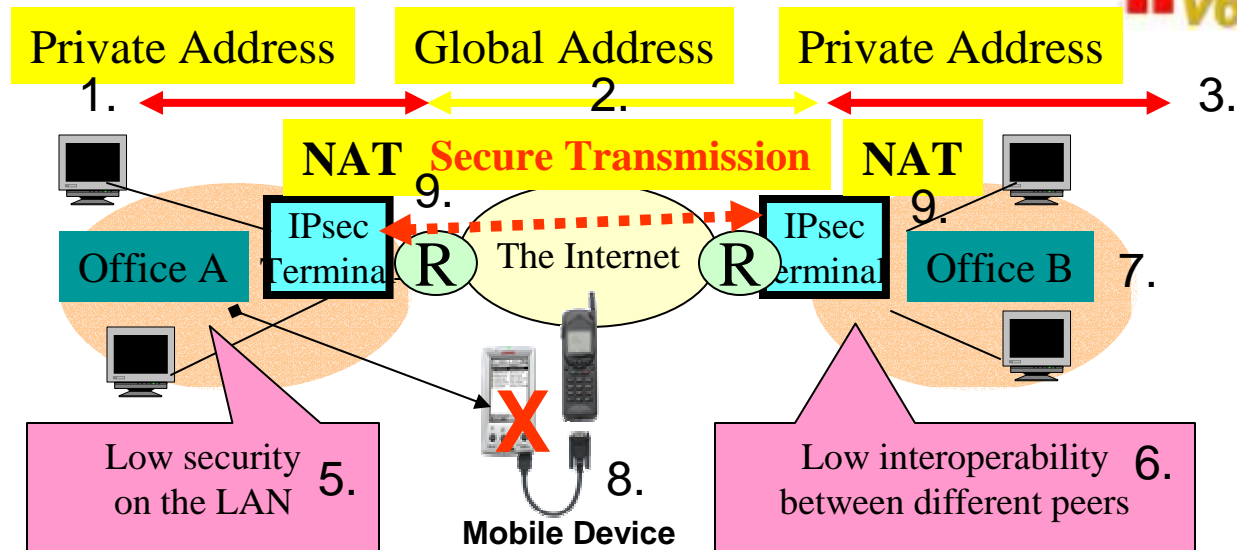


Cost of NAT

IPv4-NAT

Site-to-Site
Secure
Communication



1. Node can only communicate out of site with peer through a NAT and has reduced capability of applications.
2. Communications has only one entry point to Office A node through one router and single point of failure.
3. Attacker only has to masquerade the packet between the NATs and they will be able to enter either network.
4. Peer-to-Peer communications and security can only be done within a site behind a NAT.
5. Security on the LAN is only by NAT once attacker gets passed the NAT it can attack a node on any LAN.
6. Interoperability between peers out of the site, suppliers, partners, or other vendors has greater cost, if even possible.
7. A node not within the site cannot initiate a connection with a node behind a NAT site reducing communications.
8. Mobile Nodes cannot roam out of a site with a private address because it does not exist out of the site.
9. NAT state for translation, namespace, security, and routing must be maintained at all entry/exit points to the network.

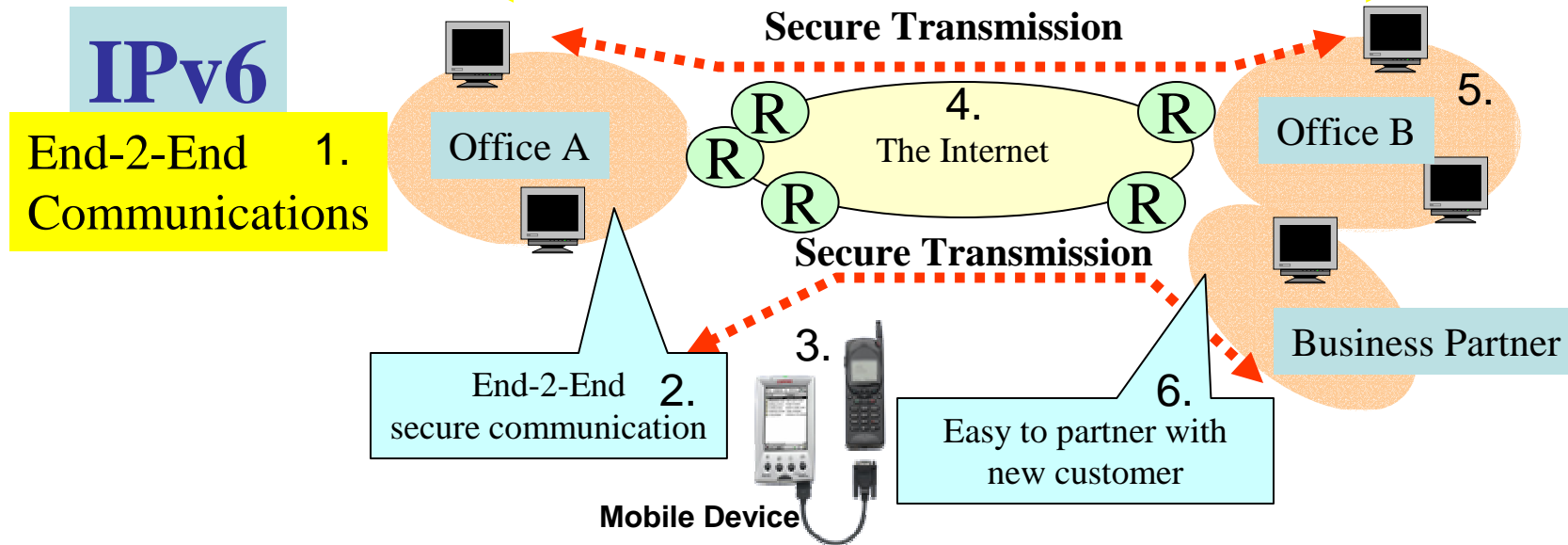
All of these points are a cost to an entity deploying networks who need for their business or operation to communicate out of the site to peers or applications. Not being able to perform communications and not having true security associations with peers out of the site for one-way communications has a significant cost. Each of these points also causes extra software and state to be maintained and administered by the network operations within the entity.



Profit from No-NAT



Global Address



1. End-2-End communications permits nodes to communicate in the site or out of the site without NAT additions.
2. End-2-End security methodology and architecture permits pervasive security in the site, and out of the site.
3. Global Addresses and End-2-End communications and security permit nodes to roam and be mobile out of the site.
4. Entry into to out of the network does not have to be a single point of failure and provide redundancy and failover.
5. A node in another site can initiate a peer-2-peer communications session with a node in another site.
6. Partners, Suppliers, or Applications can now be accessed as peer-2-peer nodes or applications.

Profit from No-NAT can be realized with greater application support and availability which cannot run in a NAT Environment, communications with peers can be initiated by a site or peers out of the site, security is based on security within the node and provides End-2-End secure communications trust and privacy model, and the business options are greater for communications and the cost of managing all the NAT state is removed.