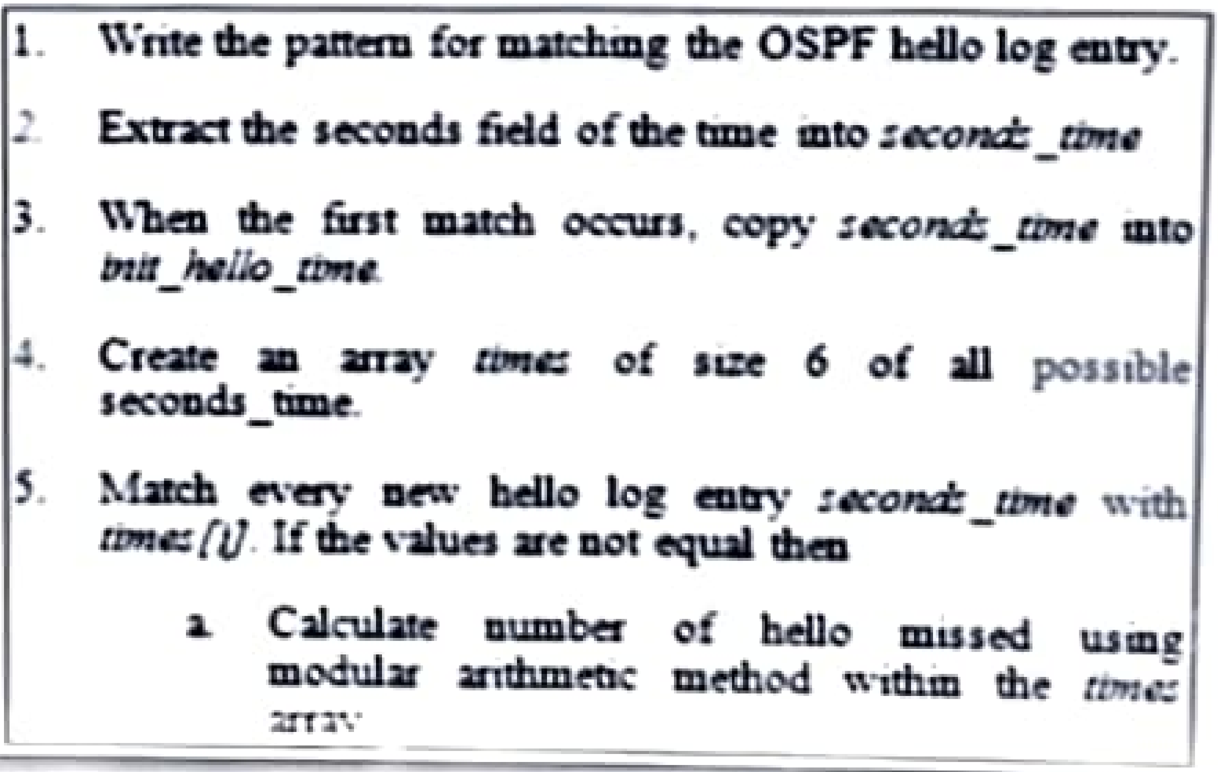
OSPF hello packet deletion attack

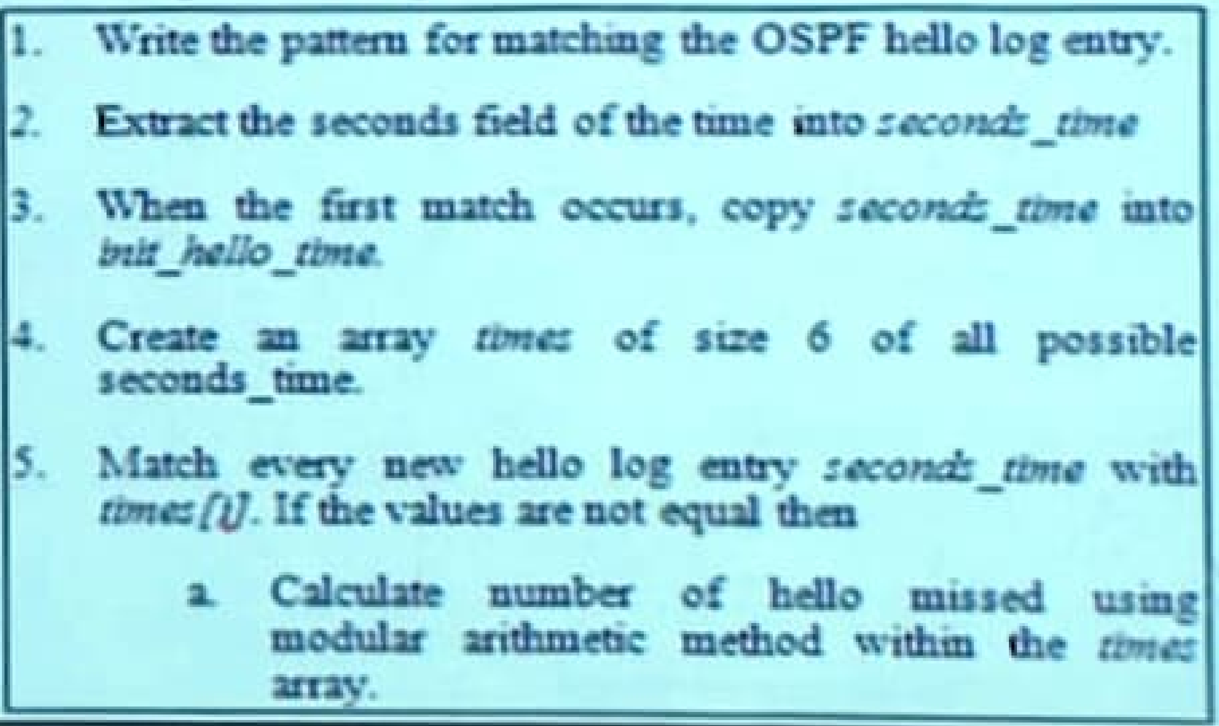
- **Detection mechanism**
- The algorithm for detecting OSPF hello packet deletion attack is as given in Fig.



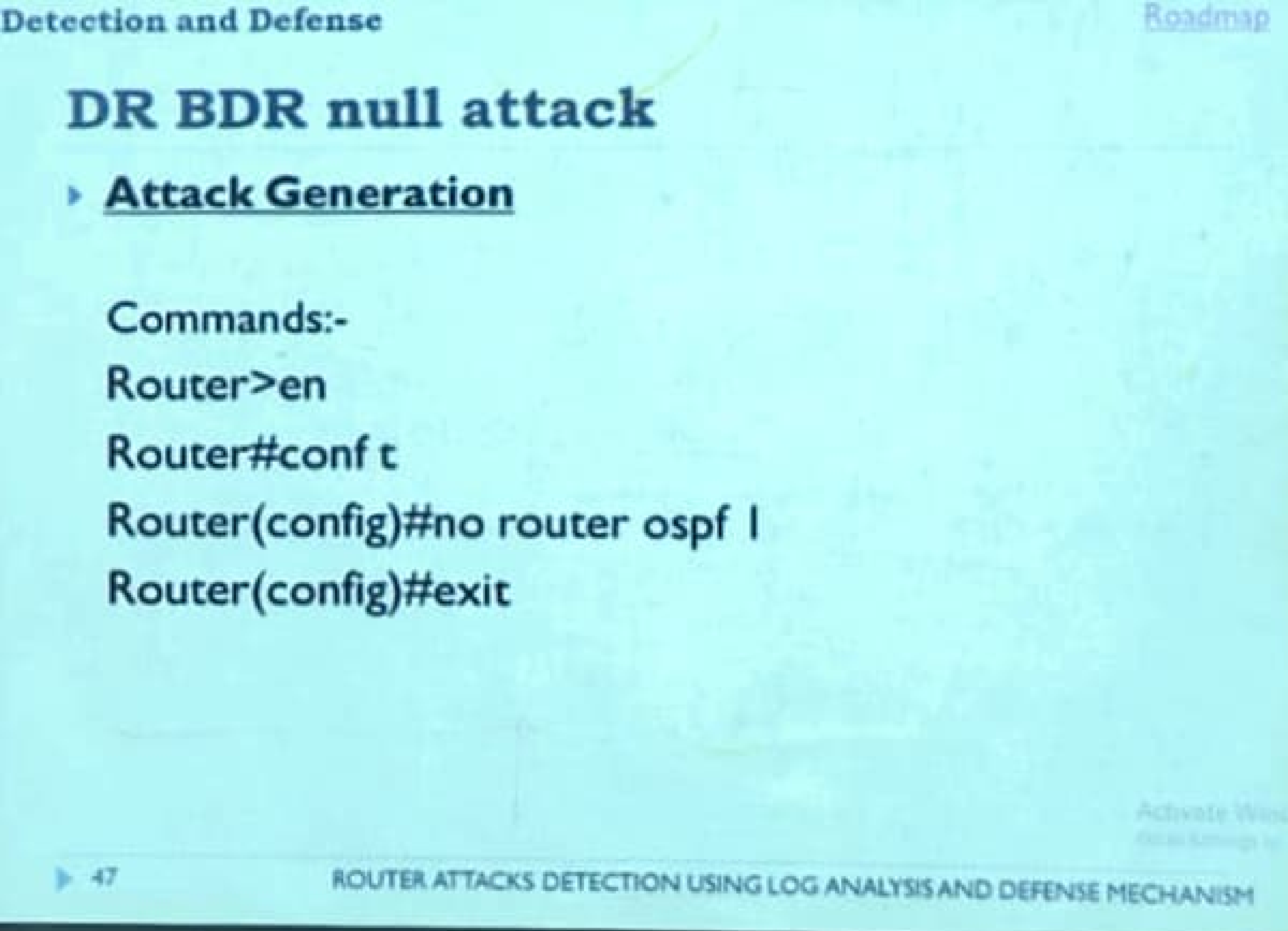
1. Write the pattern for matching the OSPF hello log entry.
2. Extract the seconds field of the time into *seconds_time*
3. When the first match occurs, copy *seconds_time* into *init_hello_time*.
4. Create an array *times* of size 6 of all possible seconds_time.
5. Match every new hello log entry *seconds_time* with *times[i]*. If the values are not equal then
   a. Calculate number of hello missed using modular arithmetic method within the *times* array

