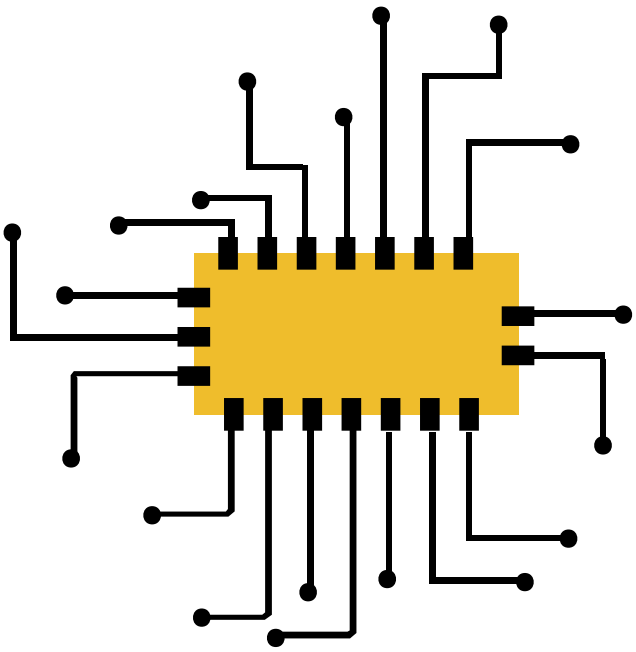
Internet Society
India Mumbai

MUTUALLY AGREED NORMS FOR ROUTING SECURITY (MANRS): AN INTRODUCTION

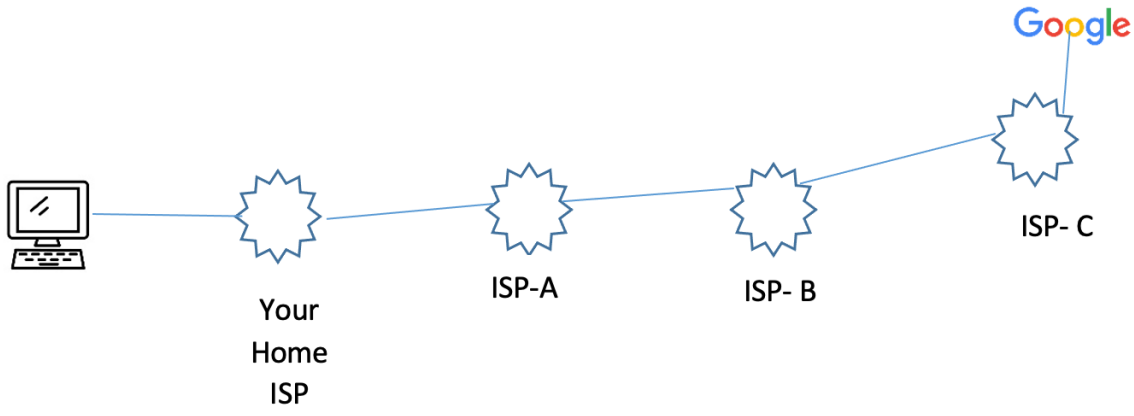


SPEAKER: AFTAB SIDDIQUI, INTERNET SOCIETY

TIME AND DATE: 11:00 HOURS IST, 13TH FEBRUARY

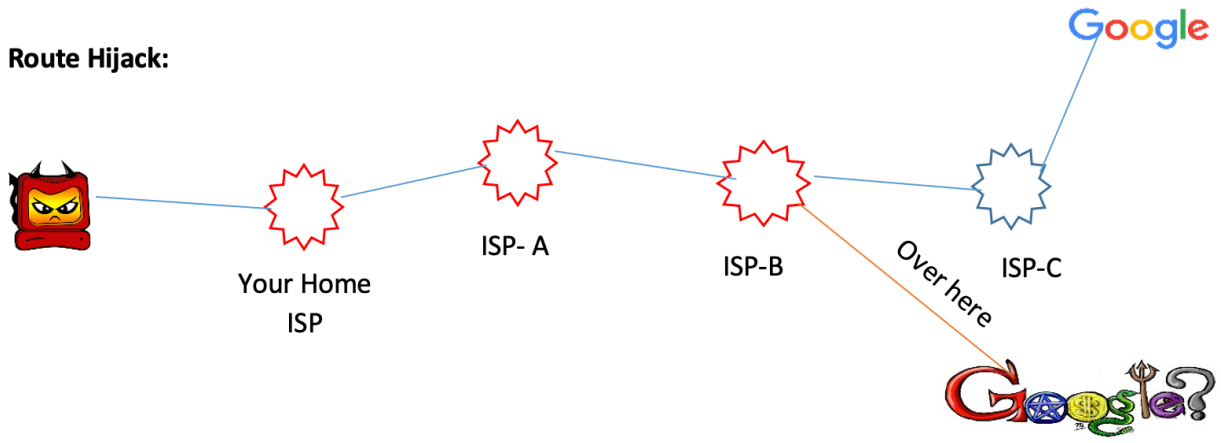
The introductory webinar started with Aftab explaining what exactly is routing and why we need it. Aftab explained that routing is needed to get packets from one destination to another and routers are specialized computing devices within an Autonomous System (AS) that are programmed to discover other routers within an AS or connected networks over other AS and forward packets to them. Routers can have single connection to external network, or be connected to two or more external networks (multi-homed) for resilience. The