Peerless Network Inc – Business Continuity Brief

Summary: Peerless Network Inc. recognizes the impact unforeseen circumstances can have on its customers, network and business. To prepare for such emergencies, the company has developed extensive disaster recovery and business continuity plans. These plans continue to evolve with the company's growth and due to ongoing changes in the business environment.

Business Continuity Philosophy: At Peerless, we view disaster preparedness and business continuity planning not as a list of hypothetical responses to unknown events, but as a continuous commitment to resiliency, redundancy and survivability in our network, processes and organization. Preparedness, recovery and continuity are at the core of our operational decisions. Since inception, Peerless has evolved into an organization not dependent upon any one locale, individual, group or network element. The company's people and network are distributed across multiple locations, each of which can operate the larger whole independently at a moment's notice.

Business Continuity Program: Our business continuity program is aligned to the ISO22301 Business Continuity Management System and the Business Continuity Institutes' Good Practice Guidelines. Under ISO 22301, Business continuity is defined as capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption. The goal of our BCM Program is to effect continual improvement of developed strategies, plans and processes and to ensure that our approach reflects the Plan-Do-Check-Act (PDCA) cycle as identified in ISO 22301.

Business Continuity Team: Business Continuity planning and real-time decision making is driven by the management team and key leadership from operations (NOC management, Service Delivery), Engineering (Network, Voice, Sustaining and Systems), IT, Finance and Customer Care. All members of this team are backed up by secondary staff within their organizations should they become incapacitated or otherwise unavailable.

Redundancy and Diversity – Network and Organization: The Company operates geo-redundant Network Operations Teams in Chicago, IL and Denver, CO, each of which is fully staffed, and capable of operating without the other. Key operational staff (Sustaining Engineering, IT and Operations), in the Denver area are fully capable of supporting the entire business from in the event of a catastrophic event in Chicago, and vice versa. All staff are equipped to work remotely as needed, whether by choice or in the event of natural disaster, government mandate or due to global pandemics.

The Peerless Network spans multiple sites across the United States and Europe, six of which function as its key switching nodes. Each of the key sites is capable of providing call control and routing for the entire network at a moment's notice.

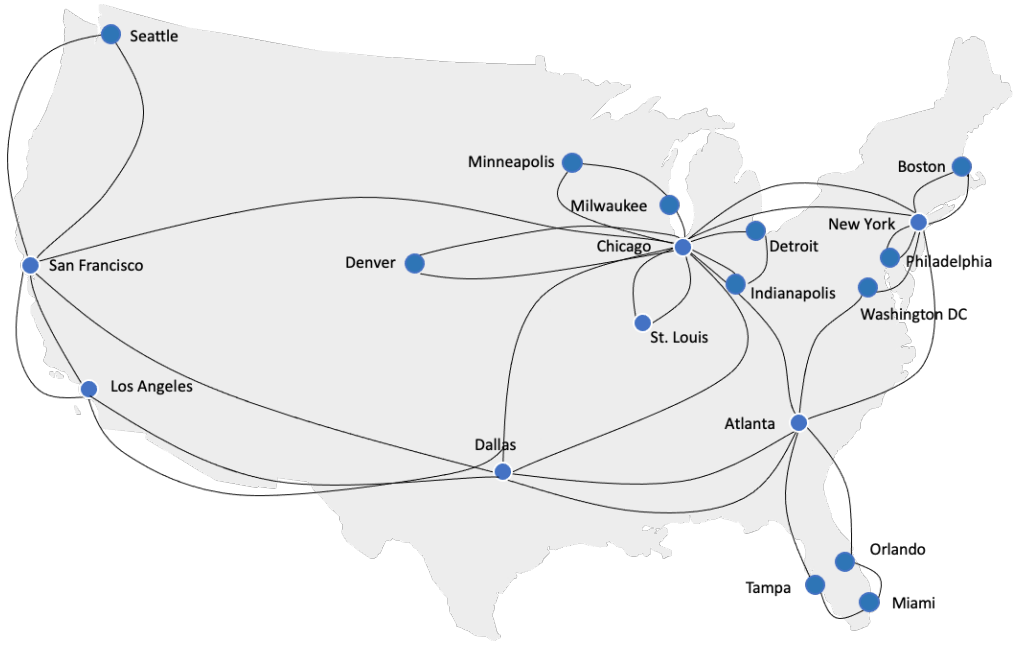

Figure 1 - Peerless Network US Core Backbone

Peerless' Backbone Network consists of aggregated links from various providers on completely diverse physical fiber paths and equipment. All sites in the core network have diverse connectivity to at least two other sites, and often more. All equipment is provisioned with the maximum possible hardware redundancy, whether 1+1 for common control elements or 1+1 or N+1 for linecards.