OSPF hello packet deletion attack

- **Detection mechanism**
- The algorithm for detecting OSPF hello packet deletion attack is as given in Fig.



1. Write the pattern for matching the OSPF hello log entry.
2. Extract the seconds field of the time into *seconds_time*
3. When the first match occurs, copy *seconds_time* into *init_hello_time*.
4. Create an array *times* of size 6 of all possible seconds_time.
5. Match every new hello log entry *seconds_time* with *times[i]*. If the values are not equal then
    a. Calculate number of hello missed using modular arithmetic method within the *times* array.



DR BDR null attack

- **Attack Generation**

Commands:-

```
Router>en
Router#conf t
Router(config)#no router ospf 1
Router(config)#exit
```

OSPF hello packet deletion attack

- **Attack Generation**

  Configure the following rule on the victim router

  Command: **access-list 100 deny ospf any any**

- **Log entry Generation**

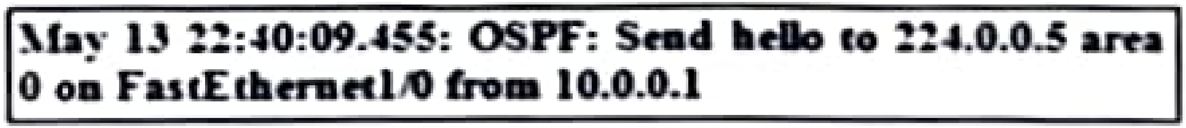
  To generate log entry for each OSPF hello packet sent or received, the

  'debug ip ospf events'

  debugging command can be used. This will enable logging for OSPF events.

