Architectural Framework for Self-Managed Networks with Fault Management Hierarchy

Mehmet Toy, Ph.D
Mehmet_Toy@cable.comcast.com

COMCAST

July, 2015

Outline

- Problem Statement and Proposed Concepts
- Self-Managing NE Architecture
- Self-Managing NMS Architecture
- Self-Managing Agent Architecture
- In-band Communications
- Fault Management Hierarchy in Centralized and Distributed Networks

Problem Statement

A. So far, the industry has been focused on
   - Monitoring of network resources and services,
   - Isolating problems, and
   - Fixing them by sending technicians to the sites most of the time or
   - Downloading certain configuration files remotely for configuration related problems.

B. Networks need to identify problems by itself, fix them, and have technicians at the site of a failure only when there is a single point of hardware failure.

Proposed Framework and Architectures

A. **Architecture for Self-Managed NE (Network Element), consisting of intelligent components (i.e. intelligent NE (iNE) and one or more intelligent agents of each type)**
B. **Architecture for Self-Managing NMS (Network Management System), consisting of intelligent components**
C. **Architecture for intelligent Agents**
D. **A self-centralized and self-distributed management architecture with intelligent systems for a self-managed network**
E. **A concept of in-band communications of failure types associated with smallest replaceable components, ESTIMATED FIX time, and fixes for failures identified by sNE, sNMS/OSS, and field technician to all related parties (i.e. sNEs, sNMS/OSS, field technician and users)**
F. **A frame format for in-band communications of failures in Ethernet networks, failure types, estimated fix time and fixes**
G. **Hierarchy for fixing of failures in the centrally and distributedly self-managed networks**

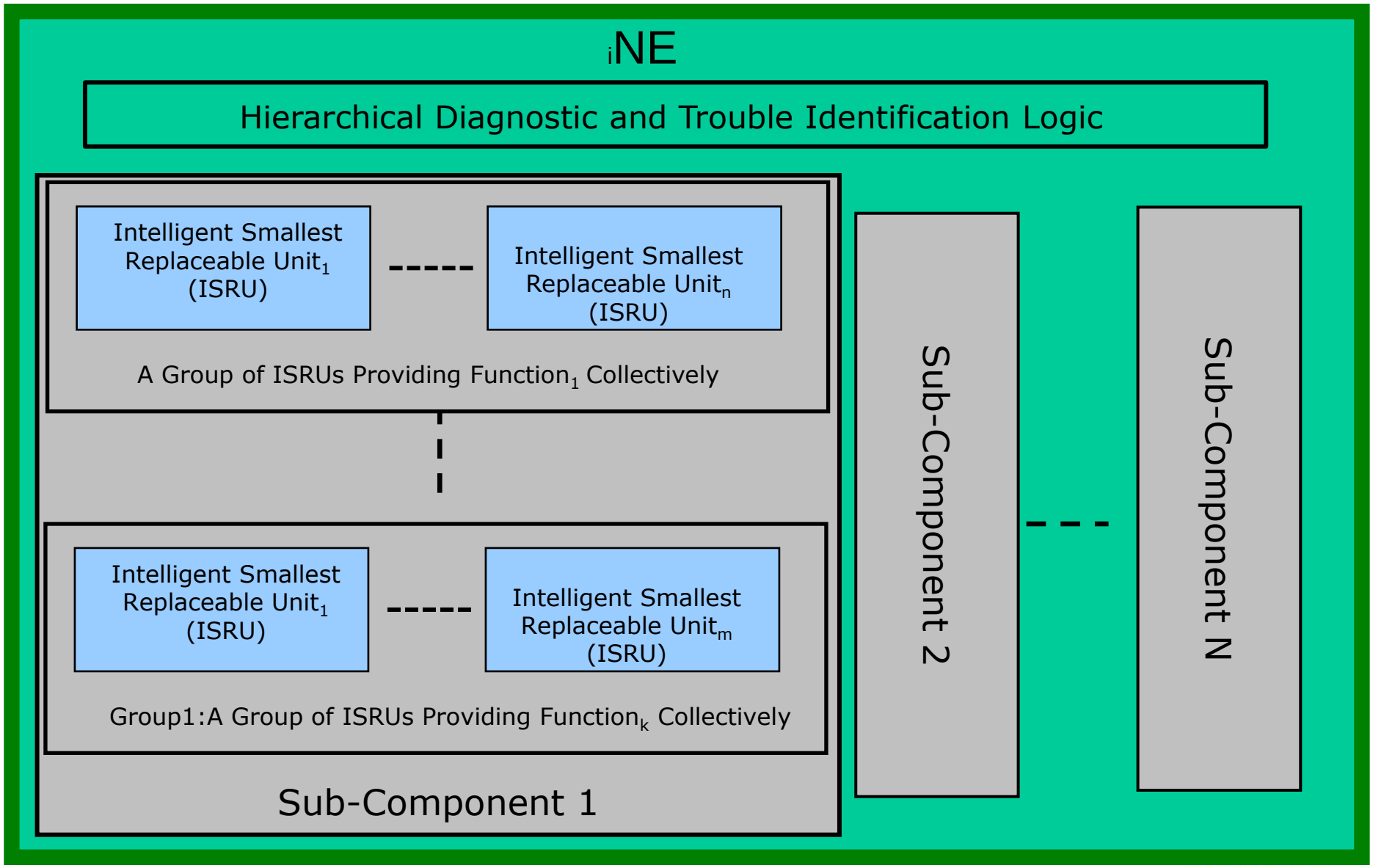
Intelligent NE (iNE)

