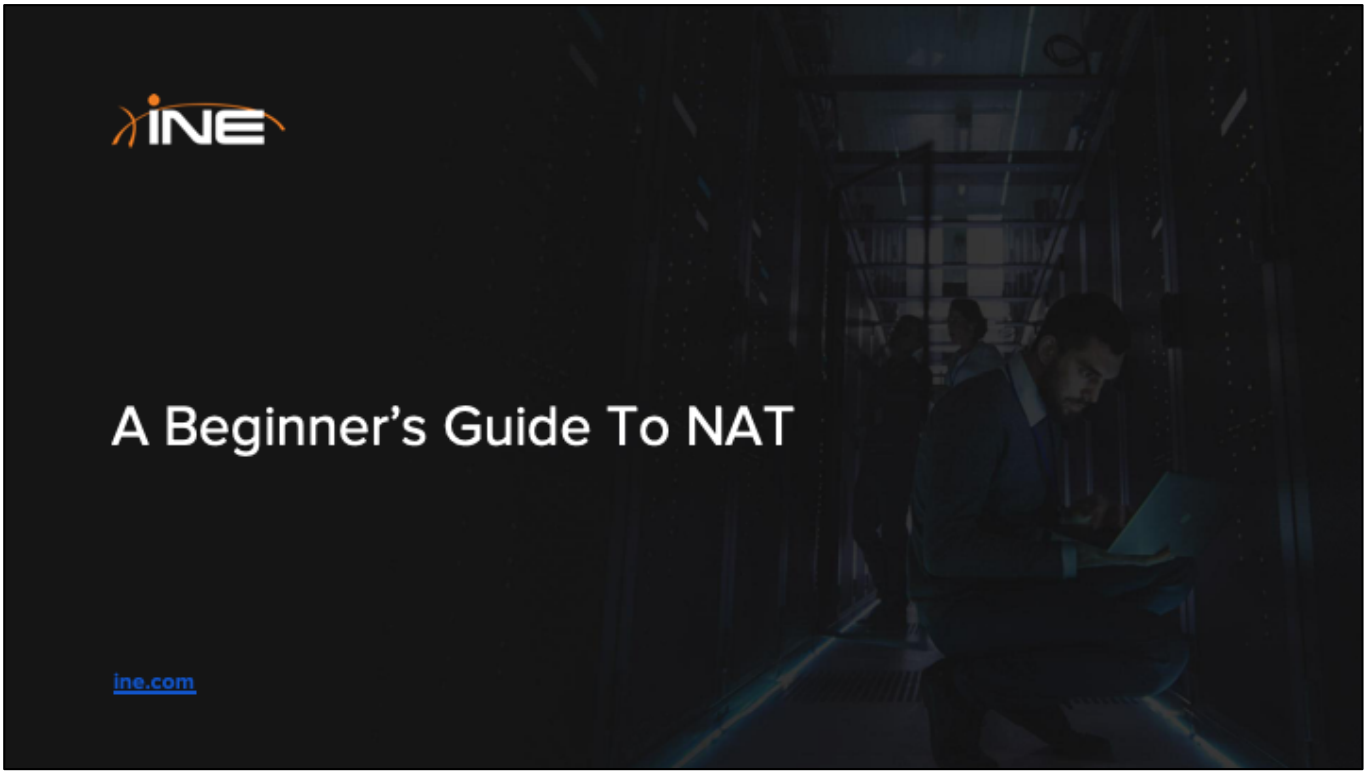

A Beginner’s Guide To NAT
ine.com

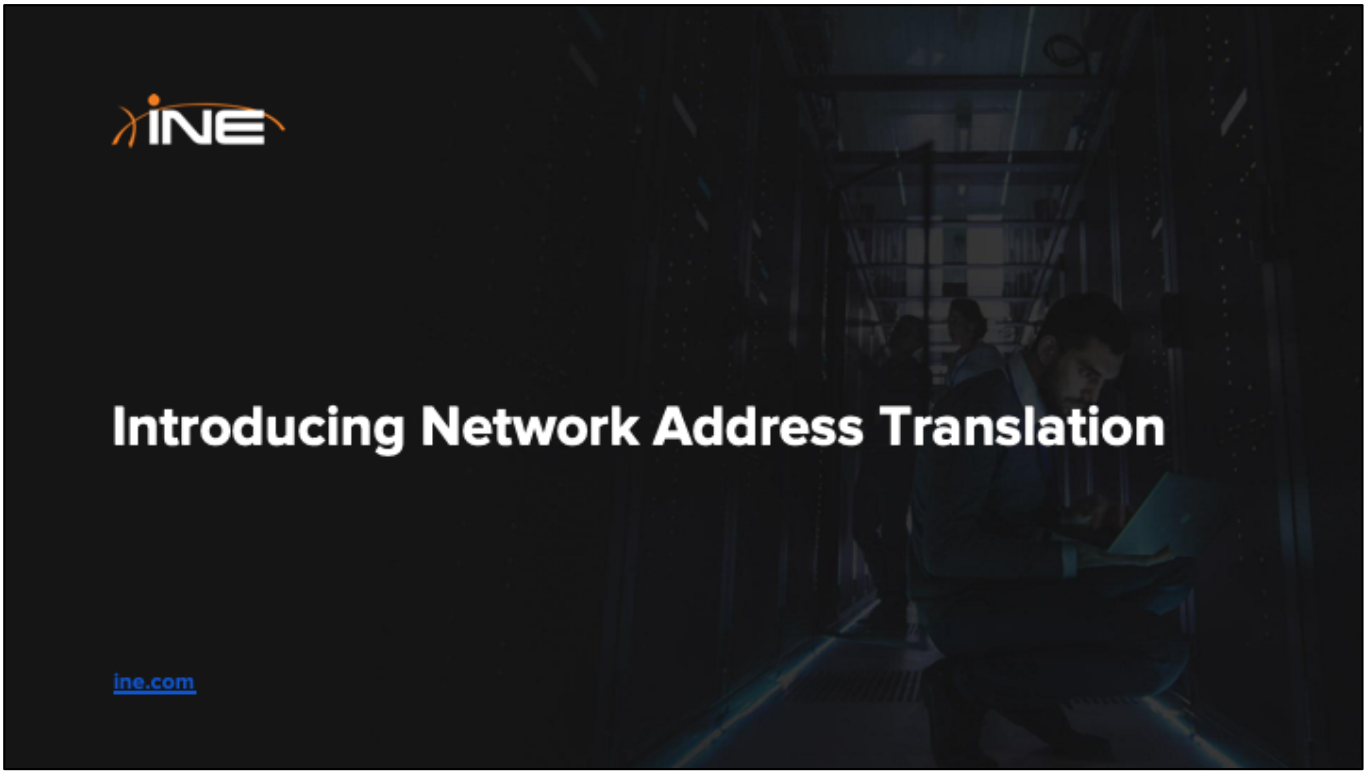

Keith Bogart
CCIE #4923
kbogart@ine.com
@keithbogart1
linkedin.com/in/keith-bogart-2a75042
CCIE Routing & Switching

Course Objectives

+ To help you gain familiarity with the concepts, and essential configuration commands for various forms of NAT

+ An understanding of how IPv4 addresses are used by routers in the routing of packets