- **Log entry format**

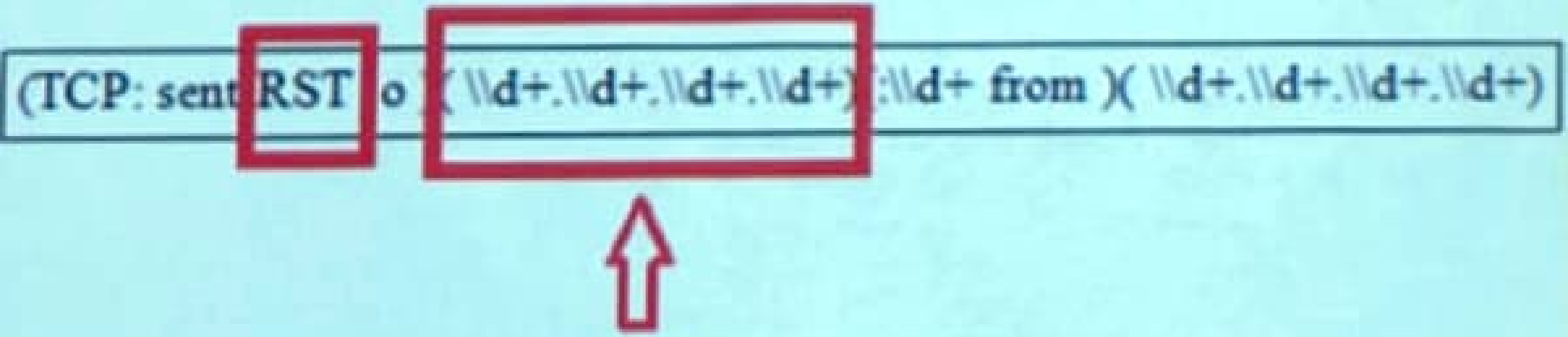
  The log entry for the hello packet is as shown in Fig



```
May 13 22:40:09.455: OSPF: Send hello to 224.0.0.5 area
0 on FastEthernet1/0 from 10.0.0.1
```

BGP session termination attack

- **Detection**
- Use the following regular expression to detect BGP session termination attack



```
(TCP: sent RST to )( \\d+.\\d+.\\d+.\\d+):\\d+ from )( \\d+.\\d+.\\d+.\\d+)
```

Attacker's IP which can be extracted as matcher_variable.group(2)

BGP session termination attack

- **Defense mechanism**
- Configure the following IP ACL

```
Router>en
Router#conf t
Router(config)#ip access-list standard unknwn_login
Router(config-std-nacl)#deny attacker's IP 0.0.0.0
Router(config-std-nacl)#exit
Router(config)#interface f1/0
Router(config-if)#ip access-group unknwn_login in
```

BGP session termination attack

- **Log entry Generation**

  To generate log entry for each BGP event, the
  'debug ip tcp packet'
  debugging command can be used. This will enable logging for BGP events.

- **Log entry format**

  The log entry after BGP session termination attack is shown below

```
May 13 22:48:42.515: TCP: sent RST to 10.0.0.100:100
from 10.0.0.1:
```

Unknown login attack

- **Defense mechanism**
- Configure the following IP ACL

```
Router>en
Router#conf t
Router(config)#ip access-list standard unknwn_login
Router(config-std-nacl)#deny attacker's IP 0.0.0.0
Router(config-std-nacl)#exit
Router(config)#interface f1/0
Router(config-if)#ip access-group unknwn_login in
```

BGP session termination attack

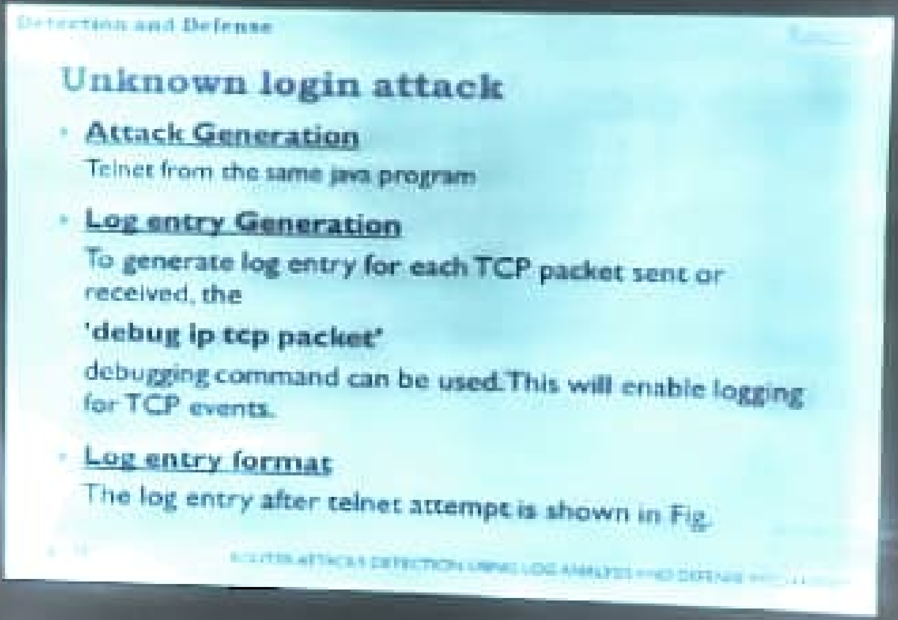
- **Attack Generation**

  Use Netwox Tool 67

  Tool Usage: Scan of IP range, for TCP port range (reset scan)

