The network is mostly used for retrieval and distribution, although host connectivity is still important. The network's access should be redesigned with the needs of users in mind. This article offers the CCN (Content Centric Networking). It also included security, scalability, and performance, which IP lacked. The fundamental idea of CCN is to maintain the bare minimal functionality, which is what made IP such a successful protocol, at layer 3, the network layer. Just more levels of protection and strategy are added. In CCN, there are two sorts of packets: interest and data. When we ask for data, we broadcast an interest packet. The node that receives this packet checks to see whether it has the required data, and if it does, it broadcasts a data packet. The contentName in the interest packet must be a prefix of the contentName in the data packet in order for the data to typically satisfy the interest. Typically, a longest prefix search is carried out, much like with IP. The FIB, content store, and PIT are the three primary data structures that it has. A list of packets, not just one, is forwarded via FIB. Buffer memory is the same as content storage. PIT maintains track of information, ensuring that only downstream information is asked. The foundation of CCN transport is an unstable packet transmission. If a requirement that is necessary for dependability is not satisfied, the packet is retransmitted. Since the CCN is local, no flow control is required, and flow control is kept during each hop. Since the sequencing is a little more complex than that of tcp, the next data reception is always retained. Since CCN uses numerous interfaces and the IP is restricted from using spanning trees for forwarding, it is not required to get an IP or MAC address. Any routing protocol that works well for IP should also work well for CCN.

When content is available in the routers but they are separated by ISPs, inter domain routing can occasionally cause issues. To address this issue, the paper advocates including domain level content into the prefixes.

Every piece of material kept on CCN is digitally signed and encrypted since the company was founded on the idea that content should be protected. The public key needed to authenticate the packet is made available by the CCN packets. Content validation is essentially just checking if it is signed by the key it supports at a lower level. Additionally, CCN fosters consumer and publisher trust. All data on CCN is encrypted, making it impossible for unauthorized servers to access the information because only approved servers are able to access and decrypt the data. If a node successfully gets data or not, it can still search for a certain interest. Additionally, it gives nodes access to tools that let them choose where and how their data is sent. It was found that CCN needed five times the pipeline of TCP for mass data transmission. TCP had a better throughput than CCN. Even if testing show that CCN's performance is equal to that of unsecured http but significantly beats secure https, it is always safe to send content over it. Since CCN was created using the same technical principles as IP, it possesses all of IP's characteristics as well as some extra ones. Although it may be used as an overlay, it was created to take the place of IP.