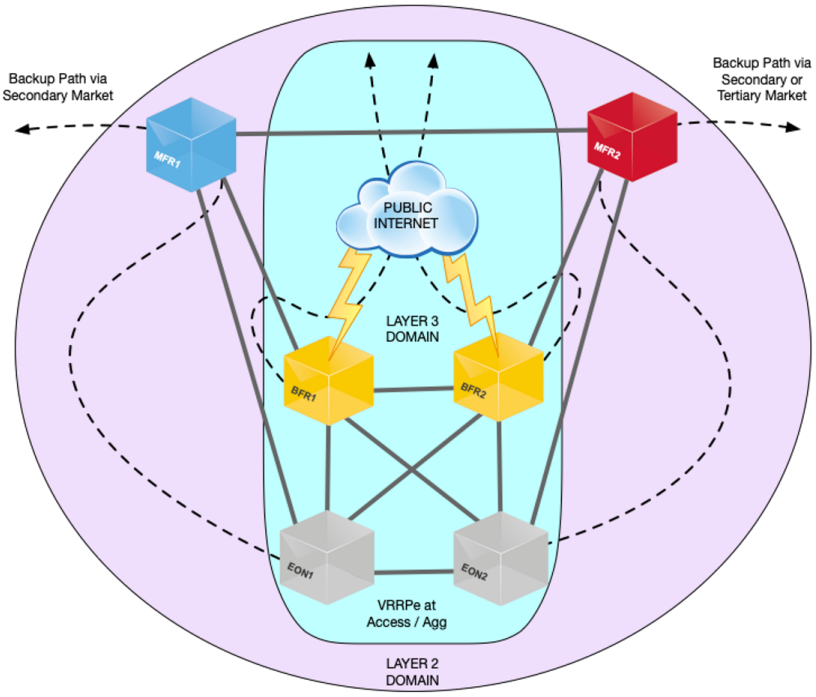

Figure 2 - Example Core IP POP Topology

Voice Switching and Call control elements are deployed with both local (N+1 or 1+1) and geographic redundancy. For example, our Session Border controllers are always deployed as mated pairs in an active / standby model. In the event one node in the pair suffers a hardware or software failure, the other node can takeover call processing without impact to new call setup or calls in process. Key call control elements are disturbed throughout the network, and all clients of these nodes are configured to use both local resources within their own location (intraPOP), and beyond when necessary (InterPOP). All customers are strongly encouraged to configure connections to multiple geographic locations to ensure local events (Fire, Flood, Storms, Power, etc) do not compromise global service availability.

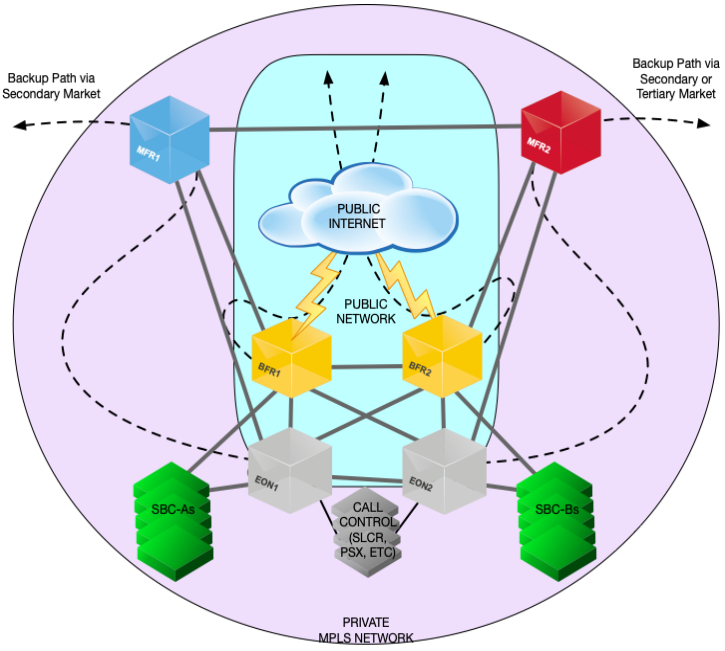

Figure 3 – Redundant Switching and Call Control Topology

All equipment is installed within carrier grade data centers, operated be industry leaders, such as Digital Realty, Equinix and Coresite, or by Peerless itself. In all cases, these locations provide generator protected power, multiple diverse utility feeds, redundant HVAC and extensive physical security. All have security measures in place necessary to achieve PCI SOC1 and 2 compliance.

