Port Address Translation - PAT

- Port Address Translation (PAT) is a feature of a network device that translates communications made between hosts on a private network and hosts on a public network.
- PAT allows a single public IP address to be used by many hosts on the private network, which is usually a LAN.
- Cisco uses term PAT, while other vendors use different names:
  - Microsoft: Internet Connection Sharing,
  - Check Point: Hide-Mode NAT
- PAT is informally called router; gateway is more appropriate.
- PAT device sits at the network perimeter where one side connects the external network, usually the public Internet, and on the other side an internal network using private IP addressing.
- PAT operation is typically transparent to both the internal and external hosts.

PAT: Principles of Operation

- When a host in the private network sends its first packet to some host in the outside network (as either TCP SYN or UDP segment), the PAT device replaces the inside source IP address in the IP header with a single public IP.
- Also, it assigns to this connection a port number from the pool of available ports, inserts this number in the TCP/UDP header source port, and places the IP packet on the outside network.
- The PAT device then makes an entry in its translation table containing the inside IP address, TCP or UDP, inside source port, and assigned outside port.
- Subsequent packets from the same TCP connection on the inside IP address are always translated to the same outside port number (and outside IP address).

PAT: Principles of Operation (continued)

- The host in the external network receiving a data packet will move the source IP address and source port as the corresponding destination fields in any response it sends back.
- For packets arriving from outside, the PAT device operates on IP destination address and TCP/UDP destination port:
  - If the destination port number of the incoming TCP/UDP segment is not found as an outside port in the translation table, the IP packet is simple dropped.
  - Otherwise, the corresponding inside IP address and inside port number from the translation table replace, in the incoming packet, the destination address in IP header and the destination port in TCP/UDP header.
  - And, the modified IP packet is placed on the inside network.

PAT: Example

- A host at IP address 192.168.0.2 on a private network may ask for TCP connection to a remote host on the public network giving source address & source port 192.1680.2&15245.
- PAT device, with its public IP address 214.35.3.4, translates this source address & source port pair to 214.35.3.4 & 16529 (16529 was available in the pool) and make an entry in its internal table that port 16529 is in use by 192.168.0.2 on the private network with TCP connection on port number 15245.
- When a packet is received from the public network by the PAT device with 214.35.3.4&16529, the packet is forwarded to the internal network with destination IP address changed to 192.168.0.2 and with the port destination changed to 15345.

PAT Conclusion

- Advantages:
  - — multiple internal hosts can share a single IP address for communication, thus conserving precious IP addresses,
  - — hosts on the private network don't have to exposed their private IP addresses to the public network, making attacks from the public network less likely.
- Disadvantages:
  - — an organization using PAT and a single IP address cannot easily run more than one of the same type of public service behind a PAT, e.g. two Web public servers using the default port 80; Also, a remote login is possible only to one (designated) host in the private network.
  - — if many hosts on the private network make many connections to the public network, the PAT device may not have sufficient room in its internal table to keep track of the connections or it may simple run out of unused ports.

PPP Link Layer Protocol

- Point-to-point protocol (PPP) has been introduced to avoid proliferation in TCP/IP networks of many different data link control protocols, i.e. network access protocols.
- PPP is based on HDLC.

01111110	11111111	00000011	Protocol ID	Information	FCS	01111110
flag	address	control	2 bytes	0-1500 bytes	2 bytes	flag

- To achieve data transparency bit-stuffing is used.
- Protocol ID value 0021hex is used to indicate an IP packet is presents in info field.
- LCP (link control protocol) runs on top of PPP (Protocol ID C021 hex) is an integral part of PPP specification.
- LCP initiates and terminates connections gracefully, allowing hosts to negotiate connection options.
- LCP can provide authentication, encryption, compression and error detection (for identifying fault condition).