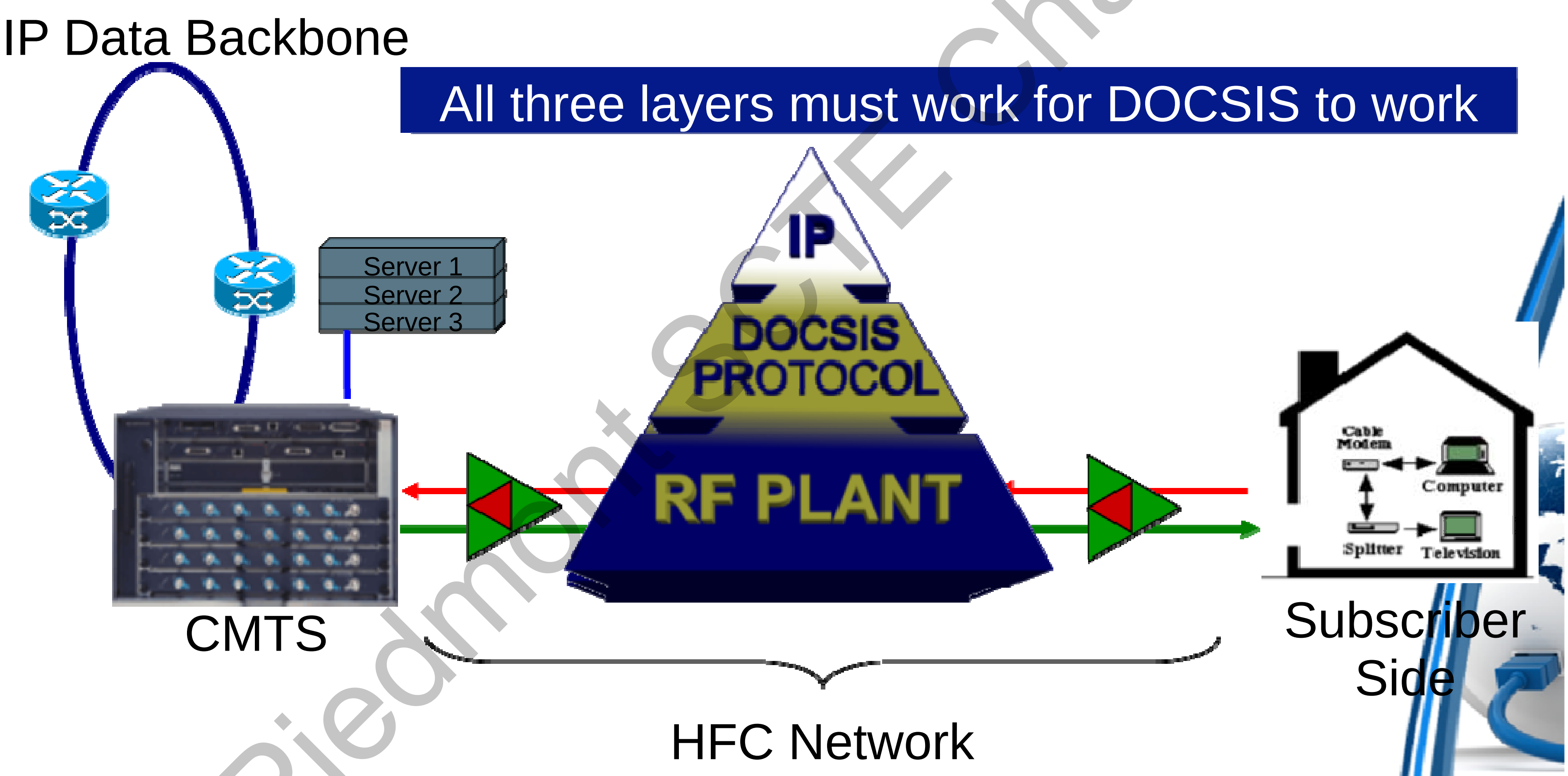
Downstream Terminology

- Primary Downstream Channel(s)
  - ✓ Master clock, UCD, MAPs, etc.
  - ✓ CMs Registration + PDU
- Non-Primary Capable Channel(s)
  - ✓ PDU only
  - ✓ D3.0 modems
- Downstream Service Group (DSG)
  - ✓ DS bonded CHs available to CM
- MAC Domain Descriptor (MDD)
  - ✓ Contains the Downstream Channel ID of the Primary DS Channel
- Receive Channel Configuration (RCC)
  - ✓ RCC encoding configures the CM's physical layer components to specific downstream frequencies

Upstream Terminology

- Upstream Channel
  - ✓ Physical Upstream Channel (DOCSIS RF), or
  - ✓ Logical Upstream Channel (share same RF ch)
- Upstream Channel Descriptor – UCD
  - ✓ MAC message to CMs describing US CH
- Upstream Bonding Group (UBG)
  - ✓ Set of US bonded channels for CM
- Transmit Channel Set (TCS)
  - ✓ Set of upstream channels that a cable modem is configured to use for upstream transmission
- Transmit Channel Config (TCC)
  - ✓ Add, delete, change channels TLV

