Telecommunications Industry Association

A FUTURE AT THE EDGE: EDGE DATA CENTER WORKING GROUP SOLUTIONS BRIEF PAPERS

ISSUE 3

February 2020

Survivability on the Edge: Redundancy, Accessibility and Survivability for Edge Data Centers

BY: Jayson Hamilton (Wavenet, Inc.)
Eric Swanson (Shared Services Canada)
Tom Widawsky (HDR)
Mark Smith (Vertical Datacom)
Kevin Monahan (ESD Global)
Neal Parker (Strongbox Data Center Services)
Damon Boyd (Grainger)
Joseba Calvo (EPI)
Shizuko Carson (Fujitsu Network Communications)

OVERVIEW

As today's emerging technologies move further away from the traditional data center, they drive a need to either reduce latency or have local computation at a more immediate level for better performance. In order to perform either of these tasks, it is necessary to develop a more efficient localized compute model to move the application closer to the end user or at the edge. Leading technologies like 5G Wireless, IoT data collection and processing, along with autonomous vehicle communications bring mission critical applications that pose great organization risk if they were to fail. Addressing these risk-averse environments requires our industry to find efficient solutions utilizing decentralized compute systems across faster and decoupled networks, as expressed in the edge compute model, to increase network performance and I/O to reduce application latency.

This paper discusses the variety of challenges faced in a typical deployment of these types of smaller data centers, many of which are mission critical, and with unique environmental requirements that fall outside the norms of the data centers previously designed.

Not all edge environments are located at the cell tower or on the far edge as some will exist in traditional data centers that utilize the edge data center (EDC) with technologies defined through the TIA 942-B standards. However, unlike a traditional 942-B data center location, each one of these EDC locations introduce different challenges, environmental impacts, latency requirements and survivability needs.

SCOPE

This paper offers a high-level view of the core technologies, along with additional insight on the need for Redundancy, Accessibility and Survivability (RAS) on the edge in order to survive in a harsh climate or even unknown conditions. In order to do so, this paper will initially focus on hypothetical 5G application and its deployment in an edge data center (EDC). With this

sample use case, the article will explore how to deploy a sustainable EDC in a remote location as an example of a RAS model. These guidelines will help to define the basic aspects of sample technologies in an EDC.

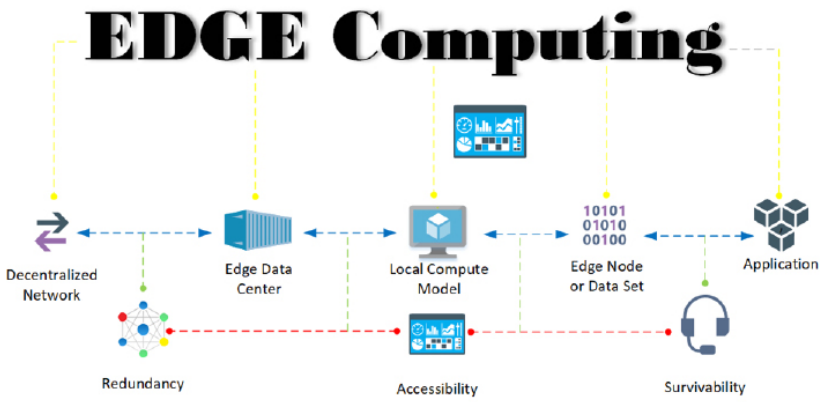


Figure 1: Typical Edge Computing Diagram

The EDC Market is projected to reach 16 billion by 2025, and, according to MarketWatch, 'ongoing IoT proliferation and adoption of smart connected devices are encouraging service providers to shift their data center facilities closer to the network edge'.[1] This article explains how the application survives in a data center facility at the edge. As we explore these system deployments on the edge, we discover not only the need for the survivability of the core technologies traditionally found in the data center (following TIA-942B as a standard), but also, additional challenges on how these electronic components and technologies can survive in an EDC.

Locations

The first paper in this series called 'TYPES AND LOCATIONS OF EDGE DATA CENTERS' has already provided examples of the typical locations where EDC's could exist. This paper will review different approaches of redundancy from systematic replication to individual site hardening, as either of these (and potentially others in between these two) will have benefits for various Edge applications. We will discuss some of the advantages to these potential solutions as we explore the systems involved. The Types and Locations group developed a series of prototypical locations that an EDC would normally reside on the edge. As a result, the following diagram was developed:

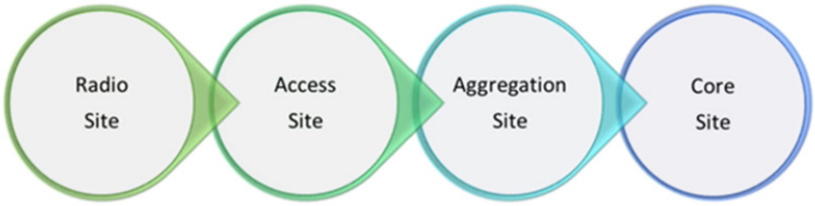


Figure 2: Site Locations (Created by Site Locations Task Group)

As the locations group will continue to help us define these locations at a granular level, we will introduce a simplified model for potential edge data centers. These edge locations will help us introduce the R.A.S model concept through different applications and emerging technologies as they will have different redundancy and latency needs depending on the criticality of the application. Please note that the diagram shown below is for reference only to the environments of what is expected to be the most commonly deployed edge systems. In order to simplify the visualization of this model, we will refer to the concept of Inner-Outer and Far Edge as shown below. The inner-outer-far edge concept allows us to set common talking points on locations

[1] 2019, November 8. Edge Data Center Market, Share, Application Analysis, Regional Outlook, Competitive Strategies & Forecast up to 2025.

and how they relate to typical environments. As we have already defined our application as a 5G wireless we will also show how to survive, in a potentially harsh environment, out on what is referred to be the Far Edge.

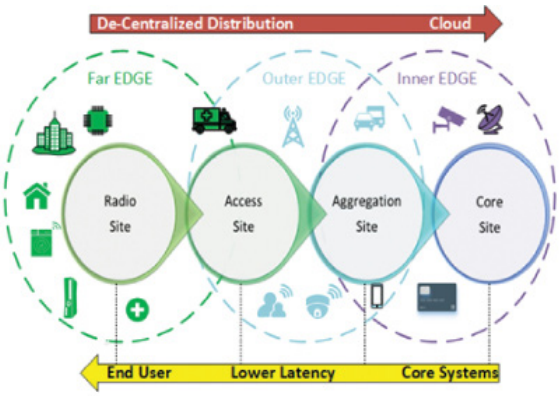


Figure 3: Visualization Model of the Inner-Outer-Far edge concept. (Created by Jayson Hamilton)

Inner Edge

A potential site location for an edge data center that is being utilized is in a traditional environment such as an existing 942-B data center, building or any facility that uses traditional compute models. This edge model can be a proximity site inside a traditional 942-B data center environment in a rural area or even at the bottom of a basement where traditional applications reside. These edge sites are relative to and additionally commonly by Core and Aggregation Sites.

