System Admin

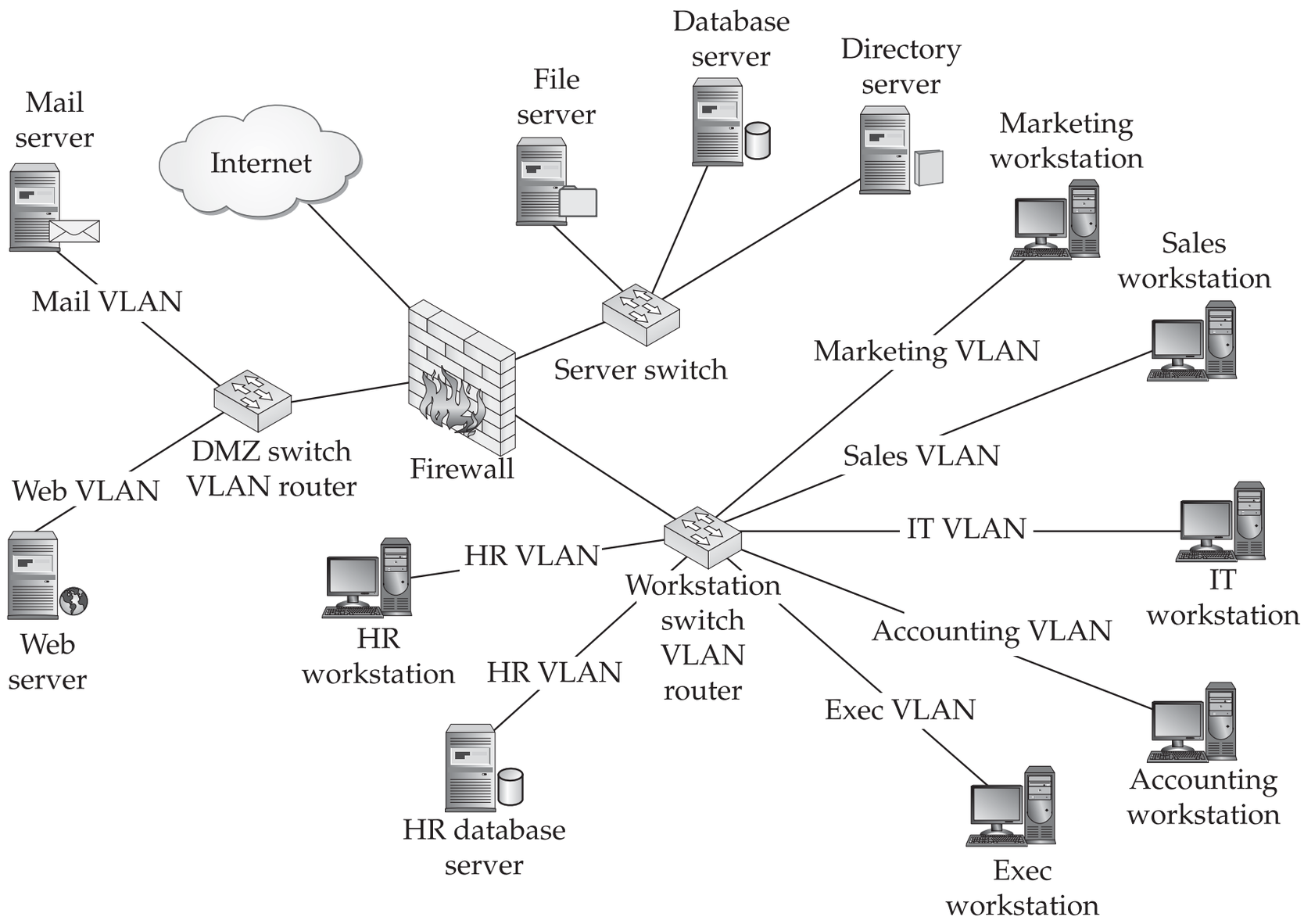
Class 5 - Security

By Ian Robert Blair, M.Sc.