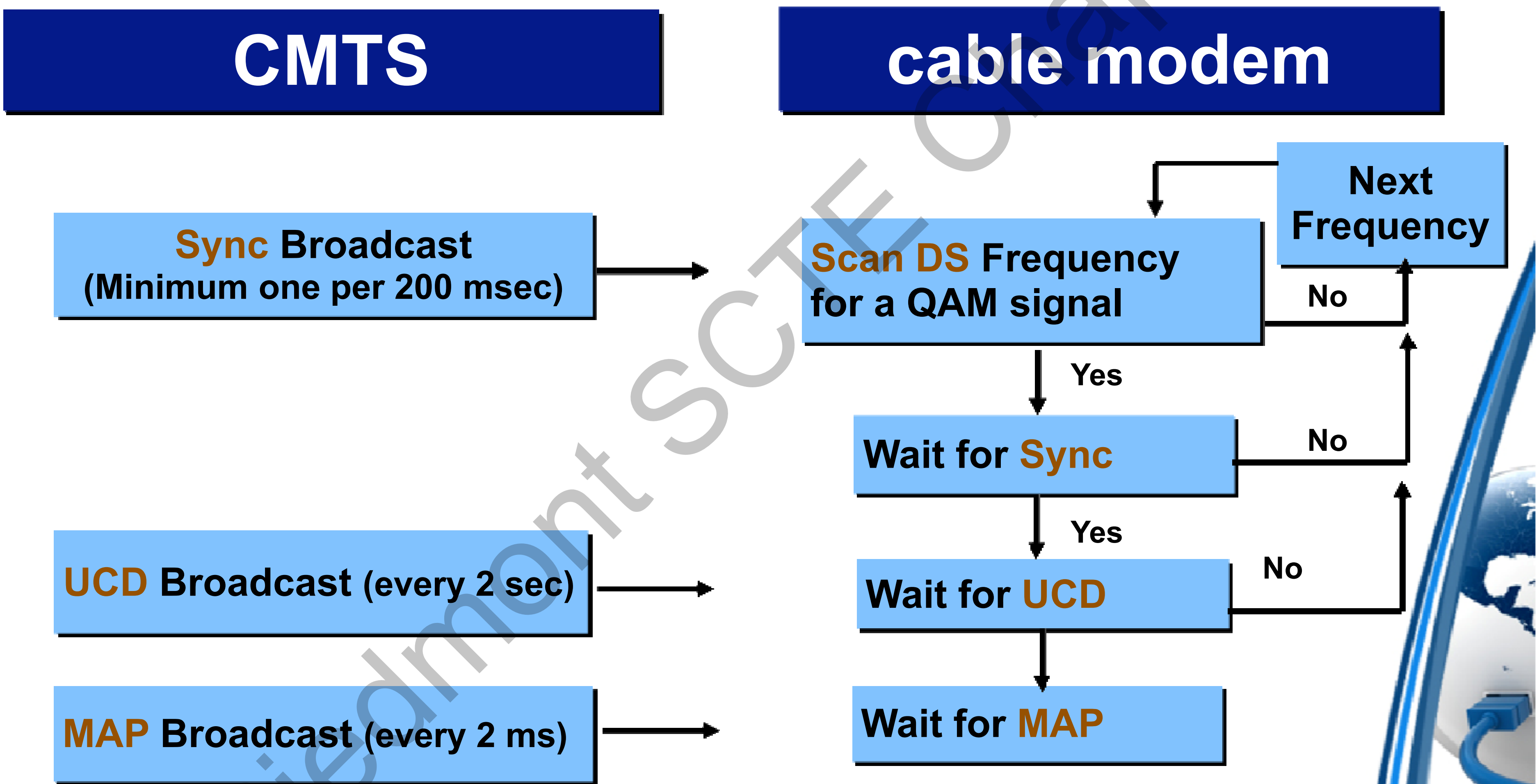
DOCSIS Communications Model



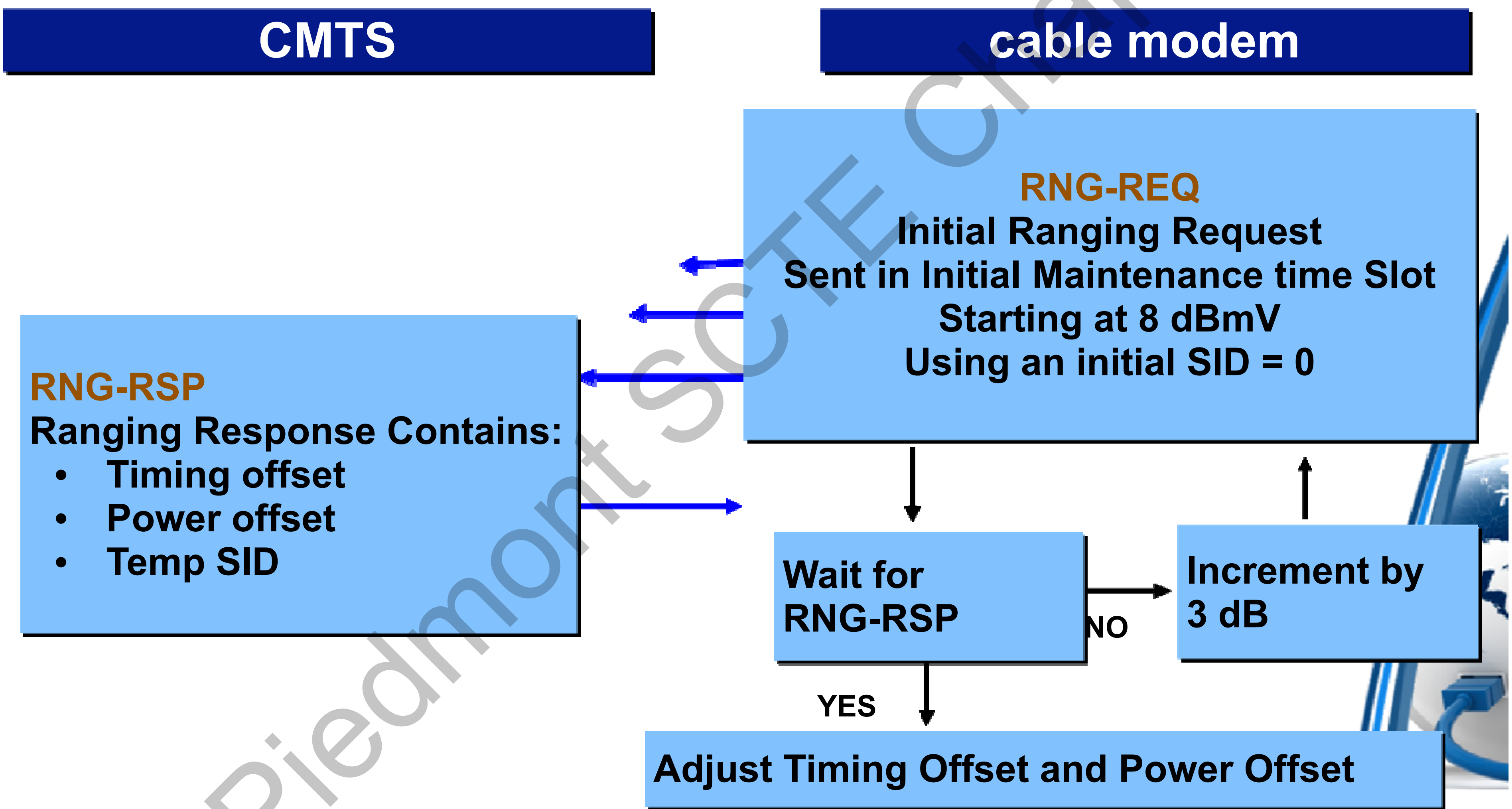
Cable Modem Registration – DOCSIS 1.x/2.0

- ✓ CM registration requires the physical layer for signal transport
- ✓ DOCSIS and IP protocol layers are necessary to communicate the proper messages for modems to come online
- ✓ The next slides illustrate the interaction of these layers

DS Freq. Acquisition



CM Ranging


CMTS
cable modem
RNG-REQ
Initial Ranging Request
Sent in Initial Maintenance time Slot
Starting at 8 dBmV
Using an initial SID = 0
RNG-RSP
Ranging Response Contains:
• Timing offset
• Power offset
• Temp SID
Wait for RNG-RSP
NO
Increment by 3 dB
YES
Adjust Timing Offset and Power Offset

DHCP Overview

CMTS	cable modem
	Bandwidth Request Use Temp SID (Service ID) →
MAP Broadcasts →	
DHCP Reply (Offer) DHCP offers an IP address →	← **DHCP Discover**
DHCP Ack (Response) Contains IP Addr, plus additional information →	← **DHCP Request** Acks Initial IP Address and requests Default GW, ToD Server, TOD offset, TFTP Server Addr and TFTP Boot Config File Name
ToD Response Contains Time of Day per RFC 868 (Not NTP) →	← **ToD Request**

TFTP & Registration

IP DOCSIS PROTOCOL

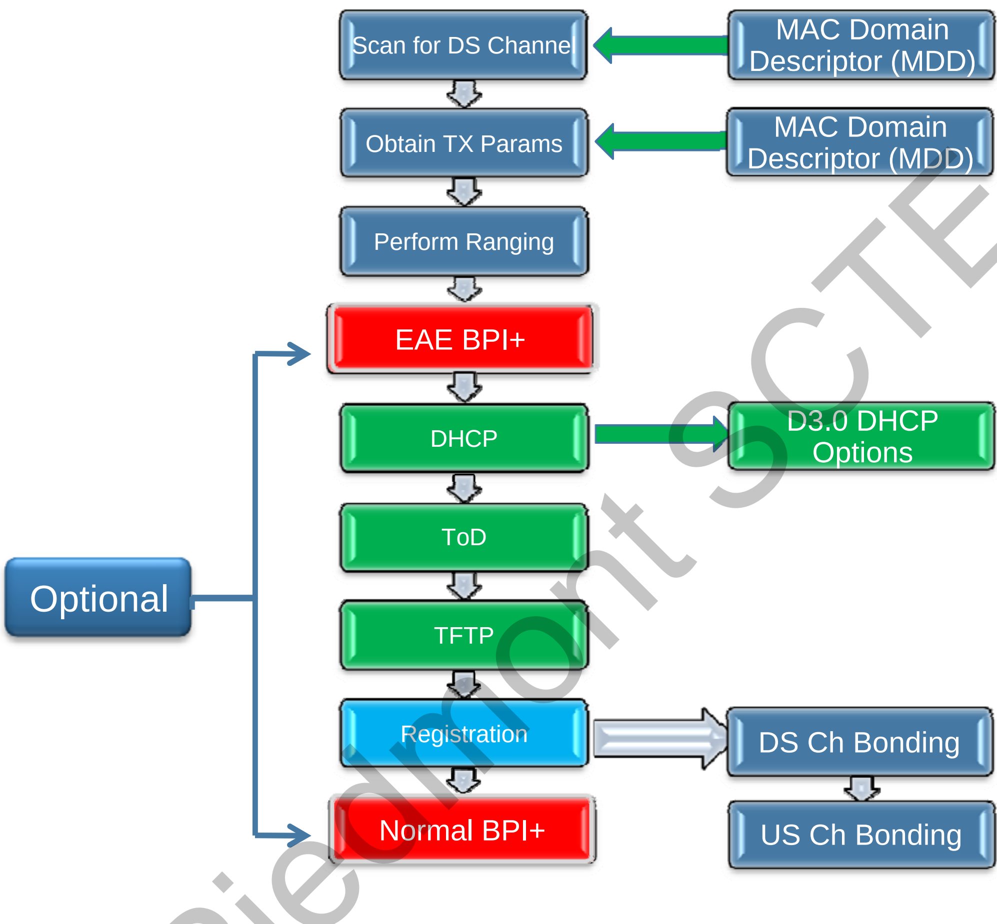
CMTS	cable modem
	TFTP Boot Request For 'Boot File name'
TFTP Boot File Transfer DOCSIS config file which contains Classifiers for QoS and schedule, Baseline Privacy (BPI), etc.	
	Validate file MD5 Checksum Implement Config
	Registration Request Send QoS Parameters
Registration Response Contains Assigned SID Modem registered	
	Registration Acknowledge Send QoS Parameters

CM Registration Summary

- ✓ Downstream channel search
- ✓ Ranging
- ✓ DHCP
- ✓ ToD
- ✓ TFTP
- ✓ Registration
- ✓ Optional BPI Encryption

- ✓ Ranging occurs at least every 30 seconds when online
  - T3 timeout if Range-Request not received within 35 seconds
  - T4 timeout if Range-Response not received within 200 ms