Course Prerequisites


Introducing Network Address Translation
ine.com

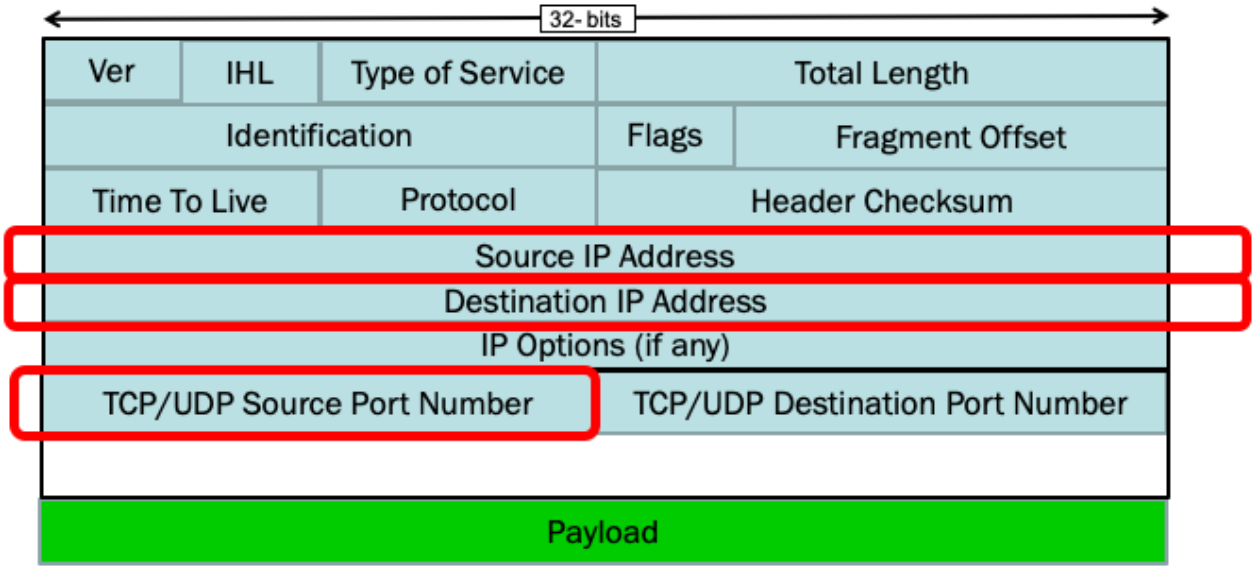
Topic Overview

+ Introduction To NAT
+ What Problem Was Solved By NAT?
+ NAT Translation Logic
+ NAT Terminology
+ Types Of NAT

Introduction To NAT

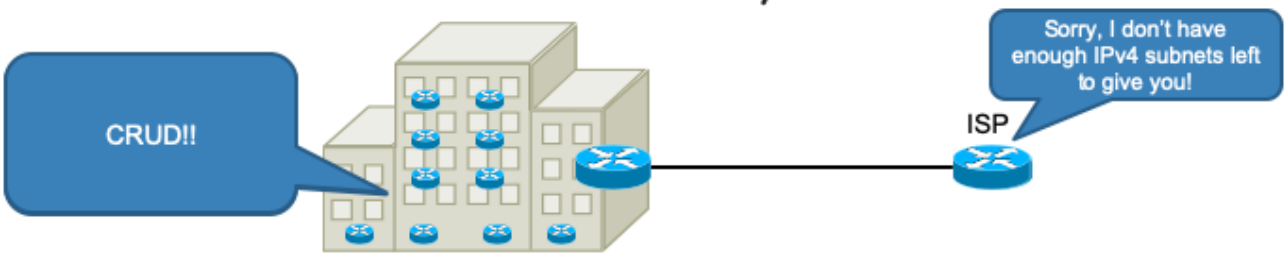
- Network Address Translation
- Translates IPv4 address in IP header
  - Typically translates source IP address
  - Can also translate destination IP address
  - Typically translates from private-to-public addresses
- NAT translation table ensures that reply packets are correctly translated back to original address

What Can NAT Change?



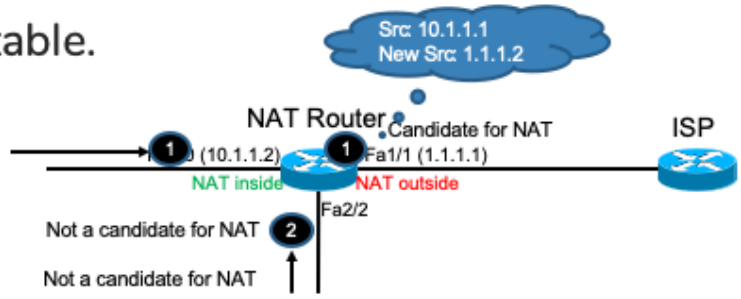
What Problem Was Solved By NAT?

- Originally, NAT was developed as a means to save $$ on the purchase of multiple, public IP subnets
- As IPv4 subnets became scarce, NAT became a viable method to extend the life of IPv4
- NAT is also useful as a security mechanism



NAT Translation Logic

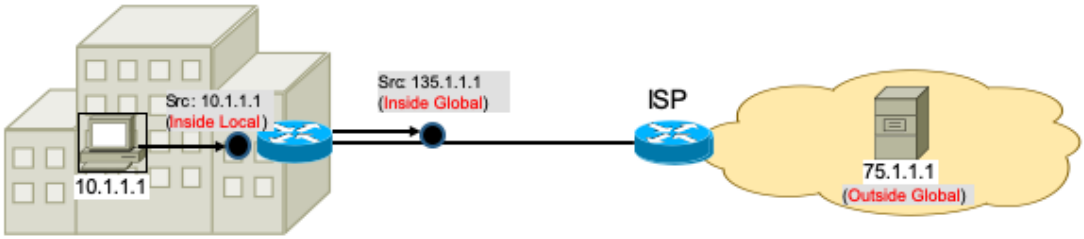
- Interfaces defined as NAT inside or outside
- Packet arrives on NAT inside interface
- Packet must be routed to NAT outside interface
- Packet must match pre-defined criteria for NAT
- Packet translated and record retained in NAT translation table.



