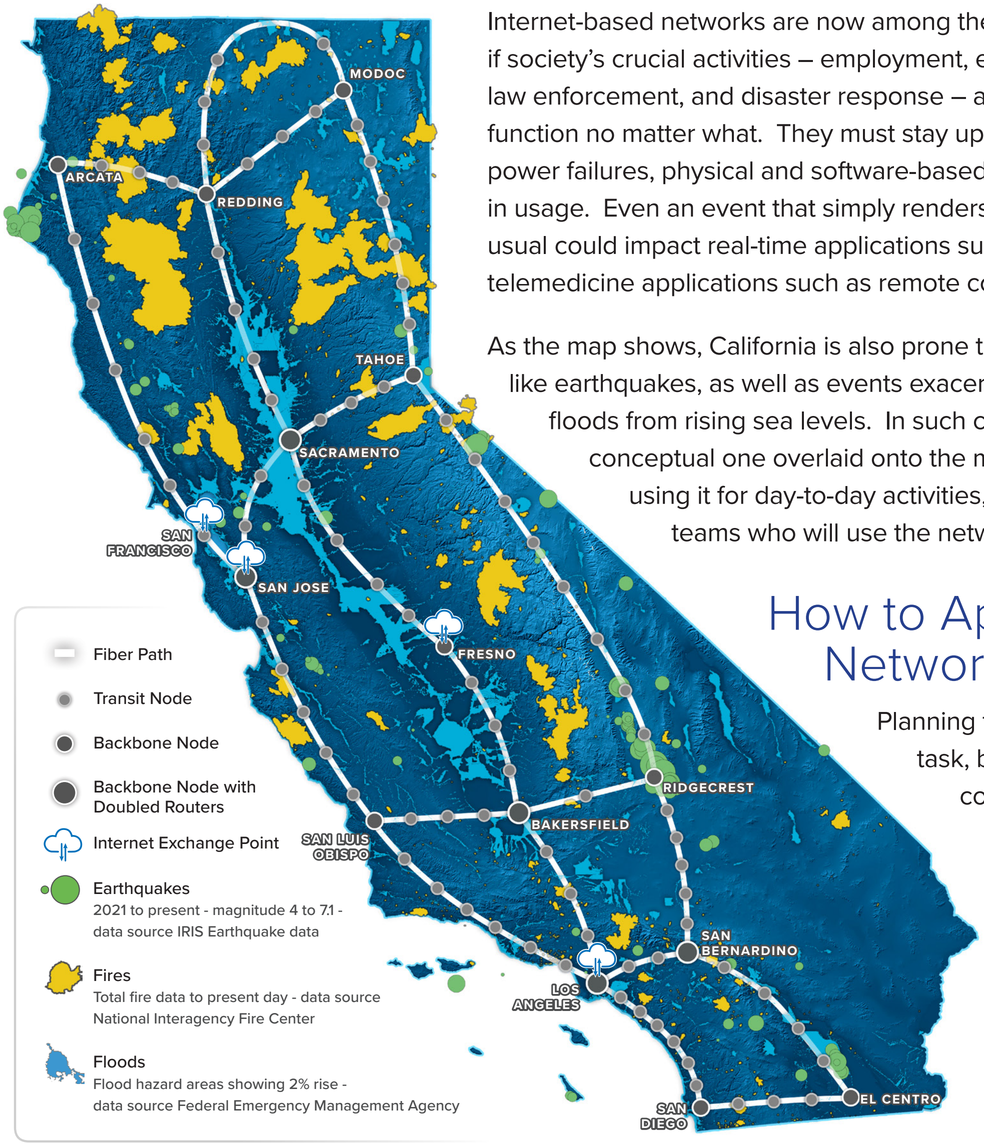
CENIC

Building a Statewide Middle-Mile Network Series: 005

Resilient Communities Need Resilient Networks


MODOC
ARCATA
REDDING
TAHOE
SACRAMENTO
SAN FRANCISCO
SAN JOSE
FRESNO
RIDGECREST
BAKERSFIELD
SAN LUIS OBISPO
SAN BERNARDINO
LOS ANGELES
SAN DIEGO
EL CENTRO
Fiber Path
Transit Node
Backbone Node
Backbone Node with Doubled Routers
Internet Exchange Point
Earthquakes
2021 to present - magnitude 4 to 7.1 - data source IRIS Earthquake data
Fires
Total fire data to present day - data source National Interagency Fire Center
Floods
Flood hazard areas showing 2% rise - data source Federal Emergency Management Agency

Internet-based networks are now among the world's foundational infrastructures, and if society's crucial activities – employment, education, commerce, healthcare, utilities, law enforcement, and disaster response – are to take place, these networks must function no matter what. They must stay up and run in the face of equipment and power failures, physical and software-based attacks, disasters, or even sudden spikes in usage. Even an event that simply renders a middle-mile network slightly slower than usual could impact real-time applications such as video meetings, online testing, or telemedicine applications such as remote consults and pacemaker monitoring.

