Network Address Translation, Remote Access and Virtual Private Networks

BSAD 146
Dave Novak

Sources: Network+ Guide to Networks, Dean 2013

Outline
- Discussion of Network Address Translation
  - How NAT devices and home routers work
- Remote Access Protocols
- Security Protocols
- Authentication Protocols

Network Address Translation (NAT)
- NAT allows you to connect multiple devices to the internet by using a single device or router (and one IP address) as a proxy (or intermediary) device
- NAT works by assigning temporary, reusable IP addresses to computers on the home network
- These computers communicate with the “outside world” THROUGH the proxy device

3 Functions of NAT
- 1) Switching
- 2) Routing
- 3) Translation

Network Address Translation (NAT)
- The NAT device sits in between the public internet and the private network it serves
- It rewrites IP addresses and port numbers in the IP datagram headers on the fly
  - The packets all appear to be coming from (or going to) a single IP address (the IP of the NAT device) instead of the actual source or destination
- This enables ALL home networks to use the “same set” of 192.168.x.x temporary reusable IPs

3 Functions of NAT
- 1) Switching
- 2) Routing
- 3) Translation

The NAT device keeps track of which PC (on the LAN) sends which information by identifying specific sockets (a combination of IP/port)
NAT
- Link to home networking info
- NAT can be:
  1) A PC configured to assign temporary IPs to home/small office network
     • This is also called PROXY SERVER
  2) A device you purchase, like a broadband router
     • http://www.dlink.com/products/broadband/di713p/

Proxy Server
- Two general types of proxy servers
  1) IP proxy
     • This is essentially the same thing as NAT
     • Assigning temporary IPs to local hosts in dynamic fashion
  2) Web proxy
     • Temporary storage of Web documents on local server
     • Reduce network traffic
     • Reduce time to receive Web documents

Web proxy server

NAT
- MS OSs
  • Come with some form of NAT or Internet Connection Sharing (ICS) built in
  • It is probably best to use a special device – like a broadband router as opposed to a PC
    • Why?

NAT
- High level applications that use TCP/IP have ports with preassigned numbers
  • HTTP = port 80
  • FTP = port 21
  • Telnet = port 23
- Port numbers 0 – 65536
  • Ports 0 – 1024 are typically reserved for specific services

NAT – How it works

You “lease” a single IP address from your provider, but you have 3 PCs on your home network that need IP addresses

Connection to ISP

PC #1

PC #2

PC #3

Hub or switch

Internet

Cat 5
NAT – How it works

NAT assigns temporary, reusable IPs to home computers on network

PC #1
PC #2
PC #3
NAT

You’re assigned 213.18.123.100 from ISP

Internet

NAT “chooses” IP address 213.18.123.100 to EVERY remote device on Internet, regardless of where the message originated locally (PC #1, #2, or #3)

NAT – How it works

PC #1
PC #2
PC #3
NAT

You’re assigned 213.18.123.100 from ISP

Internet

Internet

PC #3 sends HTTP request to remote Web server on Internet. The NAT receives packets from 192.168.0.14/port 500, and converts the outgoing message to 213.18.123.100/port 80 (for example). TCP stream coming back to NAT from Internet that are addressed to 213.18.123.100/port 80 belong to PC #3. NAT forwards these packets to 192.168.0.14/port 500 (this IP only has meaning on the home network). The Web server believes it’s communicating only with NAT – it is unaware of the existence of PC #3.

Remote Access

Remote access technologies allow users to log into a system without being physically present at the keyboard

- Remote access to a home network to access files or other resources
- Remote Desktop – more sophisticated access that essentially allows remote user to “see” and control a actual desktop from remote location

Remote Access

Services that allow users who are geographically separated from their “home” network to connect and log on to the network

- Access methods vary based on hardware and software usage (or requirements)

Remote Access

Client needs some kind of internet connection from their remote location

- Client needs to travel over an unsecure, public network, connect to the “home” network, and then go through a “home controlled” authentication process before being allowed to access resources on their “home” network

Remote Access

I’ll skip over Remote Desktop software solutions but you should check out some of the Virtual Network Computing (VNC) software available such as TightVNC (which I have used before)