In each market we serve, the company has built redundant and diverse local connectivity to all key Local Exchange Carriers (LECs) and InterExchange Carriers (ICXs). While IP connections are preferred for efficiency and resilience, TDM is still required by many LECs for local interconnections. To ensure our network resilience during failure scenarios, these TDM connections are provisioned over multiple diverse Competitive Access Providers (CAPs) within each local market:

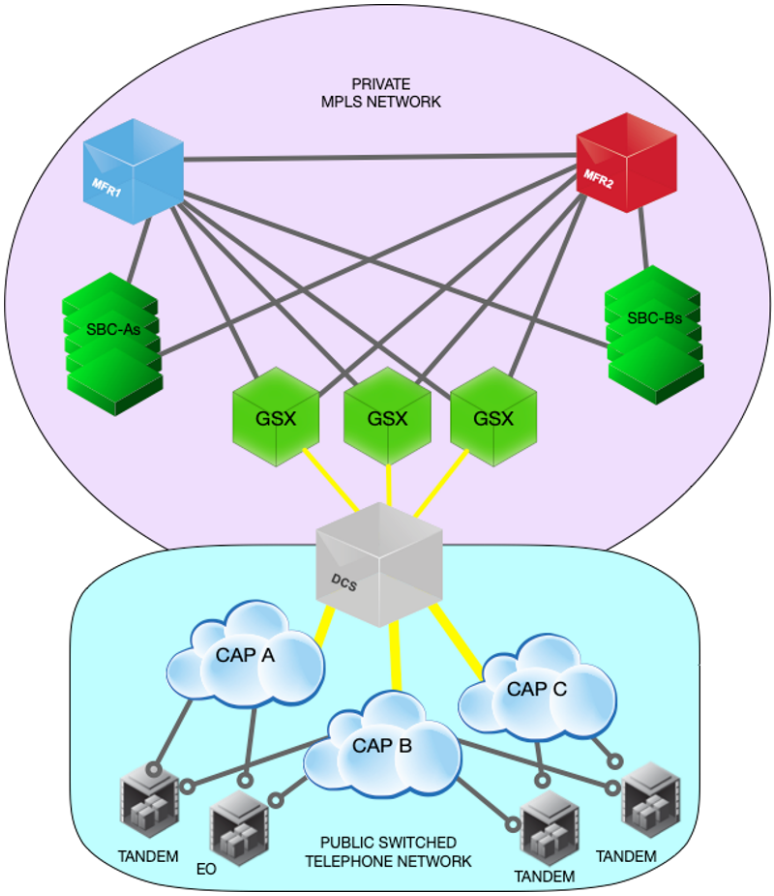

Figure 4 – Local TDM Access design

Internal Systems are mirrored between the company's two primary data centers in Chicago and Atlanta. Most systems are dual provisioned on a VMWare Hypervisor stack in each location, with some configured as active / active or active / standby, while less critical or non-realtime systems are provisioned as cold spares in their designated backup location (most often Atlanta, but occasionally Chicago when Atlanta is primary). Paired and mirror SAN arrays (Nimble and more recently Dell / EMC) provide storage for these Hypervisor clusters, and regular snapshots serve as a secondary recovery mechanism.

In the event of a complete failure or destruction of a data center due to local events (e.g. fire, flood, storms, natural disaster, civil disturbance, terrorism, etc), Peerless is able to reprovision services on geographically distant nodes to restore service to impacted customers within defined recovery point objectives. The only factor limiting complete restoration of services is potential impact to the network facilities of other carriers, such as the ILEC or Wireless provider access infrastructure. In such events, the Peerless Network often becomes key to maintaining interconnections between remaining carriers. In last two decades, Peerless has been critical to

maintaining telecom services for millions of businesses and consumers during catastrophic events, including the Nashville bombing and Superstorm Sandy.

Business Continuity Testing and Review: While non-production drills of recovery procedures have their place, our continuity processes are part of our normal course of business. When not tested during normal operations, these recovery options are tested and verified annually. Business continuity plans are reviewed semiannually, or immediately when warranted by a significant change in the company or business climate. As of 2023, existing business continuity plans are also under review by the corporate security and BCM teams of our parent company, Infobip, and are subject to annual internal and external audits.

Author's Note: *Peerless Network was acquired by Infobip in July, 2022. While this briefing describes of current BCM planning and practices, we are actively revising and improving our plans to be consistent with those of our global parent. We expect to have a revised plan and briefings available by end of 2023.*