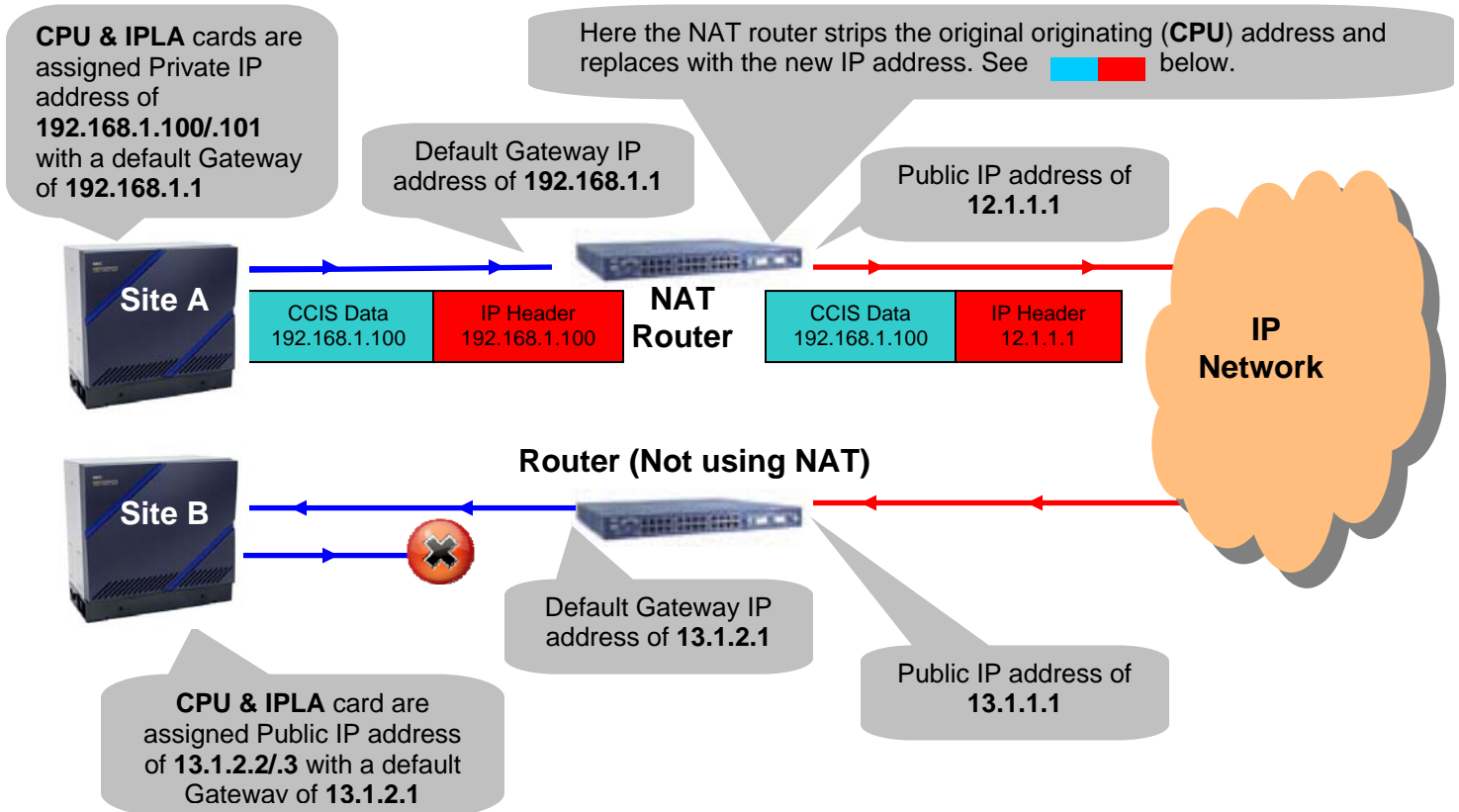## Network Address Translation (NAT) with the NEAX 2000IPS

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….

CPU & IPLA cards are assigned Private IP address of **192.168.1.100/.101** with a default Gateway of **192.168.1.1**

Here the NAT router strips the original originating (**CPU**) address and replaces with the new IP address. See   below.

Default Gateway IP address of **192.168.1.1**

Public IP address of **12.1.1.1**

Site A

| CCIS Data 192.168.1.100 | IP Header 192.168.1.100 |

NAT Router

| CCIS Data 192.168.1.100 | IP Header 12.1.1.1 |

IP Network

Router (Not using NAT)

Site B

Default Gateway IP address of **13.1.2.1**

Public IP address of **13.1.1.1**

CPU & IPLA card are assigned Public IP address of **13.1.2.2/.3** with a default Gateway of **13.1.2.1**

- 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 CPU card in Site B.