Packet-2 is not a candidate for NAT because it did not arrive on an interface defined as NAT inside.

NAT Terminology

- Addresses are categorized as either “Local” or “Global”
  - Local = IP address from viewpoint of devices located on inside (pre-translated) networks
  - Global = IP address as viewed from devices located on outside (post-translation) networks

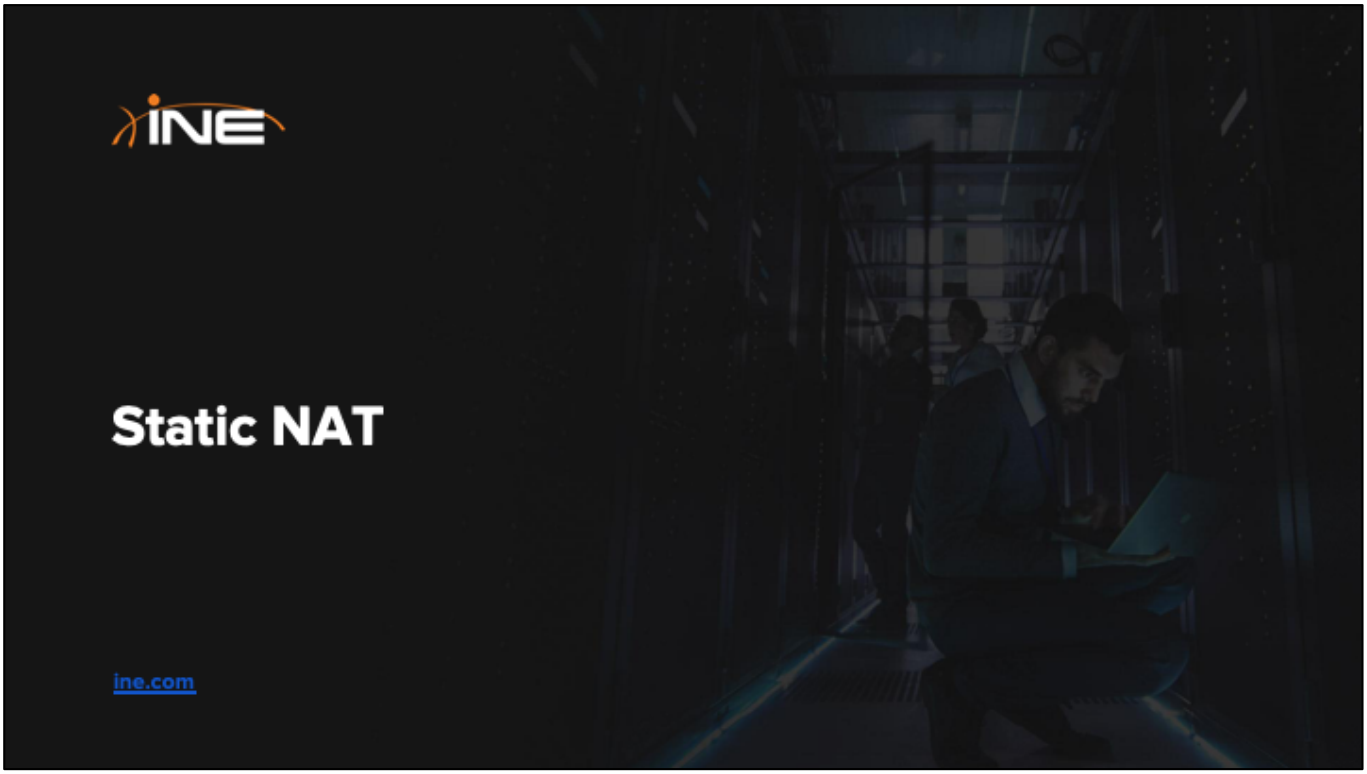


When NAT is used to translate both source and destination addresses, there is also a concept of an “Outside Local” address…which is how the outside device (server in this case) would be known by inside hosts.