  For example, to scan tcp ports between 20 and 25 of 192.168.1.2, give the following command

  command : # netwox 67 -i 192.168.1.2 -p 20-25



Unknown login attack

- **Attack Generation**

  Telnet from the same java program

- **Log entry Generation**

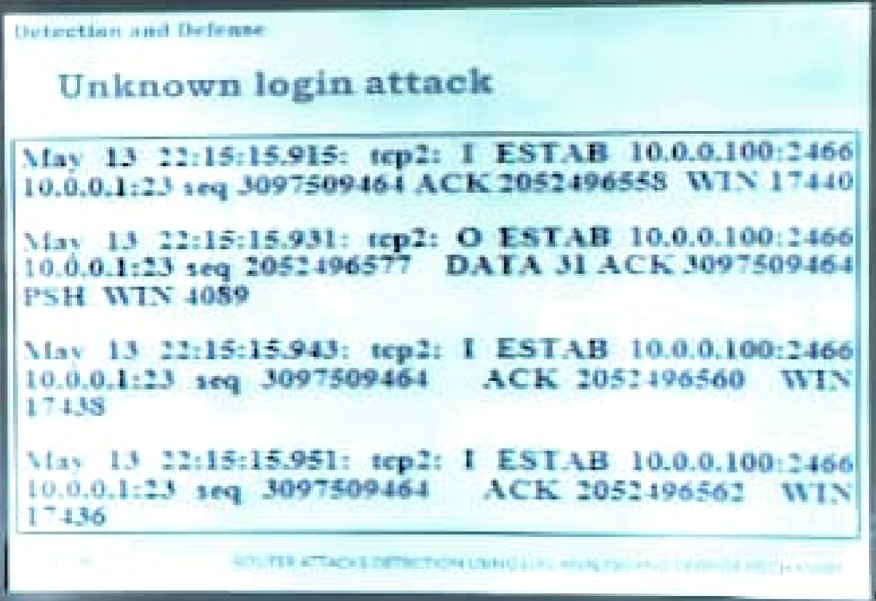
  To generate log entry for each TCP packet sent or received, the

  'debug ip tcp packet'

  debugging command can be used.This will enable logging for TCP events.

- **Log entry format**

  The log entry after telnet attempt is shown in Fig.