Outer Edge

A potential site location where the compute model is moving away from traditional data center space and into a containerized or similar type harden solutions outside on the edge near rural areas. The outer edge brings local computation closer to the end user. These edge sites are relative to and commonly defined by Aggregation and Access Sites.

Far Edge

A potential site location where the compute model is even closer to the end user but utilizing smaller devices and newer technologies to bring local computation further away from the core site and into rural, isolated or desolate areas. These edge sites are relative to and commonly defined by Utility, Radio or Cell Sites.

Many challenges out on the edge can be addressed by utilizing an EDC to provide a typical edge compute system for a service provider looking to offer a 5G wireless application in a rural environment. This deployment would typically reside on the outer edge as it moves away from traditional data center space and requires environmental survivability through hardened systems and enclosures. This paper explores this hypothetical example to understand the levels of redundancy and survivability needed. It is important to define potential common components that will be deployed for power consumption, cooling systems, physical protection, network capabilities, and processing needs. This paper will investigate examples of these typical technologies used, and how it relates to the integration in an edge or even FOG compute model. As this paper explores these common components, it will also establish a relationship to the RAS. model while looking at these systems.

I. BUILDING A BASELINE

In order to best address the baseline technologies explored in this hypothetical use-case, we need to establish some basic elements required to build-out a potential 5G deployment. This allows us to scale out the functional technologies of this Edge Data Center and show the importance of the RAS model for these environments. As stated in the Overview and Scope, this example is only a representation of a common 5G deployment as there are currently no established standards in the industry. This section establishes these elements that we will use in this solution to bring an edge computing model to a typical cell tower site for 5G applications.

IT Equipment Racks

Each Edge Data Center (EDC) will be able to accommodate equipment racks with maximum cooling processes to house all IT processing equipment. Each rack will have fiber ports for storage or server connectivity, copper ports for console management links, and monitoring nodes for the power and environmental monitoring systems. Each rack will have A&B power sources and network connectivity fabrics for redundancy. These racks will accommodate various containment and air-flow management strategies to enable the best thermal performance in meeting ASHRAE TC9.9 guidelines. All racks, network systems, and IT components will be installed per TIA/ANSI standards.

Network Systems

The EDC's network should allow for diverse pathways with opposing entrances for segregated network redundancy. Each rack will have diverse fiber feeds for network redundancy, copper feeds for PDU and Console Management for edge devices if data sets criticality requires such redundancy. Edge nodes that are not at least business critical data sets or higher could have lower redundancy requirements due to cost restrictions or application design. All racks, network systems, and IT components will be installed per existing TIA/ANSI standards.

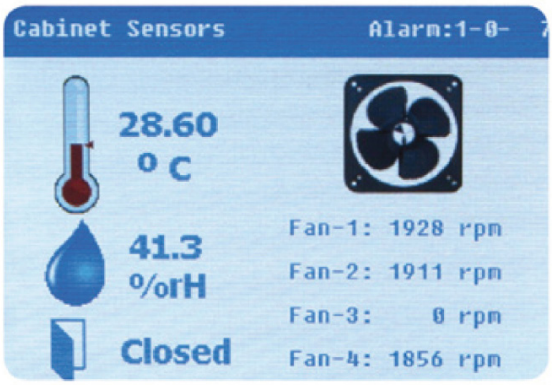
Figure 4: Common Networking Components (Switches, Power Extenders and Media Convertors) for the EDGE. (Compliments of Signamax) ***For example purposes only.***

Compute Systems

The EDGE compute model should be de-centralized from a cloud data center and/or cloud network. Some level of data protection will be needed which will be defined through the RAS model for sustainable applications on the edge. The compute model should also have local, regional and potentially geo-redundant mirroring or through agile design for application survivability.

Cooling Systems

The EDC will support numerous cooling options with a key design goal of minimizing overall environment impacts (e.g.: maximizing free cooling, minimizing power, water, etc.). The design will allow for growth with flexibility to operate individual racks from low to high density. Controls will monitor IT inlet supply temperatures and humidity to help ensure that they meet ASHRAE TC9.9 guidelines. For environmental and budgetary reasons, most will want to operate in the upper allowable ranges, reducing cooling and humidification needs. System testing should be performed including load testing and failover. All equipment, piping and associated support needs will be installed per NEC/NFPA, ASHRAE and ANSI/TIA guidelines.



Electrical Service System

Electrical service will come from the utility provider and will be supported with a backup secondary source from either a diverse utility feed or by on site backup power generation. Electrical service from both sources will be provided through an Automatic Transfer Switch (ATS) to a primary distribution panel with a circuit to a transformer in order to provide separate power distribution for lighting and general power needs. A grounding system will be installed to terminate to the site's existing main ground system, or if unavailable, the EDC owner will provide dedicated ground ring/rods as required to meet soils conditions and local code requirements. Installation will be performed according to local, state and national codes, in addition to NFPA/NEC, ANSI/-J-STD-607-A, NEMA WC 70, Telcordia GR-347-CORE, and other TIA/ISO standards where applicable.

Uninterruptible Power Systems (UPS)

The EDC will include a minimum of two UPS systems with a minimum reserve time of 10 minutes each or greater, according to the standards of the EDC owner. Typically, these systems would be two UPS systems with a 3-phase power source. The EDC owner may use UPS systems that feature hot swappable modules to improve efficiency in low load conditions. Downstream power distribution shall be with A/B redundancy as all module style UPS systems are intended to be a minimum of N+1 redundant and adhere to TIA/ANSI/EN standards. Power systems will have a sub level grounding system per NEC, ANSI/-J-STD-607-A standards to terminate to the sites main ground.

Electrical Distribution Systems

Each cabinet will have two power distribution units (PDU) for redundant rack mounted power supply. One PDU will be fed from the A Remote Power Panel (RPP) and the other will be fed from the B RPP. The PDUs will be UL Listed metered PDUs with C13, C19, and NEMA 5-15/20R outlets. System commissioning including load testing and failover should be performed prior to operational handoff.

EDC Systems

The EDC will be factory-manufactured to allow over-the-road delivery to site. The exterior shell will be designed according to the appropriate fire ratings with a minimum of 1 hour recommended. The EDC should also resist wind loads appropriate for the location and shall be rated as a NEMA-4 EDC or equivalent for electronic equipment. The roof will meet snow loading appropriate for the location. The doors for the EDC should be at a minimum of 12-gauge, galvanized steel with a factory applied enamel finish and include a dead-bolt lockset, stainless steel hinges with tamper-resistant pins. The EDC shall meet all local, state, and national building codes for the allowance of human and equipment occupancy as well as UL PQVA standards for modular data center requirements and UL 507 for ballistic resistance, if applicable.

