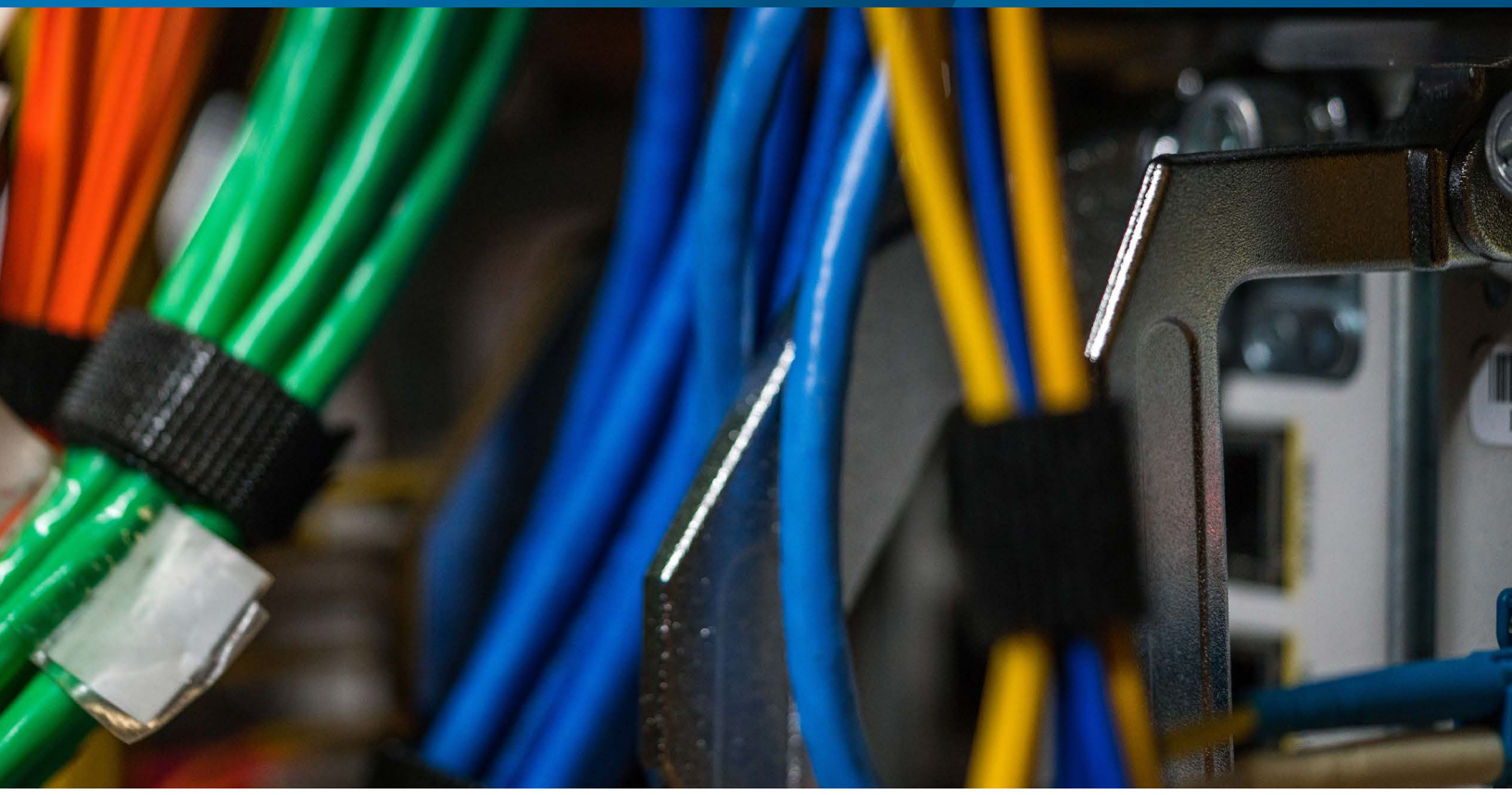
WHITE PAPER

Network diversity: The key to reliability

Four steps to evolve to true diversity



Spectrum ENTERPRISE

Table of contents

Introduction

Reliable network connectivity is critical for most businesses and enterprises today, from retail stores that depend upon fast Internet access for credit card verification to insurance companies that rely on continuous access to product and pricing databases. A variety of organizations all need Internet and data center connectivity to operate. Rather than simply being "nice to have," guaranteed access to customers, corporate offices, data centers and the Internet is vital.