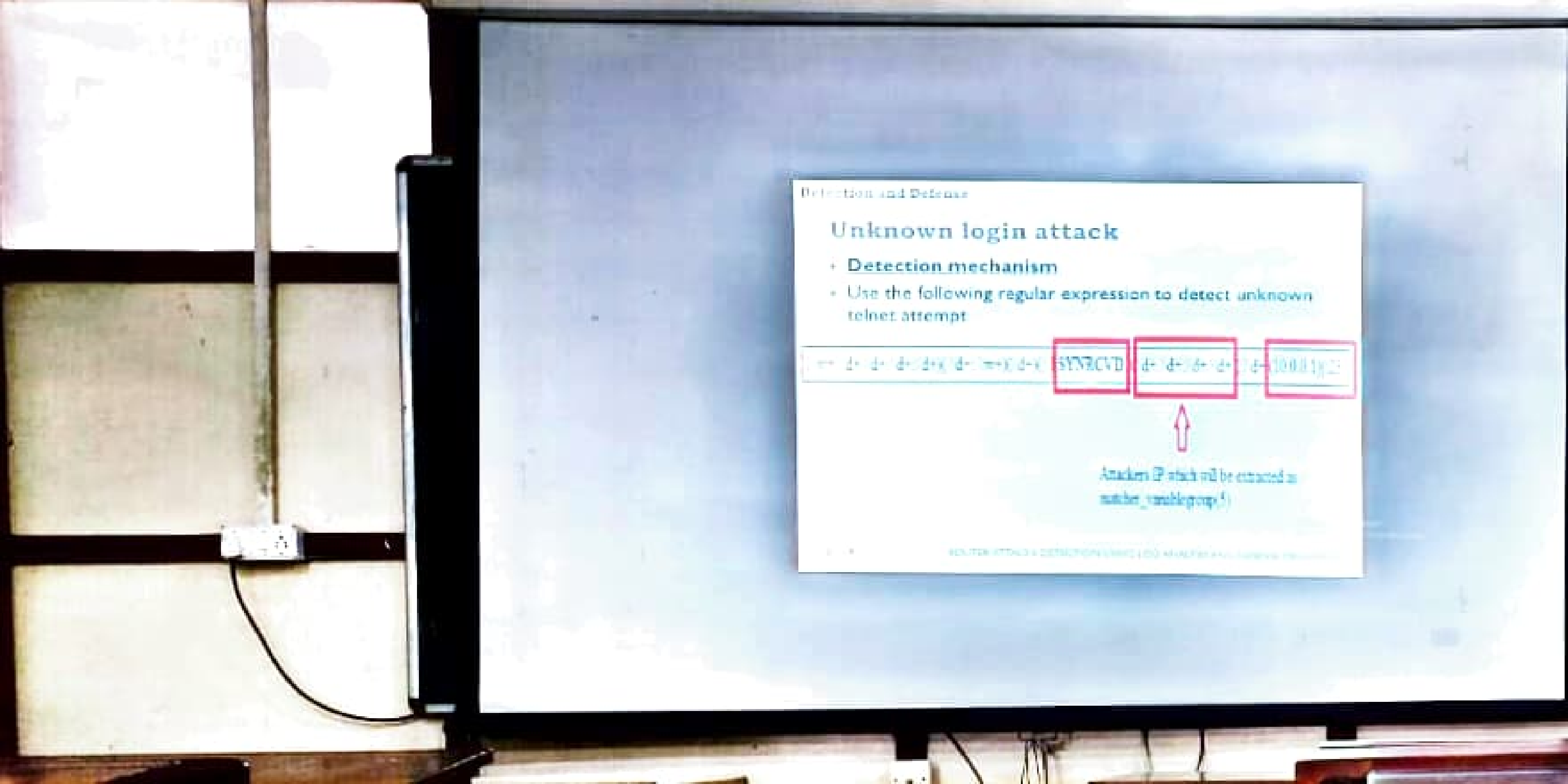
Unknown login attack

```
May 13 22:15:15.915: tcp2: I ESTAB 10.0.0.100:2466
10.0.0.1:23 seq 3097509464 ACK 2052496558 WIN 17440

May 13 22:15:15.931: tcp2: O ESTAB 10.0.0.100:2466
10.0.0.1:23 seq 2052496577 DATA 31 ACK 3097509464
PSH WIN 4089

May 13 22:15:15.943: tcp2: I ESTAB 10.0.0.100:2466
10.0.0.1:23 seq 3097509464 ACK 2052496560 WIN
17438

May 13 22:15:15.951: tcp2: I ESTAB 10.0.0.100:2466
10.0.0.1:23 seq 3097509464 ACK 2052496562 WIN
17436
```