D3.0 Modem Registration

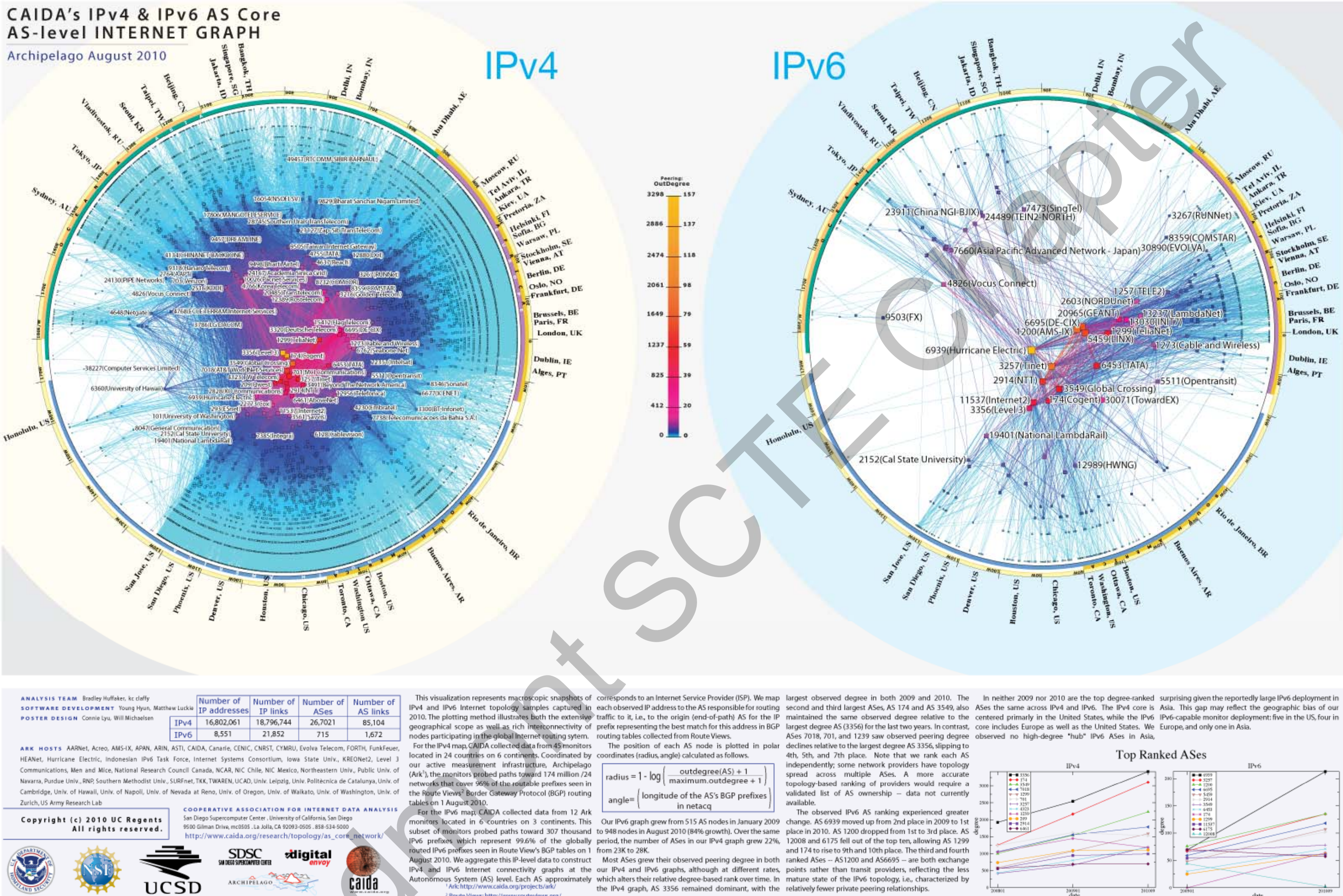


Provides Primary Ch ID on Secondary Chs

- MD-DS-SG
- MD-US-SG
- Ch Parameters: Freq, Modulation, etc.
- Security: EAE
- DHCP IPv4/IPv6 or suppressed and in config
- If no MDD → DOCSIS 2.0 mode!

- IPv4 Only (DHCPv4)
- IPv6 Only (DHCPv6)
- Alternate Provisioning Mode (APM)
  - DHCPv6 then DHCPv4
- Dual-stack Provisioning Mode (DPM)
  - DHCPv6 and DHCPv4

- RCC for downstream channels
- TCC to add upstream channels


CAIDA's IPv4 & IPv6 AS Core
AS-level INTERNET GRAPH
Archipelago August 2010
IPv4
IPv6
ANALYSIS TEAM Bradley Huffaker, kc claffy
SOFTWARE DEVELOPMENT Young Hyun, Matthew Luckie
POSTER DESIGN Connie Lyu, Will Michaelsen
	Number of IP addresses	Number of IP links	Number of ASes	Number of AS links
IPv4	16,802,061	18,796,744	26,7021	85,104
IPv6	8,551	21,852	715	1,672
Copyright (c) 2010 UC Regents
All rights reserved.
http://www.caida.org/research/topology/as_core_network/
Top Ranked ASes
UCSD
SDSC
digital envoy
ARCHIPELAGO
caida

DOCSIS IPV6

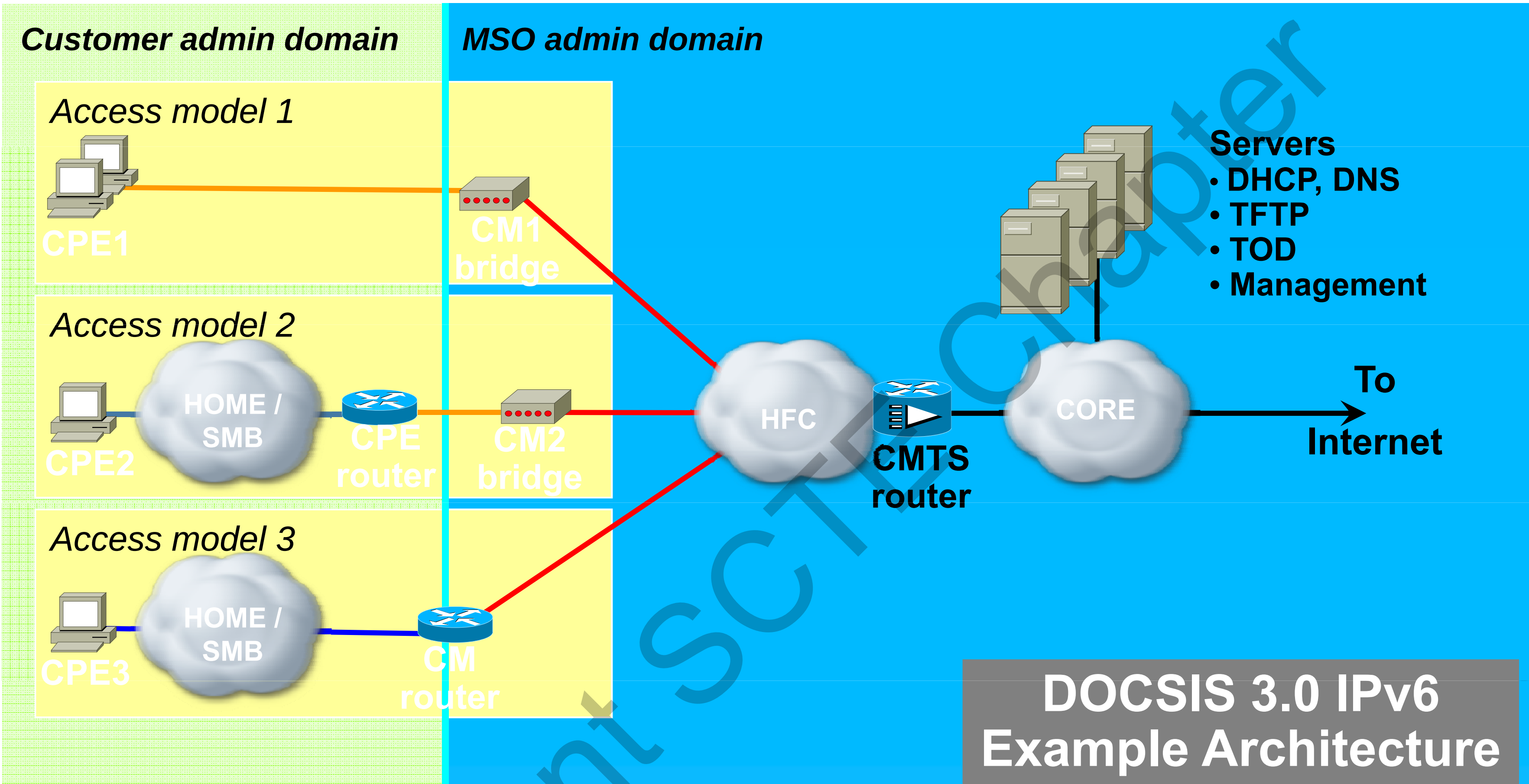
IPv6

You may not even know it happened…IPv6 Day

June 8th, 2011

IPv6 and DOCSIS 3.0

- IPv4 only (DHCP4)
- IPv6 only (DHCP6)
- Alternate Provisioning Mode
  - ✓ DHCP6 then DHCP4
- Dual-Stack Provisioning Mode
  - ✓ DHCP6 and DHCP4



Management prefix:	2001:DB8:FFFF:0::/64
Service prefix:	2001:DB8:FFFE:0::/64
Customer 2 prefix:	2001:DB8:2::/48
Customer 3 prefix:	2001:DB8:3::/48

- (red line) MSO management; assigned 2001:DB8:FFFF:0::/64
- (orange line) MSO service 2001:DB8:FFFE:0::/64
- (green line) Customer 2 premises link; assigned 2001:DB8:2:0::/64
- (blue line) Customer 3 premises link; assigned 2001:DB8:3:0::/64

SECURITY

Why better DOCSIS security?

- Various anonymous cable modem hackers have reported high success rates with zero signs of detection
  - ✓ Durandal has a machine on a business configuration that has been seeding torrents steadily for over a year
  - ✓ Many people have as many as 8 or more modems running concurrently
  - ✓ In all of these scenarios, the individuals are paying for service. They are simply splicing their line to add additional modems

Source: Defcon.org

Its beyond simple theft of service. Substantial traffic users can have a significant impact on system performance

Hacking the Cable Modem

- Which OIDs are used for hacking?
- 1.3.6.1.2.1.69.1.4.5.0
  - ✓ To figure out what the current cfg file name is for cable modem.
- 1.3.6.1.2.1.10.127.1.1.3.1.3.1
- 1.3.6.1.2.1.10.127.1.1.3.1.5.1
  - ✓ To check Up/DownStream speed of cfg file
- 1.3.6.1.2.1.69.1.4.4.0
  - ✓ To read TFTP Server IP of cable modem
- 1.3.6.1.2.1.69.1.1.3.0
  - ✓

With some software and cheap hardware – hacking is pretty darn simple in a non-BPI+ environment

BPI/BPI+ in DOCSIS 1.x / 2.0

- BPI: Baseline Privacy Interface
  - ✓ Methods for encrypting traffic between the cable modem and the
  - ✓ CMTS with 56bit DES encryption
- BPI+: Baseline Privacy Interface Plus
  - ✓ Implemented in DOCSIS 1.1 specs (Backwards compatible)
  - ✓ Introduces X.509 v3 (RSA 1024bit) digital certificates & key pairs
  - ✓ Authentication based on certificate hardware identity; validated when modem registers with a CMTS
- Makes hacking a bit more difficult, however…
  - ✓ Operators tend to leave “Self-signed certificates on
  - ✓ During registration, there is no BPI+ security, all transactions are in the clear
  - ✓ DOCSIS 1.x and 2.0 is still exposed to security breaches
  - ✓ Even with Enforce TFTP, Masking TFTP file names, TFTP Proxy, etc.

