OAM in Frames

Denton Gentry
Dominet Systems

Overview of Presentation

1. Summary of proposal

2. Security and Authentication

3. SNMP

Summary of proposal

- Functionality in MAC Control layer
- OAM in Frames
  - Send statistics from clause 30
  - Link monitor sends one frame per second
  - Failure events also send stats
- Independent of PHY
  - Works with existing PHYs
  - No additional burden for future PHYs
- Base on Slow Protocol (Annex 43B)
  - Limit number of frames/sec (5 now, can increase if needed)
  - 802.1D compliant bridges do not propagate

Summary of proposal

- Simple encapsulation
  - 1 byte code

00	TEST Request
01	TEST Response
02	Link Monitor
03	etc…

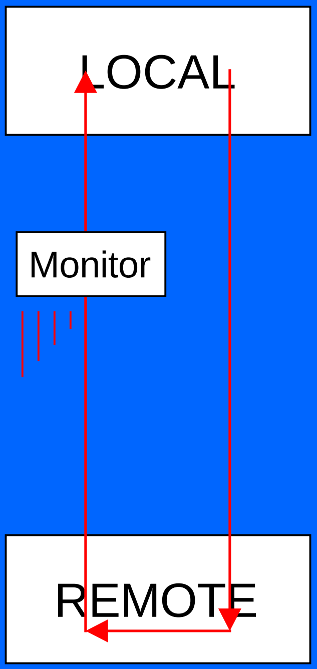
DA	SA	Slow_Protocol	subtype	code	data	FCS
6	6	2	1	1		4

Summary of proposal: Link Monitoring

- Send stats from Clause 30
  - Encoded as type,length,value
  - Type from Annex 30 arcs **<statType, statLen, statValue>**
    - Start with tuple after csmacdmgmt.
  - Define vendor extension mechanism
    - If we don’t, they’ll each choose a different mechanism
    - Distinguish via OUI?
  - Doesn’t extend to arbitrary MIB variables
    - SNMP MIBs depend on SNMP semantics
- Periodic announcement is the key mechanism
  - Could also allow queries for additional information

Summary of proposal: SNMP

- OAM intended as supplement to SNMP
  - Store stats from remote end
  - SNMP can query them later after failure
- Received stats stored in oRemoteEntity
  - New object class in Clause 30
  - Prepend source MAC address
    - Needed for shared networks



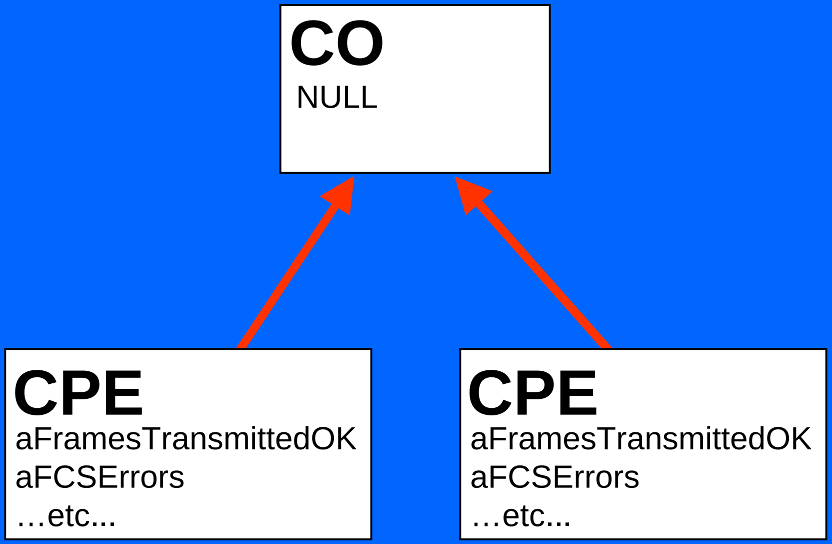
MACaddr1: <stat1><stat2><stat3>
MACaddr2: <stat1><stat2>
MACaddr3: <stat1><stat2><stat3>