protocol of internet which keeps everything together is called the BGP- Broder Gateway Protocol, which was designed ironically on a napkin in the year 1989. This protocol was designed on trust, trust between the entities that were using this protocol. But in today's time, there are around seventy thousand entities using this protocol and hence, to gain the same amount of trust with every entity is nearly impossible. With the advancing technology, there are bad actors who have emerged who disrupt the way the internet functions.

The normal route that the internet should take is something on these lines:



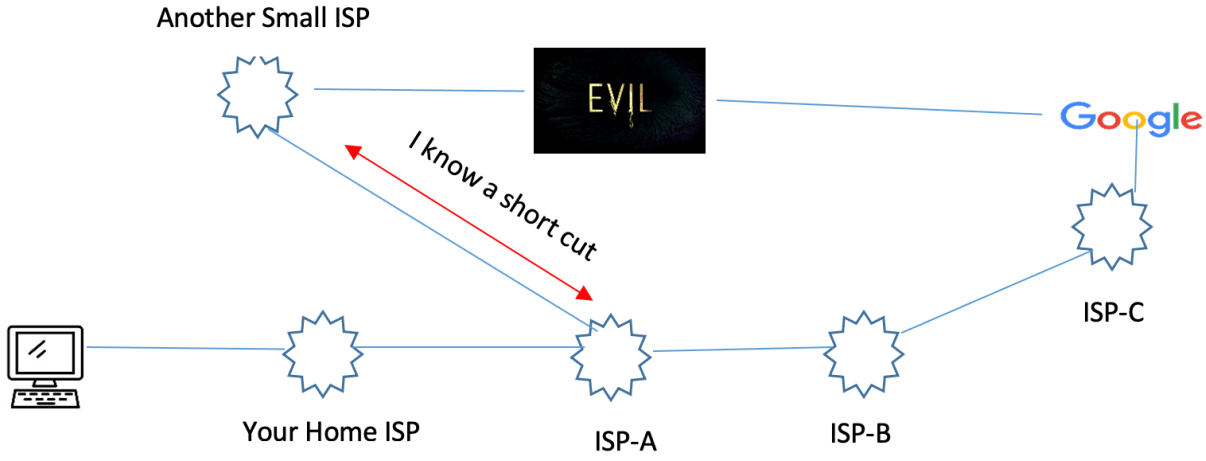
However, this normal route can be disrupted and can cause real world problems. The normal route can be disrupted by: a) Route Hijack, b) Route Leaks and c) IP address spoofing.