Types Of NAT

- Static NAT
- Dynamic NAT
- NAT Overloading (Port Address Translation)

Thanks for Watching!


Static NAT
ine.com

Topic Overview

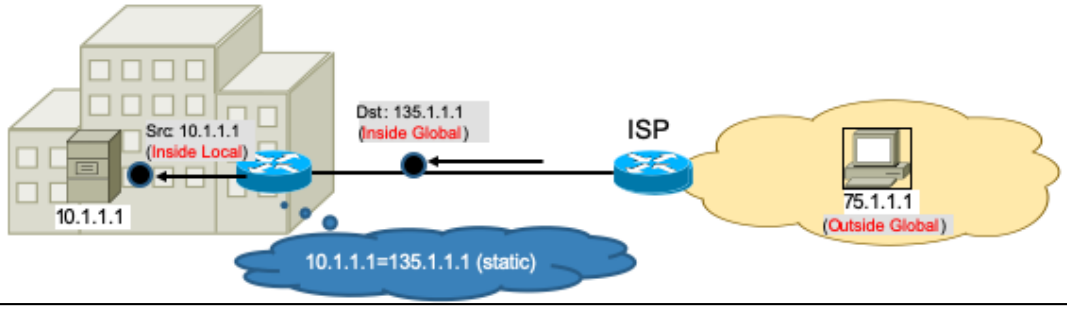
+ Static NAT Overview
+ Configuring Static NAT
+ Verifying Static NAT

Static NAT Overview

- One to one mapping
- One inside host IP requires a matching outside (global) IP address
- Usually deployed at server end
  - Removes the security of dynamic NAT
  - Useful when outside hosts need to initiate connections to inside hosts

Configuring Static NAT

- Configuration commands
  - Router(config-if)# ip nat inside
  - Router(config-if)# ip nat outside
  - Router(config)# ip nat inside source static <private address> < public address>



In this configuration, the term “private address” is synonymous with “inside local”. And the term “public address” is synonymous with “inside global”.