Agenda

- ACLs
- IP Tables

Secure Network with VLANS



Connect to Terminal

- 9600 bits/sec
- No hardware flow control
- 8-bit ASCII
- No parity bits
- 1 stop bit

Telnet, SSH, and SVI

- Both allow remote administration from network
- Telnet(port 23) sends all data in plain text, SSH(port 22) encrypts all messages
- Switched Virtual Interface (SVI) configuration

(config) int vlan 1

(config-if) ip address 192.168.2.254 255.255.255.0

(config-if) exit

(config) ip default-gateway 192.168.2.1

* (config) ip address dhcp

Configure Telnet

> enable

config t

(config)# enable secret *cisco*

(config)# line vty 0 15

(config-line)# password *cisco*

(config-line)# login

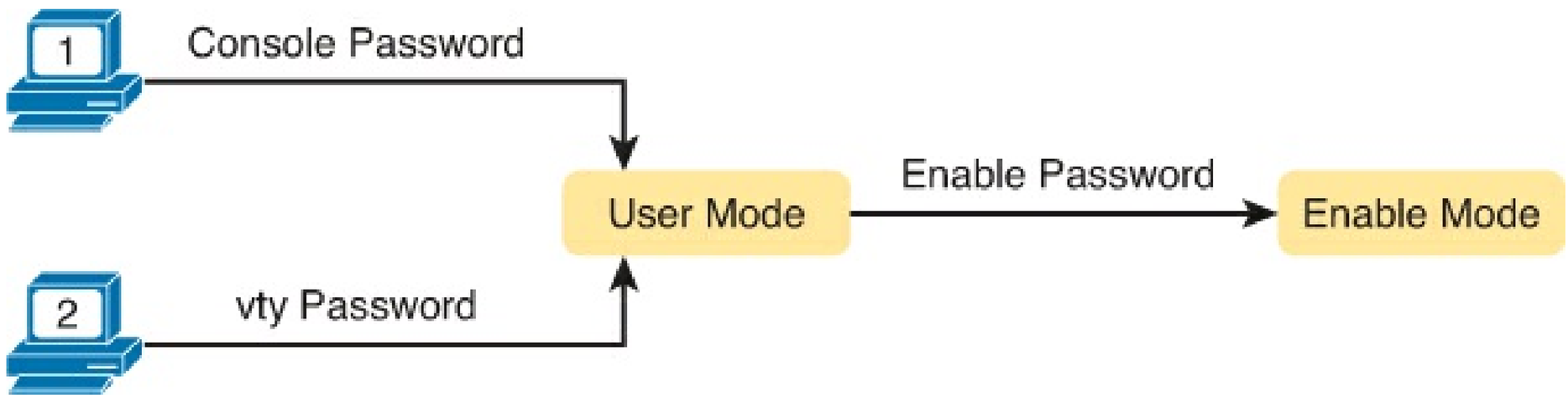
(config-line)# exit

**(optional) service password-encryption

Enable Passwords

- enable password *cisco*
- enable secret *cisco*

Securing Console and Telnet



Local Password Database

enable

config t

username *ian* secret *admin*

line vty 0 15

login local

Configuring SSH, pt. 1

enable

config t

ip domain-name lab.net

crypto key generate rsa

username ian password administration

line vty 0 15

(optional) transport input ssh

login local

exit

ip ssh version 2

Configuring SSH, pt. 2

- show ip ssh
- show ssh

Encrypting Passwords

- service password-encryption

Port Security

- Restricts access to switch ports
- Sticky secure Mac-address will allow you save mac addresses as they are discovered
- Sample Configuration:

  (config)interface fa 0/1

  (config-if) switchport mode access

  (config-if) switchport port-security

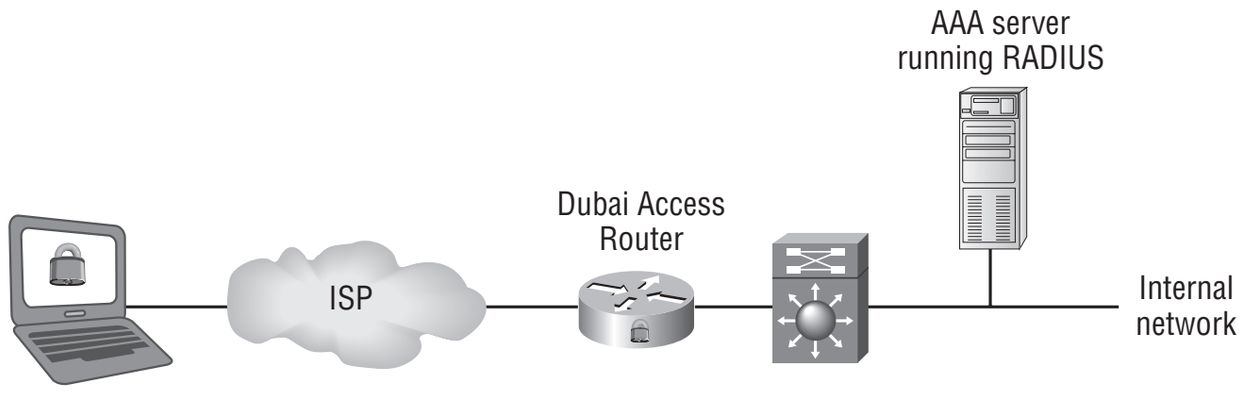
  (config-if) switchport port-security mac-address sticky

