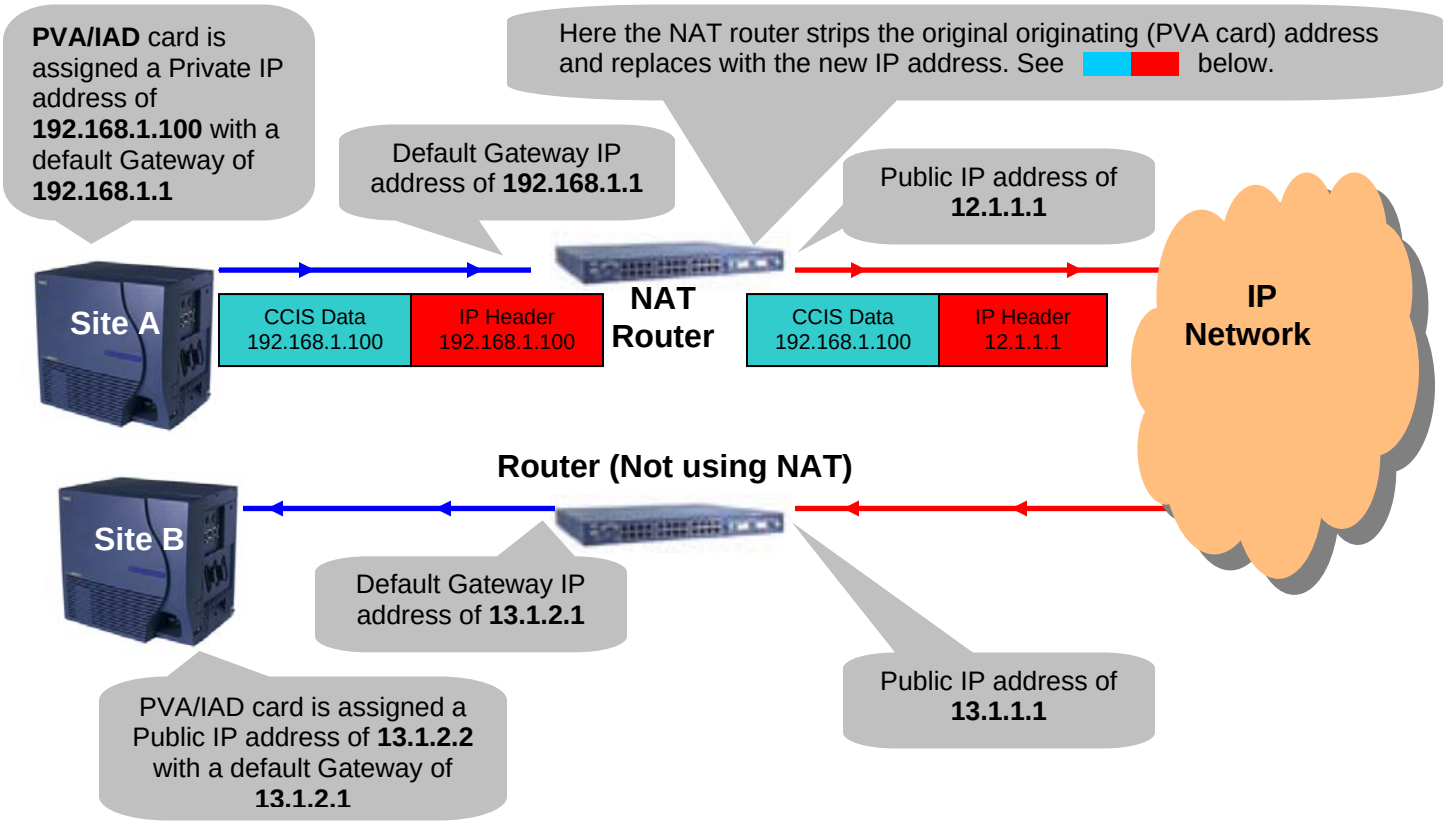
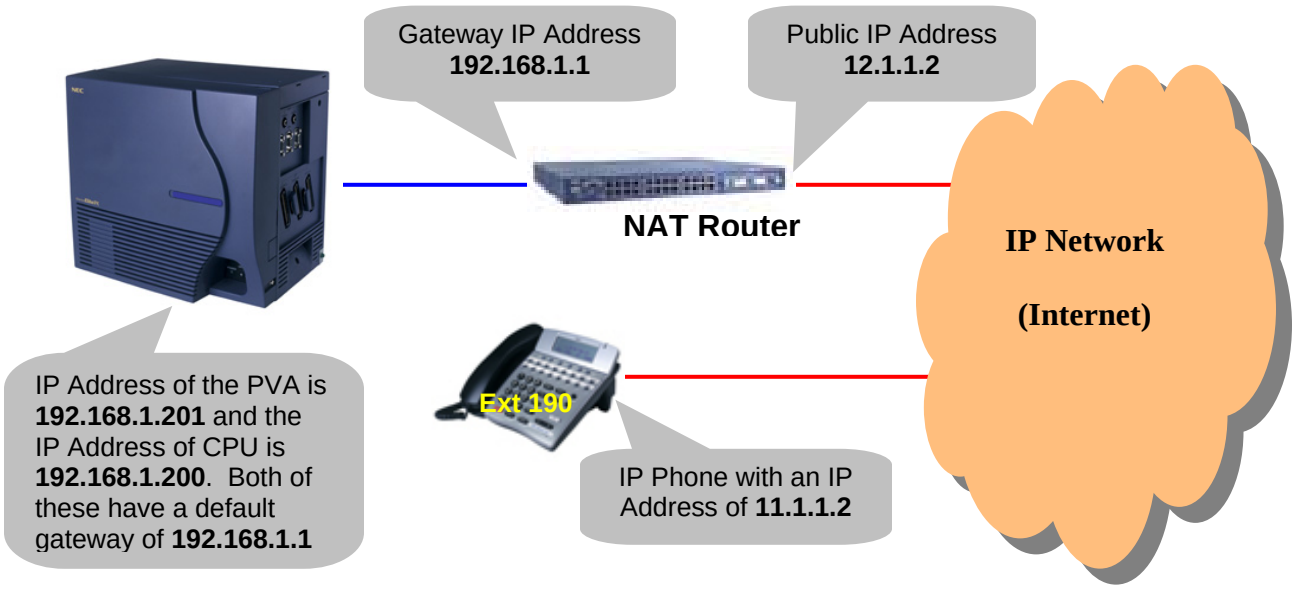
Network Address Translation (NAT) with the IPKII