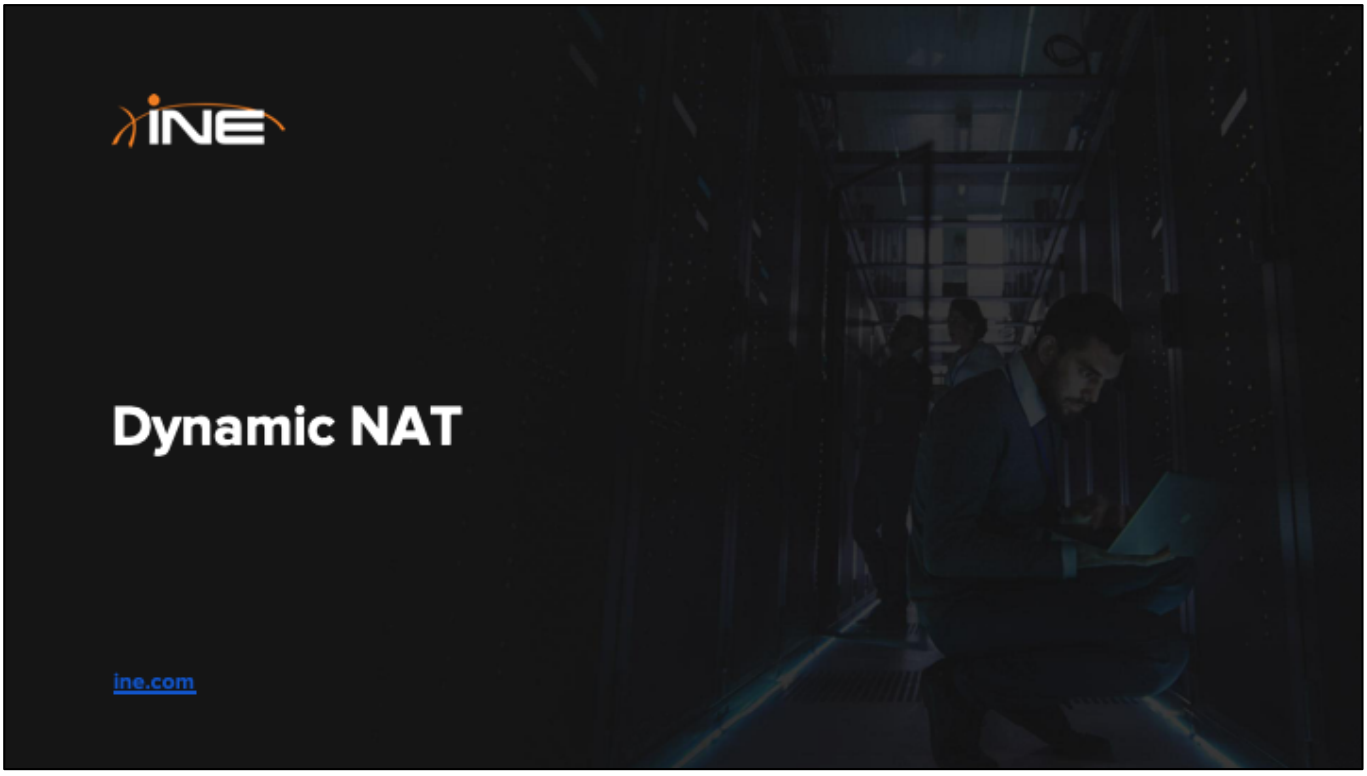
Verifying Static NAT

- Verification commands
  - Router# show ip nat translation
  - Router# show ip nat translation verbose

```
R2-NAT#show ip nat translation verbose
Pro Inside global      Inside local       Outside local      Outside global
--- 135.1.1.1          10.1.1.1           ---                ---
    create 00:03:48, use 00:03:48 timeout:0,
    flags:
static, use_count: 0, entry-id: 1, lc_entries: 0
```

The “use_count” field in this output keeps track of individual flows of traffic from the same source IP address however it DOES age out after a while.

Thanks for Watching!


Dynamic NAT
ine.com

Topic Overview

+ Overview Of Dynamic NAT
+ Configuring Dynamic NAT
+ NAT Translation Timeouts
+ Modifying NAT Timeout Values
+ Verifying Dynamic NAT

Overview of Dynamic NAT

- Many to many mapping
- One private host requires a public IP address obtained from a pool of available addresses
- Usually deployed for hosts utilizing DHCP
- Useful when Source/Destination Layer-4 port numbers need to be retained

Configuring Dynamic NAT

- Configuration commands
  - Router(config-if)# ip nat inside
  - Router(config-if)# ip nat outside
  - Router(config# access-list < acl no> <permit | deny > <source-address> <wildcard mask>
  - Router(config)# ip nat pool <name> <start-ip> <end-ip> netmask <subnet mask>
  - Router(config)# ip nat inside source list < acl no> pool <name>

```
R2-NAT(config)#ip nat pool Dynamic 135.1.1.1 135.1.1.10 netmask 255.255.255.248
%Pool Dynamic mask 255.255.255.248 too small; should be at least 255.255.255.240
%Start and end addresses on different subnets
```

Notice that the “netmask” keyword (which can also be entered as a prefix-length keyword) verifies whether enough addresses have been allocated based on the size (i.e. netmask) of the internal/local network(s) you need to translate.

NAT Translation Timeouts

- Dynamic NAT translations have an inactivity timer
- Upon expiration of the timer a translation is removed
- Different protocols have different default timeouts

