Securing and Managing Your Network with Enterprise Services

Nick Russo
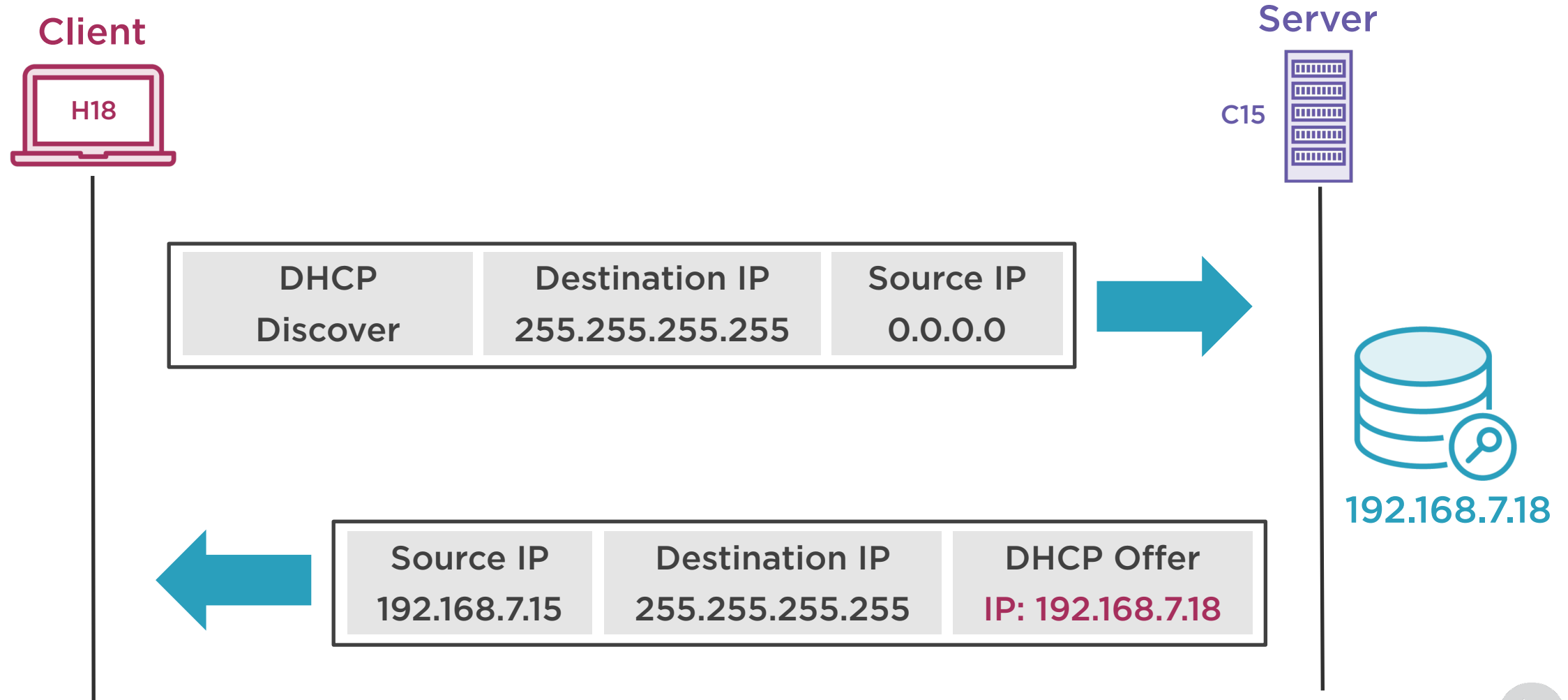
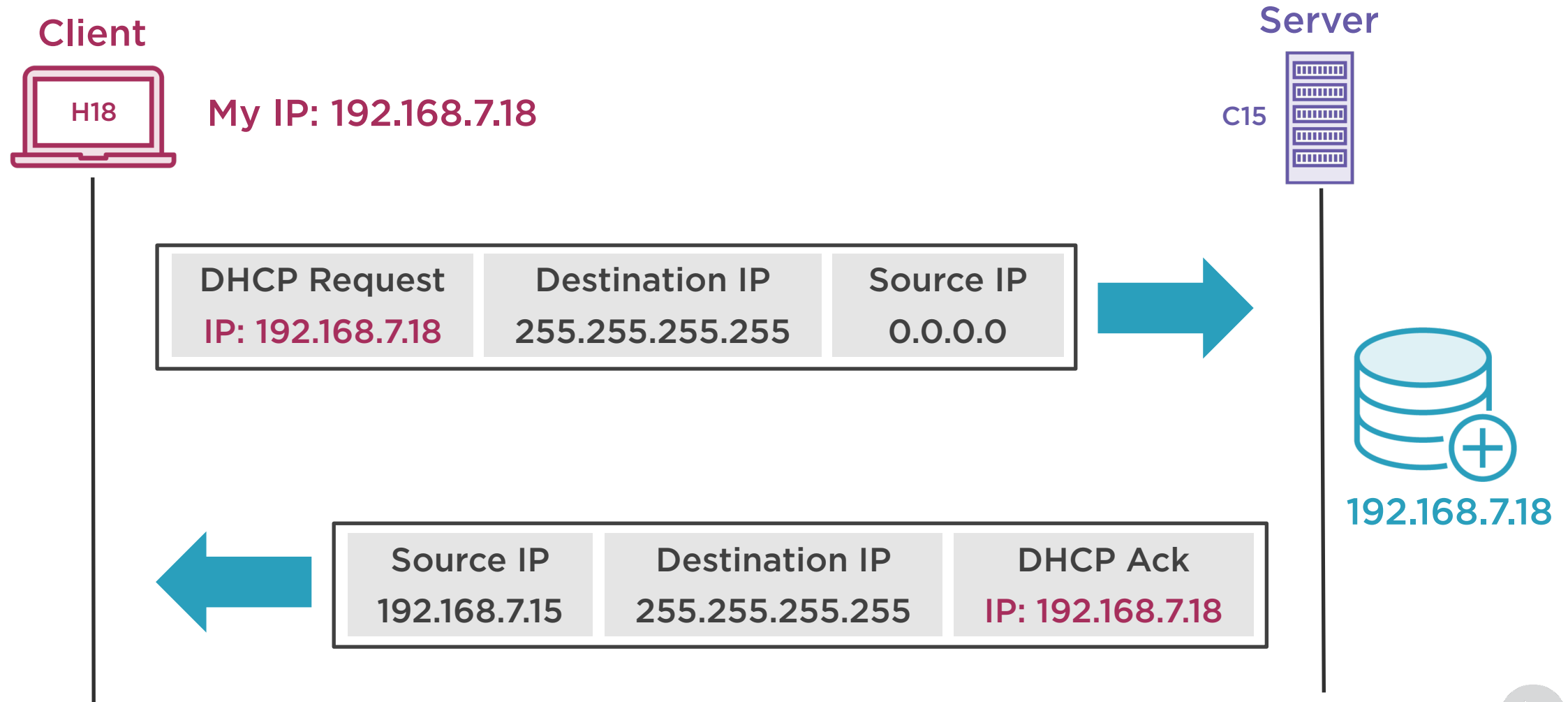NETWORK ENGINEER