In computer networking, network address translation (NAT, also known as network masquerading or IP-masquerading) is a technique in which the source and/or destination addresses of IP packets are rewritten as they pass through a router or firewall. It is most commonly used to enable multiple hosts on a private network to access the Internet using a single public IP address.
NAT ***cannot*** be used when connecting two sites via **IP-CCIS**. See explanation below….



- Site A originates the call and sends a CCIS setup message to the NAT router with a destination IP address of 13.1.2.2. Contained in this message is NEC proprietary CCIS data reporting the IP address of the originating site as 192.168.1.100.
- In the NAT router the original IP address in the IP header is removed and is replaced with the new IP address of 12.1.1.1. *The CCIS data is not changed* and continues to contain the original IP address of 192.168.1.100.
- This data then gets forwarded to the PVA/IAD card in Site B.
- Site B's PVA/IAD card analyzes the CCIS setup message (not the IP header) and attempts to respond with a CCIS acknowledgement message to 192.168.1.100.
- System B's router does not know how to route to the 192.168.1.0 network and therefore discards the packet and the call does not complete.

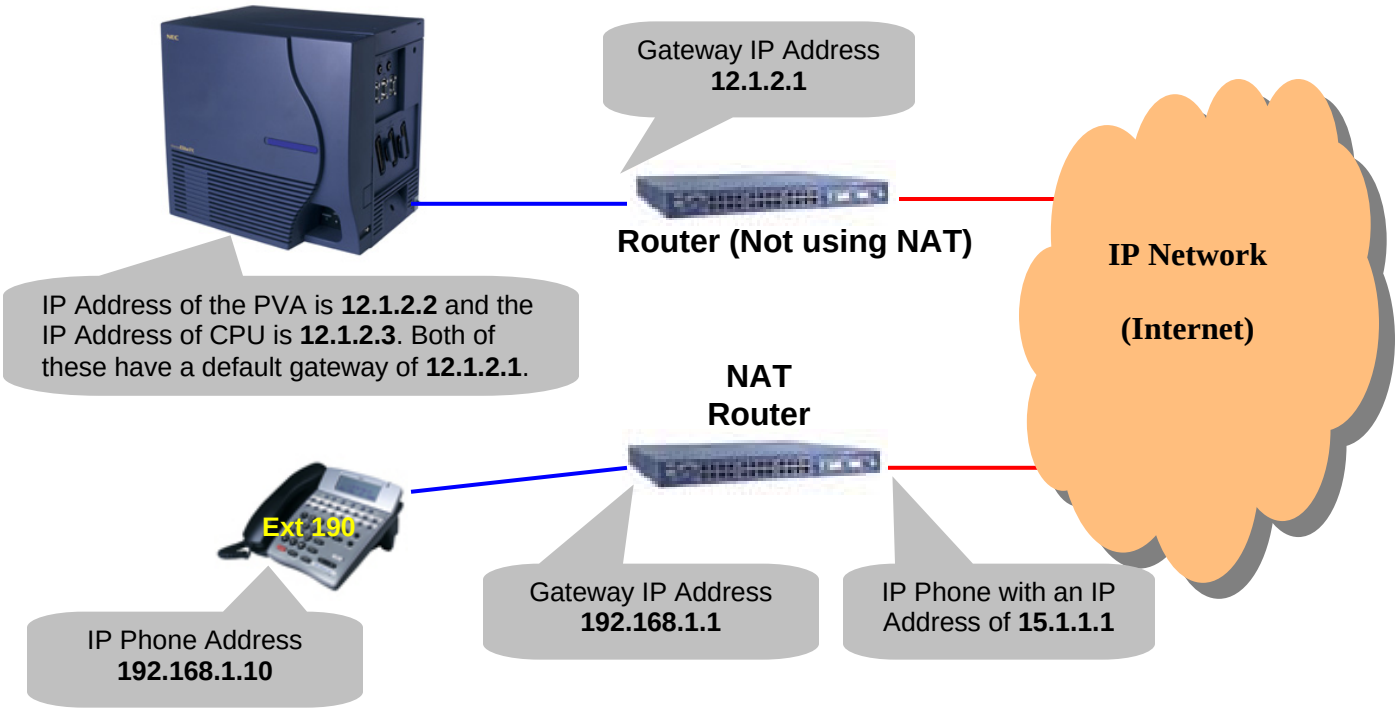
NAT is also ***NOT*** available at the KTS location when utilizing remote **IP Stations**. The issue is due to the Session Description Protocol. See example below.



- The NAT router is configured to forward all associated VOIP ports to the PVA card.
- When extension **190** boots it will send a setup/register message to **12.1.1.2**.
- **12.1.1.2** forwards this information back to the PVA card at **192.168.1.201**.
- The PVA will then send an acknowledge message back to **11.1.1.2** allowing it to register. The phone will come online with normal display. An attempted call though will allow connection but no speech path.
- Extension **190** (IP Phone) calls extension **101** (TDM Phone).
- A call setup request is sent from **11.1.1.2** to **12.1.1.2**.
- **12.1.1.2** will then forward this information back to the PVA card at **192.168.1.201**.
- The PVA card responds to the IP phone with a packet containing an IP header with an address of **12.1.1.2**. Inside of this packet there is a field called ***Session Description Protocol (SDP)***. The SDP reports the Remote Connection IP Address as **192.168.1.201**.
- The IP phone then attempts to communicate with the IP Address of **192.168.1.201** and, as this is not a Public IP Address, it cannot negotiate. The PVA card though will continue to communicate and, in most cases, a call is set up with one way speech path. Voice is heard from system to IP phone and not in the other direction.

Supported NAT Utilization

NAT can be utilized if Public IP addresses are assigned to the CPU and PVA card and the remote IP station sits behind the NAT router. See below….



