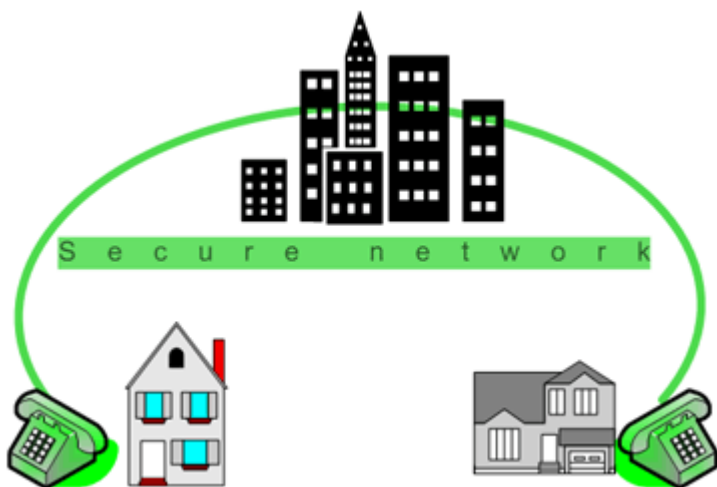


## The Vanishing Trusted Network.

By Alex Ramia, Vice President, Innofone.com, Inc.

The telecom world is seeing a shift in the challenge of its sole ownership of a Trusted Network. This erosion of its dominance started with the birth of the World Wide Web and, fortunately for Bell companies, this erosion of their control over a Trusted Network is considerably slowed as vulnerabilities are exposed on the Web. The first machines on the Internet network were connected through a secure, predictable pipe; this network pipe had fixed ends and was considered trusted.



Owners were identified and the Web was considered peer to peer. However, the peers were giant mainframes, and portable devices were concoctions of Hollywood. When the popularity of the Internet network forced its rushed growth, many things started to fail; some were quite memorable. Specifically, in 1997, 36 state attorney generals required AOL to stop advertising until it could provide reasonable modem access, allow easy cancellation and provide significant refunds.

In 1998, 20 states filed Assurances of Voluntary Compliance forcing America Online(AOL) to clarify its free trial offers, disclose its premium surcharges, communications charges, cancellation procedures, and reform its other business practices. As Ohio Attorney General Betty Montgomery said, announcing the 1998 AVC, "The problem we're experiencing with America Online is similar to a parking attendant that sells too many monthly passes — when drivers show up at the garage it's already full of cars."

In periods between 1996 and 1998, AOL's performance quality and level of customer service matched the worst in the industry. If AOL had been selling hundreds of thousands of tickets to a Rolling Stones concert in a 5,000-seat arena, and then made it difficult for frustrated customers to get refunds, it would have been indicted.

Network address translation (NAT) was introduced by Paul Francis as a way to allow more users to enjoy the benefits of the Internet. For the first time it allowed millions to realize the real dream of the Internet and the ability to get a glimpse of what could happen. It gave a segment of society almost equal access to a global resource. Unfortunately, with NAT the Internet has been set firmly on the path to repeat the follies of its youth.

While on the surface NAT just takes away trust of the network, behind the scenes it is also playing a timing game with a temporary address assigned from the Internet service provider (ISP). This is a gamble similar to the one played by AOL who, at the time, used a sophisticated sharing model. AOL analyzed the amount of usage each modem had, factored in time of day with historical usage patterns of its consumer base to deduce the number of modems needed to maintain a customer base with acceptable denial of service rates.

Sounds complicated? Not really, it's "modem pool time sharing," except NAT does this at network speeds. Each address from your ISP is on loan to you to establish a connection to the Internet. It may connect your PC, cellular phone or other appliance that interface to the network.

As AOL found out, the longer a consumer stays online the longer the network address is locked up (or modem in AOL's case), the more addresses an ISP must acquire to support a growing customer base. This formula will break as it did for AOL. This is inevitable due to the very nature of the Internet services whose historical actions are to enrich content as speed is increased, launch services that encourage stickiness and deliver applications that require the long continuous use of a fixed address.

NAT can be considered a "two-edge sword" that many great swordsmen have cut themselves on. An ISP is faced with users online longer, because more services are available, placing a strain on the address pool assigned to individual ISPs, and it is not easy to add more addresses. Imagine having the world's best web service hosted at the world premier ISP and it fails to provide reliable connections to over half its potential customers. Imagine increased customer complaints and uncontrollable churn as waves of consumers move from one ISP to another looking for the elusive low "address sharing ratio." It is here already. The complete allocation of Internet Protocol version 4 (IPv4) address space to various consumers is a map to a predictable failure.

