NAT - Network Address Translator

IP Networks Today: How We Got Here

Digital computers were invented in the 1940s, but strictly as stand-alone devices. Getting these computers to talk to each other took decades, but over time a variety of proprietary networking schemes were implemented. Eventually, Ethernet won out, but it was not practical to make Ethernet networks too large.

The solution was to create a separate Internetworking Protocol (IP). Ethernet collects user data into packets, and then creates a header which, among other things, contains the destination MAC address. IP creates an IP packet of user data, and then inserts an IP header with an IP address. This whole package is contained within the Ethernet packet, allowing the Ethernet portion of the network to perform normally. Routers at the edges of a LAN intelligently pass IP packets between themselves (contained within their own Ethernet packets), thus sectionalizing the streams. This makes the whole system manageable.

In the mid-1990s IP addresses were about to be exhausted. A new addressing scheme (IPv6) was created, but not implemented due to the disruption it would cause. Instead, various schemes to stretch the existing IPv4 scheme were implemented. One of these methods was Network Address Translation.

The idea was to isolate a portion of the internet, and use one set of addresses within the isolated portion, and another much smaller set only when needing to go into or out of the isolated portion. This is transparent to most users, since it is typically handled by a user's Internet service provider. IP addresses are generally handled behind the scenes on a dynamic basis, managed by a Dynamic Host Configuration Protocol server. As a result, the mass disruption sure to erupt if and when the Internet moves to IPv6 has been postponed, potentially indefinitely.

Definition of Terms

It should be understood that the terms LAN and WAN are quite informal. Whether a NAT device connection is on the WAN or LAN "side" is purely a function of the IP addressing scheme used to configure the device; the device itself does not care. While in a normal deployment the above reserved addresses are typically used for the "LAN side," and others only on the "WAN side," there are plenty of exceptions, and NAT devices support those exceptions.

Port is a term that can mean different things depending on the context. A physical port refers to the physical IP interface to a device, typically either an RJ-45 (for up to 1 Gb/sec) or fiber (for 10+ Gb/sec). But a port may also be a logical designation within a device. Normally a given device is running many applications, and many of these applications involve communications with some other device over an IP link. An IP address is used to indicate a particular physical port on a device, but it then an internal virtual port is assigned to a particular application. This is done at Layer 3 (UDP, TCP/IP, etc.); that is, it is an

Ethernet function, not an IP function (which is Layer 2). However, these virtual ports may also be used and altered by a NAT device. This allows individual data flows from a given device (typically via the same physical port, and hence the same IP address) to be treated individually.

As used above a data flow refers to communication between two devices using a single instance of a single application on each device. In the video world this would typically be one device sending streaming video, while another device receives it.

Simple Network Address Translation Devices

NAT devices are used for a wide variety of purposes. A simple use is to normalize the IP address schema, to put a given group of connected devices into the same address range, to simplify network administration. They can also be used as a controlled interface two or more networks, allowing defined (or all) widely separated devices to interact as if they were part of the same network.

Other Uses of Network Address Translation

While NAT certainly remains useful in its primary function of making the Internet actually usable, there are several other uses for the technology:

- The simple, one-to-one translation of one IP address to another very commonly used (it is part of what a firewall does), but there are other useful applications. For example, a device might require a static IP address, but it needs to be accessed by other devices in other networks. It is not uncommon for there to be multiple such requirements, on a data flow by data flow basis, even when using the same physical IP connection. In this case a NAT device at each location allows the connected device to act like a device on the remote network. As a slight tweak, it is quite common for data flows to be replicated. Indeed. A NAT device can readily convert between multicast (on a private network) and replicated unicast (over a non-multicast network such as the Internet).

    - A simple use is to normalize the IP address schema, to put a given group of connected devices into the same address range, to simplify network administration.

    - They can also be used as a controlled interface two or more networks, allowing defined (or all) widely separated devices to interact as if they were part of the same network.