Common Protocol	NAT Timeout Value
TCP	24-hours
UDP	5-minutes
ICMP	1-minute

Modifying NAT Timeout Values

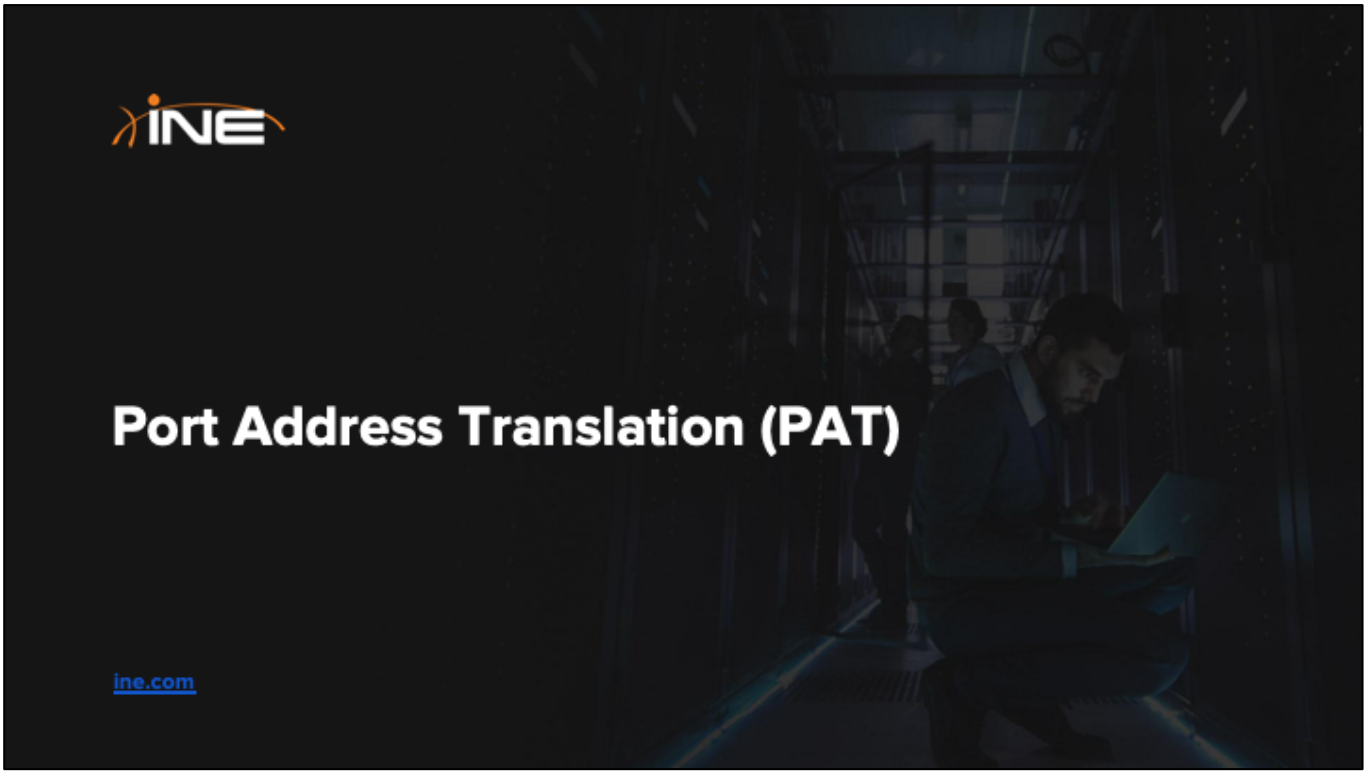
```
R2-NAT(config)#ip nat translation ?
  arp-ping-timeout        Specify timeout for WLAN-NAT ARP-Ping
  dns-timeout             Specify timeout for NAT DNS flows
  finrst-timeout          Specify timeout for NAT TCP flows after a FIN or RST
  icmp-timeout            Specify timeout for NAT ICMP flows
  max-entries             Specify maximum number of NAT entries
  port-timeout            Specify timeout for NAT TCP/UDP port specific flows
  pptp-timeout            Specify timeout for NAT PPTP flows
  routemap-entry-timeout  Specify timeout for routemap created half entry
  syn-timeout             Specify timeout for NAT TCP flows after a SYN and no
                          further data
  tcp-timeout             Specify timeout for NAT TCP flows
  timeout                 Specify timeout for dynamic NAT translations
  udp-timeout             Specify timeout for NAT UDP flows
```

Verifying Dynamic NAT

- Verification commands
  - Router# show ip nat translation

```
R2-NAT#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
tcp 99.99.99.5:35779   10.1.1.1:35779     99.99.99.3:23      99.99.99.3:23
--- 99.99.99.5         10.1.1.1           ---                ---
tcp 99.99.99.4:51183   10.1.1.4:51183     99.99.99.3:23      99.99.99.3:23
--- 99.99.99.4         10.1.1.4           ---                ---
```

Thanks for Watching!