A. Consists of intelligent sub-components that are
   - Capable of periodic self-checking,
   - Declaring a failure when it is unable to perform its functions,
   - Running diagnostics and identifying whether the faulty entity is within the subcomponent or not,
   - Escalating the diagnostics to the next level in the hierarchy within NE.

A. Able to run diagnostics for a pre-defined set of sub-components, that are collectively performing a function, and finally to run diagnostics at iNE level to determine the failure.

B. After the failure is identified to the smallest replaceable HW (e.g. chips, connectivity between chips, backplane, etc.) and/or SW entity (e.g. kernel, log, efd, etc.), iNE determines if the failure is fixable by the iNE and communicates that to related parties.

Intelligent NE (iNE)



Self Managing Agents for sNEs

A. Each sNE will have one or more Intelligent Hardware Maintenance Agent(s) (iHMA(s)) depending on the implementation
   - To monitor hardware entities such as CPU, memory, physical ports, communication channels, buffers, backplane, power supplies, etc., and take appropriate maintenance actions during hardware failures

B. Each sNE will have one or more Intelligent Operating System Maintenance Agent (s) (iOMA (s))
   - To monitor operating system and take appropriate maintenance actions during Operating System failures

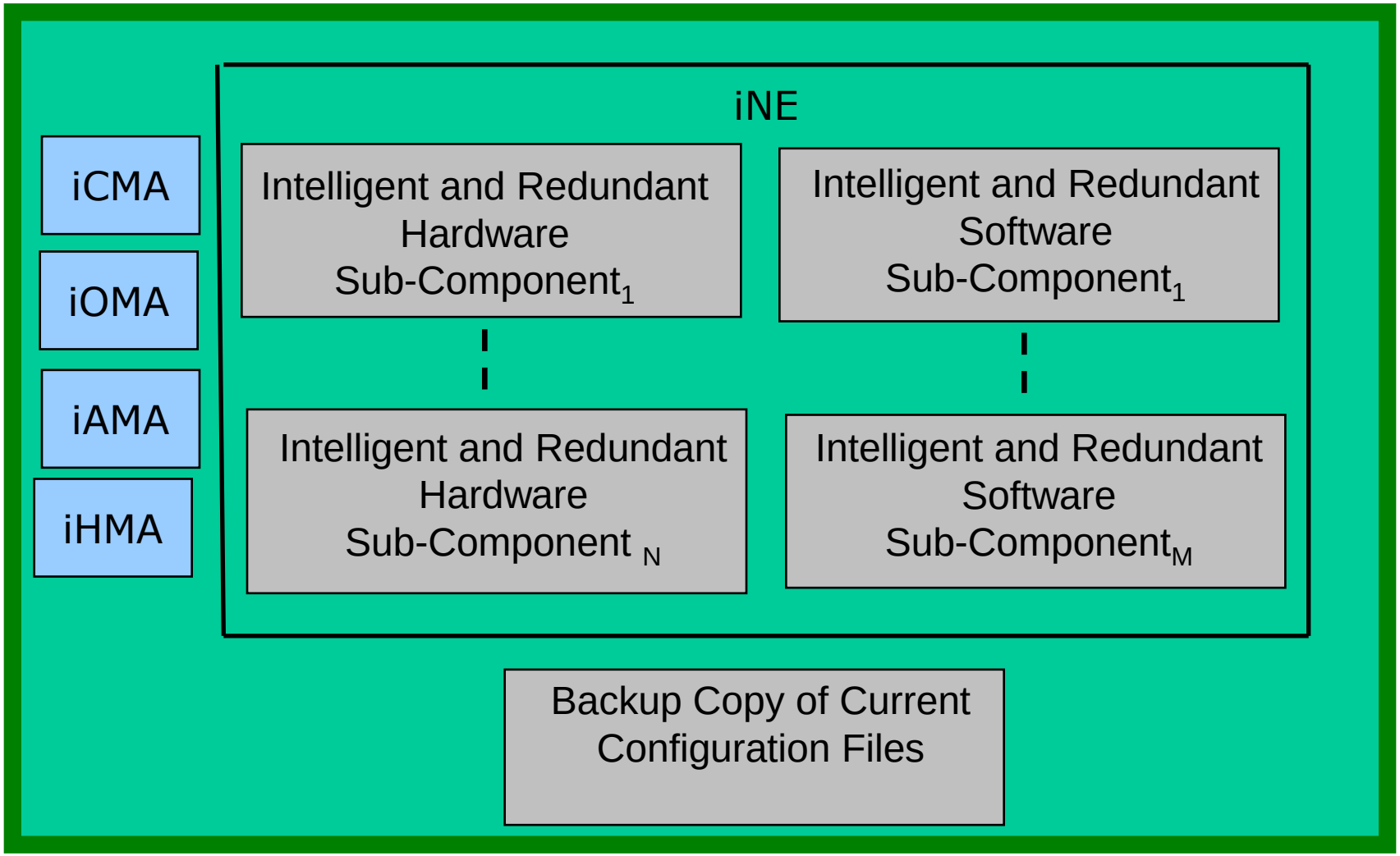
C. Each sNE will have one or more Intelligent Application Maintenance Agent (s) (iAMA (s))
   - To monitor application software and protocol software, and take appropriate maintenance actions during application and protocol software failures