Enhance DOCSIS 3.0 & IPv6 Security

- DOCSIS 3.0 Introduces
  - ✓ 128 bit AES traffic encryption
  - ✓ Early CM authentication and traffic encryption (EAE)
  - ✓ Source IP address verification (SAV)
  - ✓ TFTP proxy and configuration file learning
  - ✓ MMH algorithm for CMTS MIC
  - ✓ Certificate revocation
  - ✓ Encryption support of new method of multicast messaging

Security Recommendation

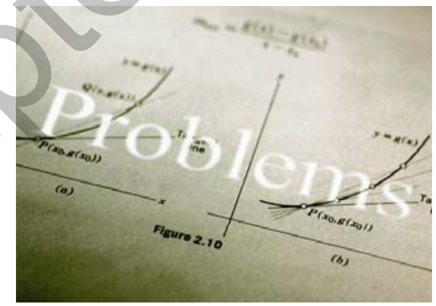
- Enable BPI+ and EAE
- Use BPI+ Enforce
- Disable Self-Signed Certificates
- Use “Secure Provisioning” by leveraging SAV
- Only allow CM software download via CVC
- Disable Public SNMP access
- Eliminate “Walled Garden” customer access points
  - ✓ Walled Garden sites are the primary gateway for theft-of-service
- Restrict access of your security department and policies to a limited, trusted number of people
  - ✓ Security breeches often come from within

ADVANCED TROUBLESHOOTING

Advanced Field Troubleshooting

- Why is DOCSIS 3 Troubleshooting Different?
  - ✓ Multiple Bonded Channels
    - Downstream
      - Not that different.
      - The channels are constant carrier
      - Multiple downstream channels have been around forever
    - Upstream
      - Still most vulnerable portion of plant
      - The modem is no longer limited to a single upstream transmit path
      - In some ways this is actually easier with DOCSIS 3.0

You Likely Know Your Problems



- Downstream – Typically not so bad
  - ✓ CTB, CSO, CNR under digital channels
  - ✓ Levels not correct into home (high, low, tilt)
  - ✓ Suck-outs, especially if you have contractors doing disconnects
  - ✓ Cheap modulators & upconverters never save you money
  - ✓ DOCSIS 3.0 headaches - Channel bonding, isolation, legacy

- Upstream – Your Achilles heal
  - ✓ Easy: AWGN noise, impulse noise, coherent noise, CPD, Laser clipping
  - ✓ Hard: Group delay, frequency response, micro-reflections
  - ✓ Insane: DOCSIS 3.0 – multiple upstreams – power levels

- Theft of Service

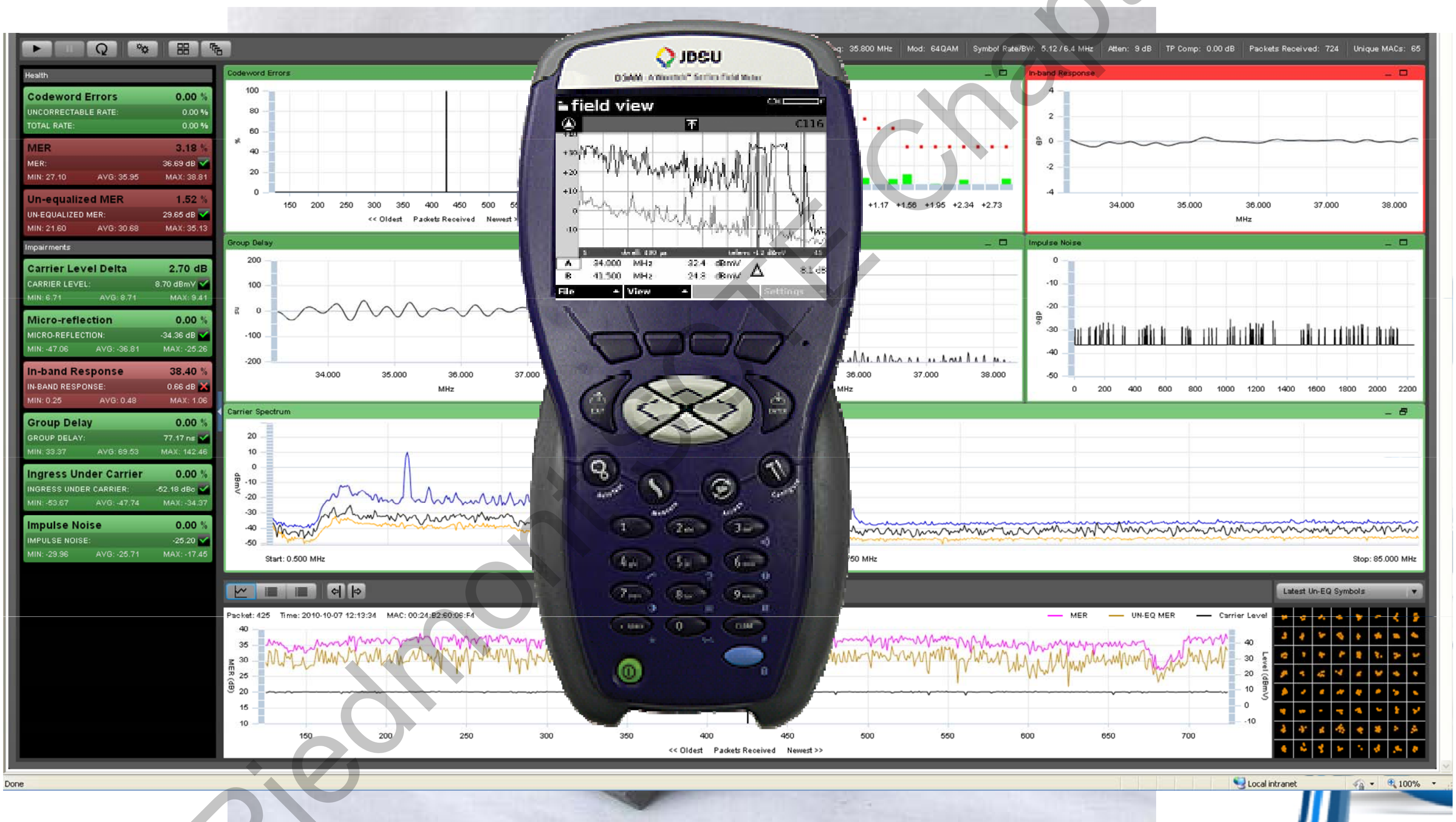
Likely Downstream Problems

- ✓ CM must lock to 4 to 8 DS channels meeting power and MER requirements of D2.0
- ✓ For M-CMTS, DTI timer must be operable
- ✓ CMTS local DS and/or eQAM DS are points of failure
- ✓ All DSs must be within 60 MHz contiguous BW
- ✓ eQAM channels must be within 24 MHz BW
- ✓ GigE interface between CMTS and eQAM is point of failure
- ✓ eQAM output is lower than conventional QAM output - headend combining may need to be changed

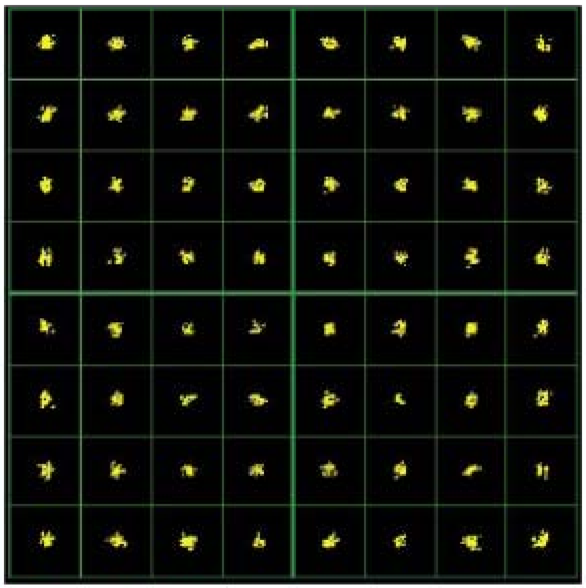
Likely Upstream Problems

- ✓ Four times the US bandwidth (four bonded channels) creates a new dynamic for troubleshooting and monitoring:
- ✓ 6.4 MHz * 4 = 25.6 MHz (without guard bands)
- ✓ Increased likelihood for laser clipping
- ✓ Increased probability for problems with ingress, group delay, micro-reflections, and other linear distortions
- ✓ Inability to avoid problem frequencies such as Citizens’ Band, Ham, Shortwave, and hop between CPD 6MHz spacing
- ✓ Where are you going to put your sweep points?

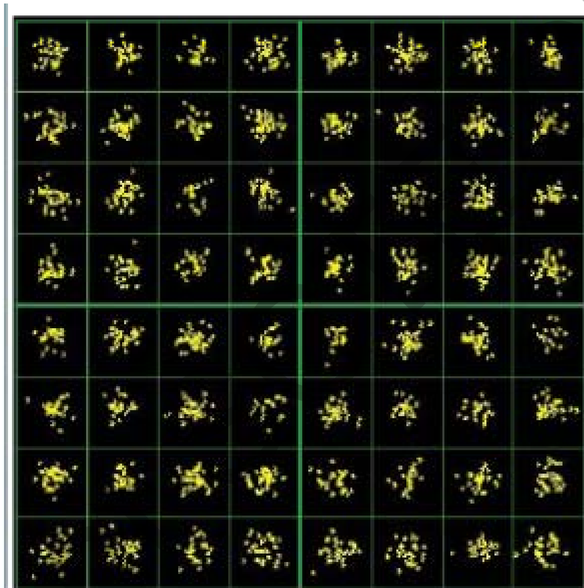
Test Equipment has Advanced!