- More basically, a user may simply want everything on a given physical port on the private network to move to and through some other network (such as the Internet). While relatively straightforward, this does require a NAT device, whether provided by the user or an Internet Service Provider (possibly both).

- Tunneling allows for the creation of dedicated links between networks. Since there is no standard for IP-to-IP tunneling, equipment allowing tunneling needs to be flexible to allow for creative solutions. This often is used to allow multicast or VLAN flows to cross the Internet (unicast) and then to be recreated as multicast and/or VLANs in the destination network(s). This can be used on a small scale for a single flow, up to bridging two or more networks together.

Evertz Solutions: 7880IPG-NAT-6-10GE, 570-NAT-X19-25G

Evertz has solutions to these problems optimized for the needs of video production and distribution: the 7880IPG-NAT-6-10GE, or the 570-NAT-X19-25G (in prototype as of this writing). These are both dual-slot cards that fit into standard Evertz frames. There are 12 physical ports, each an SFP+ slot that accepts a standard 1 Gb or (more commonly) 10 Gb SFP+ module; the 570-NAT-X19-25G can also accommodate 25 Gb. These use any or all of the six NAT Core processors, which may be paired for automatic failover. The total throughput of the 7880IPG-NAT-6-10GE is 1536 multicast or VLAN flows, the 570-NAT-X19-25G will be higher.

An Evertz NAT Core processor functions per the following diagram:

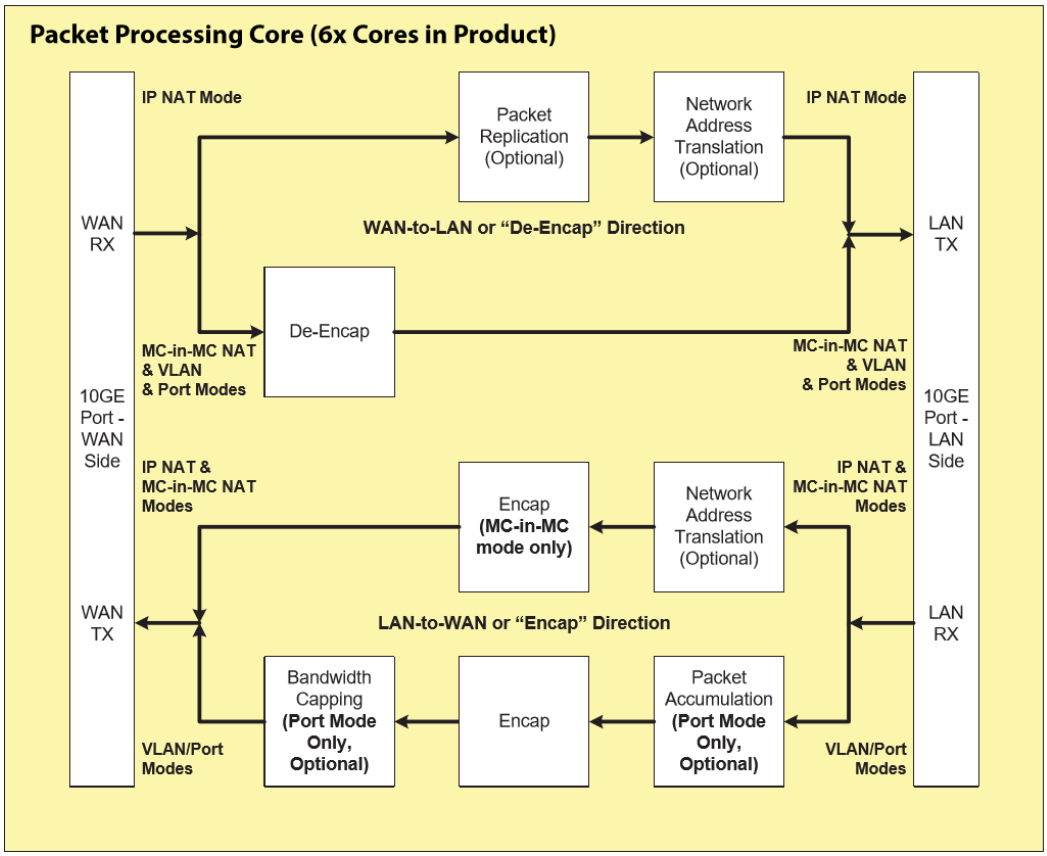


Figure 1: Functional Diagram

Control is via Evertz VistaLINK Pro™, Evertz MAGNUM™ and/or a separate Ethernet port on the card. In addition, Rest API is supported. Regardless, up to 50 virtual control interfaces may be used. Configuration is quite flexible, allowing anything from simple set-ups to detailed stream-by-stream customization. The set-up can be saved as a file, so in the event a card needs to be replaced it can be reset by copying in the saved set-up file, greatly simplifying system recovery.

Use Examples

A very simple use would be a basic one-to-one static address swap:

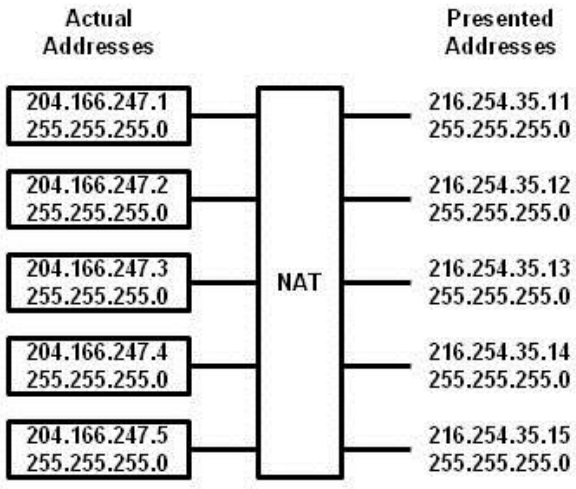
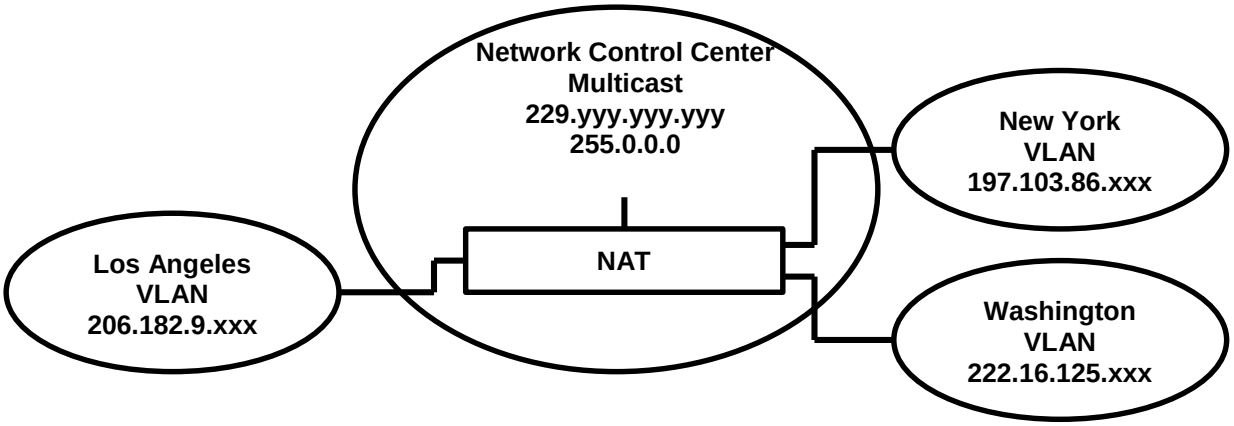