Summary of proposal: No Master/Slave

- No inherent Master/Slave relationship
  - Link Monitor stats defined by a variable
    - Configure OLT not to send stats to CPE
  - Do not embed master/slave relationship into 802.3 spec
    - 802.3 covers more than one market space

aFramesXmittedOK

aFCSErrors



CO
NULL

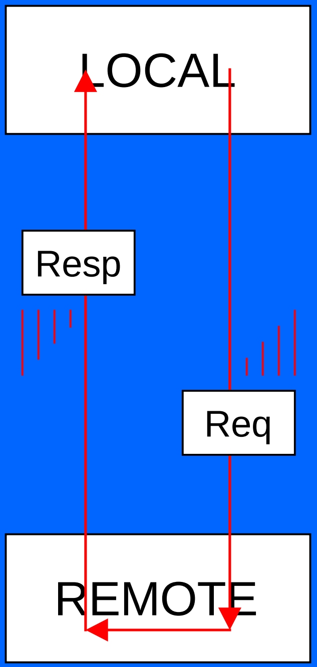
CPE
aFramesTransmittedOK
aFCSErrors
…etc...

CPE
aFramesTransmittedOK
aFCSErrors
…etc...

Summary of proposal: Remote Loopback

Remote Loopback using TEST frames

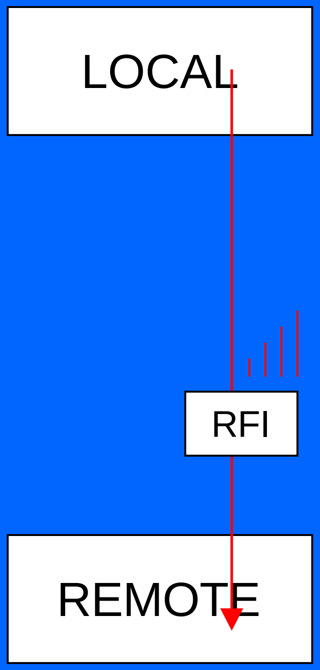
  - Send request, get response
  - Non modal (mix TEST with regular traffic)



- Intended for connectivity test
  - Limited number of packets/sec.
- Not intended as throughput test
  - Best done at L3, where the services run
- Not intended as BERT test
  - Symbol & FEC error count is measure of link quality
  - High bit rate TEST = more expensive implementation