Port Security Actions

Option on the switchport port-security violation Command	Protect	Restrict	Shutdown*
Discards offending traffic	Yes	Yes	Yes
Sends log and SNMP messages	No	Yes	Yes
Disables the interface, discarding all traffic	No	No	Yes

AAA

- AAA stands for authentication, authorization, and accounting.
- **Authentication** requires users and administrators to prove that they really are who they say they are
- **Authorization** services decide which resources the user and administrator are allowed to access and which operations they are allowed to perform
- **Accounting** records what the user and administrator actually did, what they accessed, and how long they accessed it
- AAA is used to authenticate remote users (VPN) and authenticate administrators who manage network devices
- The most widely used and supported types of AAA protocols are TACACS+ (Cisco proprietary, TCP) and RADIUS (open standard, UDP)



Management Services

- **SNMP** is a network management protocol that can be used to retrieve information from a network device or to remotely configure parameters on the device (Version 1-3)
- The **Syslog protocol** was designed to collect messages from a device that has been configured for logging to a Syslog server (Clear Text)
- **TFTP** is used for transferring configuration or system files across the network (Update IOS)
- **NTP** is used to synchronize the clocks of various devices across a network

Additional Security

- With **DHCP Snooping**, if a rogue device on an untrusted port attempts to send a DHCP response packet into the network, the port is shut down
- To enable
  - (config) ip dhcp spoofing
  - (config-if) ip dhcp spoofing trust

Cisco ACLs

Cisco Access Lists

- An **access list** is essentially a list of conditions that categorize packets
- Each line of the access list is processed in sequential order—that is, it'll always start with the first line of the access list, then go to line 2, then line 3, and so on
- Once the packet matches the condition on a line of the access list, the packet is acted upon and no further comparisons take place
- There is an implicit "deny" at the end of each access list
- if a packet doesn't match the condition on any of the lines in the access list, the packet will be discarded

Types of Access Lists

- **Standard access** lists
  - Use only the **source IP address** in an IP packet as the condition test
  - All decisions are made based on the source IP address
  - Don’t distinguish between any of the many types of IP traffic such as web, Telnet, UDP, and so on
  - Place IP standard access lists as close to the destination as possible

Types of Access Lists

- **Extended access** lists
  - Can evaluate source and destination IP addresses, the protocol field in the Network layer header, and the port number at the Transport layer header (Layer 3 and 4)
  - Has the ability to make much more granular decisions when controlling traffic
  - Place IP extended access lists as close to the source as possible