There are a few providers and governments that have recognized this inevitable end. These enlightened few have turned to Internet Protocol Address Management (IPAM), an entirely innovative business application to manage the use and allocation of a limited resource, a resource that is required for connectivity to the Internet network. To add further requirements, management of all the IP addresses assigned throughout a network play a critical role in regulatory compliance, as mandates like Sarbanes-Oxley (SOX) set out stricter controls for address management and require administrators to control and monitor who has access to what from where. For instance, to comply with a SOX-related subpoena to prove compliance, a company could be asked to produce a log of which

computers or users had leases for a particular IP address over a certain period of time. Those ISPs that did not understand this risk and acquired a small pool of v4 addresses are already experiencing the churn due to poor performance of their network.

However this article is to address the trust now completely removed by NAT. The restoration of trust on the network is the next predictable growth. The same path taken by the Bell companies in an effort to support their growth has to be embarked on to ensure the viability of the Internet. An expansion of the fundamental transport layer is required to achieve this goal.

The large numbering system of IPv6 allows multiple addresses to each individual and every device ever created that communicates over the Web. Its numbering power extends to the peer and thereby enabling trust to be established once again and due to its agreed method of deployment, unparalleled security can be deployed to strengthen that trust.

Having trust established on the Internet will enable many new services, and eliminate many nuisances associated with the old network. NAT will be a choice — not a necessity. Security will be the norm — not an omission. Spam, address spoofing and more will join the stories about personal IPv4 address and monochrome screens.

So how do you build a Trusted Network? How do you change from a world like this?

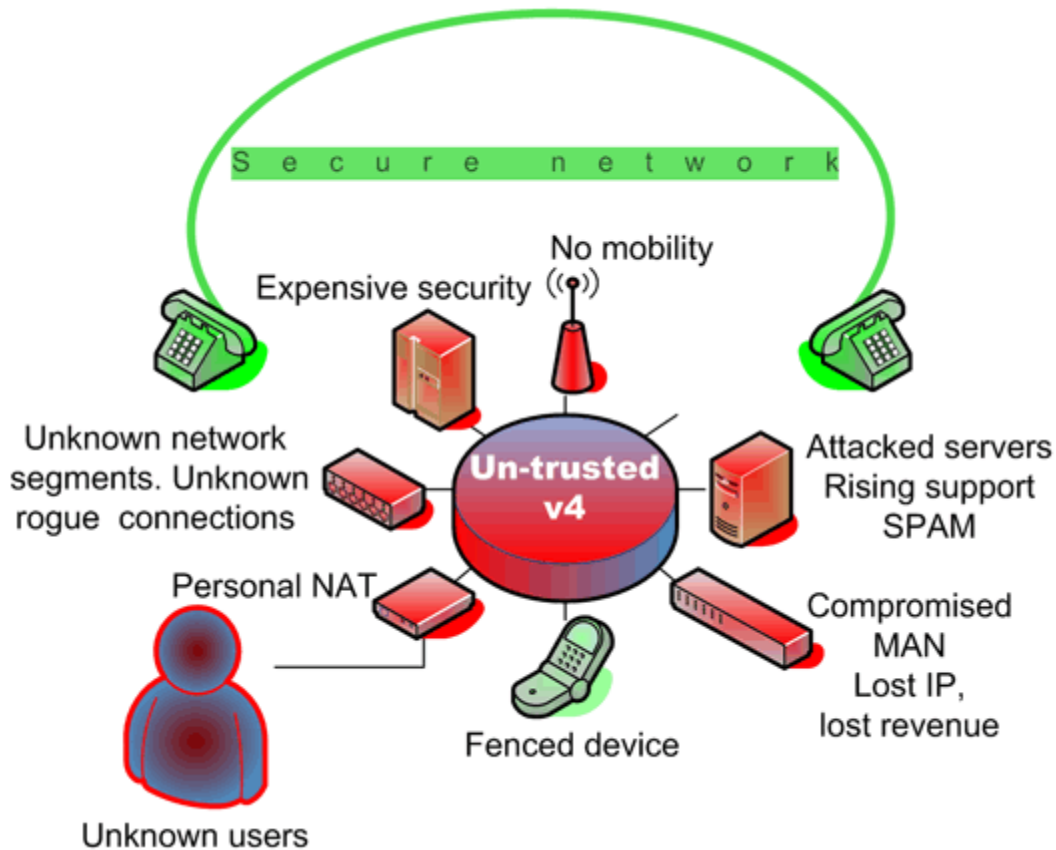


Figure 1

To a larger economically viable platform like this:

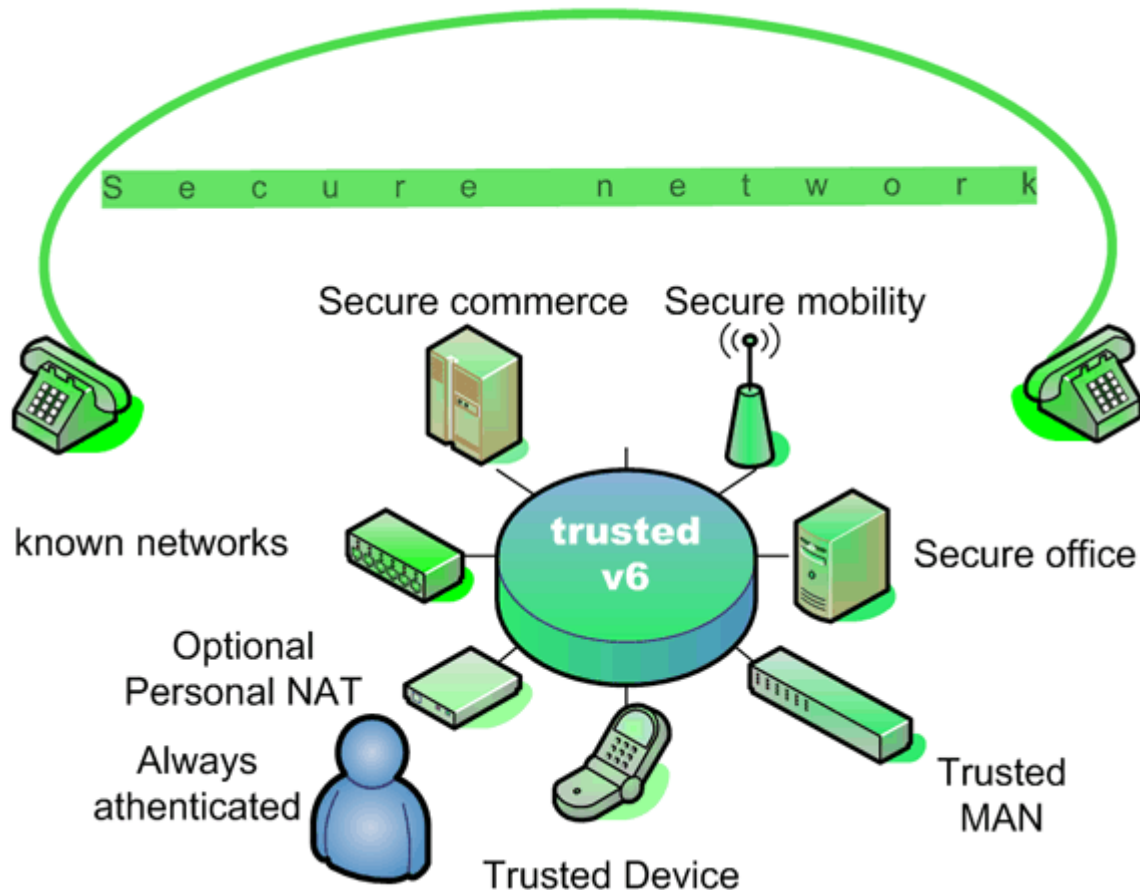


Figure 2

Not a tall order when you get the visual picture.

To enable trust between two devices an exchange of information must occur. Once the change has been completed, trust is established and further communications can proceed with confidence that the information is secure from end to end.

The enabling key to this trusted association is the ability to uniquely identify each point on the network with a number, combine that number to a device and apply security to the pair.

IPv6 is such a number; it can be routed, tracked and controlled. It is the current logical and evolutionary growth direction for the Internet. As the Bell network outgrew its infant numbering, so the Internet is outgrowing its own numbering. When the move to IPv6 is made, the Trusted Network will be enormously better, richer and with greater value adds.

Control will be expected in order to maintain this growing network economy. This growth is no longer a topic for speculation, it is a statistical fact. The current Internet's economic growth is limited by the lawless Wild West Web. The ability to enable a Trusted Network that reaches the world will give the growing global network economy a tremendous growth shot in almost every aspect of its use and design.