Guaranteed network connectivity does not happen by accident. Networks are carefully designed and implemented to ensure that they are not exposed to network issues or failures. One way to do this is to build diversity into your network. Network diversity ensures that alternative paths are available for network traffic in the event of a failure. The goal is to ensure that end users are not exposed to network issues or failures.

This paper demonstrates four steps to design and implement a more diverse network.

The importance of network diversity

Types of network diversity

Network diversity ensures there are alternative separate paths available for network traffic in the event of a failure.

There are three different types of network diversity:

- Carrier diversity is when an enterprise selects at least two different carriers to provide network connectivity
- Access diversity refers to the capability of the network to provide backup protection for the local access circuit that connects the customer location to the service provider's central office (CO) or hub
- Transport diversity is the term for providing alternative transmission paths in the network core or cross-market section of the connection

'Redundancy' and 'diversity' mean different things

It is important to understand that "redundancy" is not the same as "diversity." For example, a network may have redundant fiber connections, but if the physical fibers are both in the same conduit then there is no route diversity, which could lead to loss of service continuity in the event of a fiber impacting event.

Similarly, if redundant circuit access equipment is located in the same data center or CO as the primary access equipment, there is no location redundancy, which could lead to loss of service in the event of a power outage. Building a fully redundant network, therefore, involves more than simply duplicating the network connections and equipment.

Benefits of access and transport diversity

But why is network diversity needed? What specific benefits do access and transport diversity provide to the end user? In the simplest terms, network diversity ensures continuity of services to a location, which is important for businesses that rely on connections to data centers, the Internet or other enterprises for their revenue. And in the case of a catastrophe or failure at the organization's main location, network diversity is an important element in an effective disaster recovery plan.

From a network perspective, true diversity provides several benefits:

- Protection for the connection to the building or enterprise in the last mile and throughout the whole network, ensuring continuous connectivity
- Alternative physical connection or access from the primary network provider
- Connection diversity in the event of failure of the primary provider's last mile, metropolitan or long-haul infrastructure, which functions as "insurance" for a network outage

Design considerations

There are several important considerations when designing a diverse network:

- **Geography** – There should be at least two diverse transmission paths for the network traffic. For example, if we consider a transcontinental network, one path should take a southern route and the other a northern route
- **Hubs, points of presence (PoPs) or COs** – For ideal performance, at least two hubs should be secured by one or more service providers supporting separate circuit transmission paths

- **Redundant equipment and electronics** – These should be provided both within the customer and the service provider networks. At the customer premises, the equipment should be located in different parts of the building
- **Uniformity in network design and build** – The platform should be uniform. A network constructed with consistent technology and ownership translates into easier control when troubleshooting network components. For example, the local network architecture and physical build should look the same in New York as it does in Los Angeles to ease problem solving

Non-diverse redundant services and their impact

Many service providers will highlight the importance of having a second service delivered to allow for network failover and offer this as an alternative to diversifying those services.

Without diversity built into the services on the service provider network, it could lead to a false sense of security, and ultimately a service impacting event.

Network failover is simply the switching of traffic to an alternative link if the primary connection fails. In the case of failure of one fiber link, for example, the traffic will failover to another circuit. However, this alternative fiber may be in the same bundle as the failed link and will terminate in the same colocation facility or CO. If the fiber bundle is severed for some reason (for example, due to road construction), then both the primary link and the failover alternative will be cut and service will be lost.

This occurrence can be avoided if the service provider uses separate routes for the active and standby fibers. But if they both terminate at the same colocation facility in the network, this introduces a potential vulnerability. If there is a physical failure at that facility, service will be lost no matter how many separate fiber routes exist from the colocation to the customer premises.

How network diversity is implemented

Building a diverse network is more complicated than simply selecting a backup service provider or deploying redundant network equipment. This section will show the four steps for building a diverse network and identify the potential points of possible failure.

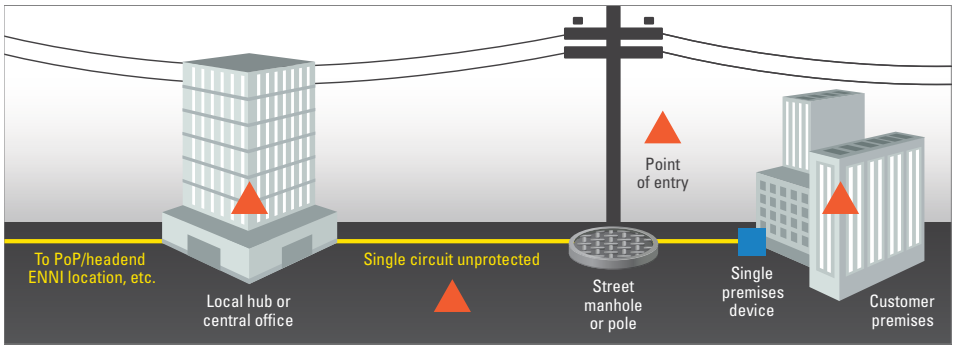
- The premises termination equipment and electronics are represented by the blue box in the customer building
- The orange triangles show the potential points of network vulnerability and failure

