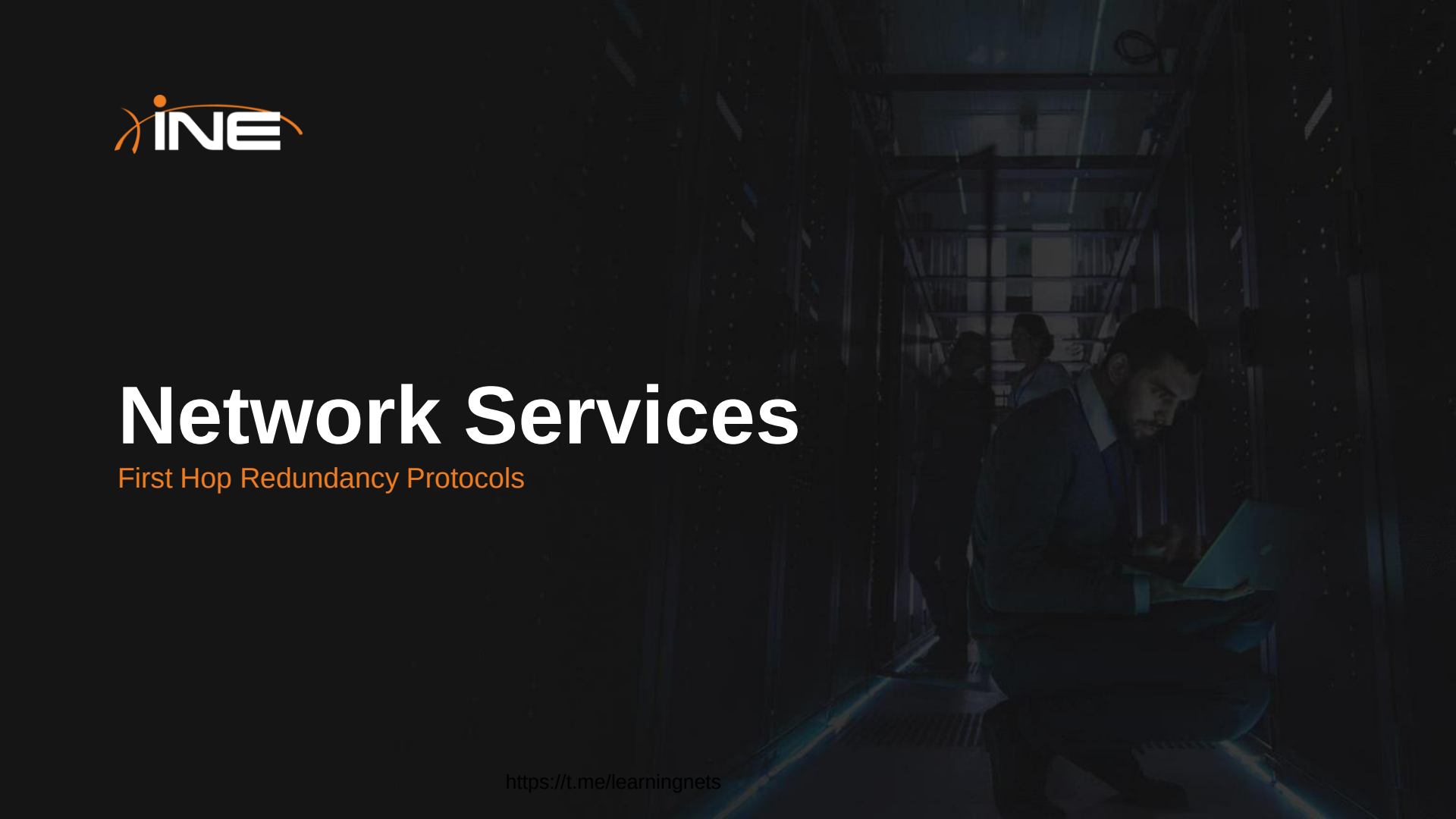


Network Services

First Hop Redundancy Protocols

In This Section

- First Hop Redundancy Overview
- HSRP, VRRP, & GLBP
- FHRPs and Enhanced Object Tracking
- FHRP Support for IPv6

What is First Hop Redundancy?