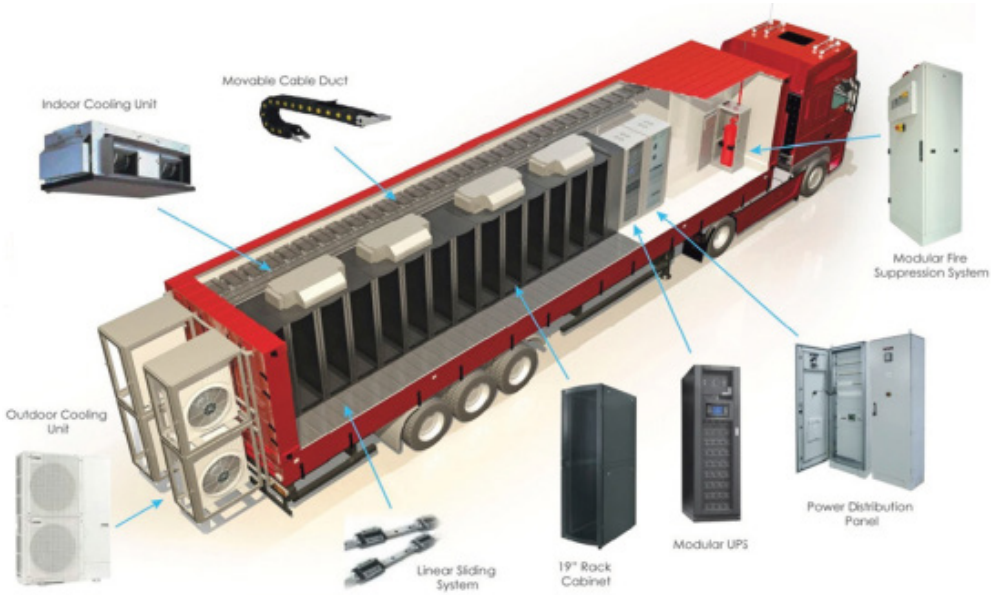


Figure 5: Example Mobile Data Center (Compliments of Canovate)

Sample EDC Dimensions: L:480" x D: 95" x H: 114"
Sizing allows inclusion of the Following Systems:

- Server Cabinets and Connectivity Racks
- Cooling and humidification options
- Outside Compressor & Condenser Unit
- Modular UPS System Battery Rack
- Modular Power Distribution Panel
- Fire Suppression Unit
- Cable ducting and Piping

Environmental Monitoring, Power Management, and Remote Reporting Systems

Mechanical, electrical, and fire protection systems will provide monitoring capabilities, management of systems, and remote reporting of systems status. Temperature, humidity, power level, power status, warnings, alerts, and alarms will all be reported, discoverable, and broadcast to remote monitoring over secure network connections as designated by the user. Capabilities for upgrades to these systems will be provided to allow for artificial intelligence and/or machine learning capabilities to provide early degradation or conditions noted on systems to allow very early alerts for potential maintenance needs to allow Maintenance & Operations servicing needs.

Physical Security Systems

There should be a complete security camera system using weatherproofed cameras for outside visibility along with 360 dome cameras inside the EDC. The system should be equipped with

remote monitoring software, video analytics, adequate storage space up to 12 TB and a form of data replication for survivability. Physical access control will need to fully integrate the access control with multiple authentication factors such as Card Readers with the security camera system.

All security systems will adhere to NEC, NFPA, IEEE and TIA/ANSI standards if applicable. In addition, EDC exterior, doors, frames, and exterior penetrations will be vandal-resistant. Physical hardware will be used at access doors in conjunction with electronic access systems similar to Central Authentication Service (CAS) and/or biometric systems. Remote access authorization should be provided through closed-circuit television (CCTV) in coordination with remote monitoring/control systems.

Fire Detection/Suppression Systems

The limited space available will require the use of a compact extinguishing system with a non-ozone depleting gaseous agent (similar to Novec™ 1230). In conjunction with this suppression system, a very early smoke detection alarm (VESDA) system shall be deployed. This system should allow for future upgrades to incorporate artificial intelligence and/or machine learning to provide increased analytics into potential smoke or fire conditions prior to the need for alarm and suppression. All designs and installations will comply with national and local NEC/NFPA standards.

Figure 6: Typical Fire Suppression Unit (Compliments of Canovate)

II. REDUNDANCY

With the established baselines noted in the previous section, we can now turn to look at how these systems will fit into the RAS model. The first element to be explored is redundancy. Redundancy is typically defined as the inclusion of extra components which are not required for function, but to provide continued availability in the event of a failure. The following represents a breakdown of these various aspects of our examples and considerations for the primary systems involved to support redundancy in an edge deployment. We want to note that the criticality of the edge application will ultimately affect the level of redundancy required, and for this example we have assumed our 5G application to be at least business critical and on the outer edge.

Facilities

Facility redundancy requirements will be based on the operational criticality of the location as it relates to the overall network of the system. In other words, if the specific location has strategic value to the overall performance of the network, then it will require higher redundancy considerations. If the site itself can be considered redundant to other sites in the network, then its redundancy needs can be reduced. Each use case will determine this value and the individual facility needs; however, all facilities should include considerations of the following:

- **Physical Segregation**: The EDC may require separation between IT systems and the supporting infrastructure.
- **Redundant EDC Components**: The EDC may require the use of a redundant exterior shell, roofing, or door system.
- **Penetration Protection**: Treatment of exterior penetrations to provide improved protection may be required for the EDC.
- **Redundant Entry Points**: Multiple network service entries to provide redundant connectivity maybe required for the EDC.

Power

As with traditional data centers, the power redundancy for the EDC is accomplished at multiple levels. Utility service will be supported through a diverse utility feed or more commonly through on-site power generation. The power load for the IT equipment will be supported by separate (A and B) UPS systems. The UPS systems may have internal power modules that support redundancy within a given UPS system. Each IT cabinet will have separate PDUs fed from separate UPS systems, allowing redundancy within the cabinet. Equipment mounted within the cabinet shall be dual corded with load sharing power supplies. Each cabinet should be inspected to ensure each device is plugged into separate PDUs. Here we will focus on:

- **Diversified Power Pathways**: Redundant pathways of power fabrics of systems A & B using different entrance locations, if applicable.
- **Grounding Requirements**: Grounding and bonding requirements at the rack level per ANSI-J-STD-607-A standards to ensure continuity.
- **Power Protection inside the Rack**: Adequate power through load sharing capacity's for A & B fabrics for the PDU that supplies inlet, PDU or socket level monitoring.

Figure 7: Typical UPS Monitoring

Cooling

Cooling redundancy is a key component of overall site redundancy as IT services are affected by even minor cooling issues while critical cooling issues can quickly lead to site outages and risk equipment failure. In addition to lowering risk, redundant cooling also increases maintenance flexibility and service-response times. With air-cooling, the goal is to meet ASHRAE TC9.9, involving equipment inlet temperature, rates of change, and humidity. Control strategies are especially critical components of redundant cooling infrastructure to ensure energy efficiency and that cooling is supplied to IT equipment within desired guidelines. With cooling infrastructure, redundancy exists at both the device and component level of the overall system. We will focus on the following redundancy aspects to cooling:

- **Thermal Controls**: The cooling system needs to regulate its cooling to the equipment supply needs across the EDC, including alerting, logging and reporting on metrics. This would include automating any lead/lag or failover situations.