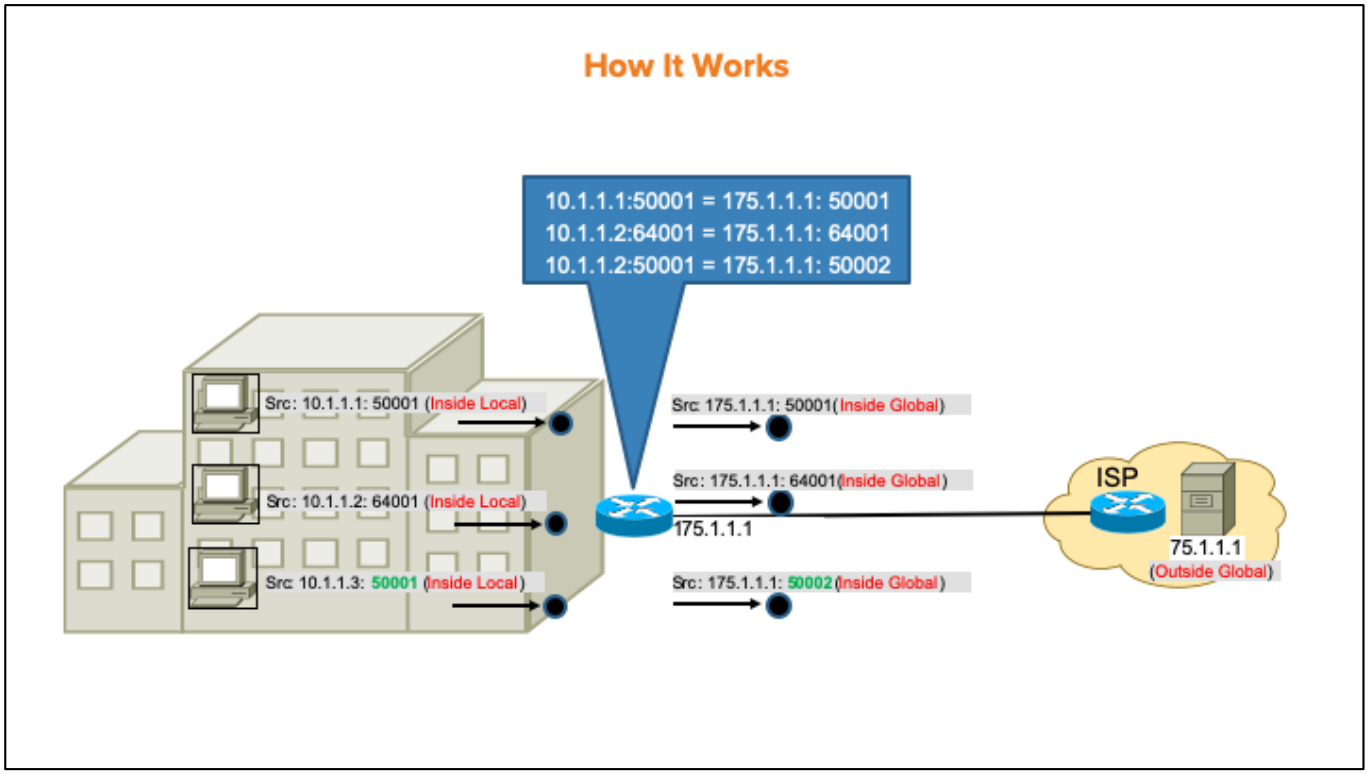

Port Address Translation (PAT)
ine.com

Topic Overview

+ PAT Overview
+ How It Works
+ Configuring PAT
+ Verifying PAT

PAT Overview

- Port Address Translation
- Also called NAT Overload
- One to many mapping
- One public address can provide multiple host connections
- Most scalable form of NAT



With PAT, it cannot be assumed that an incoming local packet will always have its source port number changed. It depends on what currently exists in the NAT Translation table. If there is no current entry using that same source port, the original source port number will be retained, unchanged. Only when an existing entry exists in the translation table with the same source port number will a new flow of traffic (using the same source port) need to be changed by PAT.

Configuring PAT

- Configuration commands
  - Router(config-if)# ip nat inside
  - Router(config-if)# ip nat outside
  - Router(config# access-list < acl no> <permit | deny > <source-address> <wildcard mask>
  - Router(config)# ip nat inside source list < acl no> interface <type/number> overload

Verifying PAT

- Verification commands
  - Router# show ip nat translation

```
R2-NAT#
R2-NAT#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
tcp 99.99.99.2:59656   10.1.1.1:59656     99.99.99.3:23      99.99.99.3:23
icmp 99.99.99.2:0      10.1.1.4:0         99.99.99.3:0       99.99.99.3:0
tcp 99.99.99.2:20697   10.1.1.4:20697     99.99.99.3:23      99.99.99.3:23
```

Thanks for Watching!