- Used to provide end host default gateway failover
  - 2 or more default gateways work together for redundancy
- Implemented by using virtual IP/MAC
  - Multiple gateways have the same virtual IP
  - End hosts use virtual IP as default gateway
  - Only one router responds to ARP requests for virtual IP
  - ARP response contains virtual MAC address
- If active gateway fails, backup becomes active
  - Failure detected via a keepalive protocol
  - The backup assumes virtual MAC and IP upon primary failure

HSRP

- Cisco proprietary, but RFC defined
  - RFC 2281 - Cisco Hot Standby Router Protocol (HSRP)
- Elects active gateway based on priority
  - 100 is the default, 255 is maximum
  - Highest IP as the tie-breaker
  - Non-preemptive by default
- Uses UDP multicast 224.0.0.2 at port 1985 for transport
  - Messages can be authenticated using clear text or MD5
- Supports multiple groups per interface
  - Group ID encoded in virtual MAC 0000.0c07.acXX

VRRPv2

- Virtual Router Redundancy Protocol
  - Standards based alternative to HSRP
  - RFC 3768 - Virtual Router Redundancy Protocol (VRRP)
  - Uses terms master/backup as opposed to active/standby
- Other concepts are similar
  - Uses own transport protocol 112 to IP 224.0.0.18
  - Virtual MAC is 0000.5E00.01XX
  - Preemptive by default

GLBP

- Gateway Load Balancing Protocol
  - Cisco Proprietary Protocol
  - Extends HSRP functionality to support load balancing
  - Transport via UDP port 3222 to IP 224.0.0.102
- Every physical gateway may now be active
  - Called Active Virtual Forwarders (AVF)
  - Each AVF assigned a virtual MAC address
- One gateway responds to ARP requests for GLBP IP
  - Called Active Virtual Gateway (AVG)
  - ARP response uses virtual MACs of AVFs to implementing load-balancing

GLBP (cont.)

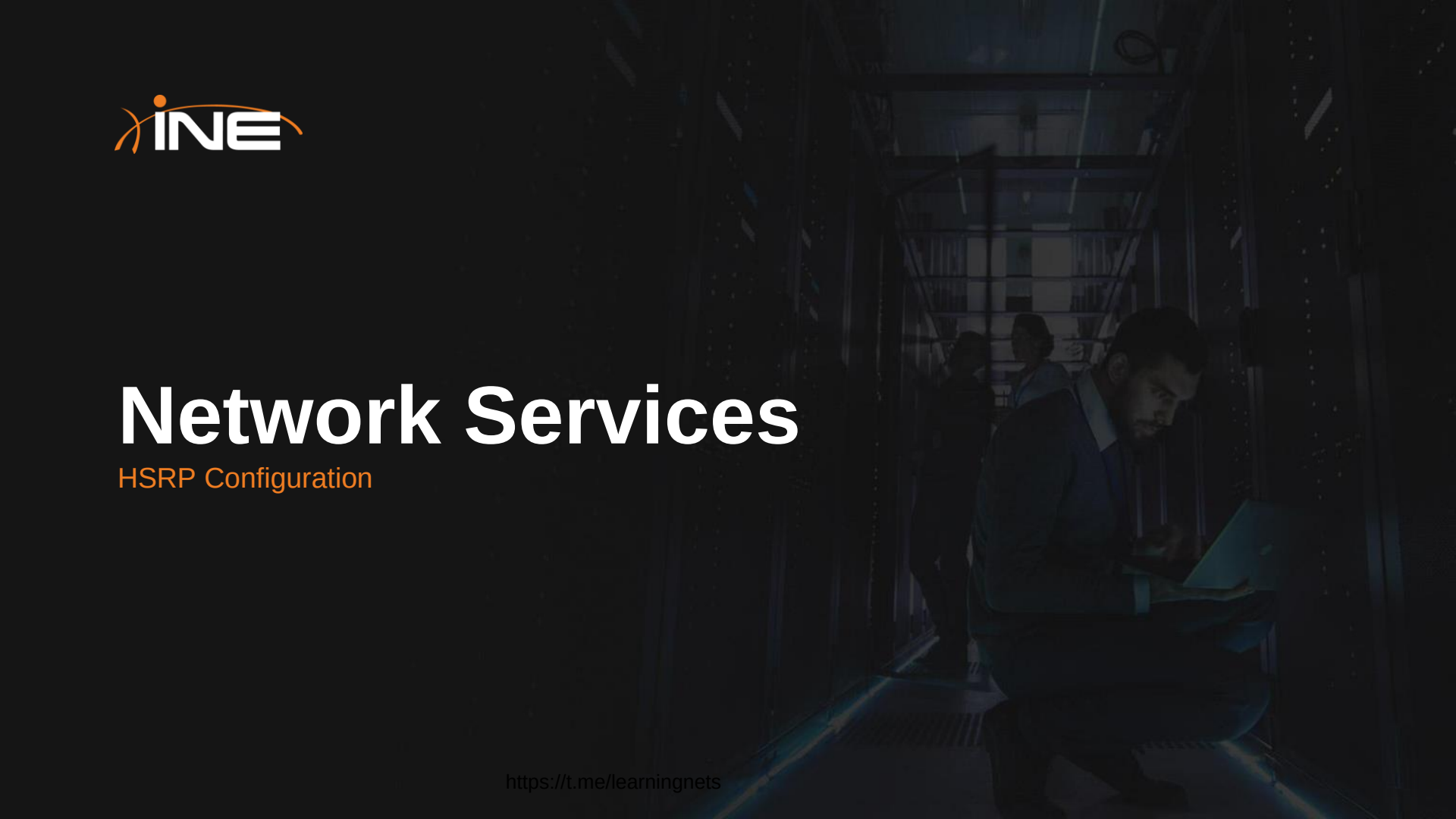
- AVG elected based on priority
  - By default AVG is the only AVF, all other are standby
  - No AVG preemption by default
    - Enable using **glbp preempt**
- To enable load-balancing…
  - Command **glbp xxx load-balancing weighted**
  - Assign weights with **glbp xxx weighting Y**
- Weight can be adjusted based on object tracking