As the map shows, California is also prone to a variety of large-scale natural events like earthquakes, as well as events exacerbated by climate change like wildfires and floods from rising sea levels. In such cases, a middle-mile infrastructure like the conceptual one overlaid onto the map must remain working not only for those using it for day-to-day activities, but also for the disaster management teams who will use the network to respond to the event.

How to Approach Resilient Network Design

Planning for network resilience is a complex task, but a network design team and their collaborators can approach it by asking the following three key questions at the bottom of the page.

This three-part approach will result in a middle-mile network that can withstand expected problems (cuts, outages, attacks, traffic spikes, etc.) and continue to support well-defined crucial applications, access, and security.

What Might Happen?

This can include natural disasters, equipment or power failures, sudden traffic spikes, and deliberate or accidental interference anywhere along the network, such as fiber cuts.

A network design team will also factor in range, likelihood, frequency, and severity.

What Activities Are Critical?

This can include functions like videoconferencing, data storage access, disaster management, and important enterprise-level activities like payroll.

The network design team and their collaborators may decide to perform industry and customer research to identify them.

What's The Budget?

The project budget and spending requirements can inform when and how much fiber, construction, software, equipment, personnel, power, etc. can be purchased.

This can also inform where partnering is preferable, which resources are most available, and which supply chains are acceptable.

Basic Guiding Principles for Resilient Design

While carrying out the above discovery and design process, a network design team and their collaborators will keep the following basic guidelines in mind as decisions are made to ensure that the network supports those who use it with the required level of performance and resilience, now and in the future.

DATA & ACTIVITIES NEED MULTIPLE PATHS

This includes network traffic as well as maintenance, power and management activities, and supply chains. This means parallel design, multiple backups, and no single points of failure.

DOCUMENTATION & PROCESS ARE KEY

Parallel design increases complexity and the potential for unforeseen network behavior in response to events. Solid documentation and well-socialized procedures mitigate this.

KEEP & REVIEW PERFORMANCE METRICS

Metrics should extend beyond network behavior to things like internal, vendor, and partner performance, so overall resilience can be studied and used to inform improvements.

The Guiding Principles in Action

When these principles are applied to middle-mile infrastructure, the end result is a network – and a society – that can function, respond, adapt, and even thrive in the face of challenges, including public safety challenges when the network is most needed while itself under threat.

FIBER PATHS AND CONNECTION POINTS

Well-designed middle-mile network topologies feature path “rings” so traffic can still flow even if a path is cut. Nearly all traffic will traverse long-haul routes and core routers, which must support high use. Regional routes also use ring topologies ideally terminating on different backbone routes, with “spurs” – routes not connecting back to the network – used rarely if at all, especially not without a separate return path (e.g. a fixed wireless path) to the network backbone to provide resilience.

NETWORK EQUIPMENT

If equipment stops functioning for any reason, standby equipment that can instantly take over is needed. Ideally this process, known as “failover,” happens transparently so anyone using the network during the event will not even realize it has happened. This can mean putting two separate “doubled” routers in place at high-traffic nodes, or doubling up equipment like line cards within a single router.

These principles are applied to more than just the network. Poorly designed management, collaboration, or documentation systems can impair a middle-mile network’s resilience as much as a poorly designed fiber route.

SOFTWARE FOR MANAGEMENT, CONTROL, AND MONITORING

Equipment failover, dynamic routing, and adapting to sudden high use all require complex software housed in multiple locations. Such software can also mitigate Distributed Denial of Service (DDoS) attacks, where a malicious attacker, perhaps thousands of miles away, floods a network with useless traffic to bring it to a practical halt.

ORGANIZATIONAL RESILIENCE

A middle-mile network operator itself must also be resilient, with no one person performing any vital function. In addition to clear, accessible, and thorough documentation; well-defined and socialized processes must be in place and followed to avoid bottlenecks and confusion.

VENDOR, SUPPLIER, AND PARTNER RESILIENCE

Resilience must also be built into relationships with vendors, suppliers, and other partners, such as purchasing electrical power or maintenance from providers on separate infrastructures and ensuring supply chain resilience so no equipment or service can be purchased exclusively from one supplier.