D. Each sNE will have one Intelligent Capacity Management Agent (s) (iCMA (s))
   - To monitor capacity, system load and system performance, collect measurements and take appropriate actions

Self Managing Agent Responsibilities

A. Monitor the entity that it belongs to, report a failure to all related parties (i.e. sNEs, sNMS, field technicians, etc), fix the problem, and report the fix to all related parties.
B. If the problem is determined to be not fixable after one, two, or three tries, send a message to sNMS asking for help at the site or remote fix.

Architecture for Self-Managed NE



Intelligent NMS/OSS (iNMS/iOSS)

A. Periodic self checking
B. Backed-up with an active iNMS/iOSS when it fails
C. Stores software modules specific to iNEs
A. Able to verify if iNE failure is not local when iNE reports that the failure is not local
B. Able to periodically monitor network, identify network level failures

Intelligent NMS

GUI

Hierarchical Network Level Diagnostic and Trouble Identification Logic

Copies of iNE Type 1 Software: Operating System, Applications, etc.

Copies of iNE Type N Software: Operating System, Applications, etc.

Periodic Network Level Monitoring, Network Level Trouble Isolation and Fixing Network Level troubles

Traffic Management Algorithms and Policies: Connection Admission Control, Load Balancing, Congestion Control

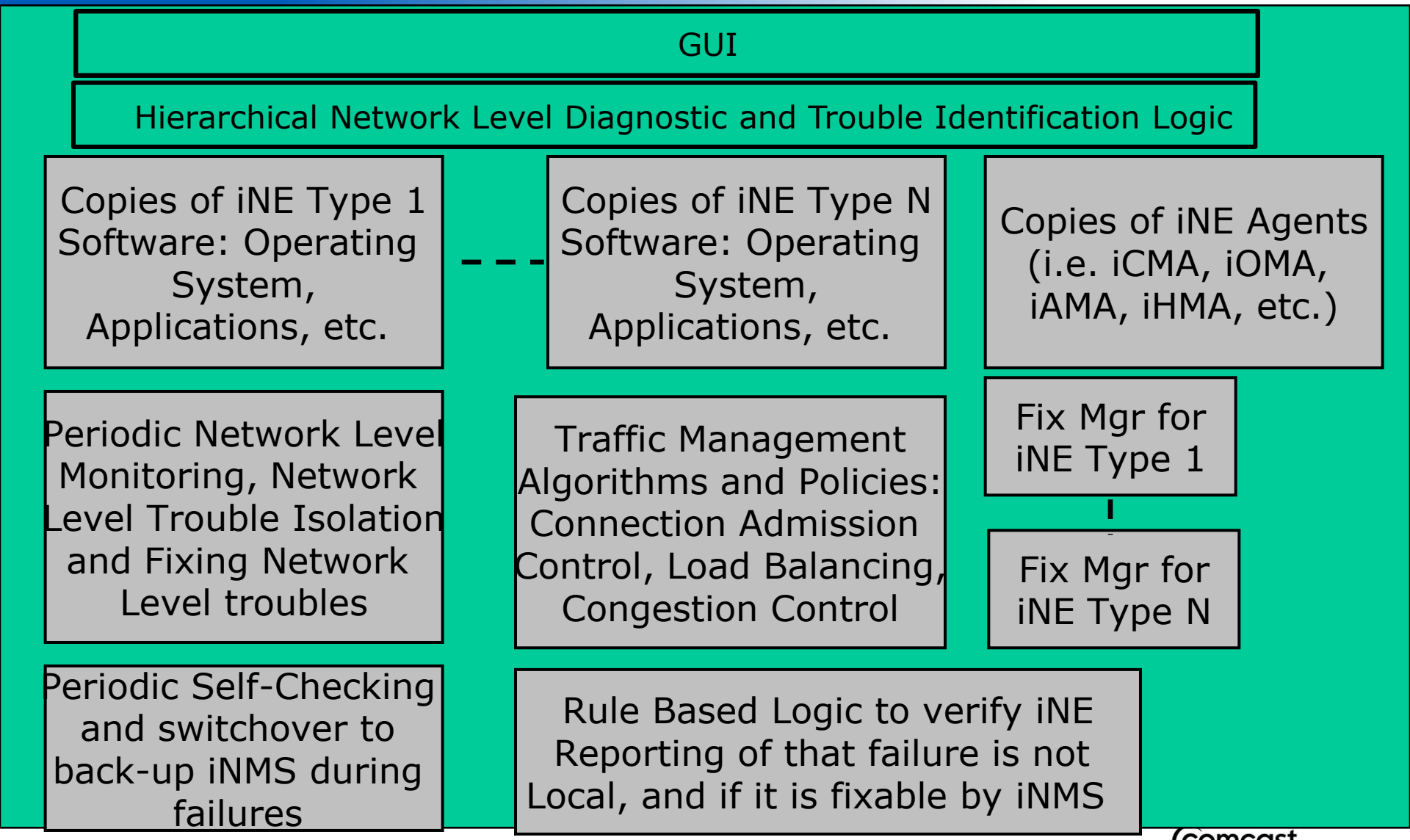
Periodic Self-Checking and switchover to back-up iNMS during failures

Rule Based Logic to verify iNE Reporting of that failure is not Local, and if it is fixable by iNMS