FHRPs and Enhanced Object Tracking

- Gateway recovery relies on correct failure detection
  - E.g. FHRP keepalives or BFD
- What if southbound link is up but northbound is down?
  - Result is Active/Master router maintains state but cannot forward
  - Solution is to integrate FHRPs with Enhanced Object Tracking
    - E.g. IP SLA
- Object tracking is bound to priority
  - Decrement priority if object is down
  - Assumes preemption is configured

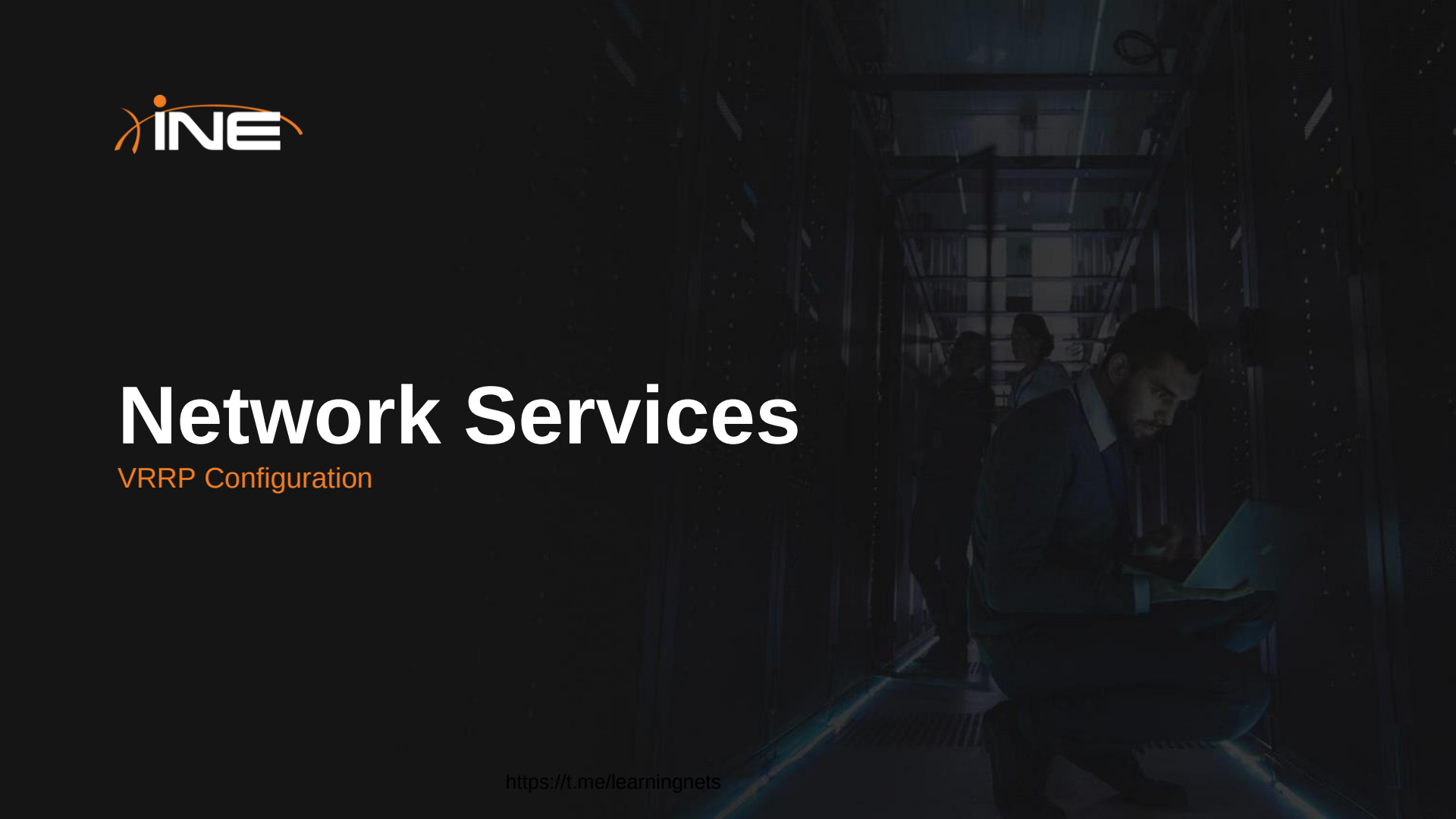
FHRP Support for IPv6

- HSRPv2
  - Increases group range
  - Adds new dedicated transport address 224.0.0.102
    - Doesn't overlap with ALL ROUTERS
  - Adds IPv6 support
  - Enabled with interface level **standby version 2**
- VRRPv3
  - RFC 5798 - Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6
  - Enabled with global **fhrp version vrrp v3**



