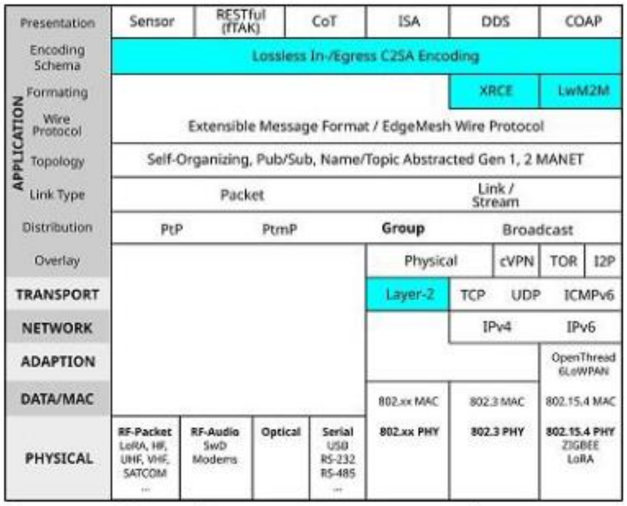

Chirp port forwarders reside on pigeon radios at Layer I.

Pigeons then port chirps to other radios and form logical Layer 2 network.

■ Protected Core Network (PCN) – Overview

The Protected Core Network (PCN) follows the current Enterprise-class, multi-echelon battlefield deployment model. Layer-3 (L-3) domain labeled data is transported/extended into the battlefield through a series of Point- of-Presence (PoP) sites. Because we currently use L-3 domain labeling, and the data secrecy controls are defined by strategic closed boundary-based network domain(s) criteria, the PoPs are inter-connected using Point-to-Point “black core” pipes, or tunnels, encrypted at the highest domain level to obfuscate source, destination, and domain level metadata during transport. Thus, highest domain encrypted pipes transporting unobfuscated data streams.

Typically, this “black core” WAN is SATCOM-based, but the NATO variant appropriately provides for Peer-to-Peer terrestrial-based “black core” WAN(s) connections. The NATO variant also supports single echelon Point-to-Point extensions from the multi-echelon PoPs to a terrestrially remote site, such as a Remote Operations Center, etc.

All “black core” transport services are hosted on private/closed Enterprise-class networks whether SATCOM and/or terrestrial. There is great concern about the Quality-of-Service (QoS), Quality-of-Class (QoC) and Service Level Agreements (SLA). These are appropriate concerns, from an Enterprise downward view of the battlefield communications architecture, since this is an Enterprise provisioned network and those responsible for its instantiation should have mechanisms to insure its robustness and performance characteristics. The PCN provisioners are the authoritative owners and thus are responsible for meeting operational requirements.

From an Edge upward point-of-view, the PCN is just another WAN service which operators at the edge may or may not be able to inherit. They do not control any of its characteristics since they are not the authoritative owner. The only QoS/QoC controls they have would be adjusting DIFFSERV and/or 802.11E header values. Thus, they can request, but not control/insure QoS/QoC. At the edge, the only comms network that is within their ability to control is the one they carry - all other comm link characteristics are inherited.

The other major concern from an agility and/or availability perspective would be that PCNs WANs are hosted on private, third-party Enterprise services which may not be available/stable in the theater of operation, nor extendable to the edge. This would be especially true for SATCOM and/or Enterprise (5G) terrestrial networks which near-peer adversaries can deny. Thus, the “deployment space” for PCNs require meeting all the IA controls for each domain with the physical security requirements, and then only in regions where the minimum Enterprise networks services are available.

In the Army and USMC, these PoP sites are transportable, mounted “data-centers” hosted on MRAP, 20K pound vehicles. Each echelon is extended into the battlefield using independent RF links with domain specific secrecy and integrity controls. Given a 3-4 hop radio-physics restricted “range” of the single echelon WLANs, the National “black core” asset needs to be within proximity of the “fight” or edge consumers.