Route Hijack:



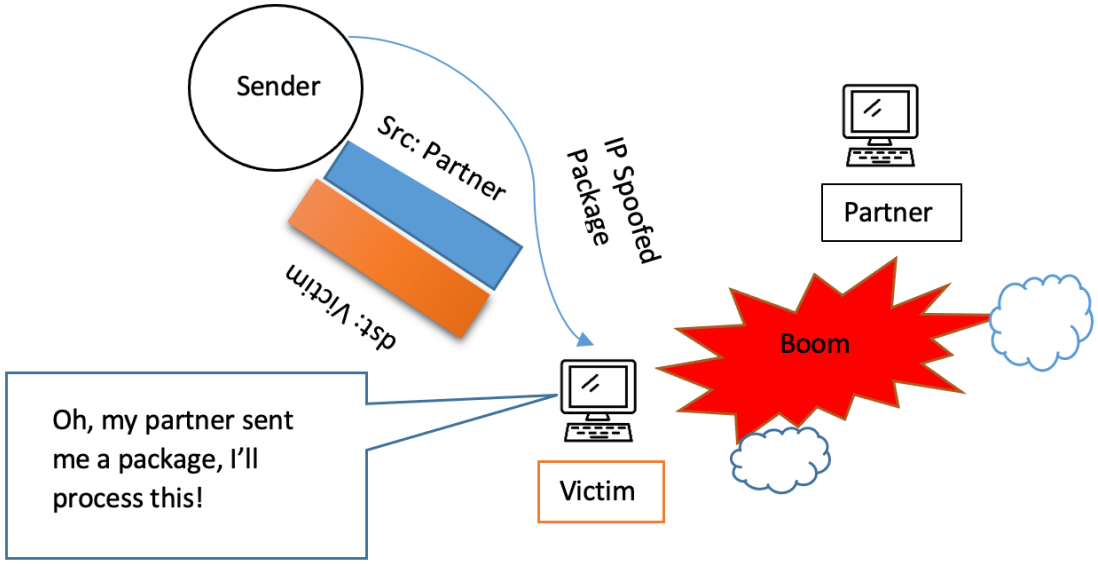
Instead of reaching Google.com (or any desired website) via ISP-C, the attacker falsely announces the ownership of IP prefixes that lead the packet to reach the wrong destination by manipulating a shorter route. When packet reaches the wrong destination, the attacker steals your information. In order to avoid this, one must look at the SSL or KLS certification or the lock sign in the browser.

Route Leak:



Instead of going to Google.com (or any desired website),via ISP-B and ISP-C, the packet goes through ISP-A due to accidental misconfiguration. Route leak happens when there is redirection of traffic through an unintended path that enables eavesdropping or enables undesired traffic analysis by the attacker.