Downstream Impairments



Good MER

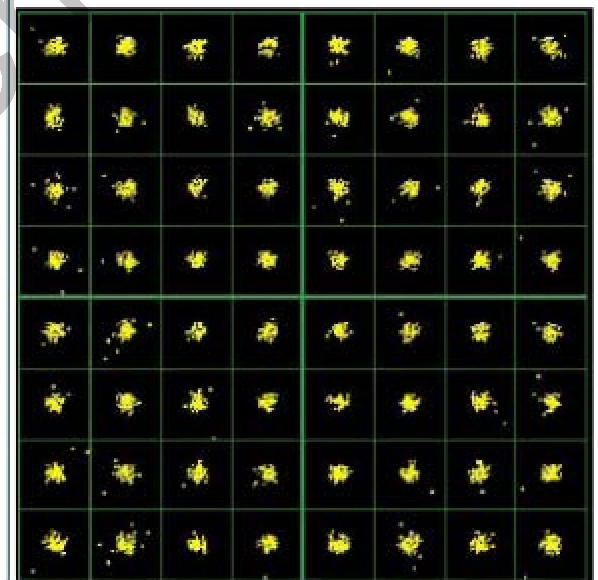


Noise

Gaussian noise impairments. Clusters poorly defined and spread out.

Possible Causes:

Low RF levels, low inputs to RF amplifiers



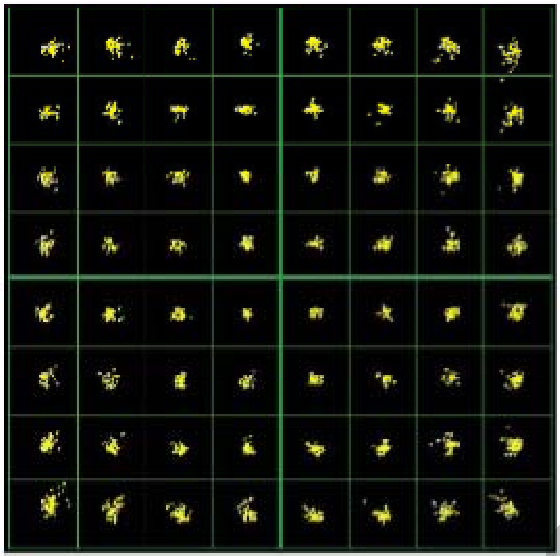
Intermittent Interference

On/Off interference below the desired QAM signal. Isolated dots appear away from the main cluster.

Possible Causes:

Laser clipping, intermittent ingress (2-way radios & paging systems)

Downstream Impairments

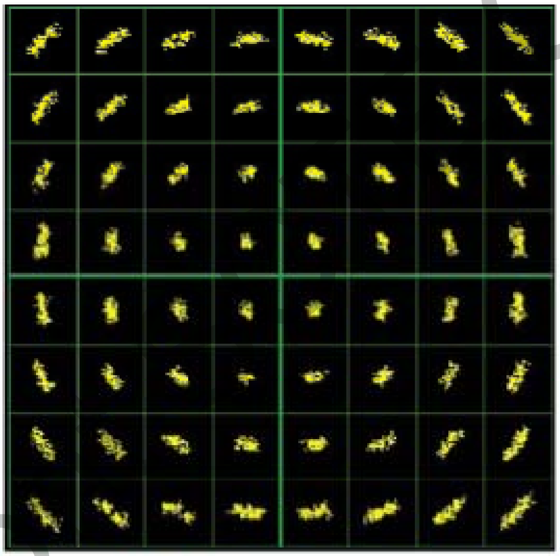


Compression

Non-linear distortion. Clusters are "pulled in" at the corners.

Possible Causes:

Overdriven or bad RF/IF amps, IF/RF filters, up/down converters, IF equalizers, bad clock recovery circuits

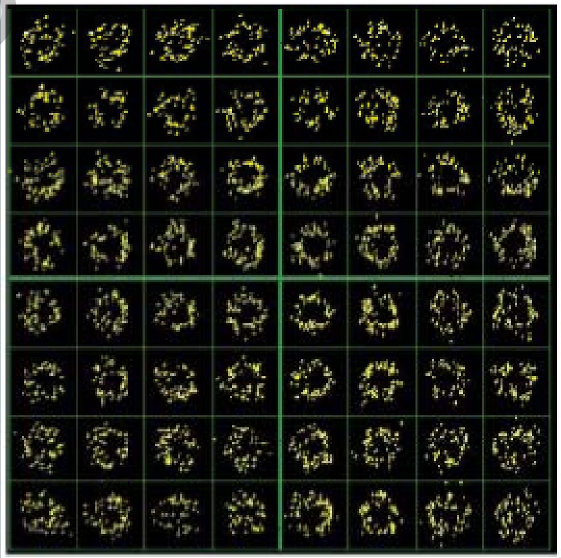


Phase Noise

Phase shift of I & Q data. The clusters appear to rotate around the center of the constellation.

Possible Causes:

Headend IF amplifiers and Up/Down converters



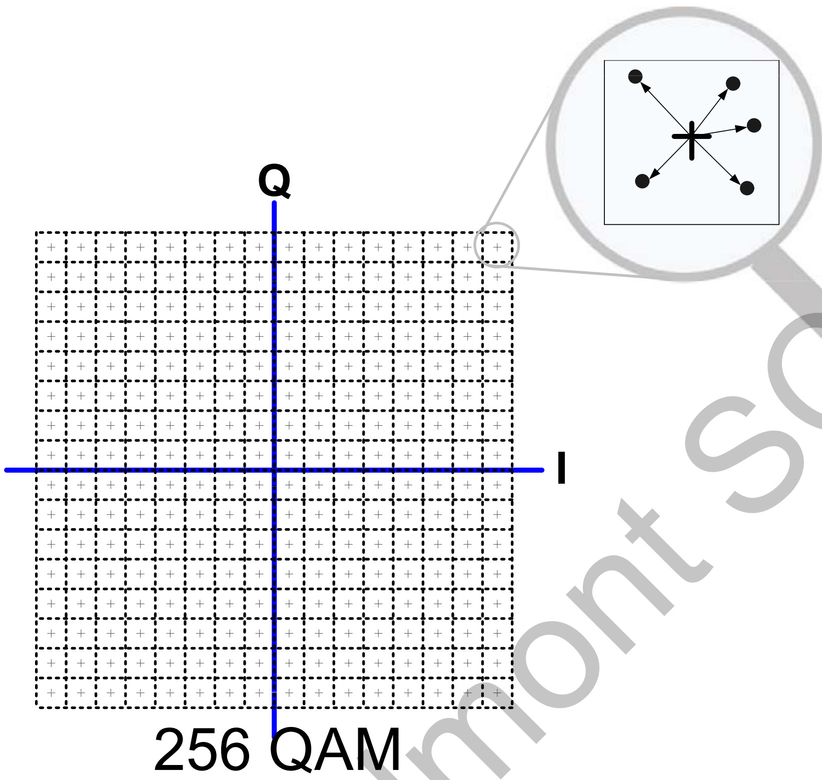
Coherent Disturbance

Interference from a signal under the desired QAM signal. Clusters appear doughnut shaped.

Possible Causes:

Ingress, CW Interference

Modulation Error Ratio (MER)



$$MER_{symb}(dB) = 10 \bullet \log_{10}\left\{\frac{E_{av}}{\frac{1}{N}\sum_{j=1}^{N}\left|e_j\right|^2}\right\}$$

- The quality of a QAM signal can be defined by the dispersion of the constellation's points considering the target value
- The error or dispersion power is calculated by the value mean square of the error vectors (real value VS target value)

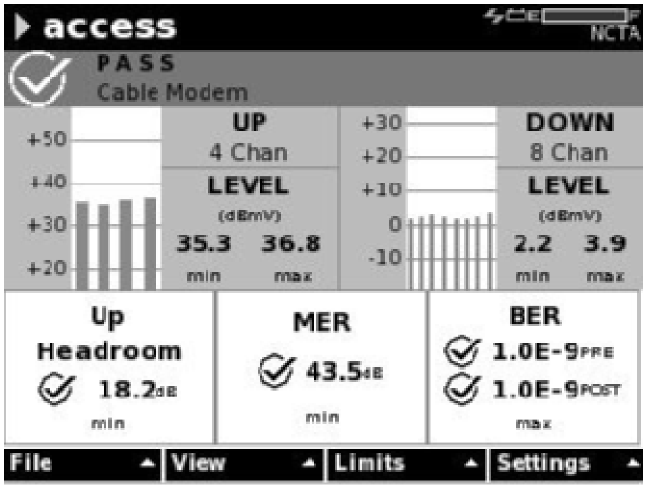
- MER is the ratio in dB between the average power of the signal and the power of the error vectors