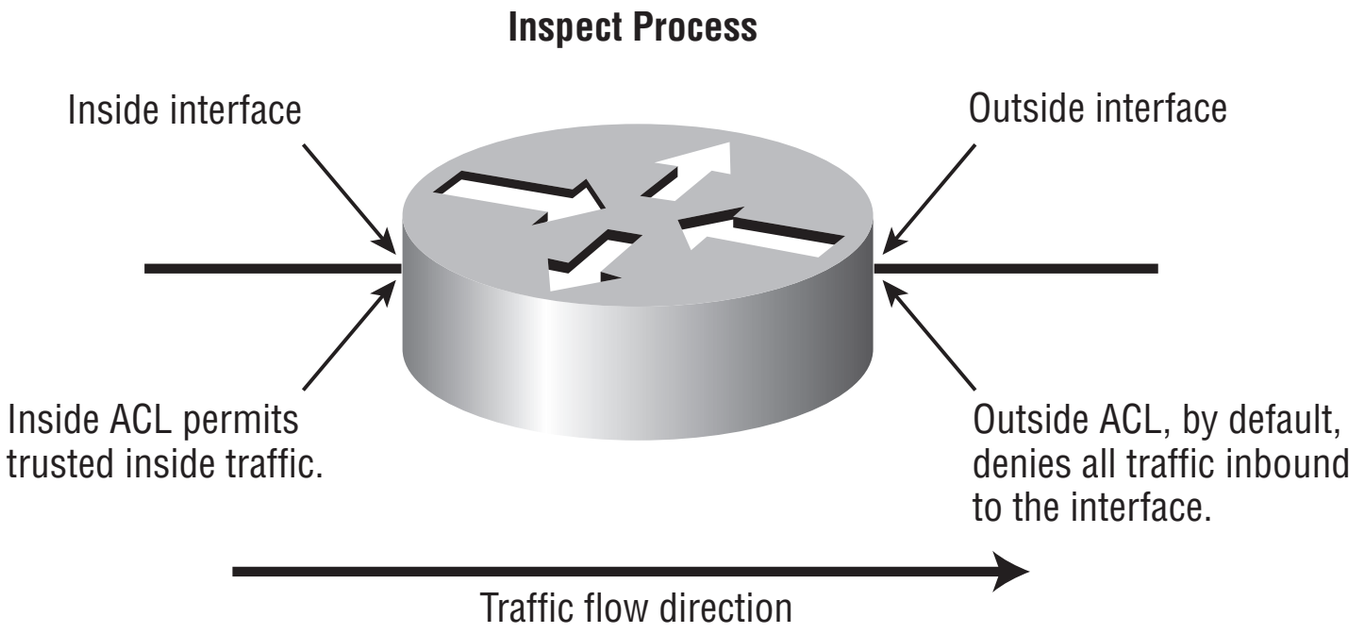
VLAN ACLS

- **VLAN Access Control Lists** (VACL) are supported in software on Cisco multilayer switches
- **Router Access Control Lists** (RACL) can be applied to any routed interface, including a switch virtual interface (SVI) or Layer 3 routed port
- **Port Access Control Lists** (PACL) filter traffic at the port level
  - PACLs can be applied on a Layer 2 switch port, trunk port, or EtherChannel port

CBAC

- **CBAC**, also referred to as stateful packet inspection, is the core component in a stateful firewall

- The inspection uses ACLs to determine traffic to filter but is augmented with the ability to monitor several attributes in TCP, UDP, and ICMP packets



Access List Direction

- Inbound
- Outbound
- You can assign **only one** access list per interface per protocol per direction

Wildcard Masking

- To block or allow a single host:
    - 192.168.1.200 0.0.0.0
- To block all hosts on the /24:
    - 192.168.1.0 0.0.0.255

Standard List Example

- Example 1
  - (config)# access-list 5 permit 192.168.1.0 0.0.0.255 (implicit deny to all automatic)
- Example 2
  - (config)# access-list 15 deny 192.168.1.0 0.0.0.255
  - (config)# access-list 15 permit any
- Apply to interface
  - (config-if)# ip access-group 5 out