IP Spoofing: Impersonation

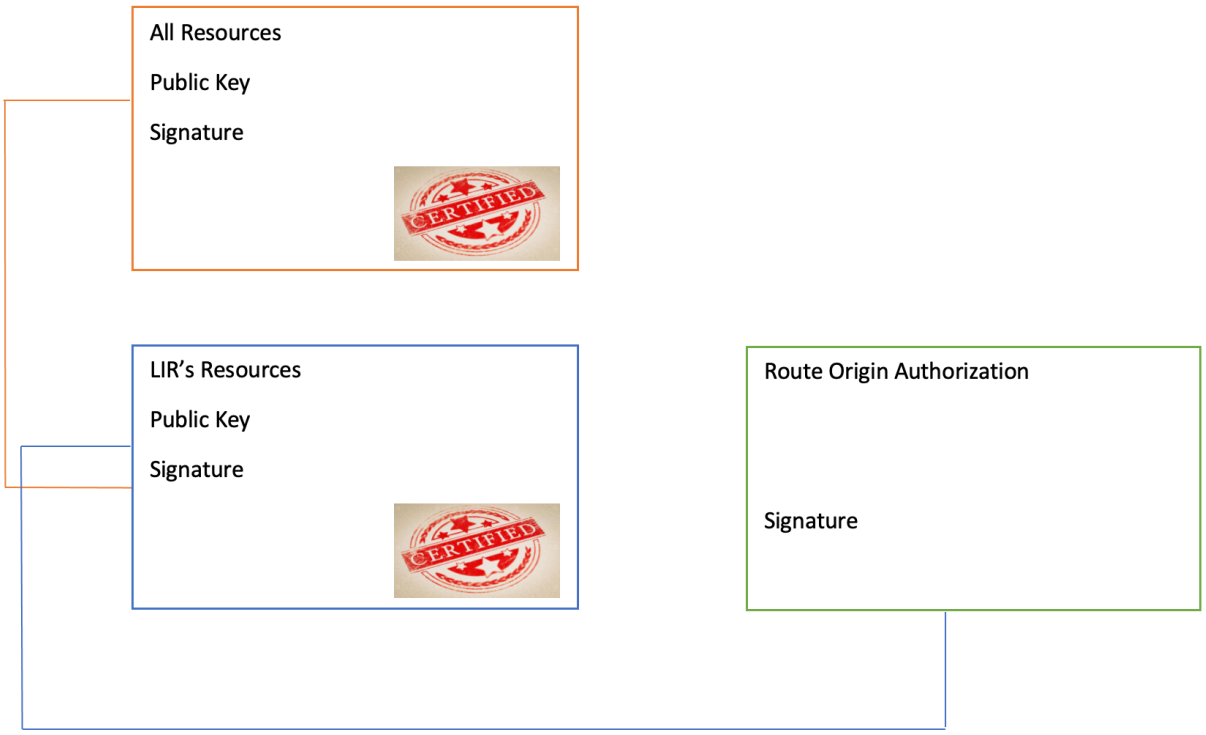


IP Spoofing is when someone creates IP packets with a false source IP address to hide the identity of the sender or to impersonate another computing system.

So how do the end users protect themselves from such problems? One should check the digital certificate of site before accessing it.

The RIR (Regional Internet Registry) maintains a database of which IP belongs to which ISP and which ASN belongs to which ISP and it should be verified through this portal.

In the Routing world, the RPKI (Resource Public Key Infrastructure) is the specialized public key infrastructure (PKI) framework for verifying the association between resource holders and their internet resources. It attaches digital certificates to network resources upon request that lists all resources held by the member.



MANRS is a global initiative that provides crucial fixes to reduce the most common routing threats. The most common practices are the following:

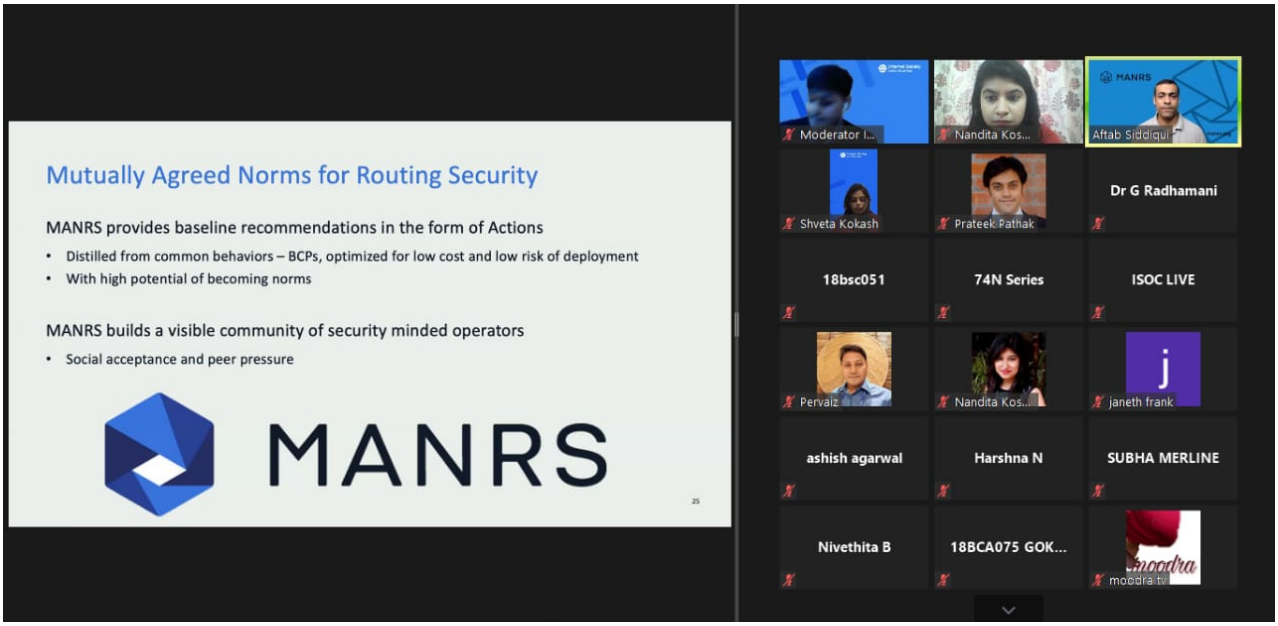
Filtering	Anti-Spoofing	Coordination	Global Validation
Prevent propagation of incorrect routing information by ensuring correct announcements	Prevent traffic with spoofed source IP address by enabling source address validation	Facilitates global operational communication and up-to date coordination.	Facilitate validation of routing information on a global scale