- Site B's CPU 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.
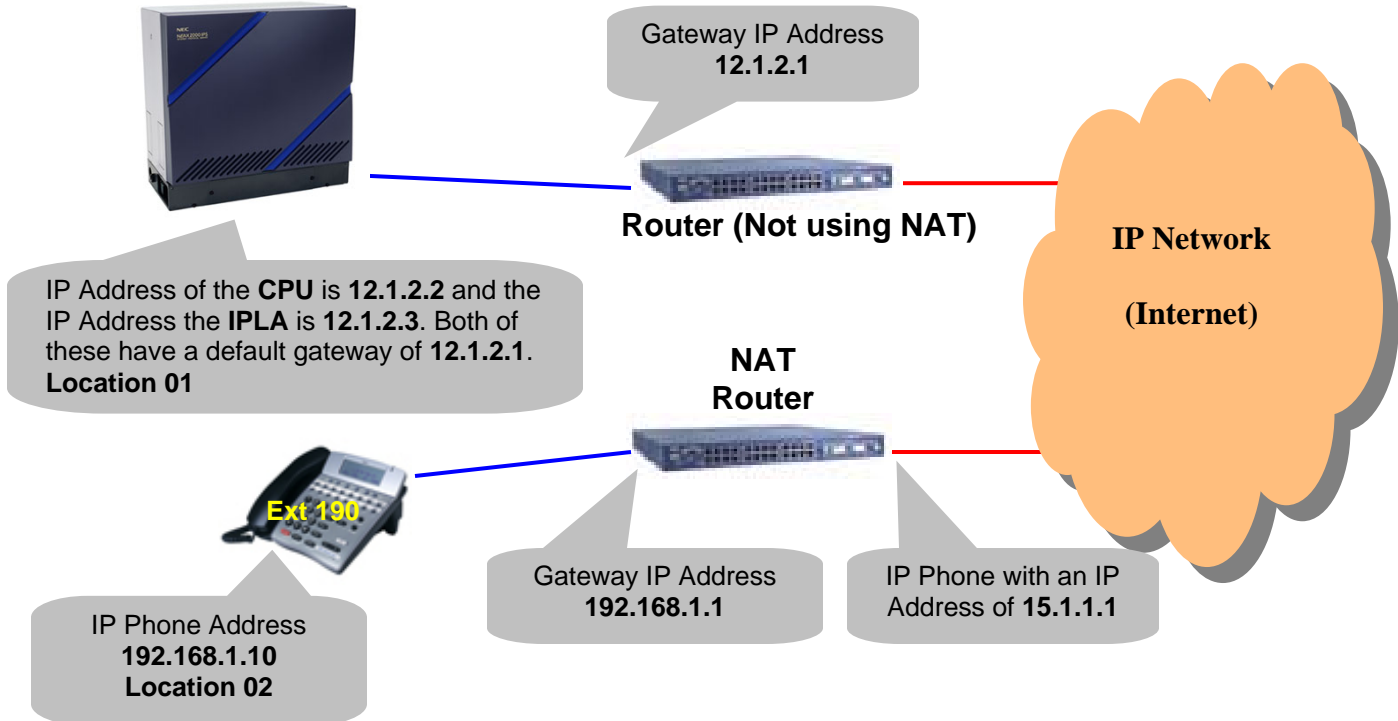
NAT is also *NOT* available at the *PBX location* when utilizing remote **IP Stations**. The issue is due to the **Session Description Protocol**. See example below.
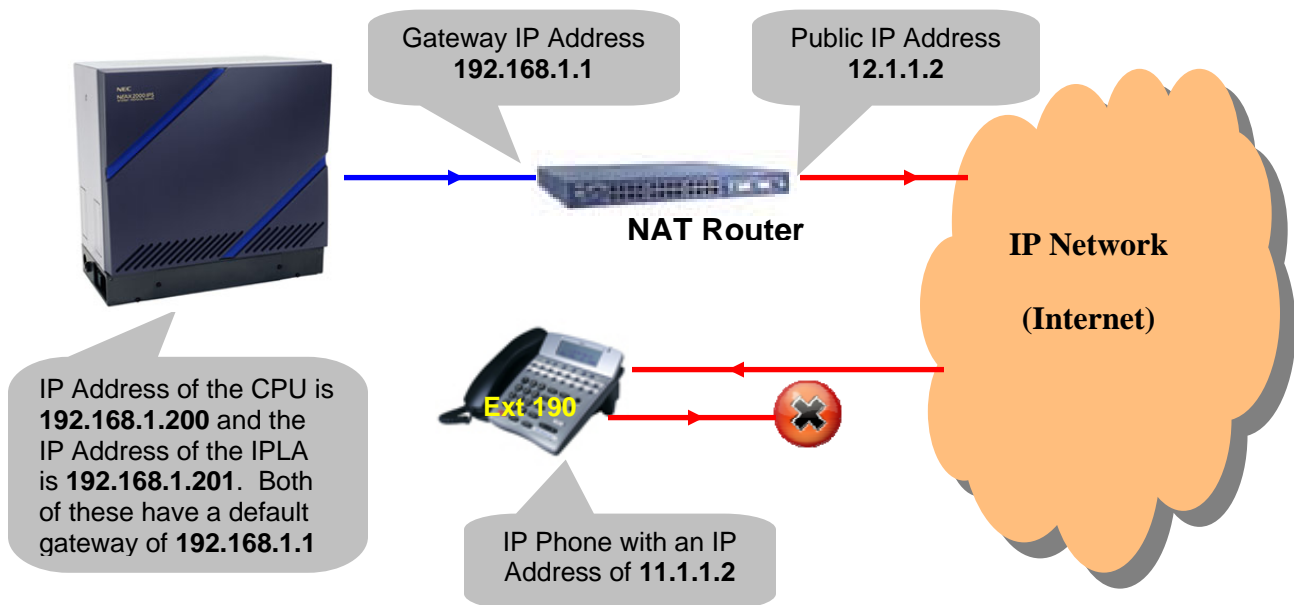
- The NAT router is configured to forward all associated VOIP ports to the CPU.