@nickrusso42518   www.njrusmc.net

Agenda

Enterprise services:

- DHCP
- AAA and RADIUS
- Telnet, SSH, and SCP
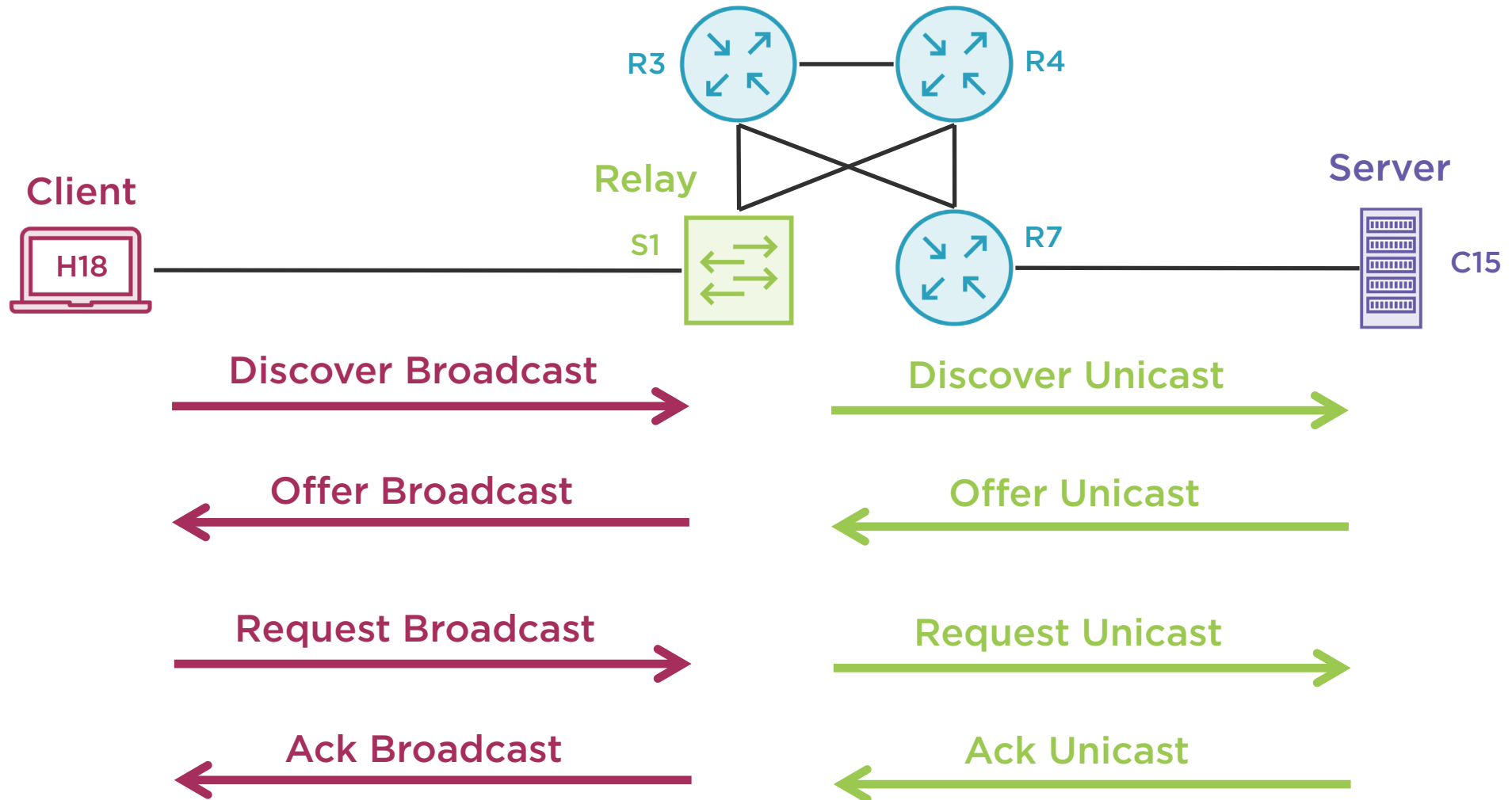- NetFlow collection and analysis
- Control-plane policing

DHCP Operations – First Exchange
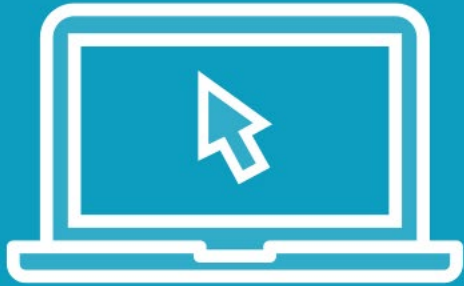
Client

H18

Server

C15

DHCP Discover	Destination IP 255.255.255.255	Source IP 0.0.0.0

192.168.7.18

Source IP 192.168.7.15	Destination IP 255.255.255.255	DHCP Offer IP: 192.168.7.18

DHCP Operations – Second Exchange

Client

H18

My IP: 192.168.7.18

Server

C15

DHCP Request	Destination IP	Source IP
IP: 192.168.7.18	255.255.255.255	0.0.0.0

192.168.7.18

Source IP	Destination IP	DHCP Ack
192.168.7.15	255.255.255.255	**IP: 192.168.7.18**