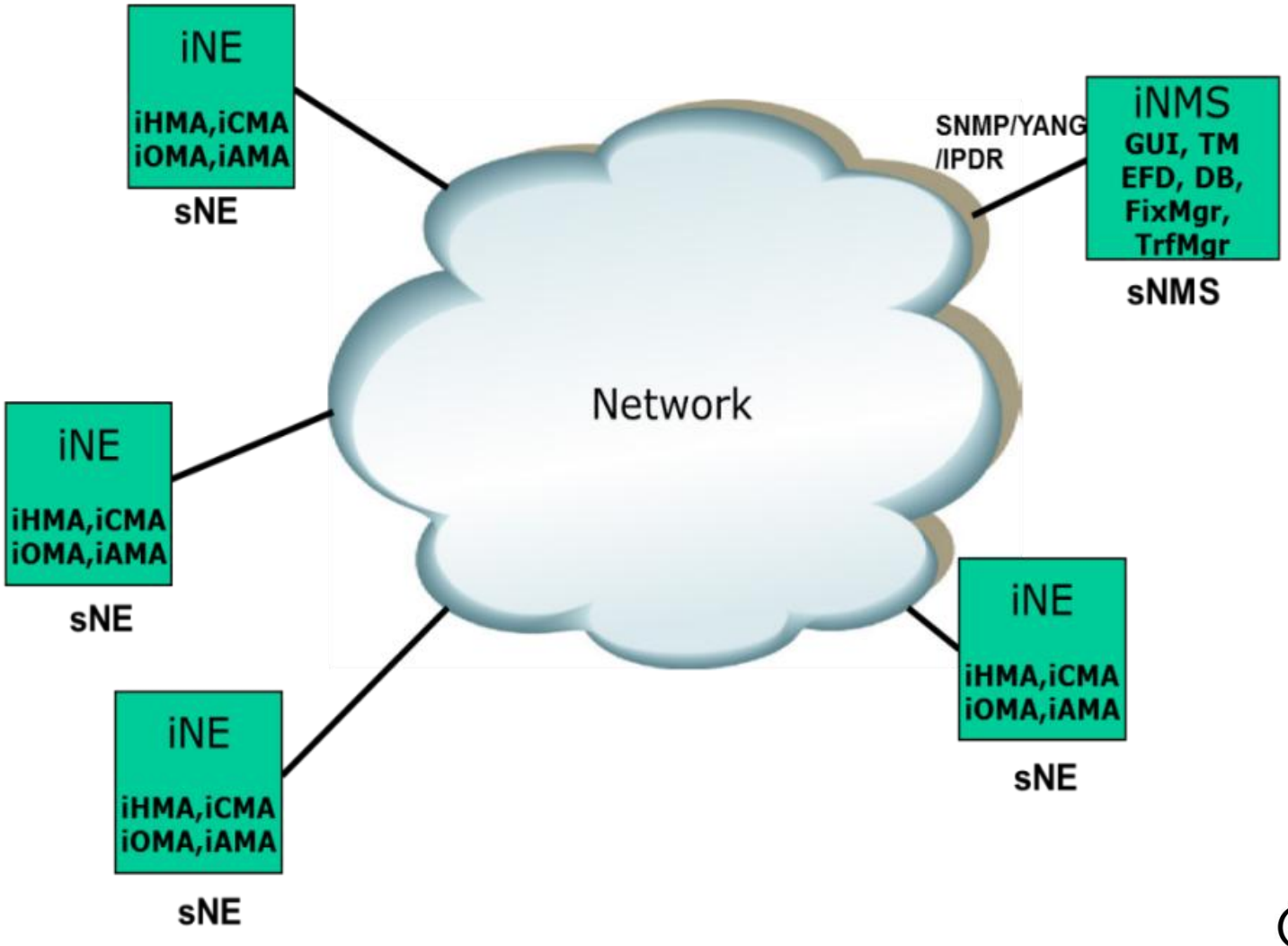
Self-Managing NMS/OSS Functions

A. Collect end-to-end connection level measurements and NE level capacity measurements and store them
B. Initiate and perform remote fixes at sNE (not fixes that can be executed locally)
C. Fix network level issues beyond the capabilities of sNEs
D. Perform Connection Admission Control (CAC), load balancing, and congestion control at network level
E. Prioritize and schedule execution of the tasks to perform repair and configuration activities that can be performed only remotely
F. Estimate the fix time for a failure that is going to repair and communicate that to related parties
G. Send info to remote clients about failures and fixes