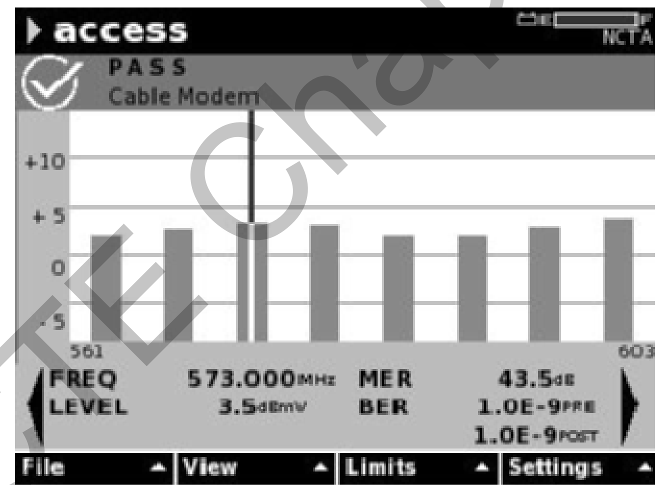
40

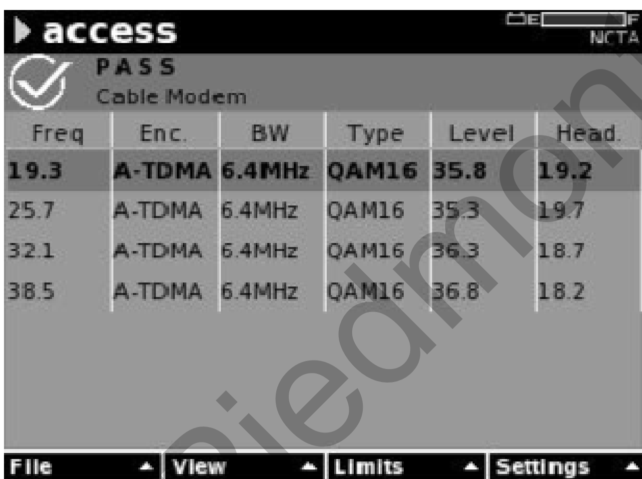
MER

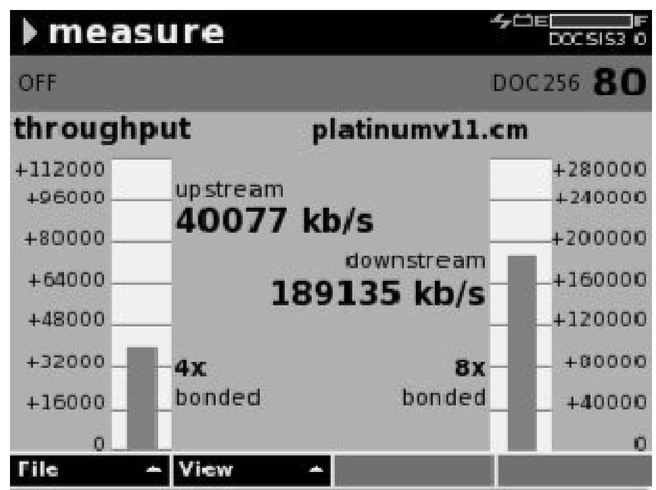
BER	64-QAM MER	256-QAM MER	Quality
10^{-10}	>35	>35	Excellent
10^{-8}	27-34	31-34	Good
10^{-6}	23-26	28-30	Marginal
10^{-5}	<23	<28	Fail

Testing DOCSIS 3.0 with a D3.0 Meter

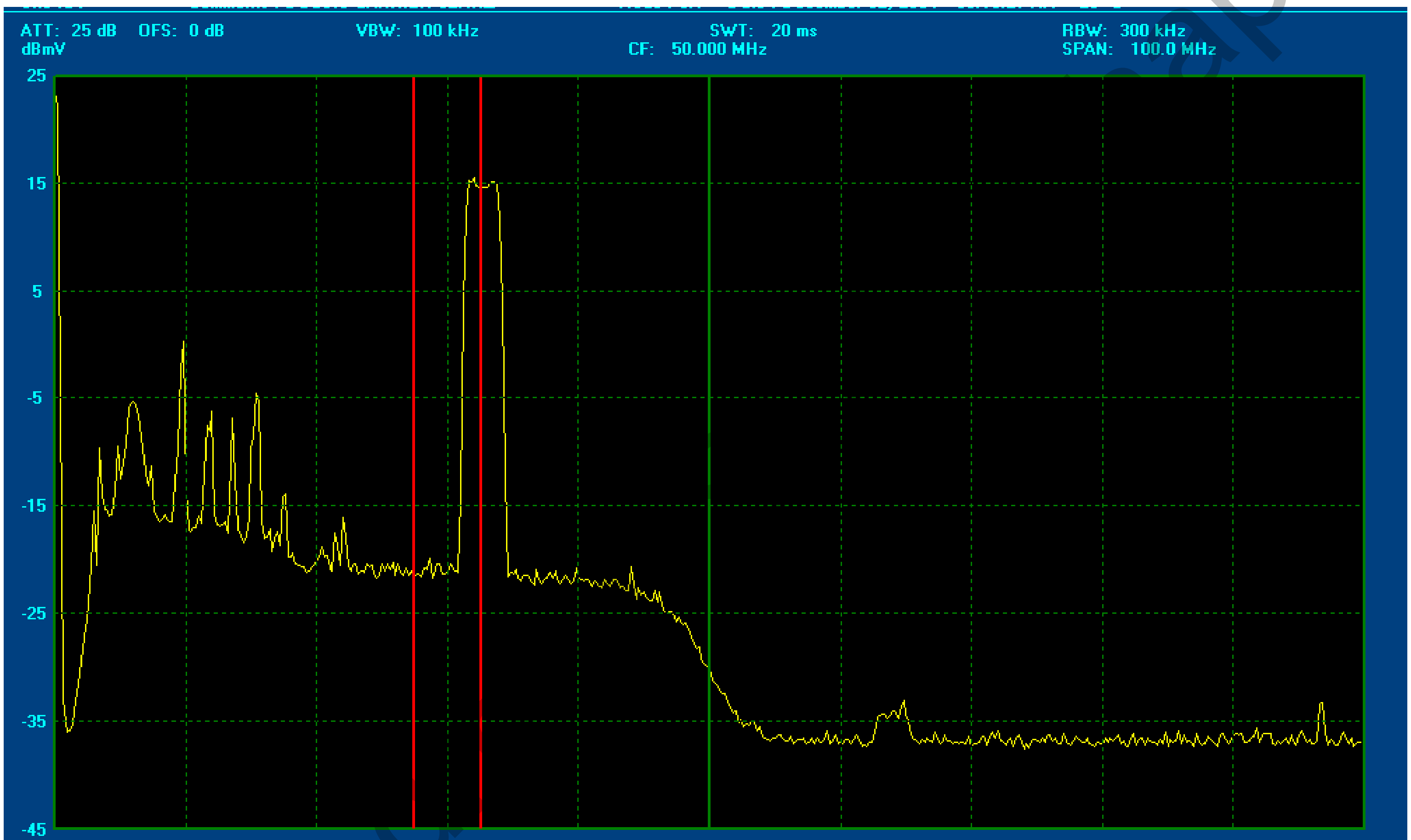








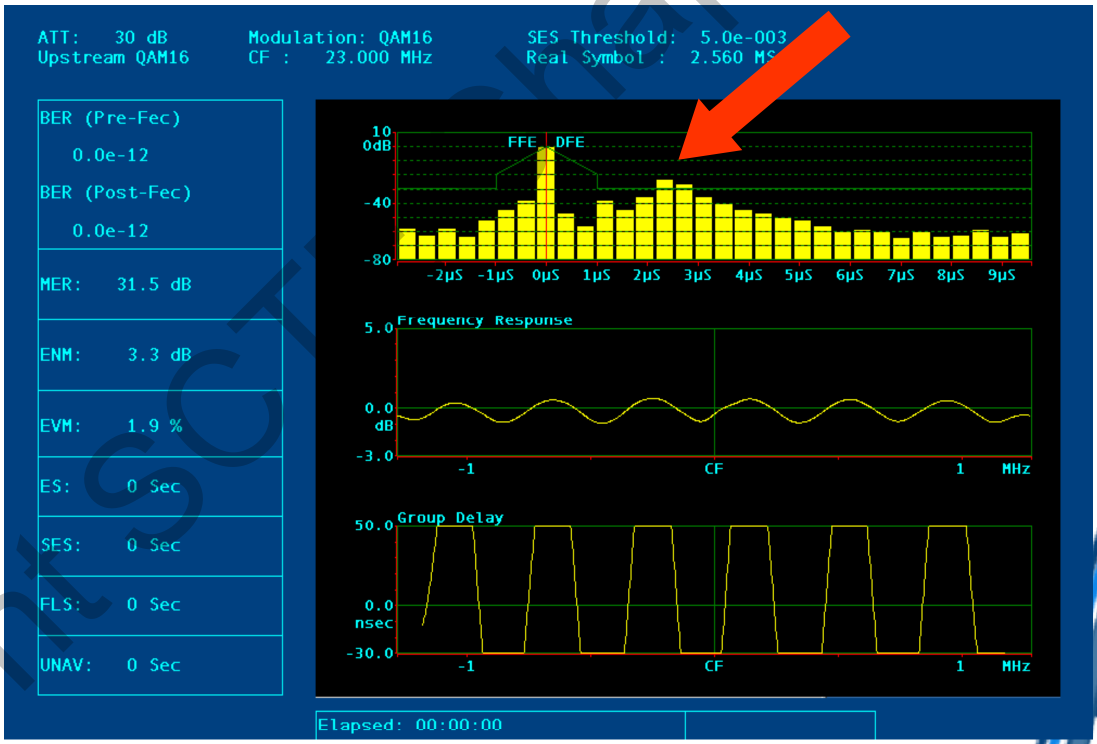
A Clean Upstream: Or Is It?



Graphic courtesy of Sunrise Telecom

Wouldn't Even Work for 16-QAM, Here's Why!