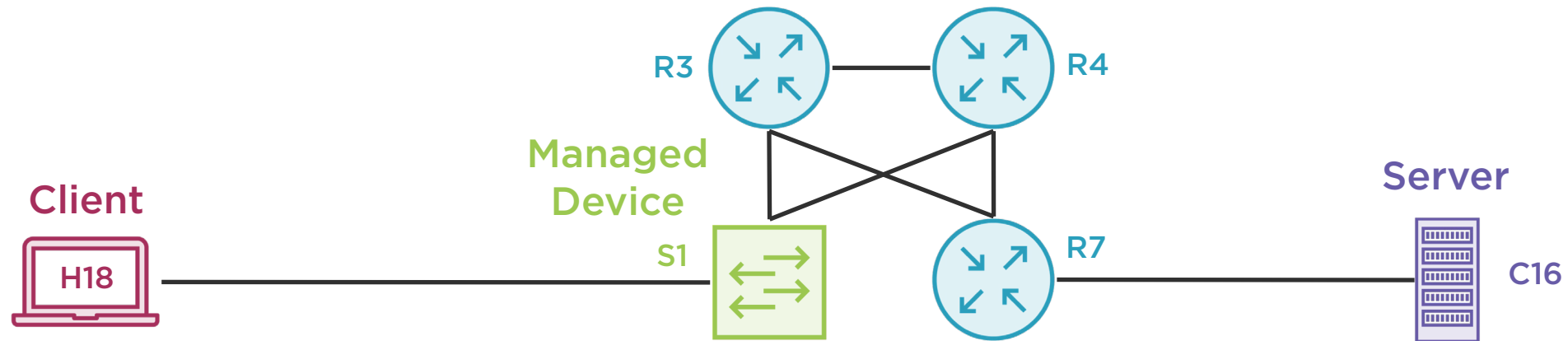# Using DHCP Relays

Demo

DHCP for LAN clients

AAA and RADIUS Defined

Authentication, Authorization, and Accounting

Remote Authentication Dial-In User Service

AAA and RADIUS in Action

User	Password
alice	pass123
bob	qwerty
chuck	echeese

Client — H18

Managed Device — S1

Server — C16

R3, R4, R7

Telnet + credentials
alice/pass123

Access-Request
alice/pass123

"Hello, Alice"

Access-Accept

Telnet + credentials
bob/wrongpass

Access-Request

"Invalid credentials"