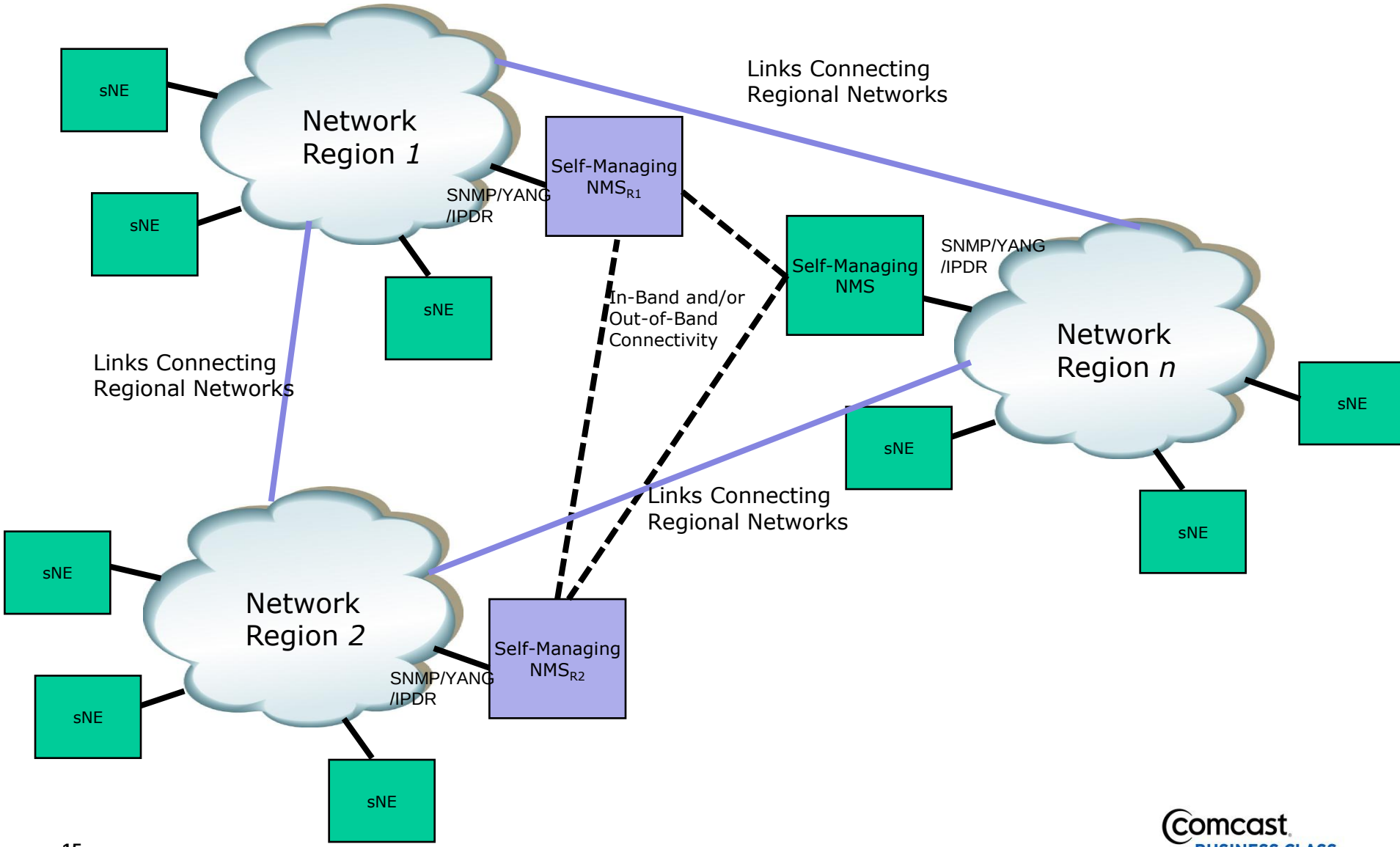
Self-Managing NMS



Self and Centrally Managed Network Architecture



Distributed Self-Managed Network Architecture



comcast BUSINESS CLASS

Distributed Self Managed Network Architecture

A. In distributed architecture, the network is divided into sub-networks (I.e. regional networks), where each sub-net has its own Self-Managing NMS_R
B. Self-Managing NMS_R provides all the centralized management functions for its own subnet and informs Self-Managing NMS about its activities.
C. End-to-end network level activities beyond region boundaries will be left to sNMS. These activities can be Connection Admission Control (CAC), load balancing, and congestion control at network level.