- **Single Point of Failure**: Design to minimize as much as possible within expected uptime and budgetary requirements (e.g.: redundant systems, fans, pumps, motors etc.)

Network

Initially defined as the ability to minimize downtime due to equipment or service failures, network redundancy provides an alternate transport medium by using separate sources of incoming fabrics for the physical medium and sending to an EDC within 15 miles of the access or site location. The network redundancy would be applying to the Wide Area Network (WAN), Local Area Network (LAN) and Storage Area Network (SAN) as a decentralized network and be referred to as the EDGE fabrics. Because our application is for a business critical 5G wireless deployment, we do assume that proper negotiations have taken place with the carrier. The following should be decided prior to or during the capacity planning phase:

- **Dedicated Circuits**: Make sure to have determined whether outside circuits are dedicated to the relevant network or if it is for public use per the carrier's protocols.

- **Multiple Service Providers**: Depending on needs for redundancy, consider using more than one network service provider utilizing diversified pathways for optimal network survivability.

- **Diverse Pathways**: Maintain separation at the point of entry by at least 300 ft in a typical data center and 10-20 ft. for an edge solution. These are redundant A&B incoming cable feeds from separate cores at N/S or W/E pathways and ensure these cable pathways do not cross for more than 50 ft outside the enclosure.

Compute

The compute is defined as the ability to minimize downtime due to equipment or service failures and to provide alternate transport medium by utilizing separate sources of incoming feeds for the physical medium along with decentralized and mirrored capacity at least 15 miles away. The edge compute model should be engineered with these minimal baselines:

- **Local Application**: Ensure that the application is designed for agile deployment through local computation at the edge to reduce application latency.

- **Mirrored Disk**: Application redundancy should happen at a local level to ensure protection against disk failure in unknown or climatic environments.

- **Data Replication**: All data sets should have some type of data protection initiated along with validation cycles. We do suggest that a form of synchronous, geo-redundant or site replication be used for mission critical environments and for non-critical environments at least utilizing incremental backups at the local level and across the WAN during non-peak hours.

III. ACCESSIBILITY

As the location and criticality of EDC's varies, the ability to provide operational continuity and resiliency will vary as well. Individual EDC's will require an ability to gain access, remove, install, or change equipment in a manner that minimizes interruption of the site. Accessibility relates to the simplicity and speed with which a system is able to be maintained without disruption due to systematic failure. This model could have some resemblance to common rating of traditional data centers, but there will be some variations due to climatic conditions that will impact how efficiently a system can recover.

Facility

Facility accessibility should provide for the allowances of both personnel and equipment to be installed, serviced, removed, and/or replaced as needed to allow for continuous operations of the EDC. More specifically, these sites should provide for the following:

- **OEM Clearances**: Accommodations within the footprint of the EDC to allow compliance with equipment and vendor clearance needs for all equipment installed or planned to be installed (including both IT and infrastructure support).

- **Code Required Clearances**: Allowance for all code required clearances for operations and maintenance of electrical, mechanical, and other systems or equipment.

- **Personnel Access**: Compliance with the Americans with Disabilities Act (ADA) clearance requirements for accessibility into and throughout the space. This should include operational compliance with latches, doorways, and other access needs. (Reference ADA (Latest Version); ANSI 117.1 (Latest Version)).

- **Facility Clearances**: The EDC should have proper space surrounding its placement to provide access to doors or other access needs, including ventilation, electrical or network connectivity points.

- **Site Clearances**: Yard, area, or space should accommodate the EDC placement and removal as required by the manufacturer including working space.

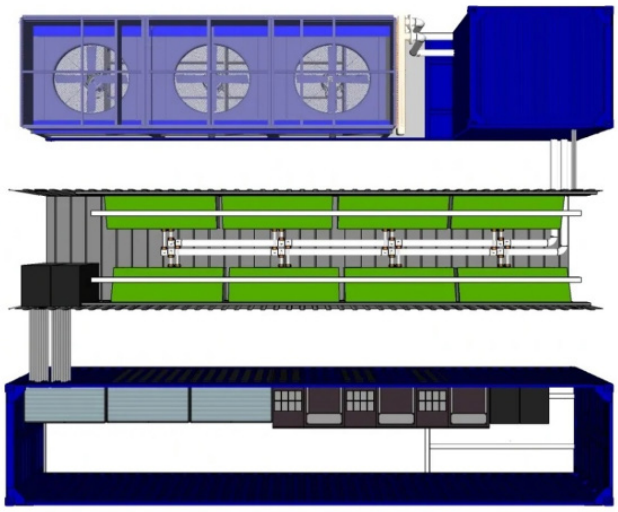


Figure 8: Typical 5G Wireless Containerized Deployment (Compliments of Immersion Edge)

Power

Power equipment should only be accessed by qualified personnel. All systems, panels, outlets, and other equipment should be correctly labeled to assist the operator in accessing the part of the system of interest and avoid opening the incorrect panel or cabinet. UPS systems should be placed to allow for operation and maintenance. Typically, these systems need only front access. All distribution panels should be wall mounted with proper clearances defined within the NEC. Power cabling should be installed within properly sized conduits and securely supported. Power cords within each cabinet should be neatly dressed and labeled on both ends.

- **Power Monitoring Controls**: All control sets should have physical redundant fabrics monitored through a single pane dashboard for live monitoring.

- **Back Up Capacity**: The capacity along with battery type should be defined by the criticality of the data set, but at minimal be able survive for at least 15 minutes in the case of an event or surge.

- **Administration**: The ability to understand the architecture and nodes of the power infrastructure through either physical labeling and an identified layout of the infrastructure via a Data Center Infrastructure Management (DCIM) or console management.

Cooling

Cooling Accessibility is driven by how accessible or protected the infrastructure is from both a physical and logistical perspective. Remote management, complete with alerting, metrics and trending capabilities are especially important for EDC's as they often will be remote. The more automation provided with the controls the better, as this enables quick, pre-managed responses and greatly reduces the need for physical access. All cooling system components required in an EDC must be easily accessible and have a minor impact on EDC security --including fans, ducts, filters, piping, water drains/containment-measures. Ideally it would have a web page interface that displays the thermal environment throughout the EDC, with controls to remotely adjust various set points as needed.

- **Remote Management**: The ability to remotely monitor and control the cooling systems of the EDC.

- **Automated Triggers**: Automated event notifications of all major events, along with potential options to be set as automated re-actions to correct or react to the trigger.

- **Cooling Component Lifecycle**: Identify all physical components that have short life cycles to develop a proactive preventative maintenance program.