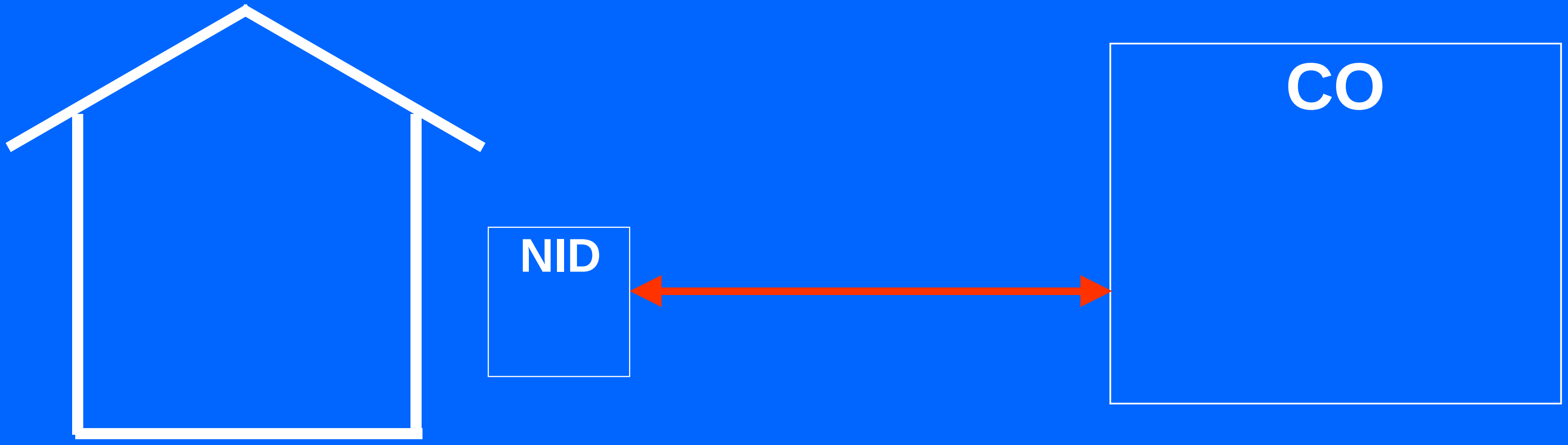
Summary of proposal: Remote Fault

- Most PHYs provide binary RFI indication
  - This is good.
- Access market may require more
  - Troubleshooting performed at CO
  - Subscriber has little expertise
  - Truck roll to subscriber is expensive
- If required, use OAM facility for this
  - Send OAM packets with information about fault
  - Alternative is complex error handling in PHY



Summary of proposal: Deployment model

- Demarc should be a bridge or L3 device
  - Has to transfer between dissimilar speed links
  - EFM <-> 10/100/1000 or 802.11, for example
- Can also work if demarc is within customer kit
  - Security dependant on implementation of device



Summary of proposal: What it isn’t

Note a few things not supported:

- No SETs
  - OAM does not modify configuration of remote
  - Ethernet links configure themselves locally
- Not a full-fledged management facility
  - OAM strives only to maintain link integrity
    - Even with an “unmanaged” device at one end
  - Managed devices must include a management protocol
- Not routable
  - Messages transit only a single link
    - Possible to design a forwarding proxy; out of 802.3 scope
  - Not intended to manage entire infrastructure

Overview of Presentation

2. Security and Authentication

Security & Authentication

- Security conscious environments
  - Require strong proof of identity
  - Do not allow unauthorized access
  - Do not reveal information to unauthorized parties
- OAM helps assure link functionality
  - If link no worky, authentication no worky
  - Need limited OAM before authentication
    - Allow full OAM functionality after authentication
  - No SETs
    - Security threat only of leaking information

Security & Authentication

- Mechanisms exist to authenticate a port
  - 802.1x
- Mechanisms exist to authenticate a node
  - DHCP w/ MD5 signature
- Mechanisms exist to authenticate users
  - PPPoE w/ RADIUS
  - login password (S/Key or otherwise)
- Mechanisms exist to authenticate mgmt packets
  - SNMPv3
  - IPsec w/ HMAC authentication
- The world does not need another mechanism
  - OAM should rely on existing facilities, not invent another one

Authentication proposal

- 802.3 should not define yet another mechanism
  - Include an attribute for authentication state
    - Enumerated Nonauthenticated, authenticated
  - Defaults to nonauthenticated
- Management agents can change state
  - … after 802.1x authentication
  - … after any user logs in via PPPoE
  - … via a secure protocol like SNMPv3
  - … etc
- 802.1x authentication would be straightforward
  - Out of 802.3 scope due to layering

Authentication proposal

- OAM Link Monitoring stats defined by attribute
- Include two attributes defining stats to send
  - Nonauthenticated and authenticated

Nonauthenticated	Authenticated
aFCSErrors	aFramesReceivedOK
	aFramesTransmittedOK
	aFCSErrors

- Allows minimal information before authentication
  - Maximal information after authentication

Authentication & Shared Networks

- What to do about shared networks
  - No way to know if every node on link has authenticated
    - Nodes are invisible until they transmit
  - Any node on the link could snoop OAM
- No simple solution to this problem
  - For example, 802.1x punts on shared networks
  - Would have to encrypt payloads, distribute keys
- Likely not an issue for PONs & access networks
  - Carrier will never send sensitive stats (authenticated or no)
  - Subscribers cannot see each others traffic
- Recommend no heroic measures be taken
  - Shared networks are what they are