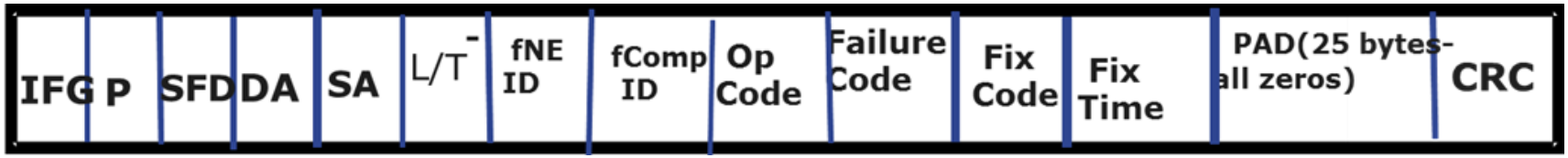
In-band Communications

A. A common message format for communicating failures and operational status whether it is LOS,AIS, LOF, RDI or operating system issues or protocol issues or hardware issues.
B. Communicating Failure Type to all related parties (i.e. sNEs, sNMS/sOSS, field technicians, etc.).
C. Indicating who will fix the failure, whether sNE or sNMS/sOSS or field technician.
D. Indicating the time interval to repair. This will help sNEs, sNMS/sOSS, field technicians, and users to decide what to do during failures (e.g. store traffic or reroute traffic).
E. Communicating operational status of the failed component after repair.