Remote Access

- Functionality of remote access protocols
  - TCP and UDP are most commonly used layer 4 transport protocols (TCP/IP stack)
  - Layer 4 protocols are encapsulated in a remote access protocol frame (at layer 2) for transport over a WAN

Remote Access

- From a Network+ perspective
  - Remote Access Service (RAS) / Routing and Remote Access Server (RRAS) a remote access solution included with Windows Server products
    - Both products essentially provide the same service and provide both dialup and VPN support in a Windows environment

RAS and RRAS

- An application program interface (API) designed by Microsoft to utilize and management remote access in a Windows environment
- RRAS protocol converts a server into a dial-up Remote Access Services (RAS) server capable of handling hundreds of simultaneous connections

Remote Access Protocols

- Serial Line Internet Protocol (SLIP)
  - Originally designed for UNIX environments
  - Provides point-to-point communications using TCP/IP
- Point-to-Point Protocol (PPP) is more widely used (popular) than SLIP
  - Has MUCH more capability than SLIP
  - PPPoE (PPP over Ethernet) is the "default" standard for connecting home computers to an ISP via DSL or broadband cable

Remote Access Protocols

- SLIP is limited because it does not support:
  - Protocol stacks other than TCP/IP
  - Network connection authentication
  - Automatic negotiation of the network connection through multiple network connection layers at the same time
- SLIP:
  - Requires substantial overhead and setup time
  - Does not support date encryption
  - Supports only synchronous transmission
Virtual Private Networks (VPN)
- Connection between remote client and a server on a private LAN that uses the internet as opposed to direct, dedicated physical circuit
- Private LAN is permanently connected to the internet and has dedicated server configured to receive incoming VPN connections
- Remote user connects to internet in some way (say dialup) as opposed to directly connecting to their private LAN
- Provides a secure connection

Virtual Private Networks (VPN)
- VPN requires special software for each connected site
  - Allows only secure communication between remote host and **VPN server** – protects from unauthorized LAN access
  - Well known VPN protocols include
    - Point-to-Point Tunneling Protocol (PPTP)
    - Layer 2 Tunneling Protocol (L2TP)

Virtual Private Networks (VPN)
- Can use different tunneling, authentication, and security protocols
- Encapsulates data before sent across a public network
- Users connect through a local ISP to the local network
- Ensures that any data sent across a public network is secure via an encrypted tunnel

Virtual Private Networks (VPN)
- Combines advantages of both public and private networks
  - Allows company with multiple sites to have secure connection, but uses public network (Internet) as a carrier
  - Tunneling protocols carry encrypted data (and other protocols) over incompatible delivery networks

Virtual Private Networks (VPN)
- Point-to-Point Tunneling Protocol (PPTP)
  - Offers PPP-based authentication techniques
  - Encrypts data carried by PPTP through using Microsoft Point-to-Point Encryption
  - Supports encryption, authentication, and access services provided by RRAS

Virtual Private Networks (VPN)
- Users can dial directory into RRAS server (part of VPN) or dial into ISP RAS 1st, then connect to VPN
- Different NOS platforms can use PPTP although it provides less stringent security than some other tunneling protocols
Virtual Private Networks (VPN)
- Point to Point Tunneling Protocol (PPTP)
- Connection established between remote host and VPN server
- Data encapsulated

Security Protocols
- Security protocols are used to create a secure communication channel so that only computers using the same protocol can communicate
  - Internet Security Protocol (IPSec) – can be used with any TCP/IP communications
  - Secure Sockets Layer (SSL) – uses public key encryption and commonly used via the web
  - Wired Equivalent Protocol (WEP)
  - Wi-Fi Protected Access (WPA) – wireless protocol that improves upon WEP

Authentication Protocols
- Authentication protocols are used to verify a user’s identity
- Typically, once you establish a secure channel using a security protocol, you use an authentication protocol to verify users
  - Kerberos Authentication – most widely used authentication protocol
  - Challenge Handshake Authentication Protocol (CHAP)
  - Password Authentication Protocol (PAP)

Summary
- Basics of NAT and how NAT works
- What is remote access?
- Basics of VPN
- Understand basic differences between remote access, security, and authentication protocols