Security Threats: DoS

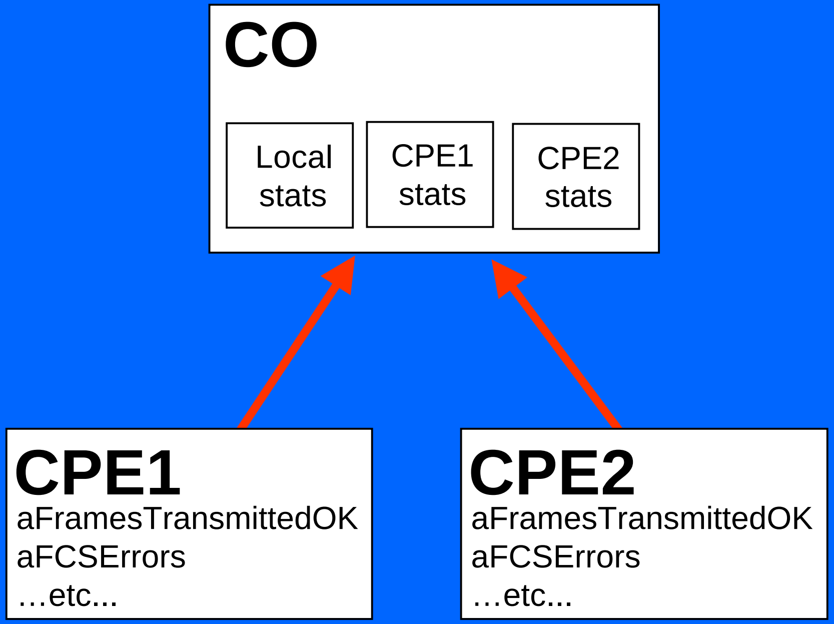
- Denial of Service: overwhelm far end with traffic
  - Attacker ignores the limit on packets/sec
  - Attacker is easy to find: OAM packets do not propagate
- OAM is stateless
  - Each packet processed independently
  - Packets can be dropped as necessary
  - Defense against DoS: drop excess packets
- Several implementation issues
  - don’t allow DoS on one MAC to affect other MACs

Overview of Presentation

3. SNMP

Supplementing SNMP

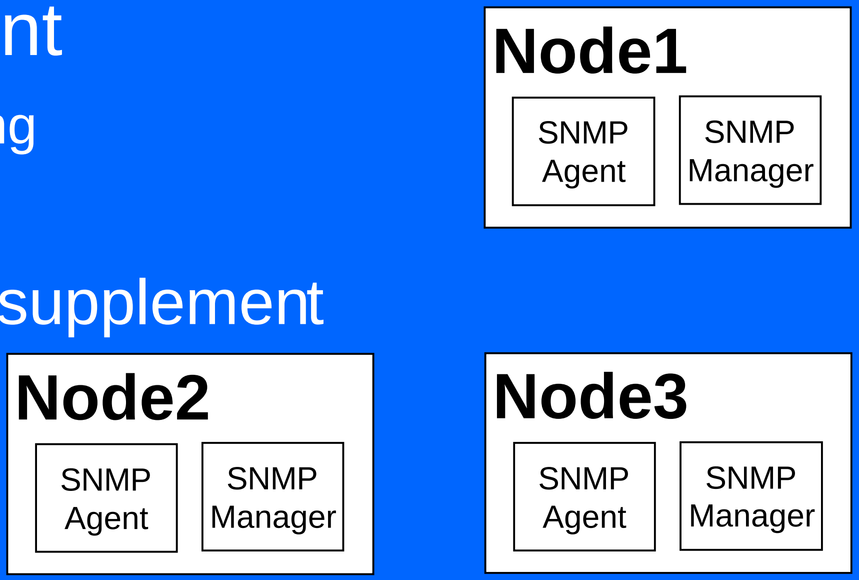
- OAM supplements SNMP
  - Upstream stores recent stats
  - Use SNMP to query stats from CO



- Question posed: why not just use SNMP?
  - CO would query stats from CPE1 and CPE2
  - Once per second

Why supplement SNMP

- Issue 1: Requires SNMP managers
  - SNMP agents answer queries, manager launch them
  - Managers not current practice in network gear
- Issue 2: SNMP is unicast
  - Must discover what nodes are out there
  - Unicasts will propagate through bridges
- Issue 3: SNMP is a MAC Client
  - Prioritization and Head of Line blocking
  - Cannot use for failure diagnosis
- Conclusion: OAM provides useful supplement



Summary

- Summarized proposal
  - OAM in MAC Control

- Security and authentication hook
  - Allow different behavior before and after authentication
  - Do not invent yet another authentication mechanism

- Supplementing SNMP