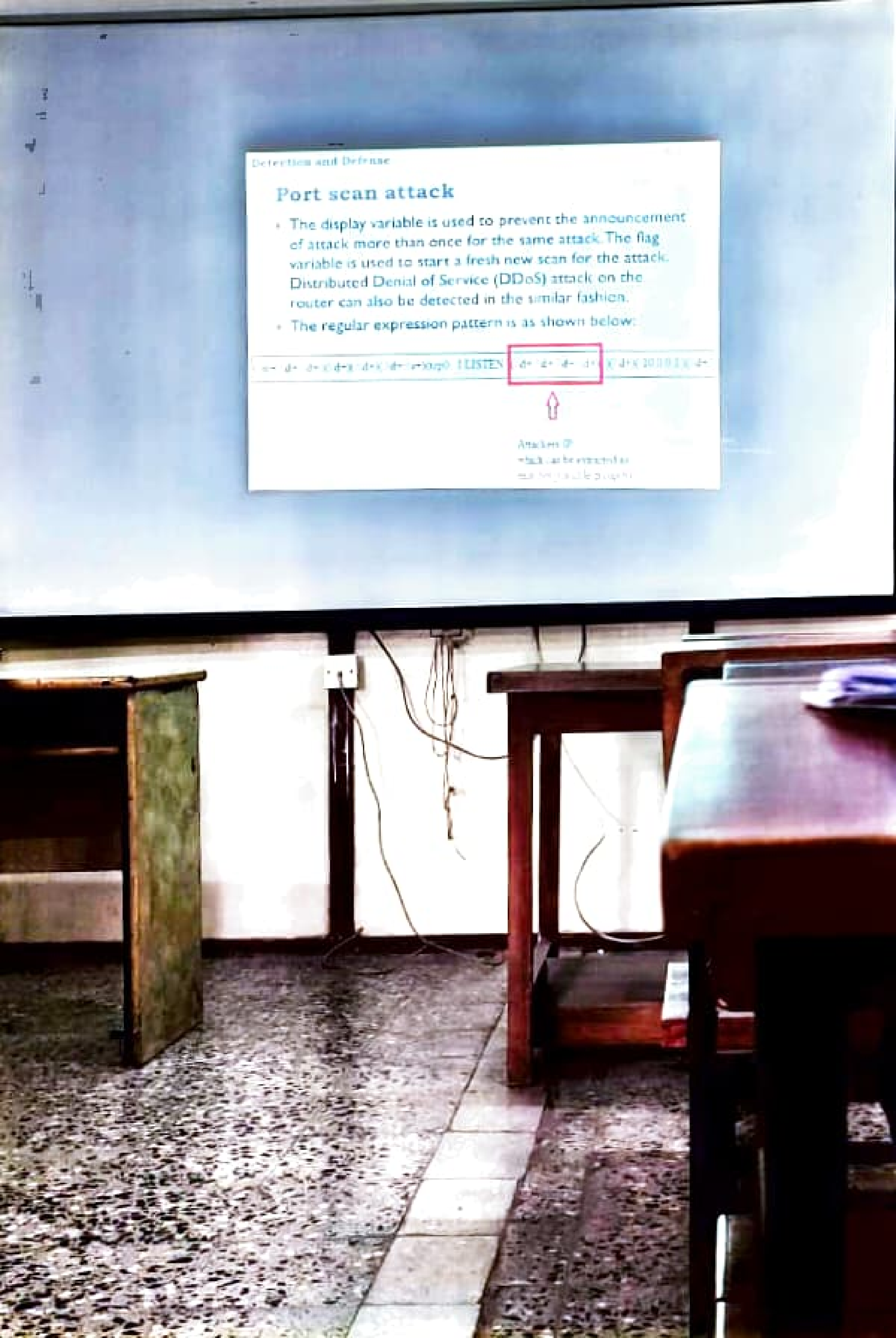


Unknown login attack

- **Detection mechanism**
- Use the following regular expression to detect unknown telnet attempt

```
[illegible] SYNRCVD [illegible] 10.0.0 [illegible]
```

Attackers IP which will be extracted as matcher_variable.group(4)



Detection and Defense

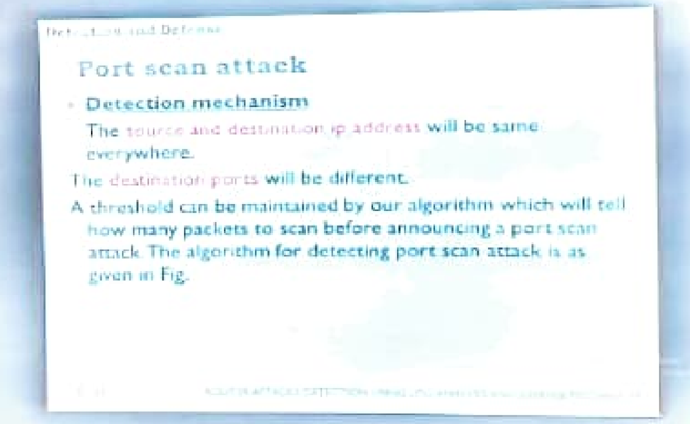
Port scan attack

- The display variable is used to prevent the announcement of attack more than once for the same attack. The flag variable is used to start a fresh new scan for the attack. Distributed Denial of Service (DDoS) attack on the router can also be detected in the similar fashion.
- The regular expression pattern is as shown below:

```
[illegible] LISTEN [illegible]
```

Attacker IP

[illegible]