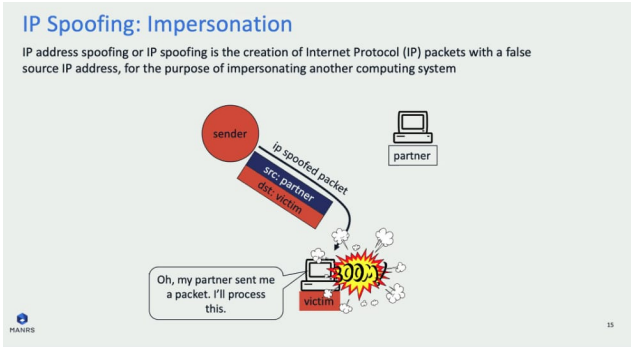
Aftab concluded the webinar thoughtfully by showing the data and citing that the number of cases of hacking and other problems discussed in India are going down. The RPKI implementation is going up, but it is still a long way to go.

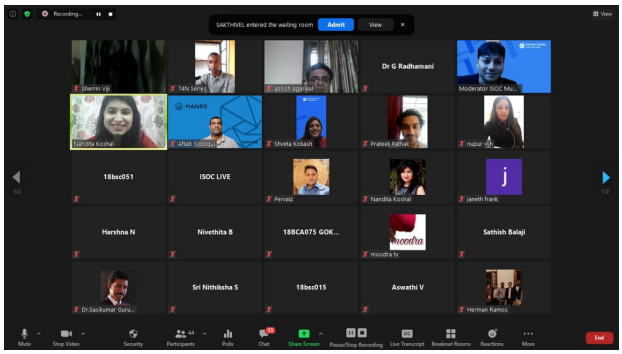
The webinar concluded with a Vote of Thanks by Nandita Koshal, Treasurer, ISOC India Mumbai to Aftab for his excellent presentation and ISOC India Mumbai volunteers Mohammad Pervaiz Ansari for moderating the session and Nupur Vijh for rapporteuring for the session. The Chapter leadership also extends gratitude to volunteer Feroza Mody for designing this report.

The webinar can be accessed here.