Figure 2: Static Address Swap

A single entity (e.g. a TV network) may have different entities (such as newsrooms) that it wants to process at a central location. The three separate locations have their own networks, and their own IP address schemes. A NAT allows the central control site to treat these as a single network:



A device in Los Angeles is sending out streaming video, and the Control Center wants to send that to New York. Rather than having some device at the Control Center having to process the video, using the NAT allows IP addressing to route the signal directly to New York, changing nothing bu the IP address. (In this example two NAT "Cores" would be used, one to change 206.182.9.xxx to 299.yyy.yyy.yyy, and then one to change that to 197.103.86.xxx.)

Figure 3: Tunneling Into Multiple Networks

In a similar fashion, a cable or satellite provider will aggregate inputs from multiple content providers, and want to treat these as part of their internal network:

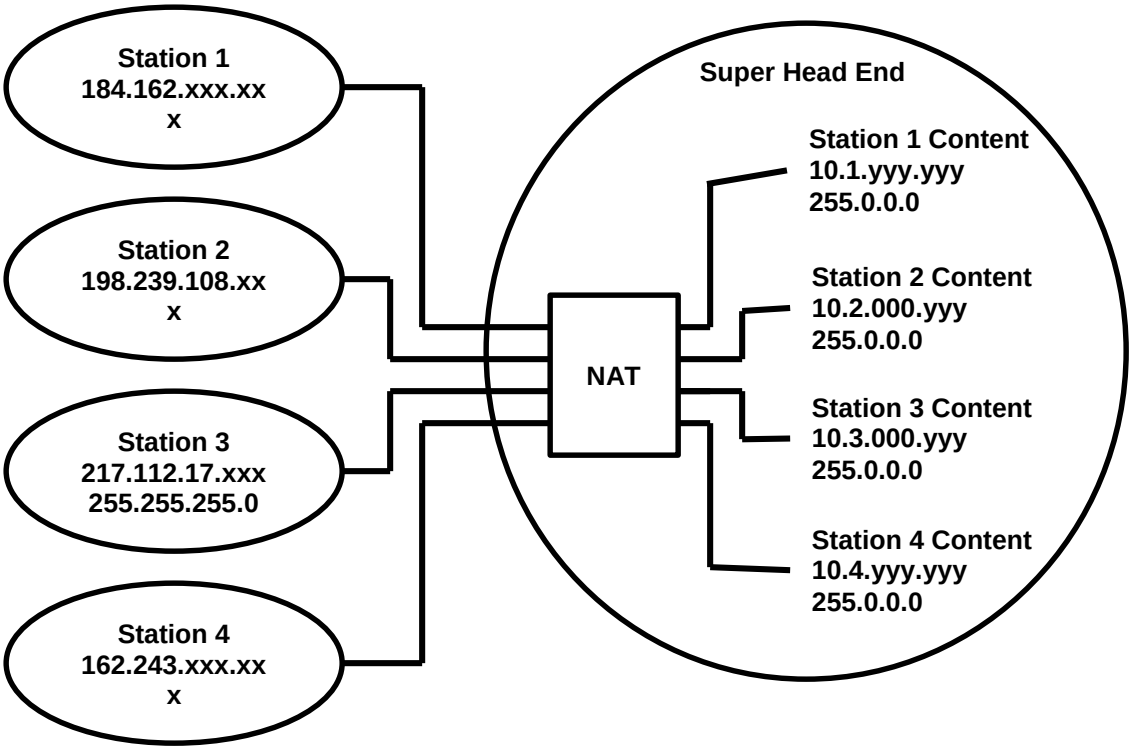


Figure 4: Feeds from Multiple Networks

It is not unusual for competing news organizations to cooperate by sharing content (for a fee), use press pooled sources, etc. Traditionally these have largely been handled through baseband video switching centers provided by telcos or other entities. NAT devices enable that to be done using Cloud services as simple as IP handoffs:

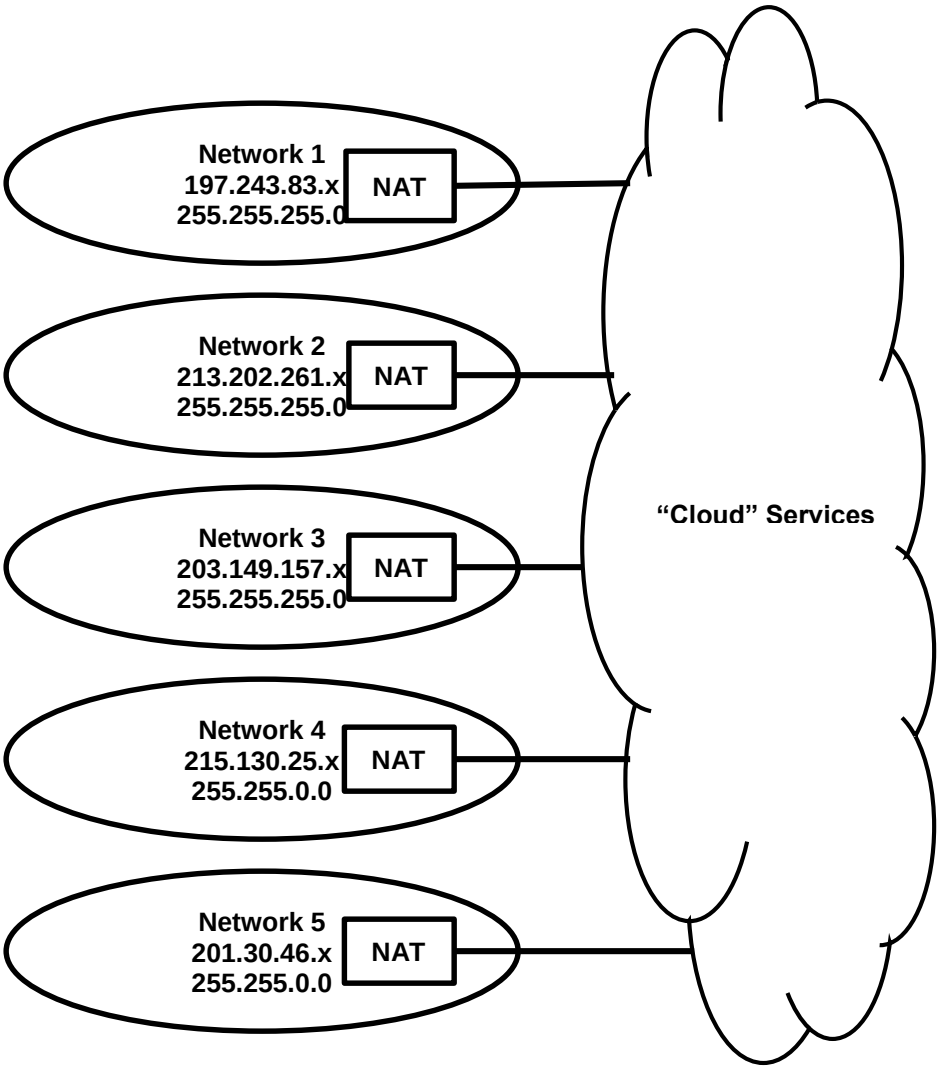


Figure 5: Using Cloud Services as a Shared Switch

Some networks support multicast, and some do not. A multicast network is more efficient at transporting one-to-many streaming videos, but to prepare the video to go out for distribution it may need to be converted to multiple VLAN connections. This can be done using the virtual ports to define the individual data flows:

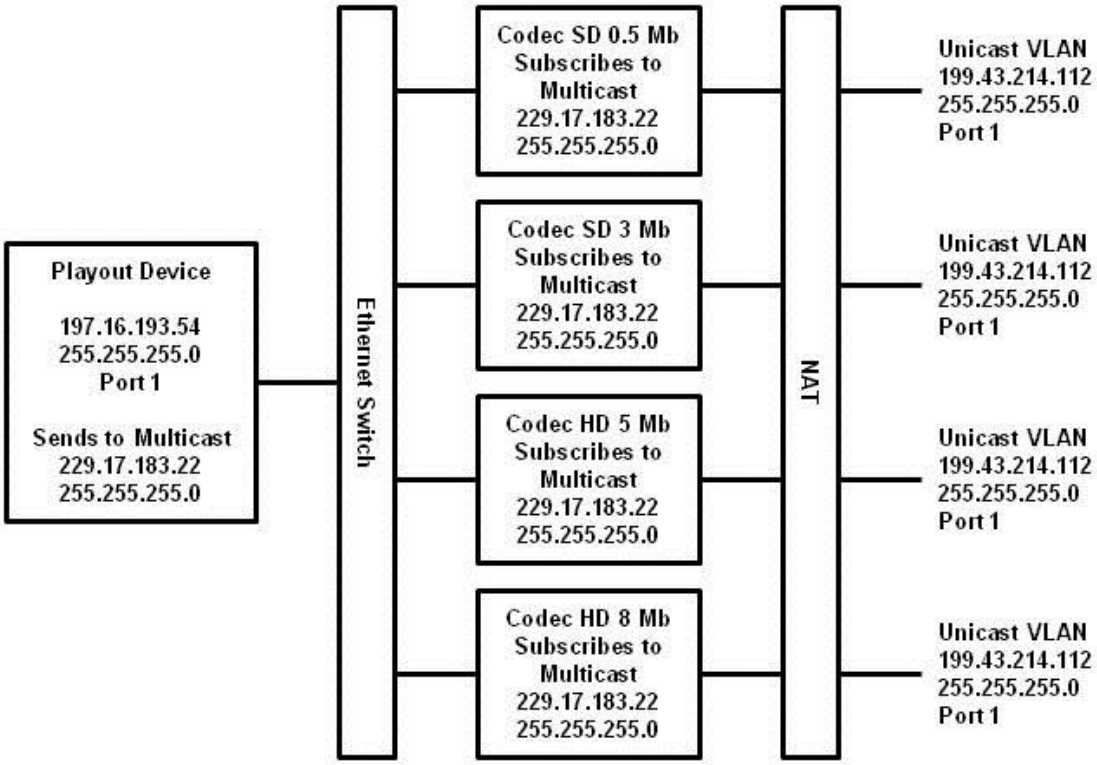


Figure 6: Combining Outputs onto one IP Address

Multicast provides an easy way to move a single video stream to multiple destinations. However, many networks do not have multicast enabled. With a NAT device, replication is easy, whether done from multicast to unicast or as native unicast:

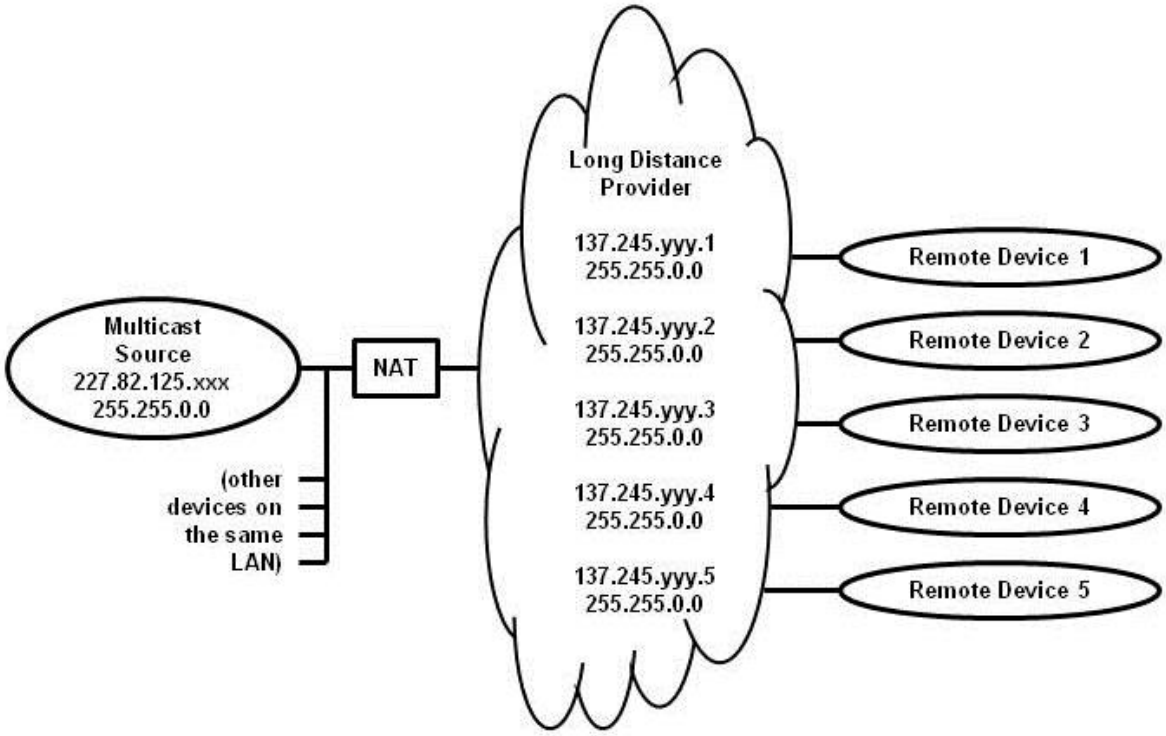


Figure 7: Replication of multicast onto unicast network

These are just a few very simple examples of the uses of NAT devices.

Redundancy and Backup

Multiple methods of backup, failover, route diversity, etc. are supported. Cores may be set up in pairs for a variety of failover arrangements, configurable down to the level of individual data flows.

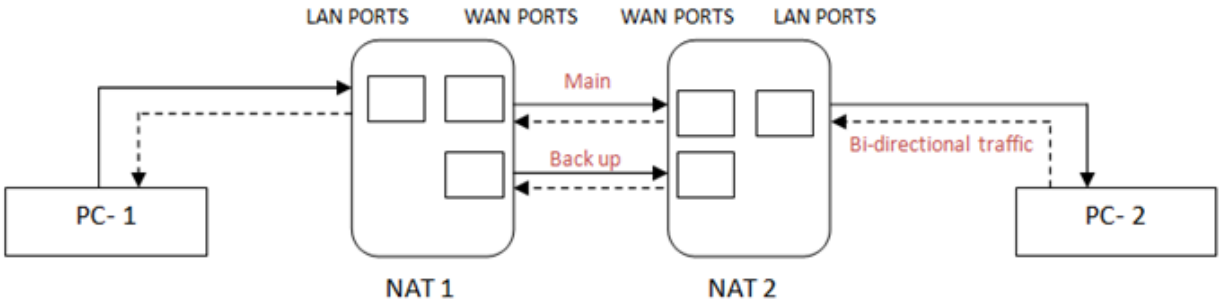


Figure 8: Redundancy Between Adjacent Cores

At either the physical port level or the data flow level, redundancy may be set up to revertive (use the main unless its bandwidth is zero), non-revertive (start on main, switch to backup if the main fails, but do not switch back to main until the backup fails), Force to Main or Force to Backup.

As the details are specific to individual installations there is no attempt here to illustrate the various backup architectures.

Summary

As video installations transition from baseband / ASI to IP new skills need to be mastered. Many of these include the uses of IP addressing schemes. NAT devices are a tool that unlocks the power inherent in IP.