Network

Network Accessibility is characterized by combined levels of both physical and logical layers that should be planned by all networked systems having remote access capability in the case of an event. Depending on the size of the deployment, relying on the need to physically visit each site for physical network moves, adds and changes is likely challenging and could be cost prohibitive. Providing a means of remote access and the ability to make real-time changes while in operation are key elements for edge network systems. The following key elements should be deployed:

- **Remote Management and Real Time Monitoring**: All systems should have some level of remote monitoring built into a console management feature, but as this network will segregated and more than likely autonomous from the core network, additional measures will need to be in place. A level of real time monitoring through Automated Infrastructure Management (AIM), DCIM or internal management will need to initiate both proactive and reactive triggers, along with remote management including an ability for change and the ability to provision new or additional resources in case of an event.

- **Port Management**: The network will need to be monitored at many levels in order to capture the real time metrics for proactive management. These metrics should, at minimum, cover the following: latency, jitter, throughput or bandwidth and the physical management of the port on the switch. This management can and will be on multiple levels of monitoring over different fabrics such as physical layer, Network Function Virtualization (NFV) for Virtual Local Area Network (VLAN) segmented networks, software defined environments and potentially open sourced links should they be deployed.

- **Time to Recovery**: Here we explore the time to recovery from an event as a specific type of proactive or reactive troubleshooting in the face of an event. A simple fact remains true in a traditional data center as well as on the edge: "it's not if the port will die but when," so in order to maintain accessibility on the edge, the proper remote or logical recovery methods need to be in place that must include remote or console management procedures.

- **Cabling and Administration**: All distribution cables should be routed through wire management with proper clearances for bend radius if needed as defined in the TIA-606 standard. Visual port to panel maps should be used for dense environments for both physical and logical routes. All cabling shall be installed within properly sized conduits to each cabinet and should be neatly dressed and labeled on both ends.

Compute

The compute model's availability is simply defined as its ability to minimize downtime due to errors or service maintenance through the server's ability to auto heal applications. This ability includes the application's local data set and its ability to replicate either through server mirroring or off-site data replication to create additional redundancy for the application and not the network.

- **Automated Healing**: The compute design should have some considerations relative to the hardware's ability to self-heal and perform automated preventative maintenance tasks without disrupting the performance of the application.

- **Application Change**: A preferred design model will have remote monitoring, along with an ability to provision or change the application states with minimal disruption. This could be achieved through many methodologies including but not limited to: Change Management through terminal services, Remote Desktop Protocols (RDP), DCIM, Virtual Private Network (VPN) tunneling or even pushing a Server Profile across the WAN.

- **Time to Recovery (Application)**: As we did for the network subcategory, we must also examine the application's ability to recover from an event through remote methodologies. The primary functionality needed will be through remote management protocol to initiate some level of back-up recovery to minimize downtime. The processes should have full system health view with basic level restart capabilities via common protocols such as Windows Management Instrumentation (WMI), DCIM, Application Access Server or PowerShell to name a few.

IV. SURVIVABILITY

As the location and criticality of EDC's varies, the ability to provide operational continuity and resiliency will vary as well. Survivability is defined in how it relates to the percentage of time a facility is actually available versus the total time it should be available. The metrics used to gauge performance or success of survivability can be compared to the tier levels of traditional data centers, as established by the Uptime Institute, but without the standardized ratings system of Uptime Institute and substituting with the upcoming rating system of the TIA Edge Data Center Ratings work group. Of course, on the edge we will have many modified variations due additional unknown climatic challenges or even harsh conditions that will have negative impacts. This section will also help define the requirements from the electrical components and the needed equipment to survive in these unknown elements, climatic or harsh environment and in the case of a catastrophic event.

Facility

Facilities' survivability requires consideration of the site in relation to its importance to the overall network. Once again, a site which is critical to the continuous operations of the network is considered more important than a site which itself can be redundant to another. This individual importance will affect the following categories for consideration:

- **External Environment**: Environmental ingress like NEMA ratings for environmental protection from dust, dirt, or other solids plus water infiltration and potential snow/ice accumulation. (Reference NEMA Standards)

- **Internal Environment**: Environmental egress like R-value/U-value to provide consistent internal HVAC and humidity control. (Reference ASHRAE TC 9.9 Standards)

- **Fire Resistance**: Fire resistance ratings (in cases of proximity to other structures) to protect from adjacent fire conditions. (Reference NFPA 75-76 Standards)

- **Penetration Protection**: Penetration detailing for piping, power, and network connectivity to provide protections for the three bullets above.

- **Physical Protection**: Physical security to prevent unauthorized ingress and protection of associated systems. Should include physical, access control, and monitoring, due to the unmanned nature of the site.

- **Anchoring**: Anchoring and structural support to provide operational stability for environmental influence (wind, seismic, and others), and accidental or purposeful unauthorized movement.

Power

One way to measure the survivability of the power system is to define the mean time to failure (MTTF), which represents the length of time the system is expected to operate until its failure. There are multiple mechanisms which can cause failure; however, we will focus on the following as the primary stressed areas:

- **Failure due to lack of adequate power source**: Make sure simple power outages due to human error are limited (i.e. no bad connections or wiring, poor systems installations or cut power feeds).

- **Failure due to mechanical element failures**: Identify all moving components with short wear-and-tear lifecycles such as diodes, fans, capacitors, and integrated circuits (IC).

- **Failure due to thermal stress**: This will focus on eliminating failures due to inadequate thermal management like events similar but not limited to: 1. Fan failure within a UPS causing system to overheat, 2. High ambient temperatures causing IT equipment to operate outside of typical temperature ranges and 3. Poor hot/cold airflow in dense power output areas.

- **Preventive Maintenance**: This covers a potential preventive maintenance schedule that utilizes local human resources to maintain the power system in case of an event or to minimize downtime.

Once failure occurs to the power system, the length of MTTR (mean time to repair) varies depending on the EDC location and available repair service. In most cases, power redundancy or back up is beneficial or may be required and we will take a deeper look into these cases throughout the series.

Cooling

Cooling survivability is dependent on the ability to service or maintain the cooling system and what preventive maintenance or precautions are taken to reduce or eliminate unplanned downtime or unforeseen outages due to system failures. These procedures should be built upon not only best practices outlined by TIA 942-B EDC Standards, but also by following Original equipment manufacturer (OEM) preventative maintenance specifications while adhering to local, state and national standards or regulations. Depending on the infrastructure and location, this may include legal obligations, including records to support that appropriate preventative maintenance was being done. Any cooling system should retain self-control from any control system, such that if it senses a cooling need above a high set point, it will attempt to provide the cooling and thereby automate protective action to a failure in the cooling control system.

- **Preventive Maintenance**: Regular scheduling of local authorized technicians to maintain the cooling system.

- **Automated Processes**: The cooling system as defined under availability needs to have automated communication protocols to remote staff and locally vetted integrators in the case of an event.

- **Autonomous Control Sets**: The control sets for the entire cooling system should be autonomous of all other control sets and have built in redundant controllers for real time monitoring.