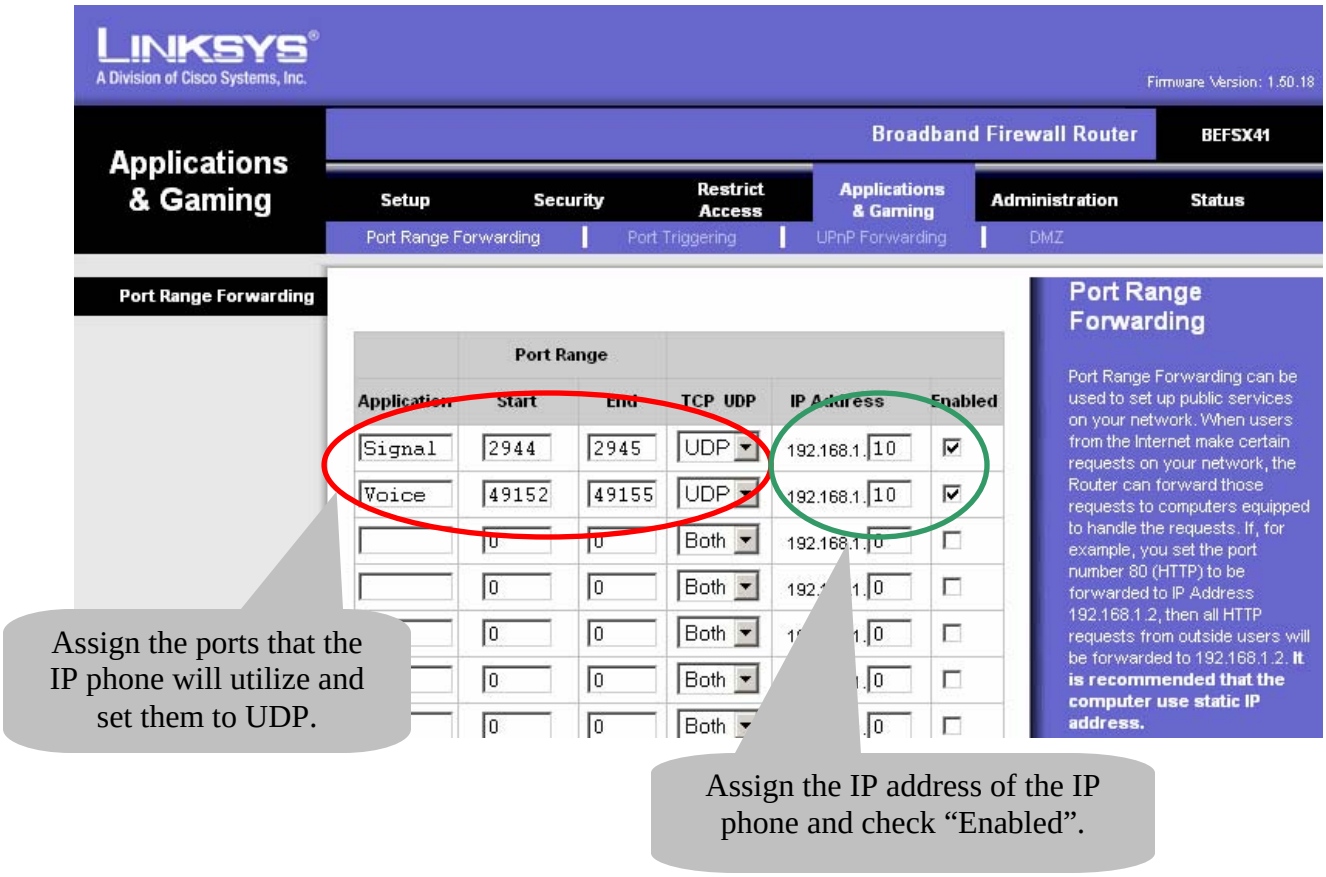
- The remote NAT router is configured to forward all associated VOIP ports to the IP Phone.
- When extension **190** boots it will send a setup/register message to **12.1.2.2**.
- The PVA will then send an acknowledge message back to **15.1.1.1** (the NAT router). The NAT router then forwards this data to the IP Station allowing it to register. In the previous example we said that the messaging would contain a non-routable private address (**192.168.1.10**). This is still valid and when the phone boots up it is sending this private address, along with its routable address to the PVA card. The card, unlike the IP Terminal, has the ability to analyze more than just the application data allowing it to identify the routable address for the IP Station as **15.1.1.1**.
- When calling from an IP phone you will have speech path even though the IP Station, during setup, will still send an **SDP** message reporting the IP Address of **192.168.1.10**. The PVA card, again, can analyze more than just the application data (unlike the IP Station) allowing it to identify the routable address of **15.1.1.1** and negotiating with the station for a successful, two way, VOIP session.

Sample NAT setup

- By default the IP phones use the following ports:
  - Signaling = 2944/2945 UDP
  - Voice RTP1 = 49152/49153 UDP
  - Voice RTP2 = 49154/49155 UDP

- If an IP phone is sitting behind a NAT router the above ports need to be forwarded to the IP address of the phone.

- Below is an example of how to forward the ports to the IP phone in a Linksys BEFSX41 router. The private IP address of 192.168.1.10 is assigned to the IP phone.



- ***Note*:** If you have more than one IP phone behind the same NAT router you must assign unique signaling and voice UDP ports to each IP phone. The default ports can be changed in the IP phone configuration. From the main menu select **9** for ***Advanced Settings*** and then **9** for ***Port Settings.*** Select **2** for ***MGC Self Port*** (Signaling port, E.g. 2nd station use 2946), then option **3** ***RTP Port 1*** (Voice port, E.g. 2nd station use 49156), and finally option **4** ***RTP Port 2*** (Voice port, E.g. 2nd station use 49158).