Create Extended Lists

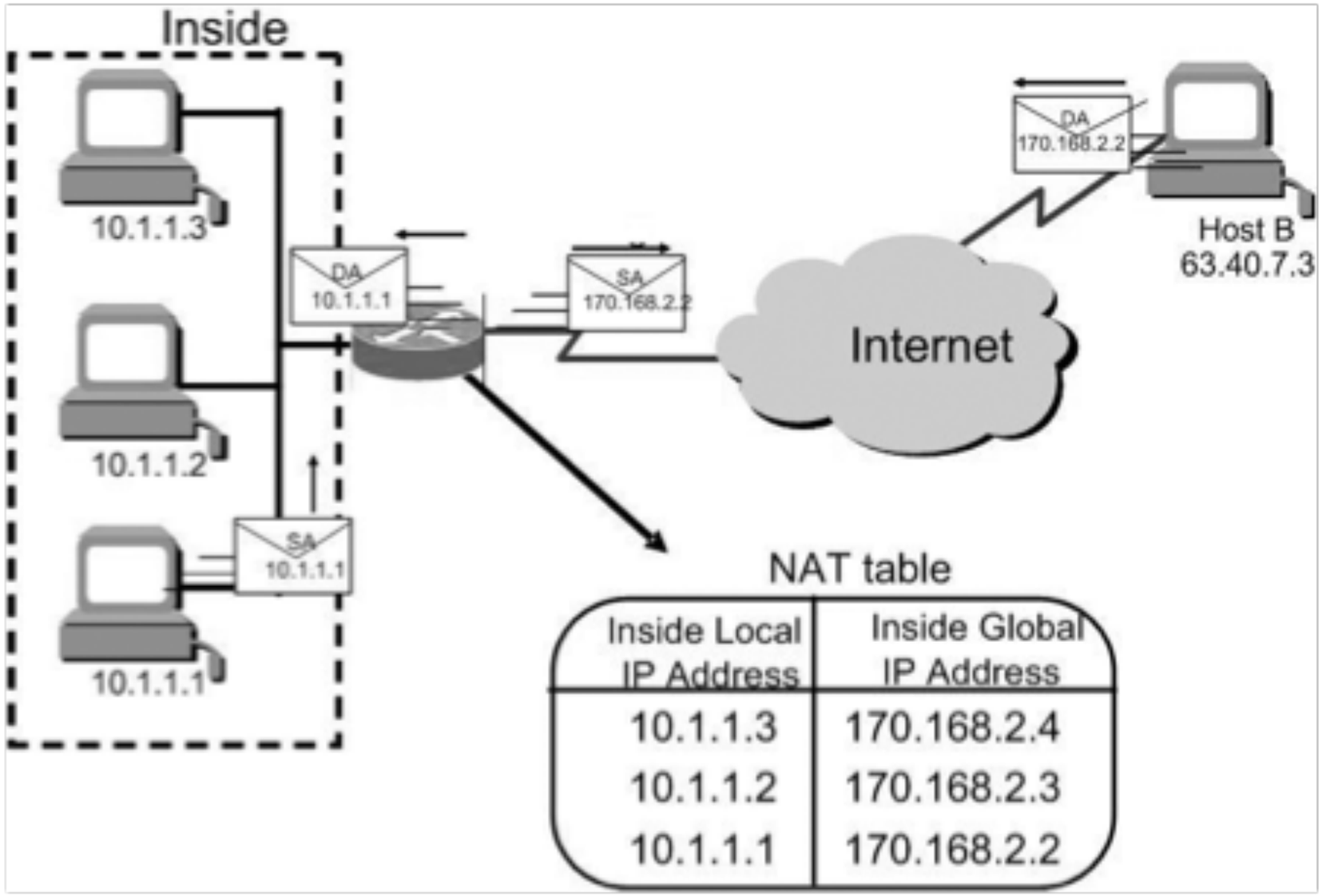
- access-list <100-199> (Permit/Deny) (Protocol) (Source) (Destination)
- access-list 150 deny ip 192.168.10.50 0.0.0.0 192.168.3.50 0.0.0.0
- access-list 150 deny ip 192.168.10.50 0.0.0.0 host 192.168.3.50
- access-list 150 deny tcp 192.168.10.50 0.0.0.0 any eq 80
- int fa0/1
- ip access-group 150 out

Network Address Translation(NAT)

Network Address Translation(NAT)

- Static NAT
  - One-to-one mapping between local and global addresses
- Dynamic NAT
  - Maps an unregistered IP address to a registered IP address from out of a pool of registered IP addresses
- Overloading
  - Maps multiple unregistered IP addresses to a single registered IP address—many-to-one—by using different ports

Basic NAT


Inside
10.1.1.3
10.1.1.2
10.1.1.1
DA
10.1.1.1
SA
170.168.2.2
SA
10.1.1.1
Internet
DA
170.168.2.2
Host B
63.40.7.3
NAT table
Inside Local IP Address
Inside Global IP Address
10.1.1.3
170.168.2.4
10.1.1.2
170.168.2.3
10.1.1.1
170.168.2.2