Network

Here we will take a deeper look into what remote management or monitoring capabilities the EDC has and how accessible or protected the infrastructure is from both a physical perspective as well as any hardened requirements to protect electronic components and survive in harsh weather environments. We will also explore physical failures and time to recovery through the critical and non-critical response times of internal tiger teams, external remote hands and Service level agreements (SLA) through manufacturers or even local integrators.

- **Redundant Fabrics**: While under network redundancy, we covered diversified pathways to the enclosure. In this section, we will focus on fabrics A&B in between the systems to make sure we have adequate fiber feeds. The redundant feeds along with additional autonomous fabrics will be determined by the criticality of the applications data sets.

- **Human Capital**: While the designs should contain adequate remote monitoring and management, there will always be some level of human touch needed for the physical layer or components like small form-factor pluggable (SFP), disk and network cards. These will require the assistance of a trained or certified technician as we typically will be in an unmanned facility in rural areas with typically limited staffing pools of qualified personnel. We suggest looking to some level of staff augmentation to offer remote or smart hands-type services to provide preventive maintenance checks and reactive break-fix of physical components.

- **Commercial vs. Industrial Grade Equipment**: As there can be unknown environmental impacts and climatic events, we suggest that a cost/benefit analysis be run to determine the proper equipment for each edge environment, taking into consideration the following: Seismic Vibrations, Extreme Temperatures (hot or cold), Geographical Weather Patterns and Catastrophic Events. This analysis will once again be dependent on the criticality of the application and data sets to determine the evaluation criteria between cost and benefit of all active and passive network components.

Figure 9: Typical Industrial (IP Rated 55 or Higher) Switches (Compliments of Signamax)

- **Time to Recovery (Components)**: This time we will look at time to recovery from the aspect of port recovery in case of failure. In a future technical white paper, we will look into best practices for remote testing and configuration, product lifecycles, planned events and inventory levels of common break-fix components and how to minimize downtimes.

Compute

Defined as the ability to minimize downtime due to errors or service and the server's ability to auto heal applications or local data sets either through replication or server mirroring technologies on and off-site.

- **Application Failover**: In terms of failover here we will show a baseline to the failover of the compute nodes in order to maintain operations in case of an event. This failover can be through many different types of compute architectures like Active-Active or Active-Passive clustering of the database set.

- **Data Replication or Mirrored Disk**: We will look into the replication of data sets at the local level to enable backup/restore operations in order to survive a major event. Application replication can also be used to back up aggregate sites depending on the survivability requirements of the applications and data as well as the potential costs.

- **Physical Components**: While the designs should possess adequate remote monitoring and management, there will always be some level of human touch needed for the physical layer or components like disk, memory and cables. These components will need the assistance of a trained or certified technician. However, an unmanned facility will typically be in rural areas with limited staffing pools of qualified personnel. As a result, we will examine staff augmentation for remote or smart hands-type services to provide preventive maintenance checks and reactive break-fix of physical components.

Figure 10: Common Connectivity Components (Compliments of Wavenet)

- **Commercial vs. Industrial Grade Equipment**: Just like the network, the compute models still reside on physical hardware that carry some limitation and tolerances to events. A cost/benefit analysis should be run to determine the proper equipment for each edge environment, taking into consideration the following: Seismic Vibrations, Extreme Temperatures (hot or cold), Geographical Weather Patterns and Catastrophic Events. This will once again be dependent on the criticality of the application and can be within the application or as an autonomous application like DCIM or Element Management System (EMS) software.

V. CONCLUSION

As many faults, errors and events can occur on the most stable compute model, it is important to understand how to replicate that stability with the challenges of unknown variables and environmental impacts. While these events can be minor, it is imperative to have adequate Redundancy in the systems in order to recover with minimal service impact; to have 24/7 Accessibility to the core systems to enable acceptable response times; which will, in turn, best ensure Survivability of the application.

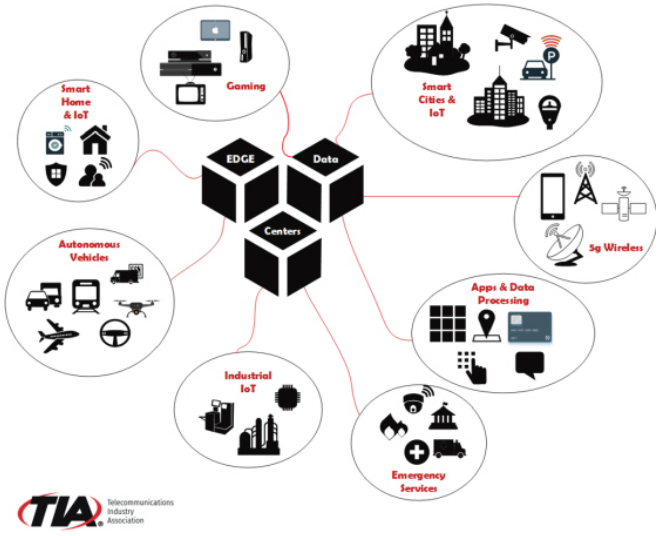


Figure 11: EDGE Application Types (Created by Jayson Hamilton)

In future Edge Data Center Working Group Solutions papers, we will take a deeper look into the importance of all of the RAS model in the edge data center and how these baseline standards will help any compute model to survive on the edge.

To learn more about the TIA's Working Group efforts in developing information and standards on Edge Data Centers (EDCs), go to the TIA website: **www.tiaonline.org**. If you have opinions or expertise to lend to this effort, please reach out to **edcinfo@tiaonline.org**.

APPENDIX A: GLOSSARY

Note: TIA collaborates with the Linux Foundation in maintaining the Open Glossary of Edge Computing. Terms included in this paper are listed below. **For the full list of Open Edge Compute Glossary terms refer to the official repository: https://github.com/State-of-the-Edge/glossary**

3G, 4G, 5G

3rd, 4th, and 5th generation cellular technologies, respectively. In simple terms, 3G represents the introduction of the smartphone along with their mobile web browsers; 4G, the current generation cellular technology, delivers true broadband internet access to mobile devices; the coming 5G cellular technologies will deliver massive bandwidth and reduced latency to cellular systems, supporting a range of devices from smartphones to autonomous vehicles and large-scale IoT. Edge computing at the infrastructure edge is considered a key building block for 5G.

Access (Edge Layer)

The sublayer of infrastructure edge closest to the end user or device, zero or one hops from the last mile network. For example, an edge data center deployed at a cellular network site. The Access Edge Layer functions as the front line of the infrastructure edge and may connect to an aggregation edge layer higher in the hierarchy.

Access Network

A network that connects subscribers and devices to their local service provider. It is contrasted with the core network which connects service providers to one another. The access network connects directly to the infrastructure edge.

Aggregation (Edge Layer)

The layer of infrastructure edge one hop away from the access layer. Can exist as either a medium scale data center in a single location or may be formed from multiple interconnected micro data centers to form a hierarchical topology with the access edge to allow for greater collaboration, workload failover and scalability than access edge alone.