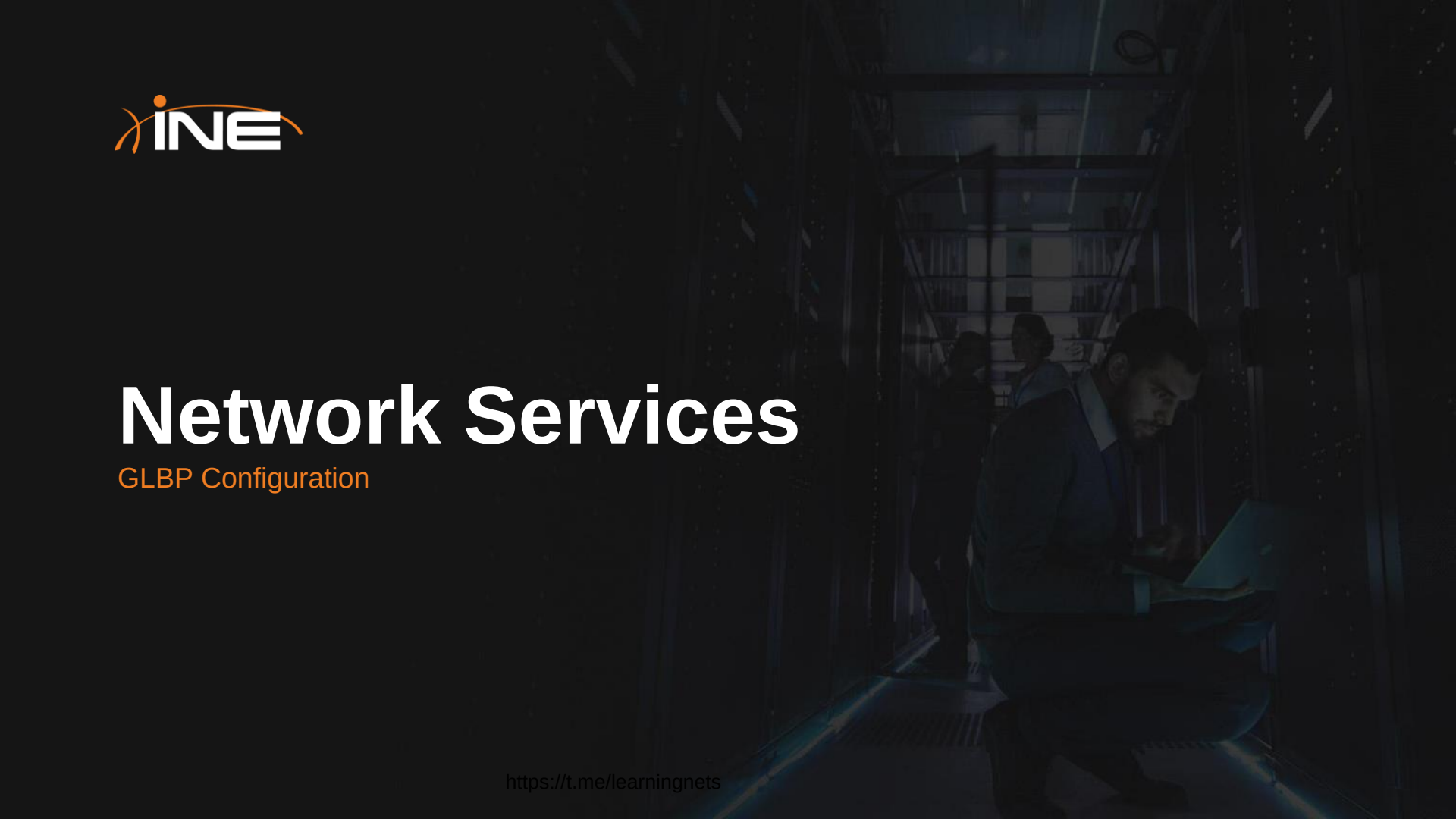
Network Services

HSRP Configuration



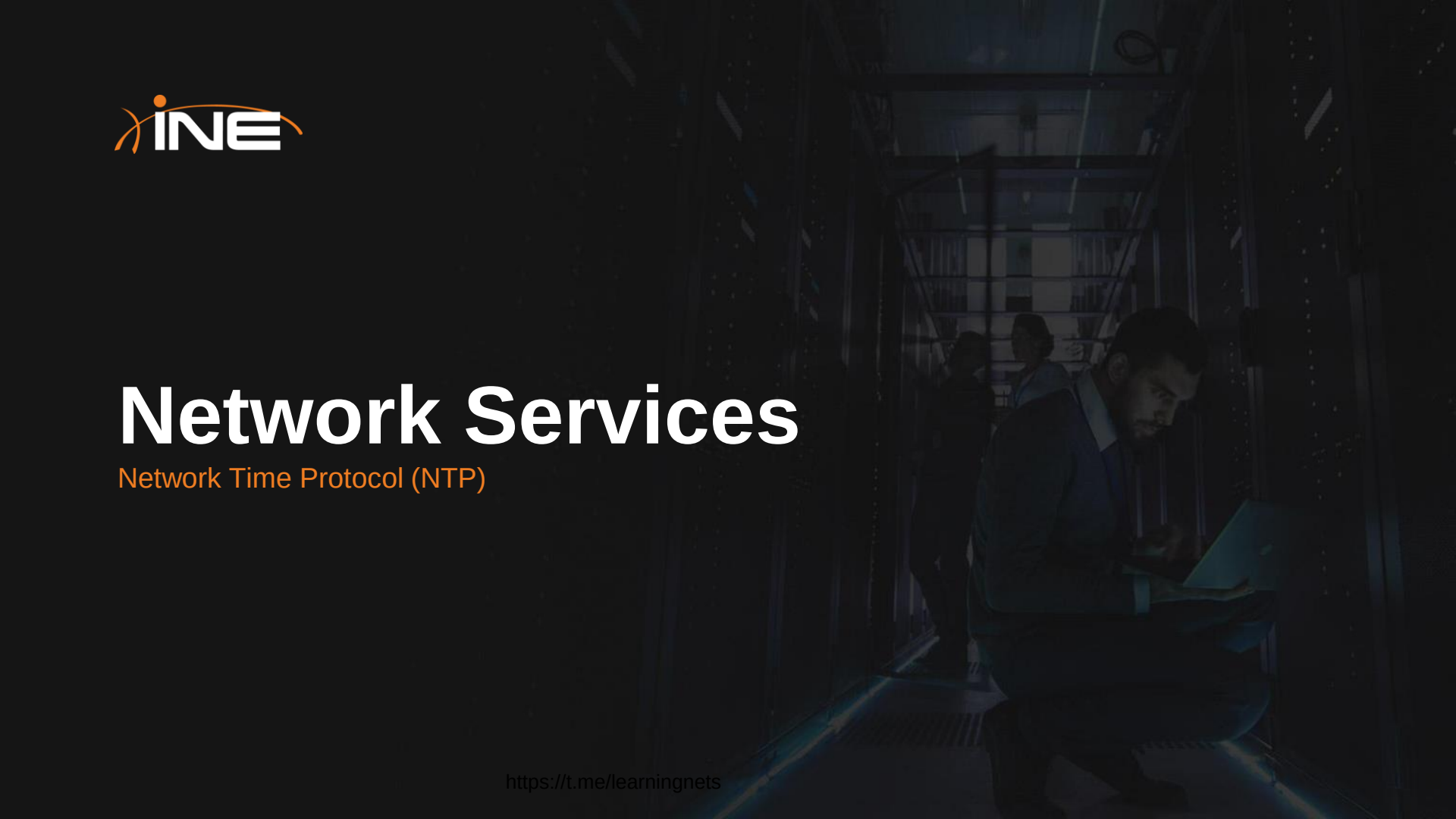
Network Services

VRRP Configuration