■ Key Challenges related to Scalability and Sustainability.

It is unclear how this architecture will support the emerging near-peer adversary-based USMC Expeditionary Advanced Basing Operations (EABO) CONOPS, where all squads are socially distanced across the battlefield and dynamically associated to execute a mission. EABO also places these troops and their C2 operations within the adversary’s Area-of-Operations/Responsibility (AoR), thus rendering previous “front-/rear-line” force topologies null and void. There will only be “non-safe” and “safer” areas and they will be highly dynamic. Thus, physically secured highly agile and resilient tactical edge links with low latency are paramount to Mission Assurance.

PCN and/or similar extensions of Strategic networks into the Tactical Edge have several “fatal” or “deployment” flaws which limit their scalability into the Tactical Edge. It is not that we do not, or cannot do it, we have for 40+ years. It’s a question of whether we should continue do it and can we afford the hardware/manpower costs of extending “boundary protected” strategic domains into adversary-controlled environments. Since the Tactical Edge is driven by real-time distributed Command & Control/Situational Awareness (C2SA), the need for low- latency, Peer-to-Peer (P2P) data exchange across all allied participants in the AoR, including allied services and FVEYs coalition forces. PCN and PCN-like architectures do not scale to support these (desired) requirements.

■ GreyNet Tactical Edge Ecosystem based on Receiver Oriented Messages (aka Chirps Protocols).

GreyNet (GN) the moniker for a family of loosely coupled software-based technologies/capabilities which in various combinations throughout the global battlespace enable a high assurance, highly resilient Tactical Edge Network (TEN). The Tactical Edge Network is defined by NSA-Nuclear Command & Control doctrine as an open network with true source/sink End-to-End encryption (EtEE) with cipher strengths appropriate with its data classification. Additionally, data is ephemeral/temporal. Data's "half-life" is determined by its cryptographic endurance. Operationally, this is defined as the time required by the Red Forces to use the exploited data against the Blue Forces. Cryptographic endurance is a function of the cipher type and strength and does account for multiple encryption layers and independent key asynchrony.

Tactical temporal data can be pushed through existing Cross-Domain Products/PoPs globally located where that level of Enterprise services can be supported. Strategic data can be pulled into the tactical edge at the appropriate secrecy and temporal controls. This approach minimizes the exposure and complexity of tactically deploying Strategic networks by allowing them to stay far rearward where appropriate physical security and support functions can safely exist.

The TEN does not have any trust or secrecy requirements placed on transport elements. They are all considered untrusted. This significantly increases vendor diversity and significantly reduces unit cost. All elements are not controlled interfaces and thus could be considered disposable.

At GN's core is a boundary-less, Zero/No Trust cloud native network architecture with maximum reliance/performance at the edge and secure global reach using opportunistic BLOS/WANS. It is designed to operate on open, untrusted networks and is self-forming, self-healing on all ISO layers - physical, transport, data, etc. GN TENS has a deterministic development pathway to true Multi-Level Security nodes, dynamic asynchronous group re-keying, decentralized dynamic attributes, and GreyWire capability.