Autonomous Vehicle

A vehicle capable of navigating roadways and interpreting traffic-control devices without a driver actively operating any of the vehicle's control systems. In the case of the autonomous vehicle, the contextual edge becomes an integrated component of in-vehicle computing and applications that provide autonomous and extreme low-latency processing.

Availability

The ability of a system to maintain above average levels of uptime through design and resiliency characteristics. At the edge, availability is even more important due to the unique requirements of the use cases and the compute support necessary. Due to the distributed nature of edge data systems, they will be able to provide the high availability required.

Central Office (CO)

An aggregation point for telecommunications infrastructure within a defined geographical area where telephone companies historically located their switching equipment. Physically designed to house telecommunications infrastructure equipment but typically not suitable to house compute, data storage and network resources on the scale of an edge data center due to their inadequate flooring, as well as their heating, cooling, ventilation, fire suppression and power delivery systems.

Central Office Re-architected as Data Center (CORD)

An initiative to deploy data center-level compute and data storage capability within the CO. Although this is often logical topologically, CO facilities are typically not physically suited to house compute, data storage and network resources on the scale of an edge data center due to their inadequate flooring, as well as their heating, cooling, ventilation, fire suppression and power delivery systems.

Centralized Data Center

A large, often hyperscale physical structure and logical entity which houses large compute, data storage and network resources which are typically used by many tenants concurrently due to their scale. Located a significant geographical distance from the majority of their users and often used for cloud computing.

Cloud Computing

A system to provide on-demand access to a shared pool of computing resources, including network servers, storage, and computation services. Typically utilizes a small number of large centralized data centers and regional data centers today.

Cloud Native Network Function (CNF)

A Virtualized Network Function (VNF) built and deployed using cloud native technologies. These technologies include s, service meshes, microservices, immutable infrastructure and declarative APIs that allow deployment in public, private and hybrid cloud environments through loosely coupled and automated systems.

Cloud Node

A compute node, such as an individual server or other set of computing resources, operated as part of a cloud computing infrastructure. Typically resides within a centralized data center.

Co-Location

The process of deploying compute, data storage and network infrastructure owned or operated by different parties in the same physical location, such as within the same physical structure. Distinct from Shared Infrastructure as co-location does not require infrastructure such as an edge data center to have multiple tenants or users.

Cooked Data

This data set is raw data that has been analyzed and processed, also known as cooked.

Core Network

The layer of the service provider network which connects the access network and the devices connected to it to other network operators and service providers, such that data can be transmitted to and from the internet or to and from other networks. May be multiple hops away from infrastructure edge computing resources.

Data Center

A purpose-designed structure that is intended to house multiple high-performance compute and data storage nodes such that a large amount of compute, data storage and network resources are present at a single location. This often entails specialized rack and EDC systems, purpose-built flooring, as well as suitable heating, cooling, ventilation, security, fire suppression and power delivery systems. May also refer to a compute and data storage node in some contexts. Varies in scale between a centralized data center, regional data center and edge data center.

Decentralized, Distributed Architecture OR Distributed Edge Cloud Architecture

Distribution of computing power and equipment at the edge of the network spread across different physical locations to provide closer proximity to the use cases of said compute. Components are presented on different platforms and several components can cooperate with one another over a communication network in order to achieve a specific objective or goal. A distributed system is a system whose components are located on different networked computers, which then communicate and coordinate their actions by passing messages to one other.

Device Edge

Edge computing capabilities on the device or user side of the last mile network. Often depends on a gateway or similar device in the field to collect and process data from devices. May also use limited spare compute and data storage capability from user devices such as smartphones, laptops and sensors to process edge computing workloads. Distinct from infrastructure edge as it uses device resources.

Device Edge Cloud

An extension of the edge cloud concept where certain workloads can be operated on resources available at the device edge. Typically, does not provide cloud-like elastically allocated resources, but may be optimal for zero-latency workloads.

Distributed Computing

A Compute Model that has shared software resources across multiple computing systems to allocate processing needs. Using multiple distributed computing systems helps you improve efficiency and performance because you can pool resources, so they don't max out processing units or graphics cards.

Edge Computing

The delivery of computing capabilities to the logical extremes of a network in order to improve the performance, operating cost and reliability of applications and services. By shortening the distance between devices and the cloud resources that serve them, and also reducing network hops, edge computing mitigates the latency and bandwidth constraints of today's Internet, ushering in new classes of applications. In practical terms, this means distributing new resources and software stacks along the path between today's centralized data centers and the increasingly large number of devices in the field, concentrated, in particular, but not exclusively, in close proximity to the last mile network, on both the infrastructure and device sides.

Edge Cloud

Cloud-like capabilities located at the infrastructure edge, including from the user perspective access to elastically allocated compute, data storage and network resources. Often operated as a seamless extension of a centralized public or private cloud, constructed from micro data centers deployed at the infrastructure edge.

Edge Data Center (EDC)

A data center which is capable of being deployed as close as possible to the edge of the network, in comparison to traditional centralized data centers. Capable of performing the same functions as centralized data centers although at smaller scale individually. Because of the unique constraints created by highly distributed physical locations, edge data centers often adopt autonomic operation, multi-tenancy, distributed and local resiliency and open standards. Edge refers to the location at which these data centers are typically deployed. Their scale can be defined as micro, ranging from 50 to 150 kW of capacity. Multiple edge data centers may interconnect to provide capacity enhancement, failure mitigation and workload migration within the local area, operating as a virtual data center.

Edge Node

A compute node, such as an individual server or other set of computing resources, operated as part of an edge computing infrastructure. Typically resides within an edge data center operating at the infrastructure edge and is therefore physically closer to its intended users than a cloud node in a centralized data center.

Far Edge

A potential site location where the compute model even closer to the end user but utilizing smaller devices and newer technologies to bring local computation further away from the core site and into rural, isolated or desolate areas. These edge sites are relative to and commonly defined by Utility, Radio or Cell Sites.

Fog Computing

A distributed computing concept where compute and data storage resource, as well as applications and their data, are positioned in the most optimal place between the user and Cloud with the goal of improving performance and redundancy. Fog computing workloads may be run across the gradient of compute and data storage resource from Cloud to the infrastructure edge. The term fog computing was originally coined by Cisco. Can utilize centralized, regional and edge data centers.

Infrastructure Edge

Edge computing capability, typically in the form of one or more edge data centers, which is deployed on the operator side of the last mile network. Compute, data storage and network resources positioned at the infrastructure edge allow for cloud-like capabilities similar to those found in centralized data centers such as the elastic allocation of resources, but with lower latency and lower data transport capacity due to a higher degree of locality to user than with a centralized or regional data center.

Inner Edge

A potential site location for an edge data center that is being utilized is in a traditional environment such as an existing 942-B data center, building or any facility that uses traditional compute models. This edge model can be a proximity site inside a traditional 942-B data center environment in a rural area or even at the bottom of a basement where traditional applications reside. These edge sites are relative to and additionally commonly by Core and Aggregation Sites.