Network Services

GLBP Configuration

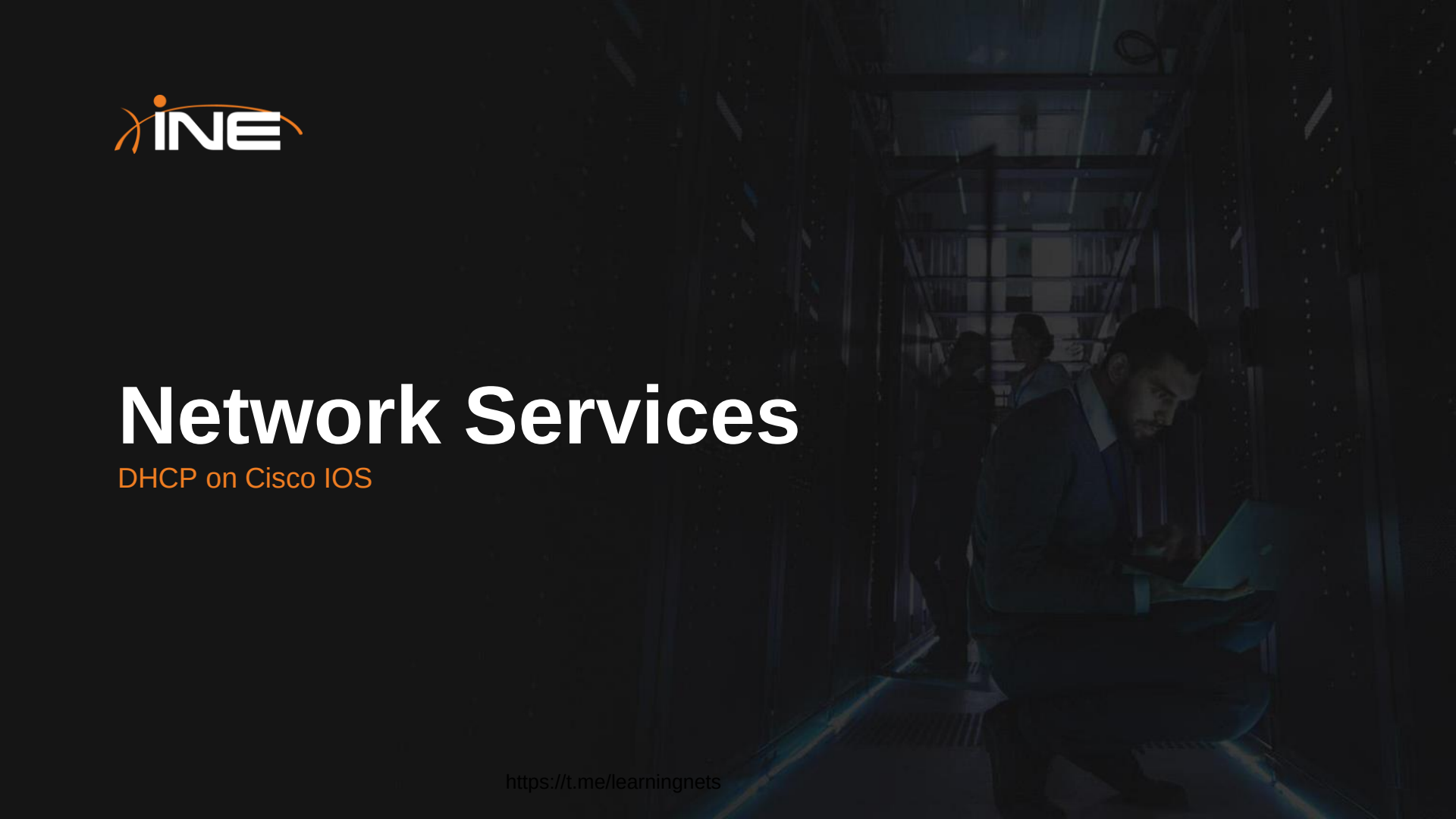


Network Services

Network Time Protocol (NTP)

In This Section