Estimated Fix Time and Fix Communications

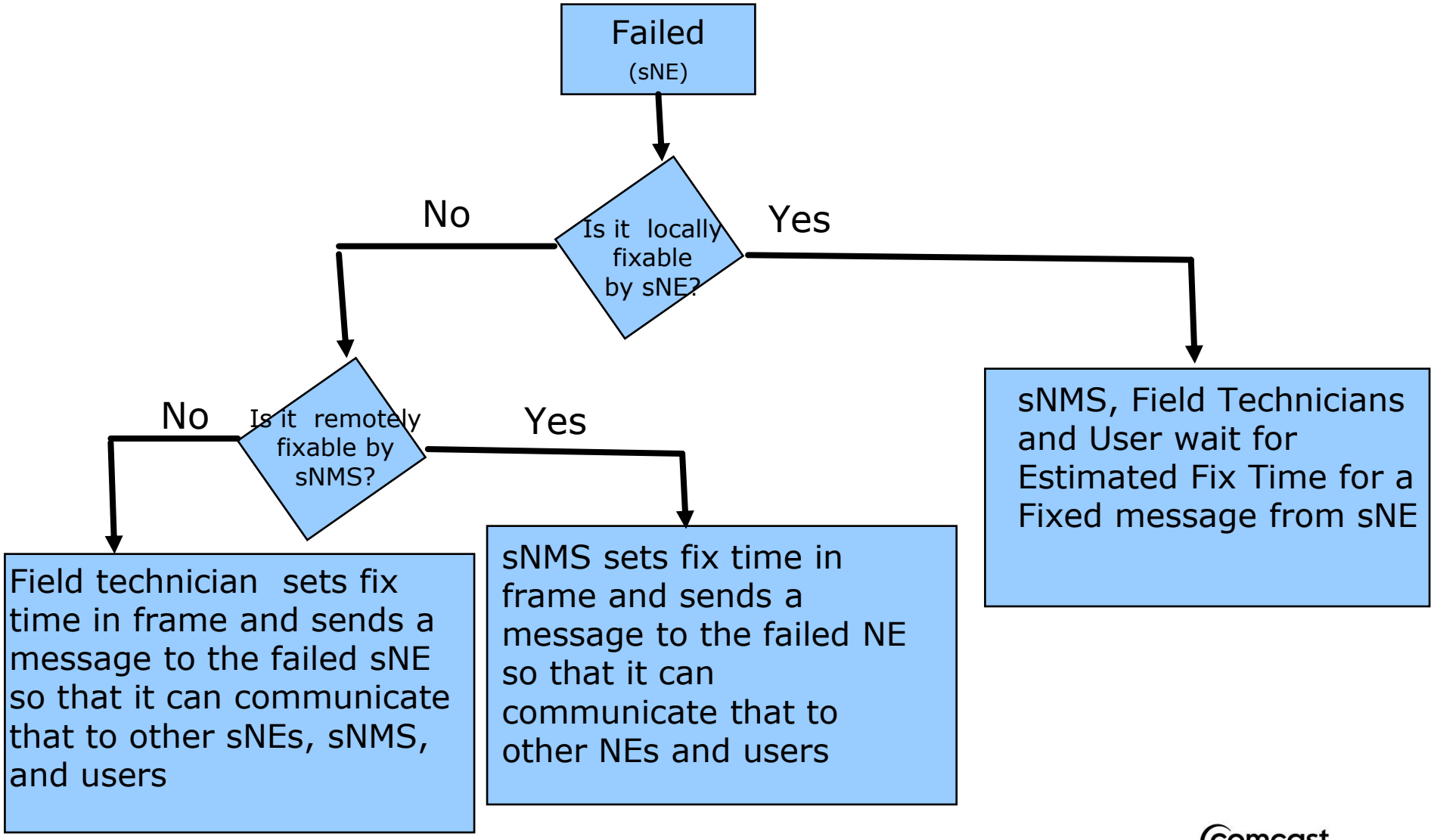
- **Failure type, estimated fix time and failure status are communicated among Self Managing NEs, Self Managing NMS/OSS, and field technicians**
- **This should allow NEs to divert traffic from the failed NE(s), store messages of failed NE(s) if needed, warn Network Operations and users for the failure and allow them to prepare for the outage by indicating estimated fix time.**
- **The estimated fix time can be adjusted by field technician and NMS if needed, and communicated to NEs, NMS and users.**

Frame for in-Band Communications of Failures, Fixes and Estimated Fix Times in CEN

