NETWORKING 3.0
Network Only Provably Cryptographically Identifiable Devices

INSTANT OVERLAY NETWORKING

Highly Available  Remarkably Simple  Radically Secure
IP complexity is holding your business back

As organizations take on the challenge of digital transformation— moving towards cloud, mobility, and big data analytics — there are considerable architectural, operational, and security implications for network infrastructure. The explosion of connectivity has significantly increased the complexity of networks and expanded the available total attack surface.

The result is inflexible and complex networks that introduce costly security and networking challenges for organizations that are impractical, if not impossible, to solve. The main cause of this complexity and restricted mobility stems from a fundamental flaw in the basic framework of IP networking, which was never addressed when originally implemented.

Transforming your business with Networking 3.0

Networking 1.0 was all about simple connectivity, networking PCs and servers to give access to the early versions of IP networks. The current era, Networking 2.0, has been focused on networking everything, especially mobile devices and IoT nodes, as businesses want to take advantage of increased and converged connectivity that can provide cost-saving data for example. However, the lack of provable identity is a compounding problem that makes networking much more complex and costly. As the number of connected devices increases, so do network attack vectors, introducing significant business risk.

It’s time we evolved beyond traditional IP networking to a trusted networking architecture based on cryptographic identities.

Connect any device, anywhere in the world

We believe the time has arrived for Networking 3.0, moving beyond the old address-defined networking paradigm towards a trusted and mobile architecture. This next generation architecture fixes the broken trust model of IP networking by going from blindly networking everything with an IP address towards networking based only on provable host identities. Networking 3.0 delivers networking of only trusted and cryptographically IDENTIFIED things, enabling a much more secure and flexible network architecture.

The End of IP Address-Defined Networking

Moving beyond Address-Defined Networking to Identity-Defined Networking
IP networking is broken

In the late 1960’s, computer scientists ran an experiment connecting one computer to different computer in another building, implementing the basic framework of IP networking. Since end-to-end networking was the only goal at the time, not endpoint mobility or security, TCP/IP was designed in a way that aligned with connectivity. The IP address took on a dual function, determining the name and network location of a machine on the internet (identifier and locator).

The problem was the scope of the experiment kept growing, and 45+ years later, it is still going. However, because the IP address should really only be used for location, the very foundation of this experiment was flawed from the beginning as the dual-use function of the IP address lacks the basic mechanisms for flexibility and security.

This fundamentally flawed architecture forces IT teams to perform a lot of time-consuming and meticulous tasks on a daily basis with box-by-box configuration of switching, routing, firewall rules, VPN policies, creating VLANs and mapping them across switches and uplinks, and on and on. This process is ineffective and costly. At Tempered Networks, we believe a different approach is needed that is simple, flexible, and secure.

"If I could turn back time, I would go back and do a better job on trusted authentication and mobility, which we did a very poor job with and are paying for now, with additional hard work."

Vint Cerf, father of TCP/IP

Host Identity Protocol - a fundamental evolution of IP networking

Tempered Networks is the first to commercially leverage the Host Identity Protocol (HIP), an open standard network security protocol which provides provable host identities. Recognized by the Internet Engineering Task Force (IETF) community as the next possible big change in IP architecture, HIP is a paradigm shift in networking that solves the fundamental flaw in TCP/IP created by the dual use of IP addresses.

The protocol was formally ratified by the IETF in 2015, which crowned over 15 years of development, testing and deployment in co-ordination with several large companies (such as Boeing, Ericsson, Nokia, Verizon, TeliaSonera) and standard bodies (Trusted Computing Group, IEEE 802).

HIP separates the role of an IP address as both host identity and topological location, where hosts are instead identified using strong cryptographic identities in the form of 2048-bit RSA public keys. By binding permanent, location-independent cryptographic identities to machines or networks, security is enabled by default with verifiable authentication, authorization, and host-to-host encryption.

Recommended Reading

Article: Washington Post - Net of Insecurity: A flaw in the TCP/IP design
Whitepaper: A Primer on HIP (Host Identity Protocol) by Dr. Andrei Gurtov
Book: Host Identity Protocol (HIP): Towards the Secure Mobile Internet (Wiley Series on Communications Networking)
Book: Beyond HIP: Then End of Hacking As We Know It – by Richard Paine
The Host Identity Namespace

Currently there are two globally deployed namespaces that allows us to uniquely identity a host or service on the network: IP addresses and DNS names. However, due to the fundamental flaw of TCP/IP, both namespaces have several shortcomings. HIP introduces a third namespace, the Host Identity Namespace (HIN), which is backwards compatible and complimentary to the current namespaces. The HIN is what provides global IP mobility and migration, overcoming many of the fragile and costly challenges associated with traditional networking. Networking and security policies are now based on unique cryptographic identities, not spoofable IP addresses.

Improving the outdated OSI model

The left side of the diagram below shows the structure of the current IP stack, where routing is done via IP addresses. The upper layers of the OSI model represent software that implements network services like encryption and connection management, and the lower layers of the OSI model implement hardware-oriented functions like routing, addressing, and flow control.