+ NTP Configuration Examples



Network Services

DHCP on Cisco IOS

In This Section

+ IOS DHCP Server, Client, & Relay

DHCP in IOS

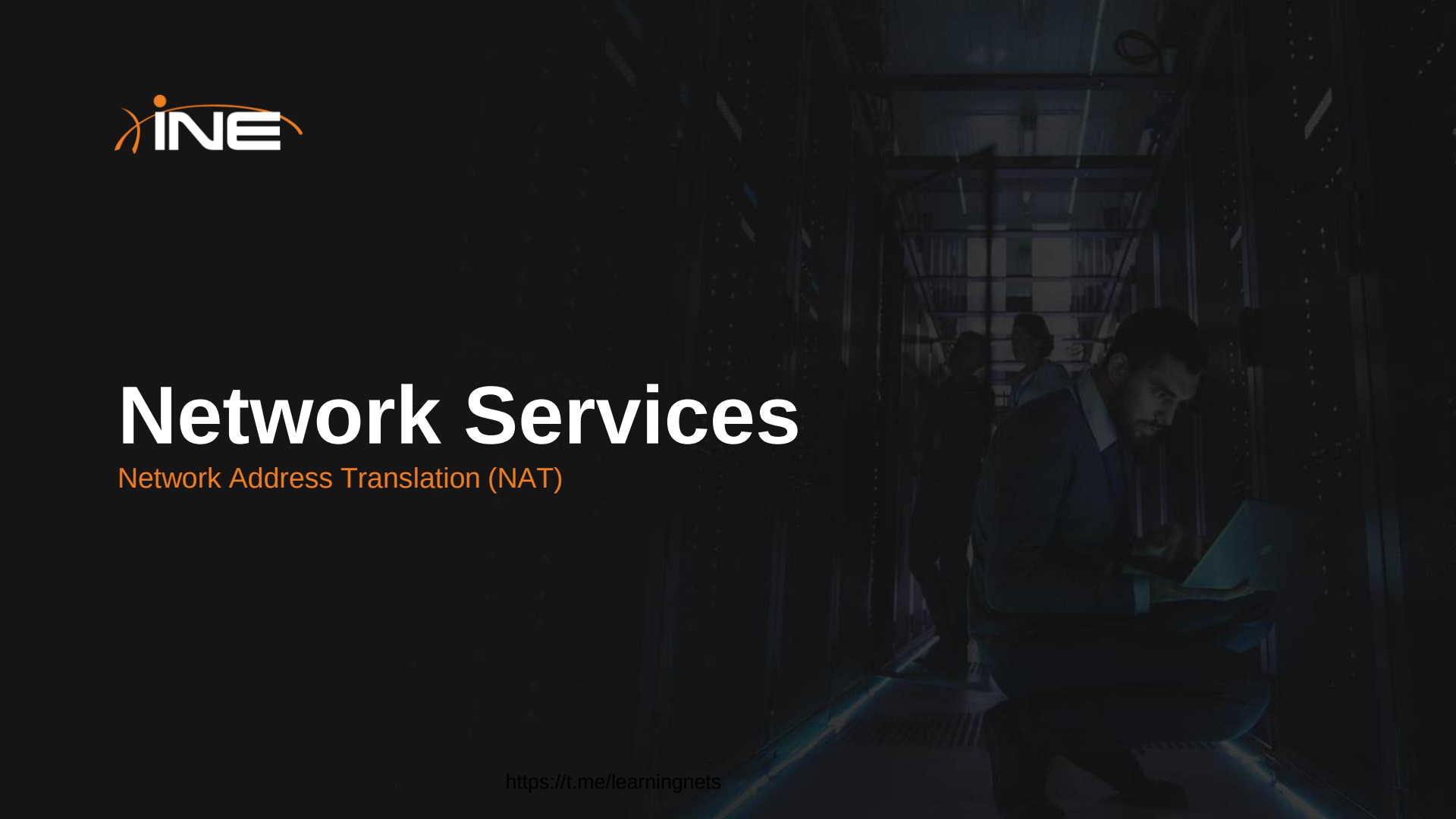
- DHCP in IOS supports…
  - DHCP server
  - DHCP client
  - DHCP proxy
    - E.g. translate IPCP request into DHCP
  - DHCP relaying