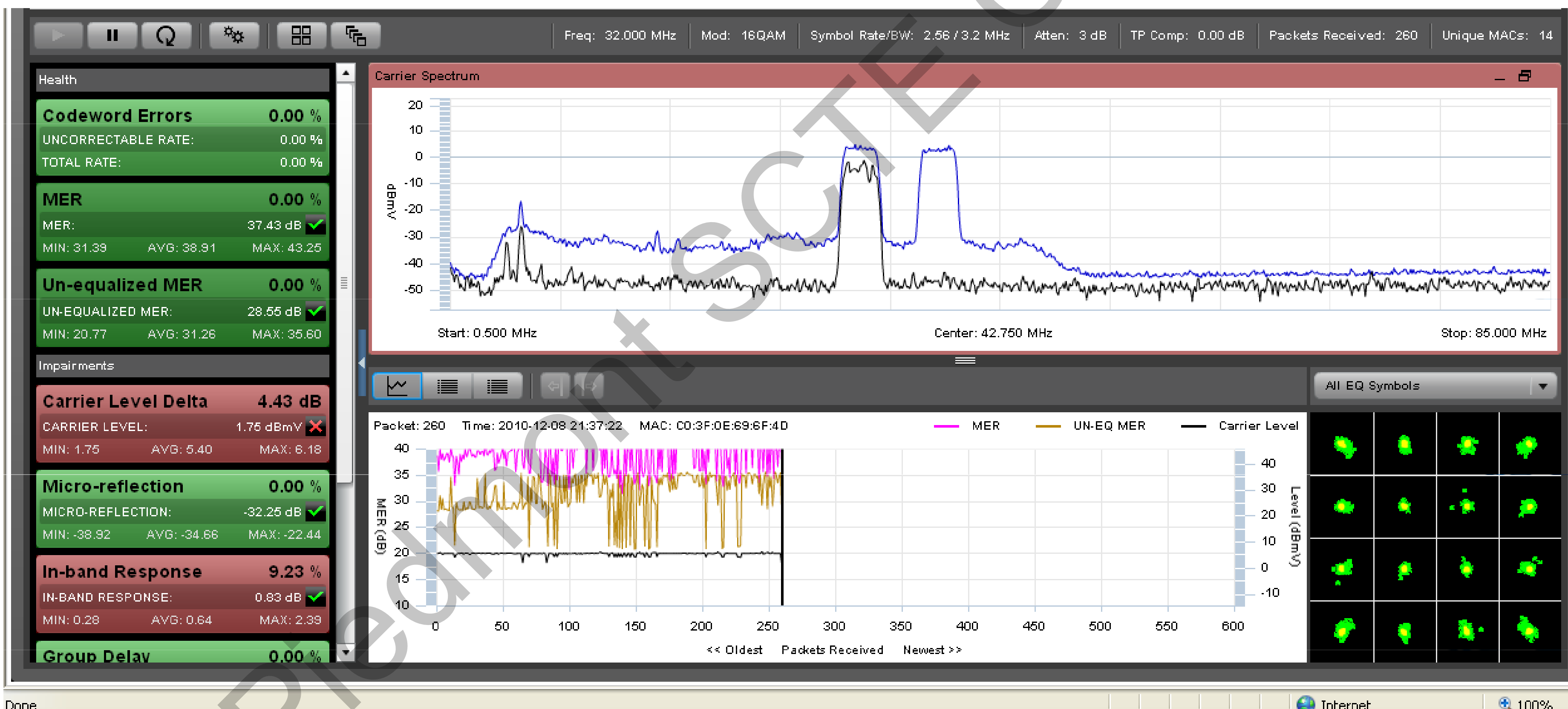
- Note ~ -22 dBc echo at 2.5 µsec (arrow)
- Echo does not meet DOCSIS US -30 dBc at >1.0 µsec parameter
- In-channel amplitude ripple is 1.6 dB, and group delay ripple is about 270 ns peak-to-peak



Graphic courtesy of Sunrise Telecom

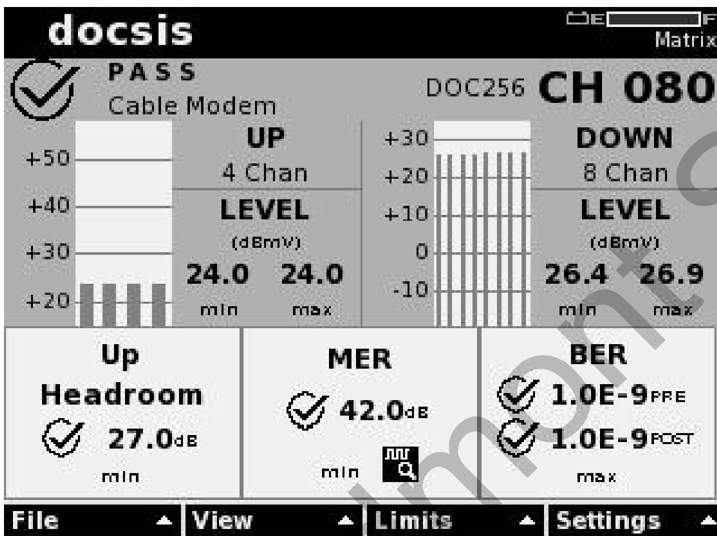
What are we looking for?

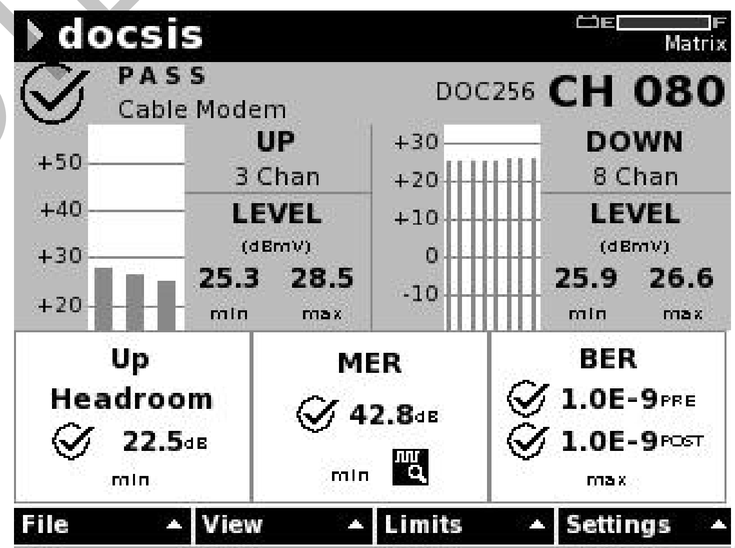
- Got DOCSIS 3.0 on your mind…
  - ✓ Plan on laser clipping being a popular word



Partial Service Troubleshooting

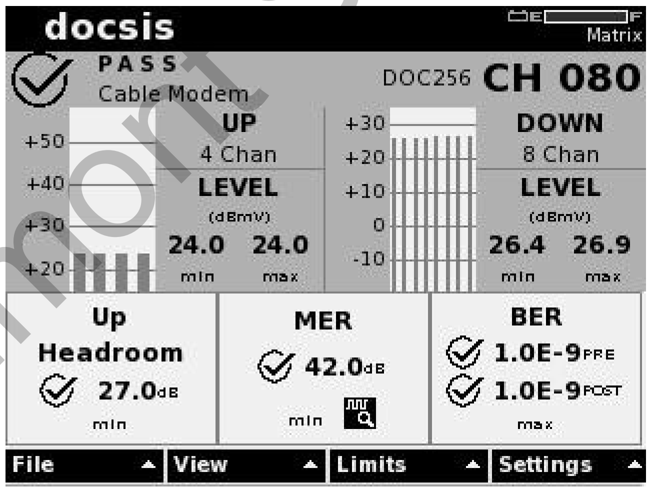
- Partial Service exhibits itself as missing channels
- Does not exhibit as Packetloss or Throughput issue



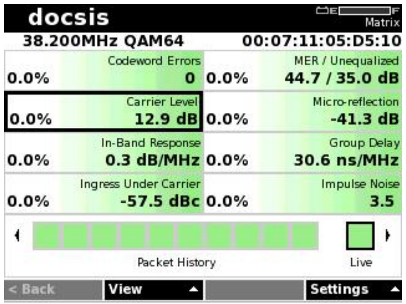


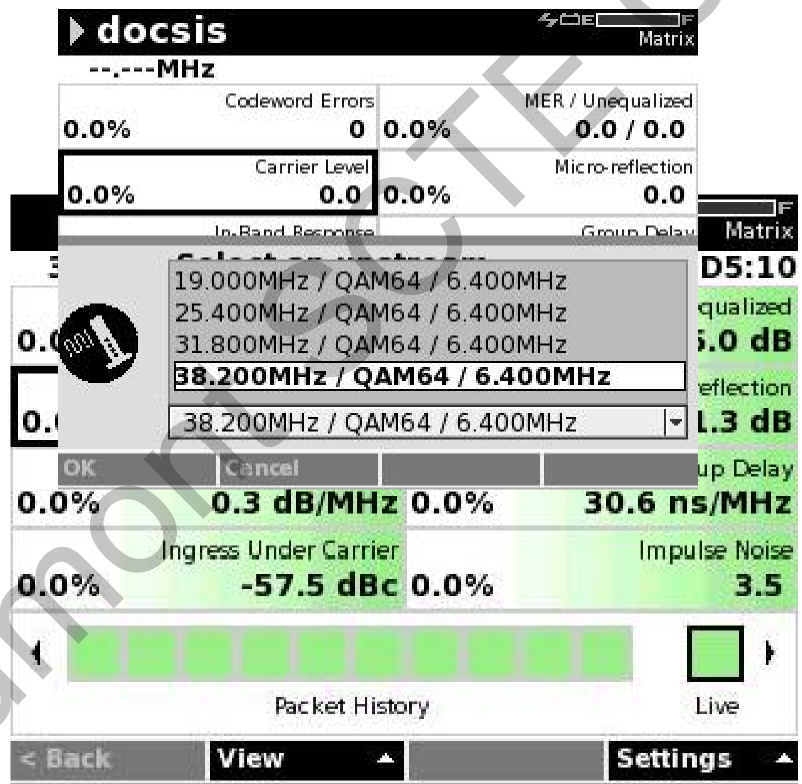
Impaired Service Troubleshooting

- ✓ An impaired service may or may not exhibit codeword errors and packetloss
- ✓ When troubleshooting impaired service, it is critical to view the performance of the individual upstream channels.