On the right side, HIP takes place as a shim in the stack between the network and transport layers (i.e. Layer 3.5). Now the applications and transport protocols use the host identity tag in their traffic, instead of the IP address. Each host is now identified on the network with a unique cryptographic identity, while the IP address is used only for location. Transmission of the packet afterward follows the same pattern as in a regular IP stack.

Identity-Defined Networking: An industry first

Our technology is the first commercially available solution to assign a cryptographic identity to every IP-enabled device, and enable easy orchestration of these identities across physical, virtual, and cloud domains, creating a unified networking and security fabric.

The future of networking: orchestration of provable host identities

Our vision is to make provable host identities to all networked things the cornerstone of unifying and simplifying networking and security, making it easier than ever before to give the right devices and individuals access to the right resources. The IDN design objective is based on the principle that it must be easy to connect, cloak, segment, move, failover, and disconnect networks and individual resources.

Our approach is not only a fraction of the cost of alternatives, but also the only simple approach focused on making the vision of a secure and flexible Internet a reality. It’s simply never been possible – until now.
Identity-Based Routing

Identity-based routing offers a game-changing approach to secure host-to-host connectivity for previous un-routable systems and devices. The result is a new identity networking paradigm where security and networking are unified, and the security perimeter is set where it belongs – at the host or service level. By moving towards an identity-first architecture based on provable cryptographic identities, our customers are now uniquely capable of bridging layer 2 and layer 3 networks, without modifications to underlying switching and routing infrastructure. For the first time, it’s simple and fast to connect, segment, encrypt, and disconnect any networked device over separate networks, across physical, virtual, and cloud domains.

Evolve without disruption with a proven technology

The technology has been in production for over 12 years at a Fortune 100 company, until recently commercialized for the broader market. It’s a proven alternative to traditional networking that enables a network virtualization fabric-based architecture, where all aspects of the network are for the first time software-defined, encrypted, segmented, cloaked, and orchestrated.

The IDN fabric is non-disruptive and can be deployed over any IP network, and is extensible across all networking domains: physical, virtual, and cloud. Unlike traditional IP networking and SD-WAN approaches, our solution requires few, if any, changes to the underlying network or security infrastructure, significantly reducing complexity and the risk of human errors.

This proven and effective approach to networking enables organizations to achieve superior flexibility, security, and economics. It’s the industry’s first comprehensive and scalable networking platform that addresses enterprise-wide requirements.

A simpler, more secure networking architecture

**Architecture**: An integrated approach to augment the enterprise network with secure host-to-host connectivity anywhere in the world with trusted authentication, encryption, and easy orchestration.

**Security**: Host authentication using permanent-location independent cryptographic identifiers with end-to-end encryption (AES-256), unbreakable segmentation, and cloaking.

**Mobility**: Simplified and consistent global IP mobility and migration become a reality across the IDN’s Host Identity Namespace, with minimal changes to underlying infrastructure.

**Simplicity**: A powerful orchestration engine makes it incredibly easy to manage your network, even when scaling to thousands of devices.
A simple deployment

**IDN Fabric = easy policy orchestration + networking enforcement**

In an identity-first architecture, all provable host identities across the fully encrypted fabric are centrally managed through the Conductor, a powerful management and orchestration engine. As the intelligence behind an IDN deployment, the Conductor was designed with an ‘orchestration and manageability first’ mindset, making it incredibly easy to manage your network, even when scaling to tens of thousands of devices.

Tempered Networks' HIP Services are software products delivered in different form factors to support our design principle of secure networking for any device, anywhere. The HIP Service endpoints are available in flexible deployment options that span nearly any type of resource, location, or environment, and act as identity enforcement points within the IDN fabric.

The last thing organizations want is a different security and networking architecture for their physical IT environment, another for their physical industrial and manufacturing environment, a different one for their virtual environment, and yet another for their cloud environment and workloads. Having different architectures and narrowly focused solutions only adds more complexity, which opens up vulnerabilities and makes secure networking more difficult, costly and ineffective.

With the IDN fabric, securely networking and managing thousands of endpoints across physical, virtual, and cloud environments is now for the first time easy and practical.

**Top Customer Use Cases**

- **VENDOR-NET: ADVANCED THIRD PARTY ACCESS CONTROL**
  Segmented third party access with instant provisioning and revocation - down to host level.

- **FLEXIBLE NETWORK EXTENSION**
  Secure connectivity for an IP resource across layer 2/3 networks over wired, Wi-Fi, cellular, and serial over IP.

- **INTER- AND INTRA-CLOUD NETWORKING**
  Secure, cross-realm connectivity and segmentation across private / public clouds

- **REMOVE CONSTRAINTS OF IP CONFLICTS**
  Move any resources across subnets, networks, and clouds, without IP address conflicts

- **SECURE NETWORKING FOR IOT, M2M, & LEGACY DEVICES**
  Enable secure and scalable connectivity for vulnerable devices that cannot protect themselves

- **INSTANT DISASTER RECOVERY, FAILOVER, AND QUARANTINE**
  Enable real-time networking for business continuity and remediation

- **BAC-NET: BUILDING AUTOMATION AND CONTROL SYSTEMS**
  Securely connecting and segmenting BACnet devices and systems across shared infrasctructure

To learn more, email info@temperednetworks.com or visit www.temperednetworks.com