Baseline network architecture

The evolution to a fully diverse network starts with the baseline network design. In this network, a single circuit is connected to a single manhole or pole on the street and then to the customer premises.

- A single network hub or CO is used, which is connected to the PoP/headend, external network-to-network interface (ENNI) location
- A single circuit is used, which is unprotected
- There is a single point of entry into the customer premises from the manhole or pole
- In the customer premises, there is a single network termination device

Baseline network: Non-diverse access, single building point of entry



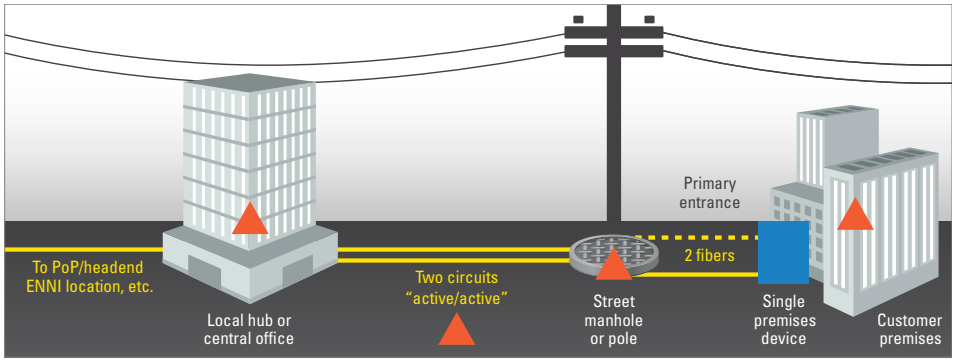
Indicates point of potential vulnerability

Step 1: Dual entrance facilities

The first step in the network evolution is to use a second entrance into the customer premises (Fig. 1). While this gives a diverse route into the building, note that potential vulnerabilities still exist with the single network termination device and with the single manhole or pole. And while two circuits connect the hub to the manhole/pole, a single hub/CO is still used.

Also, the two circuits follow the same route and could, therefore, both be cut at the same time by a single incident. The two circuits are configured as "active/active" with no protection switching.

Figure 1: Dual entrance facilities



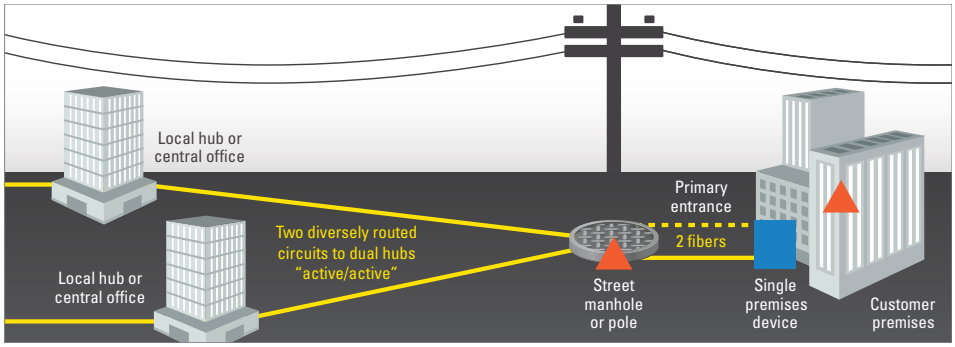
Indicates point of potential vulnerability

Step 2: Diverse hubs and routes

The next step is to use diverse hubs and diverse routes for the two circuits to the street manhole or pole (Fig. 2). Now the circuits are more secure since both cannot be cut by a single incident (this assumes the two hubs or COs are in different locations and the circuits follow completely different routes).

Now the points of failure are the single manhole or pole and the customer premises equipment.