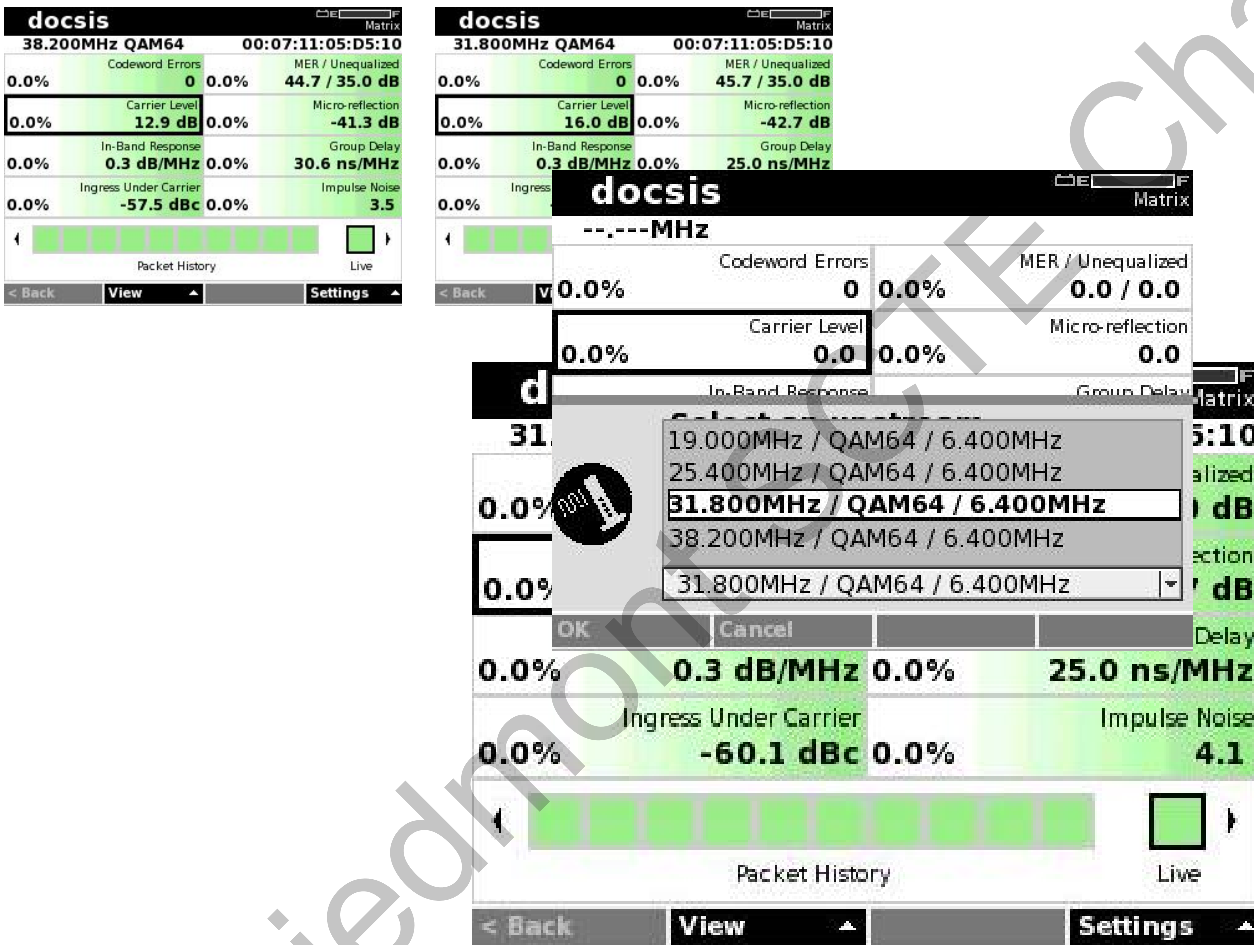


Impaired Service Troubleshooting

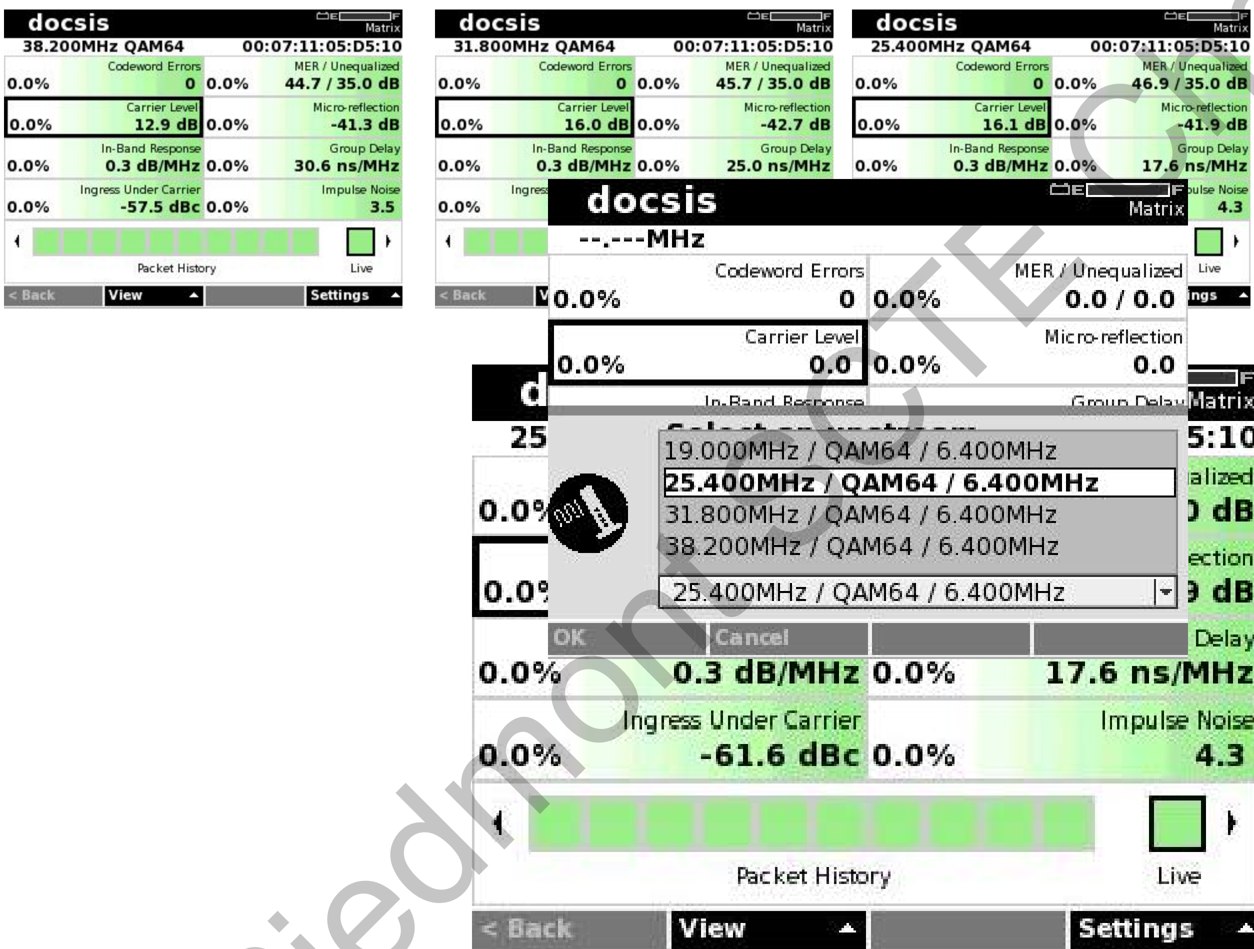




Impaired Service Troubleshooting

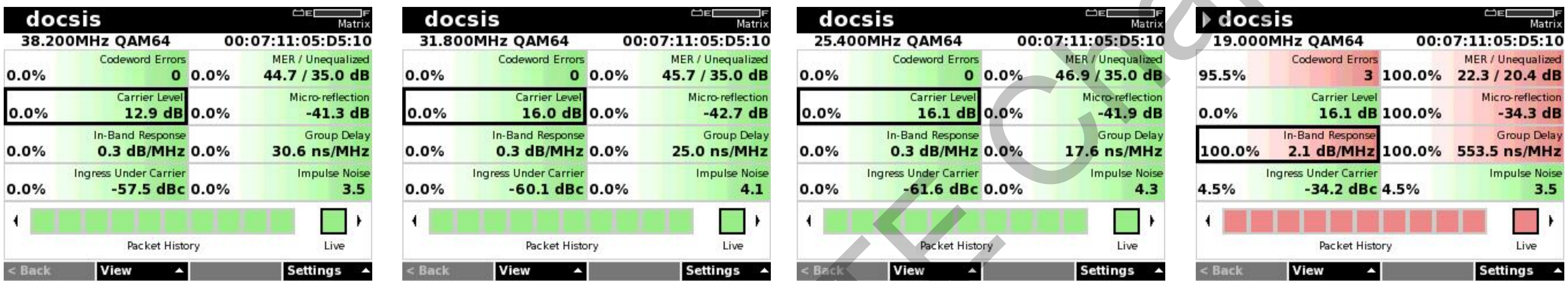


Impaired Service Troubleshooting



Impaired Service Troubleshooting

Impaired Service Troubleshooting



- Obviously there is an issue with the channel at 19 MHz

- Utilize this method to traverse the network and find the impairment causing this issue

Summary

- CMTS and SNMP data provide good troubleshooting
  - ✓ But not all of it
- DOCSIS 3.0
  - ✓ Significantly more throughput
  - ✓ Supports legacy D2.0 modems
  - ✓ D3.0 modems load balance in the upstream w/o loss of service
- Advanced test equipment is an investment that
  - ✓ Saves you time and money
  - ✓ Gets your subscribers back online and keeps them there
  - ✓ Makes you a predictable and reliable service provider
  - ✓ Seamlessly integrates headend & field – 2 places / 1 person

For more information go to:

http://bradyvolpe.com

http://volpefirm.com