GreyWire is the capability to obfuscate domain labelled data at Layer-2 in open networks. It is an extension of EdgeMesh. EdgeMesh is a cryptographic, receiver-based protocol, with perfect secrecy and inherent DAR Delay/Disruptive tolerant. It is physical layer (PHY) agnostic and supporting a 250 b/S (HF-Narrowband RF) to 1Gb/S throughput span over packet/IP radios, software-defined acoustic modems, RS-232/485, USB, optical/laser,and TCP/IP Ethernet. Thus, EdgeMesh can operate seamlessly across the complete throughput/latency span of sub-1G (10%) to saturate 5G on any physical link type. It will degrade gracefully, well below the failure point of TCP/IP, yet operate at wire speed when available. Highly distributed Micro-ledger-like DAR Store/Forward capability enhances data transport performance on Denied, Disrupted, and Intermittent and Limited Bandwidth (DDIL) links. Multi-PHY EdgeMesh bridging and/or Store/Forward cache hubs can be hosted anywhere in the network, and at any scale. Hub software is hostable on highly constrained unattended edge and/or handheld devices. EdgeMesh is fully compatible with GN's local WLANs (sensor, voice, video, data) as well as GN's, CloudVPN, L-2 self-forming, self-healing, Peer-to-Peer, and structured L-2 virtual network(s) (VN). CloudVPN supports one or more VNs terminated as virtual NICS (vNIC), switch port, and/or router port. It is a structured L-2 product which can be used a covert channel, Community-of-Interest (CoI), and/or to provide one/two layers of EtEE transparent to legacy protocols. It is used to securely connect geo-spatially isolated Robust Tactical Wireless WLAN trees into a single Global L-2 network on open opportunistic WANs. Here CloudVPN is used as a hardware devoid virtual switch on the Internet. Also, CloudVPN can provide secure supports remote end-users access to the all or portions of the TEN from remote open networks such as Starbucks WiFi. It also can extend legacy tactical networks (i.e., high-through-low, low-through-high) while supporting secure access to the "bridged" network from within the hosting network as well as vice versa.

EdgeMesh will be enhanced with dynamic group re-keying, and cryptologically obfuscated domain labels at Layer-2 attributes. It is deployable on highly constrained embedded devices to Enterprise cloud services. It provides self- forming, self-healing non-IP-based path (vs route) determination as well as organic PHY MAC support. EdgeMesh provides obfuscated topic-oriented source/destination indices provide for undetectable data consumption to/from individuals and/or groups. Additionally, it is a native high assurance store, forward protocol with transparent streaming.

GN currently supports open reference policy, bare metal SELINUX on any Debian-based OS (i.e., Ubuntu). We determined the way-ahead and proposed an effort to expand this capability to open containers, Container- SELINUX. The combination of bare metal SELINUX with embeddable Container-SELINUX for the foundation implement the Bell-Lapadula confidentiality and access control, and the BIBA data integrity mathematical proof (Multi-Level Security (MLS) platform). This environment would be augmented with tactical edge deployable dynamic attributes, and L-2 data domain labels, to provide the basis for dynamic policy-based multi-echelon Mandatory Access Controls. Thus, a tactically deployable decentralized multi-echelon environment capable of transparently supporting dynamic mixed coalition and multi-service Peer-to-Peer voice, video, and/or data exchange and teaming. These edge deployed tools scale to Enterprise class, where an Enterprise downward approach may not.

This ecosystem is augmented with a hands-free biometric, EAL5 cryptographic storage based two-factor authentication capability. It is used in the TEN for proximity-based personal identification (pID), such that when devices (i.e., radios) are activated by pID, they are "personalized" to that user for the period of time they are in use by that individual and when not in use by that individual, they are returned to a "grey" or unassigned state. This transforms Blue Force Tracking (BFT) (of assigned devices) to Individual, Friend, and Foe (IFF) of people. As a EAL5 cryptographic data store, pID securely provides TEN issued identity certificates.

Secure Tactical Voice (sVoice) is a guaranteed delivery, multi-channel prioritized tactical voice application that is agnostic to the transport layer and "floor control" mechanisms employed. It is capable of bridging and extending fielded legacy radios over any EdgeMesh link type using simple Earphone & Microphone (E&M) cables and/or software defined modems. The current capability would be expanded to use EdgeMesh-GreyWire as its underlying transport protocol and augmented with a speech-to-text, text-to-speech engine supporting transparent NATO language cross-translation. Thus, producing a secure, dynamic attributes-aware, tactical C2SA tool with transparent multi-lingual text/voice fusion product capable of guaranteed delivery over opportunistic, untrusted DDIL links.