Access-Reject

Demo

AAA/RADIUS with local testing

- Server hosted on Linux

Telnet, SSH, and SCP
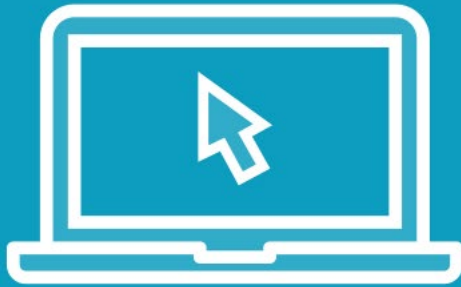

Unsecure Telnet

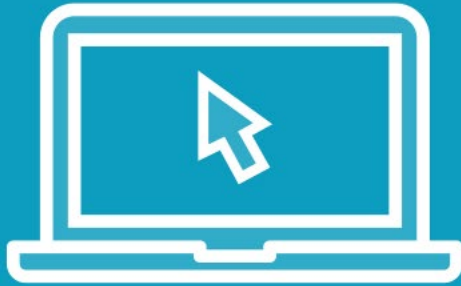**Secure Shell (SSH)**

**Secure Copy Protocol
(file transfer via SSH)**
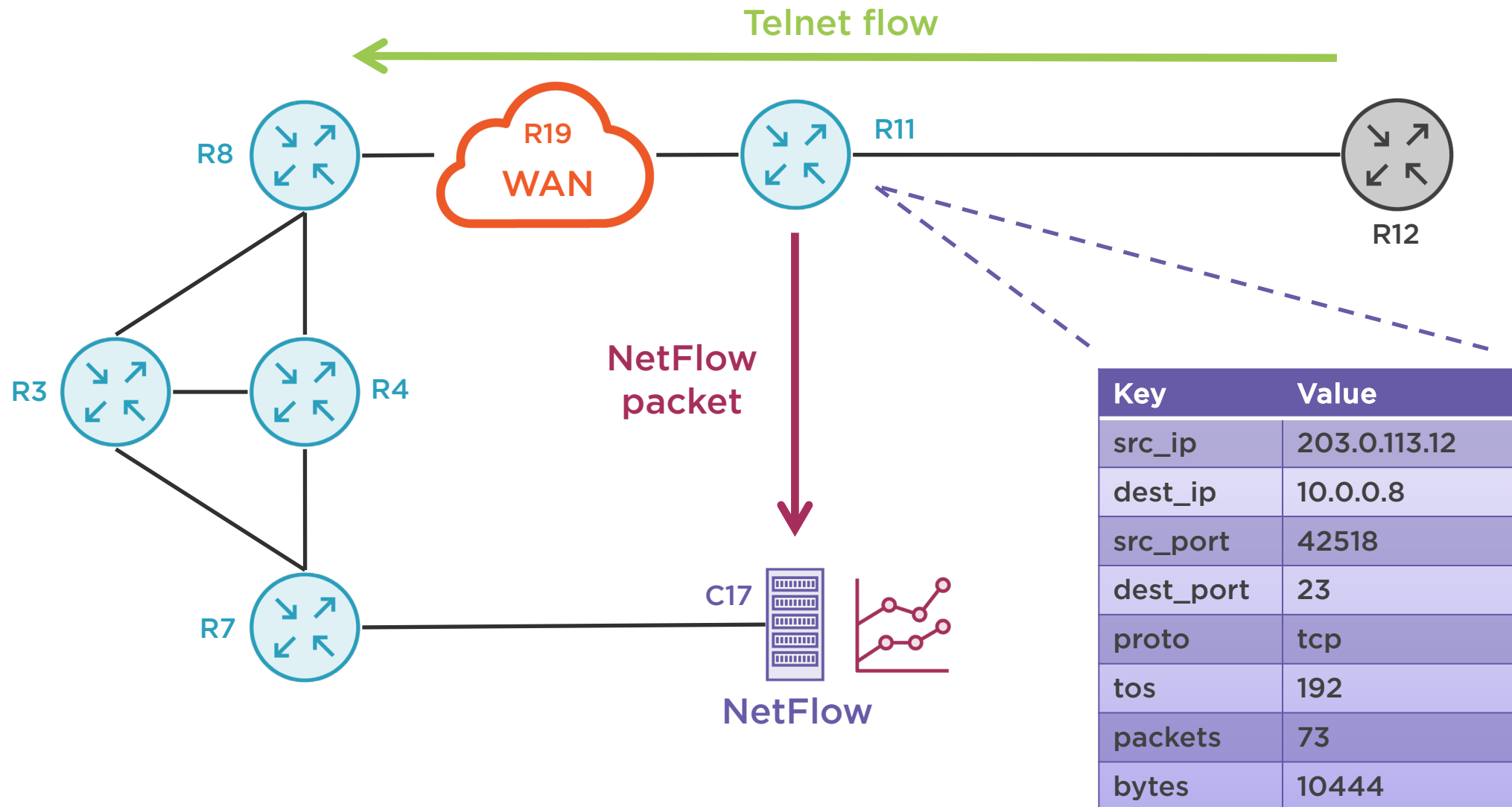
Demo

Testing AAA/RADIUS with Telnet/SSH

Demo

Transferring files with SCP

Fundamentals of NetFlow

Telnet flow

R8

R19
WAN

R11

R12

R3

R4

NetFlow
packet

R7

C17

NetFlow

Key	Value
src_ip	203.0.113.12
dest_ip	10.0.0.8
src_port	42518
dest_port	23
proto	tcp
tos	192
packets	73
bytes	10444

Demo

Classic NetFlow using "top talkers"
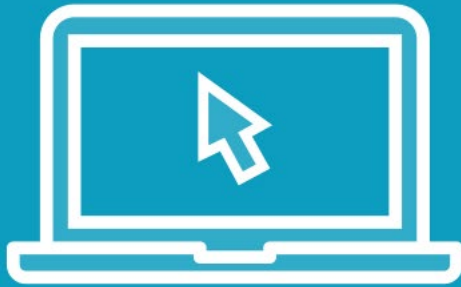
Demo

NetFlow collection and analysis

- Reviewing some Python code!

Demo

Protecting devices with CPP

- Device management

- Routing protocols

- ICMP ping

Summary

Device onboarding with DHCP

Securing remote access

Data visibility and device security