IOS DHCP Server

- Server configured using DHCP pools
  - Each pool has an IP subnet for allocation
  - Host pools are supported
- Pool is selected based on…
  - DHCP Client ID (could be any string)
    - Supplied by Windows clients but not Linux
  - DHCP Hardware Address if ID is missing
  - Relaying gateway IP address
  - Receiving interface IP subnet if no matching pool found and no relay IP address present

IOS DHCP Relaying

- Broadcast can be relayed to unicast
  - **ip helper-address <IP>** interface command
- In case of DHCP, relaying router inserts interface IP address
  - Known as “giaddr” or gateway address
  - Other options could be inserted, e.g. Information Option
- DHCP server matches pool based on giaddr



Network Services

Network Address Translation (NAT)

In This Section

+ NAT Overview
+ NAT Configuration Examples

Network Address Translation

- Rewrites source IP addresses in packet
  - Normally to hide private IP addresses
  - Can also resolve overlapping subnet issues
- Destination IP rewrite may be used for redirection
  - Normally configured as static mapping
- Port Address Translation
  - Many to one translation based on TCP/UDP port
  - Common for overloading scenarios

NAT Terminology

- Inside zone - networks that translator wants to hide
  - Inside local - Inside IPs before translation
  - Inside global - Inside IPs after translation
- Outside zone - networks that are external to translator
  - Outside global - Original outside IP address
  - Outside local - Outside IP after translation as it seen inside

NAT Order of Operations

- On the inside
  - Packets are first routed and then have sources translated
  - Destination addresses are global so this is OK
- On the outside
  - Packets have destinations un-translated first
  - Routing occurs after translation
  - Allows proper routing for returning packets with translated sources

VRF Aware NAT

- Used to leak traffic from VRF table to global table
- Requires static routing with next hop and **global** keyword
  - **ip route VRF1 0.0.0.0 0.0.0.0 gig0/1 1.2.3.4 global**
- NAT statement is VRF aware
  - **ip nat inside source list 1 interface gig0/1 vrf VRF1 overload**

VRF Aware NAT on IOS XE

- Classical inter-vrf nat configuration not supported in IOS XE
- Inter-vrf NAT on IOS-XE is achieved via VASI implementation
  - VRF-Aware Software Infrastructure
- Configured as VASI pairs
  - Each VASI interface is associated with a different VRF instance
  - Uses **interface vasileft** and **interface vasiright** interfaces
- VASI is the next-hop interface for packets that needs to be switched between these two VRF instances
  - Result is traffic leaking between VRFs using NAT