Static NAT

(config)# ip nat inside source static 10.1.1.1 170.46.2.2

(config)# int E0/0

(config-if)# ip address 10.1.1.10 255.255.255.0

(config-if)# ip nat inside

(config-if)# int S0/0

(config-if)# ip address 170.46.2.1 255.255.255.0

(config-it)# ip nat outside

Dynamic NAT

(config)# ip nat pool todd 170.168.2.2 170.168.2.254 netmask 255.255.255.0

(config)# ip nat inside source list 1 pool todd

(config)# int E0/0

(config-if)# ip address 10.1.1.10 255.255.255.0

(config-if)# ip nat inside

(config-if)# int S0/0

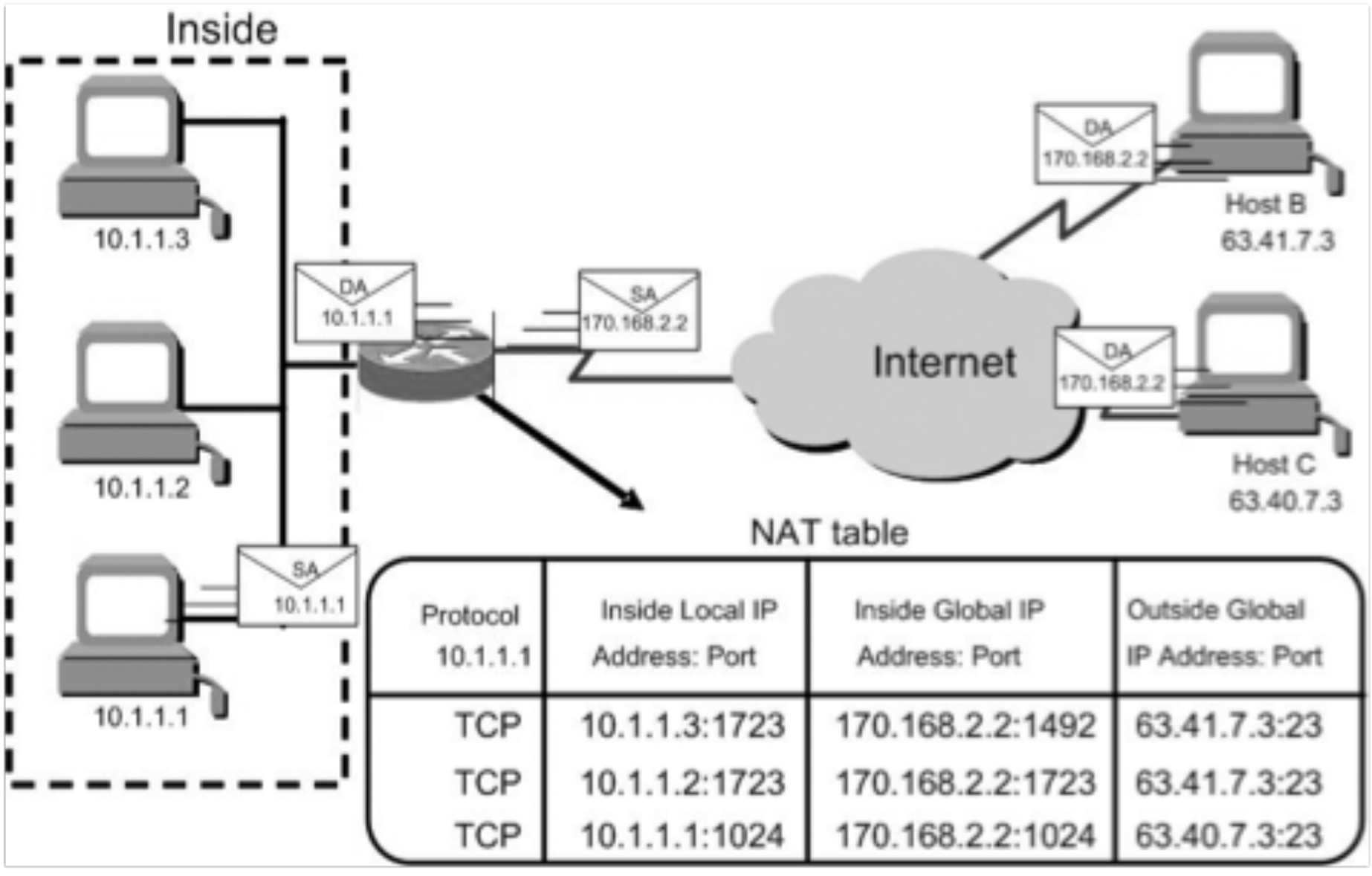
(config-if)# ip address 170.46.2.1 255.255.255.0