Intelligent device

This is any equipment, machine or instrument that has its own computing capability. Aside from personal computers and smart phones, examples include cars, home appliances and medical equipment.

Interconnection

The linkage, often via fiber optic cable, that connects one party's network to another, such as at an internet peering point, in a meet-me room or in a carrier hotel. The term may also refer to connectivity between two data centers or between tenants within a data center, such as at an edge meet me room.

Internet Edge

A sub-layer within the infrastructure edge where the interconnection between the infrastructure edge and the internet occurs. Contains the edge meet me room and other equipment used to provide this high-performance level of interconnectivity.

Internet Exchange Point (IXP)

Places in which large network providers converge for the direct exchange of traffic. A typical service provider will access tier 1 global providers and their networks via IXPs, though they also serve as meet points for like networks. IXPs are sometimes referred to as Carrier Hotels because of the many different organizations available for traffic exchange and peering. The internet edge may often connect to an IXP.

Internet of Things (IoT)

A large increase in machine-to-machine communication will produce large increases in bandwidth requirements. Machine response times are many times faster than human interactions, creating even more opportunities to benefit from ultra-low latency communication. Data traffic patterns will change, with local peer-to-peer relationships and localized IoT data/control systems generating data that does not need to traverse backhaul links that will be hard pressed to carry the flood of traffic to come. Distributed EDCs will transform large volumes of raw data into valuable information that can then be transferred to more centralized DCs where required.

IP Aggregation

The use of compute, data storage and network resources at a layer beyond the infrastructure edge to separate and route network data received from the cellular network RAN. Although it does not provide the improved user experience of local breakout, IP aggregation can improve performance and network utilization when compared to traditional cellular network architectures.

Jitter

The variation in network data transmission latency observed over a period of time. Measured in terms of milliseconds as a range from the lowest to highest observed latency values which are recorded over the measurement period. A key metric for real-time applications such as VoIP, autonomous driving and online gaming which assume little latency variation is present and are sensitive to changes in this metric.

Latency

In the context of network data transmission, the time taken by a unit of data (typically a frame or packet) to travel from its originating device to its intended destination. Measured in terms of milliseconds at single or repeated points in time between two or more endpoints. A key metric of optimizing the modern application user experience. Distinct from jitter which refers to the variation of latency over time. Sometimes expressed as Round-Trip Time (RTT).

Latency Critical Application

An application that will fail to function or will function destructively if latency exceeds certain thresholds. Latency critical applications are typically responsible for real-time tasks such as supporting an autonomous vehicle or controlling a machine-to-machine process. Unlike Latency Sensitive Applications, exceeding latency requirements will often result in application failure.

Last Mile

The segment of a telecommunications network that connects the service provider to the customer. The type of connection and distance between the customer and the infrastructure determines the performance and services available to the customer. The last mile is part of the access network and is also the network segment closest to the user that is within the control of the service provider. Examples of this include cabling from a DOCSIS headend site to a cable modem, or the wireless connection between a customer's mobile device and a cellular network site.

Lights-out management (LOM)

The ability remotely monitors and manage servers. Hardware for this setup comes in a module and logging software, which tracks microprocessor utilization and temperature within the edge data center.

Network functions virtualization (NFV)

A network architecture concept that uses the technologies of IT virtualization to virtualize entire classes of network node functions into building blocks that may connect, or chain together, to create communication services.

Raw data

This data is collected but not applied to any specific use case; sometimes, it is automatically filed into a database before any type of processing. This raw data can come from a variety of devices and infrastructure components that are a part of the company's IT network.

Redundancy

Redundancy is typically defined as the inclusion of extra components which are not required for function, but to provide continued availability in the event of a failure. Part of the RAS Model

Shared Infrastructure

The use of a single piece of compute, data storage and network resources by multiple parties, for example two organizations each using half of a single edge data center, unlike co-location where each party possesses their own infrastructure.

Outer Edge

A potential site location where the compute model is moving away from traditional data center space and into a containerized or similar type harden solutions outside on the edge near rural areas. The outer edge brings local computation closer to the end user. These edge sites are relative to and commonly defined by Aggregation and Access Sites.

Survivability

Survivability is defined in how it relates to the percentage of time a facility is actually available versus the total time it should be available to provide operational continuity and resiliency.

Unmanned Edge Data Centers

Due to their size and distributed nature, most edge data centers are expected to be unmanned, creating new security (surveillance, anchoring, alarms, etc.), maintenance (additional monitoring systems and sensors), operational (increased automation), and resiliency considerations that do not exist with manned data centers.

APPENDIX B: REFERENCES

1. NEMA Standards Publication 250-2003, Enclosures for Electrical Equipment (1000 Volts Maximum)
2. ANSI/TIA-942-B-2017 Telecommunications Infrastructure Standard for Data Centers
3. TIA-607-D Generic Telecommunications Bonding and Grounding (Earthing) for Customer Premises
4. Ethernet Alliance. (2019). Product Roadmap. Retrieved from ethernetalliance.org: https://ethernetalliance.org/the-2019-ethernet-roadmap/
5. Fiber Channel Industry Association. (2019). FCIA. Retrieved from fibrechannel.org: https://fibrechannel.org/roadmap/
6. ASHRAE, Thermal Guidelines for Data Processing Environments, Fourth Edition
7. Montstream, C. (2016, June 21). ANSI/TIA-607-C: A newly released version of a standard that has come a long way. Retrieved from https://www.cablinginstall.com/standards/cabling-standards/article/16465183/ansitia607c-a-newly-released-version-of-a-standard-that-has-come-a-long-way.
8. Telcordia (n.d.). Retrieved from https://telecom-info.telcordia.com/site-cgi/ido/docs.cgi?ID=220374802SEARCH&DOCUMENT=GR-347. Covers: GR-347, GR-63, GR-1275, GR-209, and GR-492 Standards
9. BICSI International Standards Program. (n.d.). Retrieved from https://www.bicsi.org/standards/bicsi-standards/standardization. Covers: TIA/ANSI Standards for the ICT Community
10. UL Standards. (n.d.). Retrieved from https://ulstandards.ul.com/. Covers: UL 507, UL PQVA, UL 115, UL 139 and other UL standards not defined in this article
11. NFPA, Codes-and-Standards. (n.d.). Retrieved from https://ulstandards.ul.com/. Covers: NFPA 75, NFPA 76 and NFPA 70 standards
12. The Global Data Center Authority. (n.d.). Retrieved from https://uptimeinstitute.com/

** Disclaimer: The information and views contained in this article are solely those of its authors and do not reflect the consensus opinion of TIA members, TIA or TIA Engineering Committee TR-42. This article is for information purposes only and it is intended to generate opinion and feedback so that the authors and TIA members can learn, refine, and update this article over time. The Telecommunications Industry Association does not endorse or promote any product, service, company or service provider. Photos and products used as examples in this paper are solely for information purposes and do not constitute an endorsement by TIA.*