Photo Gallery







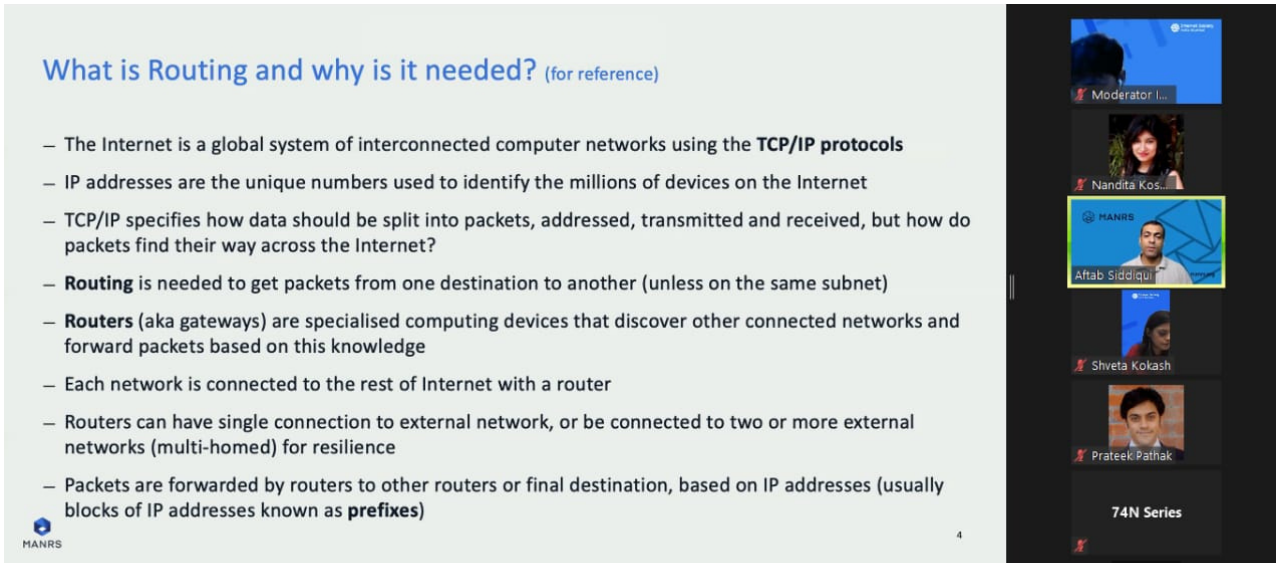
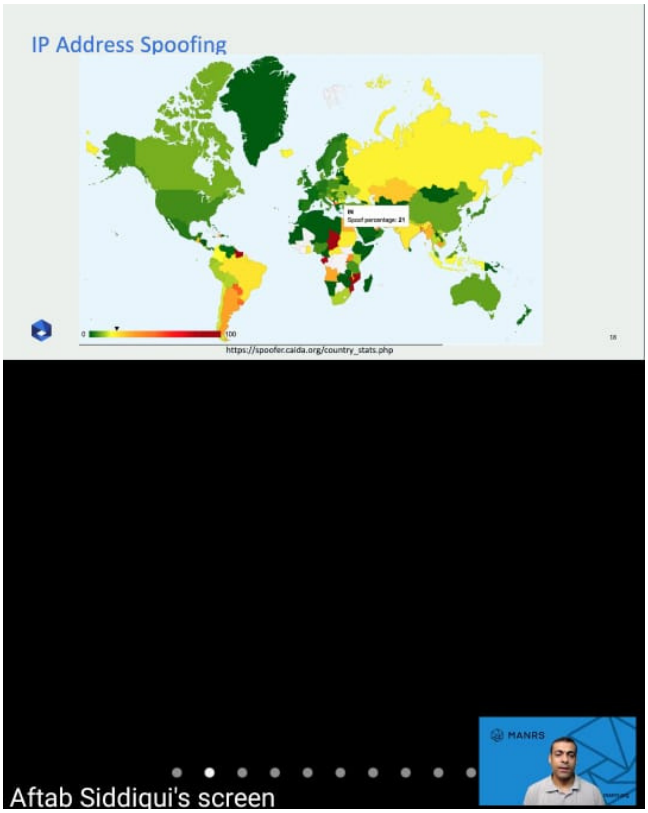
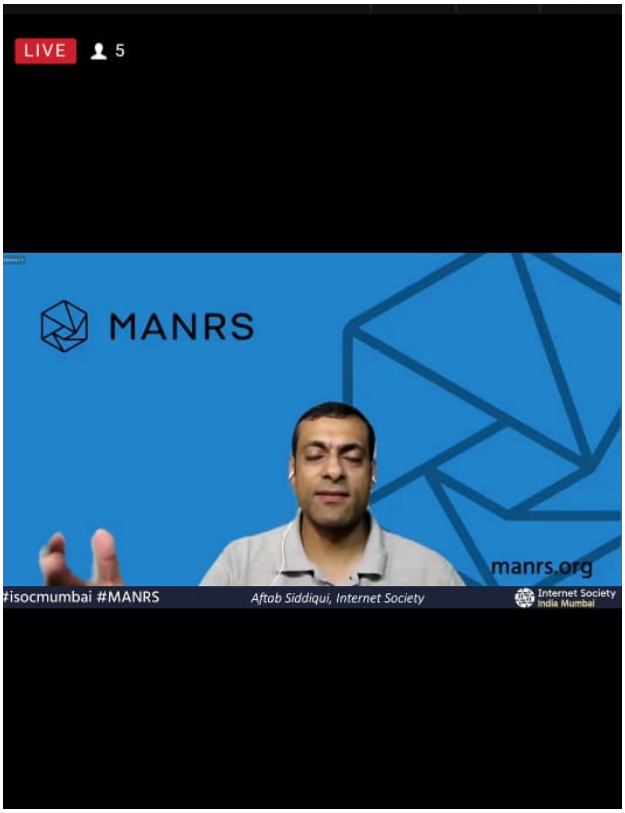
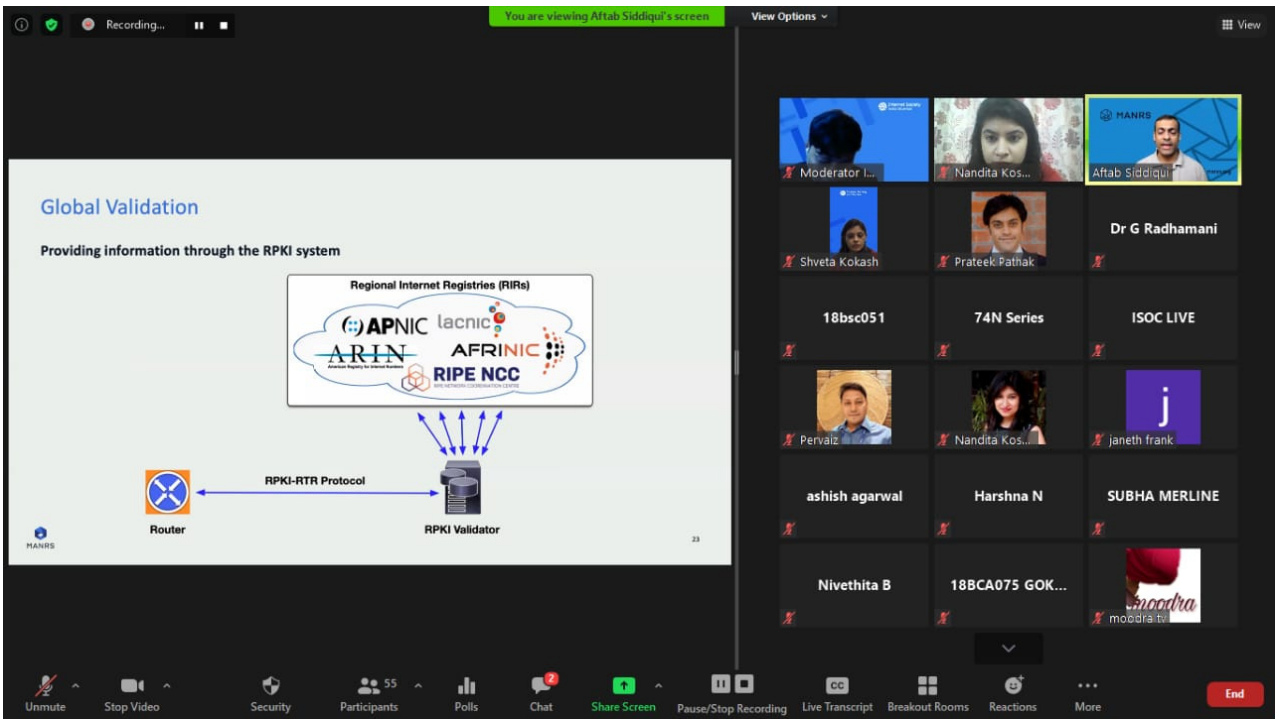


Photo Gallery







Internet Society
India Mumbai

MUTUALLY AGREED NORMS FOR ROUTING SECURITY(MANRS):AN INTRODUCTION

Aftab Siddiqui, Internet Society

13th February,11:00 hours IST, Saturday