(config-if)# ip nat outside

(config-if)# exit

(config)# access-list 1 permit 10.1.1.0 0.0.0.255

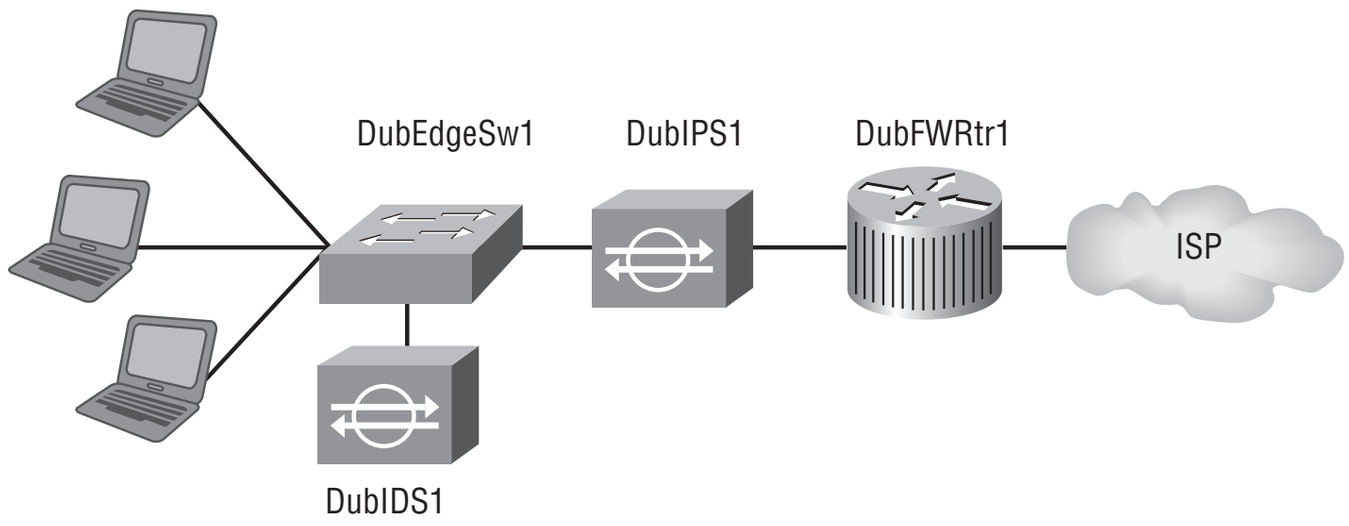
NAT Overloading



Protocol 10.1.1.1	Inside Local IP Address: Port	Inside Global IP Address: Port	Outside Global IP Address: Port
TCP	10.1.1.3:1723	170.168.2.2:1492	63.41.7.3:23
TCP	10.1.1.2:1723	170.168.2.2:1723	63.41.7.3:23
TCP	10.1.1.1:1024	170.168.2.2:1024	63.40.7.3:23

IDS and IPS

- IDS is typically characterized as a passive device that listens promiscuously to all traffic on the network
- IDS/IPS can:
  - Send an alert to a management station
  - Configure a network device to block traffic
    - Send TCP reset to the traffic source
- IPS is characterized as an active device (Inline sensor)



Malicious Traffic Identification Approaches

- IDS and IPS sensors have a few different approaches they can use to scan for and identify offending traffic
  - **Signature-based** - looks for a specific sequence of bits in a packet or content that is known to be malicious
  - **Policy-based** - uses an algorithm to make decisions (ex. block mmap scans)
  - **Anomaly-based** - look for network traffic (over time) that is outside the definition of what is considered normal
  - **Honeypot** - a dummy server or host is used to attract attacks

Inspect

ip access-list extended INBOUND deny ip any any

int fa0/0
description OUTSIDE
ip access-group INBOUND in
ip inpsect FWOUT out
ip address 1.1.1.1 255.255.255.0 ip nat outside

int fa0/1
description INSIDE
ip address 192.168.0.1 255.255.255.0 ip nat inside

Lab Assignments, pt. 1

- Build a test environment with two computer systems and one or two routers
- Practice filtering using Standard and Extended ACLs
- Add SSH access to your routers

Homework

- Read Chapter 9, 11, 12 and 18
- Find an academic article on one of the following technologies:
  - OSPF or RIP
  - SSH
  - NAT
  - IDS/IPS
- Write a summary of the article (site the article as a reference)

Contact

Ian Robert Blair, MSc.

ian.robertblair@icloud.com

QQ: 2302412574