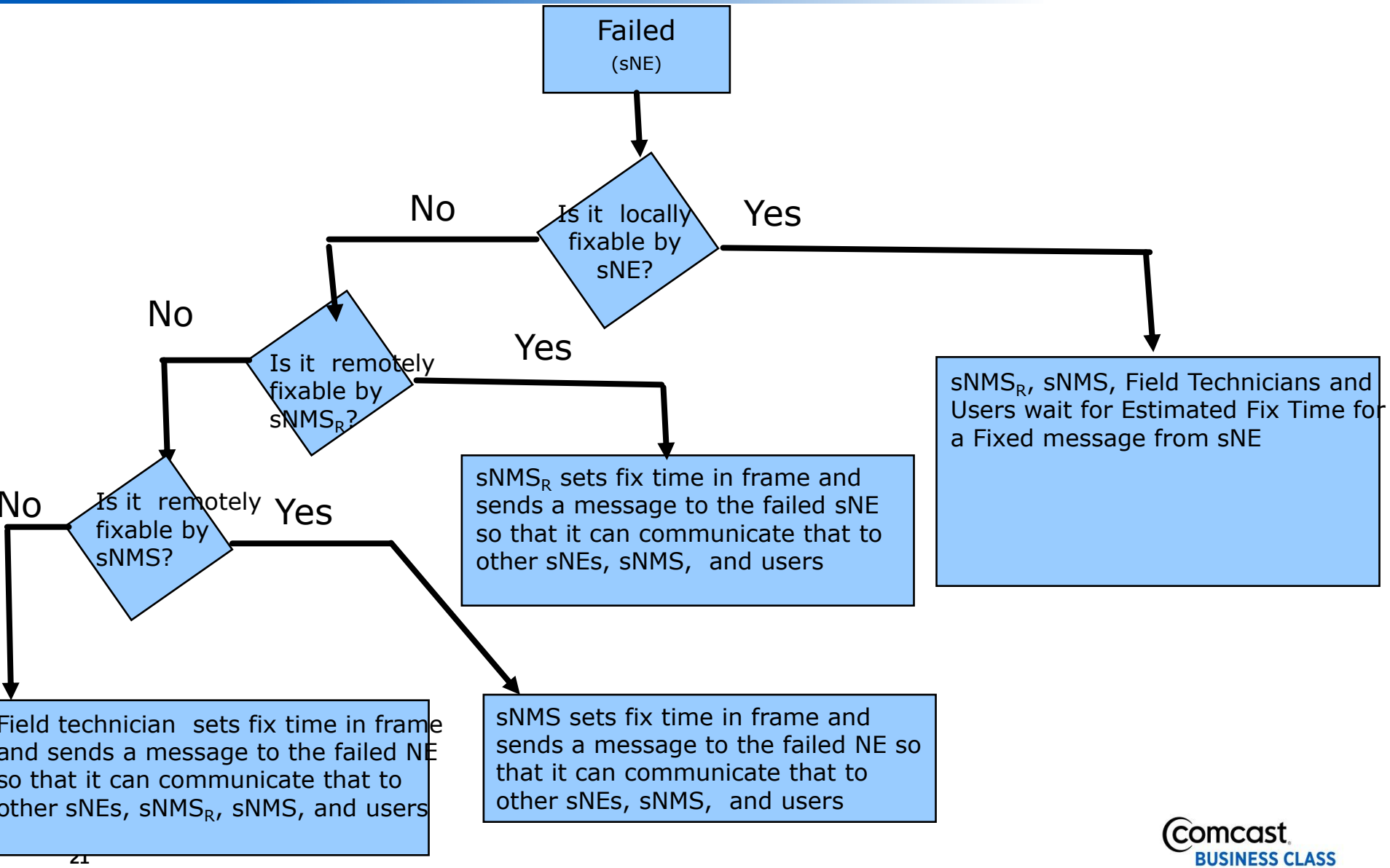


- IFG: Interframe Gap, 12 bytes
- P/SFD (Preamble/Start of Frame Delimiter)-8 Bytes (P-7 bytes, SFD-1 byte)
- L/T (Length/Type) : Length of frame or data type , 2 bytes (0x8808)
- CRC: 4 bytes
- DA: 01:80:C2:00:00:02 (6 bytes)-Slow protocol multicast address
- fNE ID: 6 bytes, Failed NE Identifier
- fComp ID: 4 bytes, Failed Component Identifier
- Op Code: 2 bytes-0x0202 for Disabled and 0x0303 for Enabled status
- Failure Code (ITU list+): 4 bytes
- Fix Code: 1 byte identifying fixing entity, sNE (x00), sNMS (x01), $sNMS_R$ (x02), field technician (x07), unidentified entity or inconclusive diag(x08)
- Fix Time in seconds: 4 bytes indicating fix time by sNE, or $sNMS_R$, or sNMS, or field technician

Fault Management Hierarchy for Centralized Networks



Fault Management Hierarchy for Distributed Networks



Thank you!