- 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 CPU at **192.168.1.201**.

- The CPU 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 CPU at **192.168.1.201**.

- The CPU sends back to the IP phone a packet containing an IP header with an address of **12.1.1.2**. Within this UDP packet there is a field called the *Session Description Protocol (SDP)*. The *SDP* reports to the IP Phone the Remote Connection IP Address (CPU) as **192.168.1.201**.

- The IP phone then attempts to communicate with the *SDP* IP Address of **192.168.1.201** and, as this is not a Public IP Address, it cannot negotiate. The CPU though will continue to communicate and, in most cases, a call is set up with one way speech path. Voice is heard from the PBX to the IP phone but not in the other direction.

Supported NAT Utilization

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

Gateway IP Address
12.1.2.1

Router (Not using NAT)

IP Network

(Internet)

IP Address of the **CPU** is **12.1.2.2** and the IP Address the **IPLA** is **12.1.2.3**. Both of these have a default gateway of **12.1.2.1**.
Location 01

NAT Router

Ext 190

Gateway IP Address
192.168.1.1

IP Phone with an IP Address of **15.1.1.1**

IP Phone Address
192.168.1.10
Location 02

- 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 CPU 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 CPU. The CPU, 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 CPU 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.

Programming

1. By default location groups assigned to the IP Dterms are not permitted to communicate with each other within the same NAT. If you have more than one IP Dterm behind the NAT router the ability to call between these 2 stations is restricted by default. To enable this assign the following…

   CM 6707>**XXYY**>**0** Where **XX** = **Location Group** (00~63) of calling **LG** and YY = called **LG**. **0** = Communication between locations, behind the same NAT, allowed. Default setting is 1 (LG under different NAT.

2. It is possible in some case scenarios to have IP-Dterms utilizing NAT within a system that is *also* supporting **IP-CCIS/Remote** PIM. To stop non-supported call attempts to these particular types of connections Location Group restrictions should be set. As explained on page 2, in some cases, a call attempt may setup but with only one way speech path. Restricting these calls is recommended to help reduce confusion. To restrict assign the following…

   CM 6708>**XXYY**>**0** XX = **Location Group** (00~63) of calling **LG** and YY = called **LG**. **0** = Communication between locations restricted.

3. Finally the IPLA PAD card at the main site must be identified.

   CM 0A65>**00~31**>**IP Address** Where **00~31** = the **LAN Interface** of the IPLA PAD card.

Conditions

1. NAT is supported with these devices only.

   Dterm85 (Series i) (IP Adapter Type)
   Dterm85 (Series i) (IP Bundled Type)
   DtermSP30
   PN-8IPLA (IP-PAD)

2. 3700 (R12.1) software is required for this feature.

3. NAPT Network Address Port Translation is not supported.