Figure 2: Access diversity — Dual hub/single entrance facility

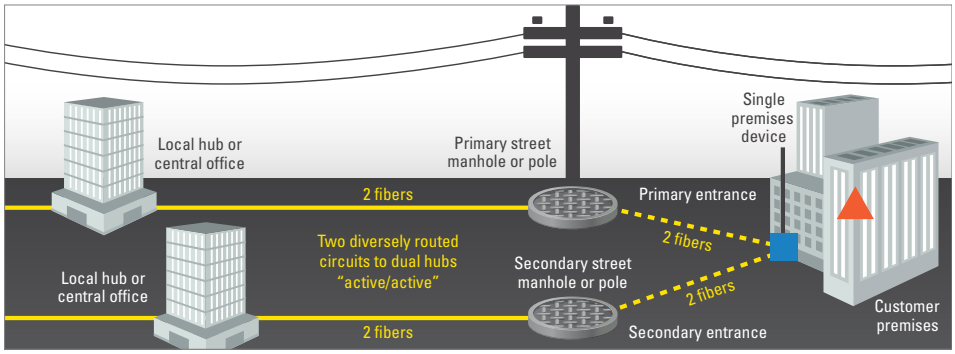


Step 3: Dual hubs, diverse routes and dual entrance facilities

Figure 3 shows how the potential weakness of the single manhole or pole can be addressed: Simply, two manholes/poles are used with separate (route-diverse) entrances into the customer premises. Also note that each of the circuits has two fibers and are route-diverse. There is also a connection between each of the manholes/poles for full route diversity.

Now, the single point of potential failure is the customer premises termination equipment. Note that while this may be a single piece of equipment, it may have very high uptime metric or have resilient device features such as redundant power supplies.

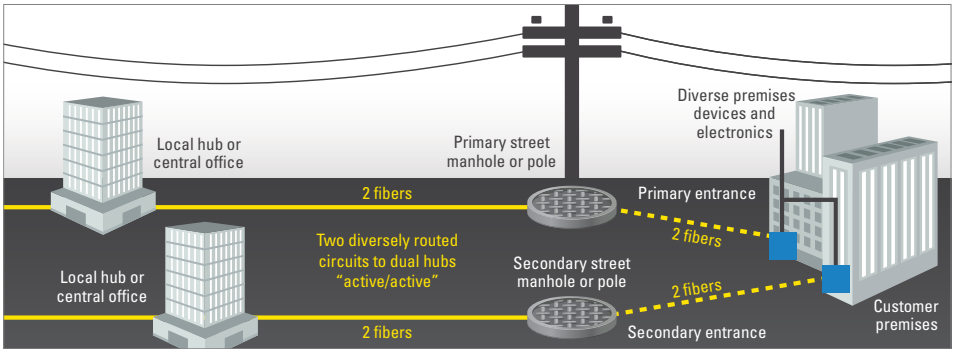
Figure 3: Dual hubs, diverse routes, dual entrance facilities



Step 4: True access diversity

The final step in the network evolution is shown in Figure 4, where separate customer premises network termination units are shown, ideally housed in separate locations in the building. The network is now considered diverse.

Figure 4: Access diversity: Dual hubs, diverse routes, dual entrance facilities



Leveraging the Spectrum Enterprise network

Spectrum Enterprise operates a nationwide network that offers diversity and specialized designs to help achieve desired reliability. Spectrum Enterprise is a recipient of the 2019 MEF Award for Enterprise Application of the Year in Manufacturing and 2018 MEF Awards for Enterprise Application of the Year in Health and Government categories and Retail Service Provider of the Year for North America. We support clients with a highly redundant and reliable fiber network. The network has more than 230,000 fiber route miles across the U.S., connecting over 217,000 buildings with fiber, making Spectrum Enterprise the fourth-largest provider of Ethernet services in the U.S.[1]

Conclusion

A reliable network is a requirement for most organizations. Guaranteed connectivity to customers, corporate offices, data centers and the Internet is critical. Yet guaranteed network connectivity does not happen by chance; truly diverse networks are the result of careful design and implementation.

Ensure diversity is a part of your network design by following the four steps to building a diverse network detailed in this paper. Only a truly diverse network protects your users — and your bottom line — from network issues or failures.

To learn how Spectrum Enterprise can help you build a highly reliable network, visit our website.

Resources

1. Vertical Systems Group, "Mid-Year 2019 U.S. Carrier Ethernet Leaderboard," (accessed 6/13/19), https://www.verticalsystems.com/2019/09/10/mid-2019-us-ethernet-leaderboard/.

ABOUT SPECTRUM ENTERPRISE

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. Spectrum Enterprise's industry-leading team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. More information about Spectrum Enterprise can be found at enterprise.spectrum.com.