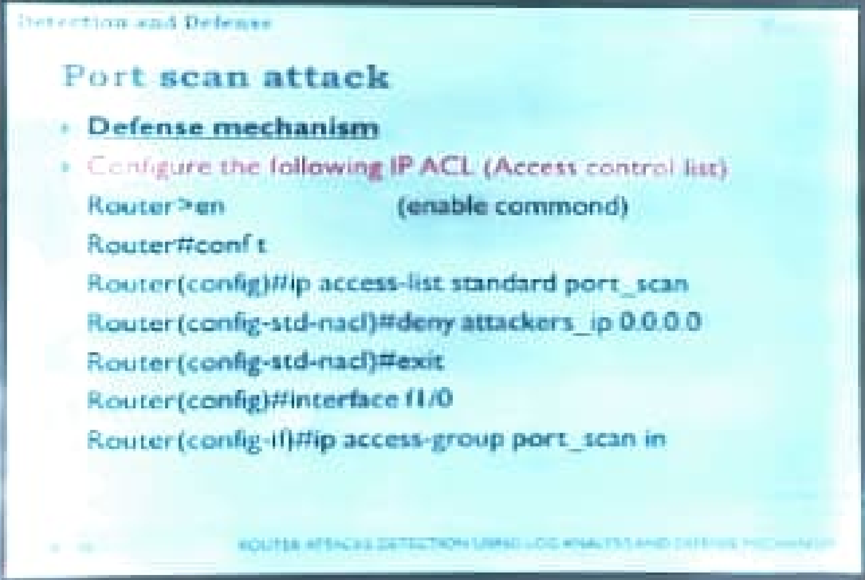
Port scan attack

- **Detection mechanism**

  The source and destination ip address will be same everywhere.

The destination ports will be different.

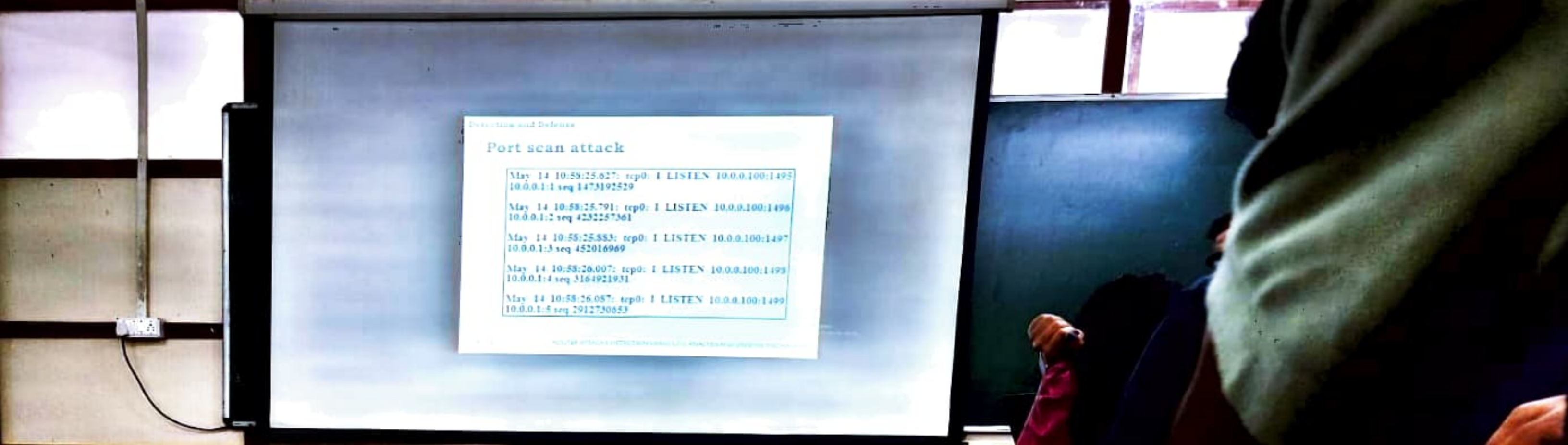
A threshold can be maintained by our algorithm which will tell how many packets to scan before announcing a port scan attack. The algorithm for detecting port scan attack is as given in Fig.



Port scan attack

- **Defense mechanism**
- Configure the following IP ACL (Access control list)

```
Router>en                     (enable commond)
Router#conf t
Router(config)#ip access-list standard port_scan
Router(config-std-nacl)#deny attackers_ip 0.0.0.0
Router(config-std-nacl)#exit
Router(config)#interface f1/0
Router(config-if)#ip access-group port_scan in
```



Detection and Defense

Port scan attack

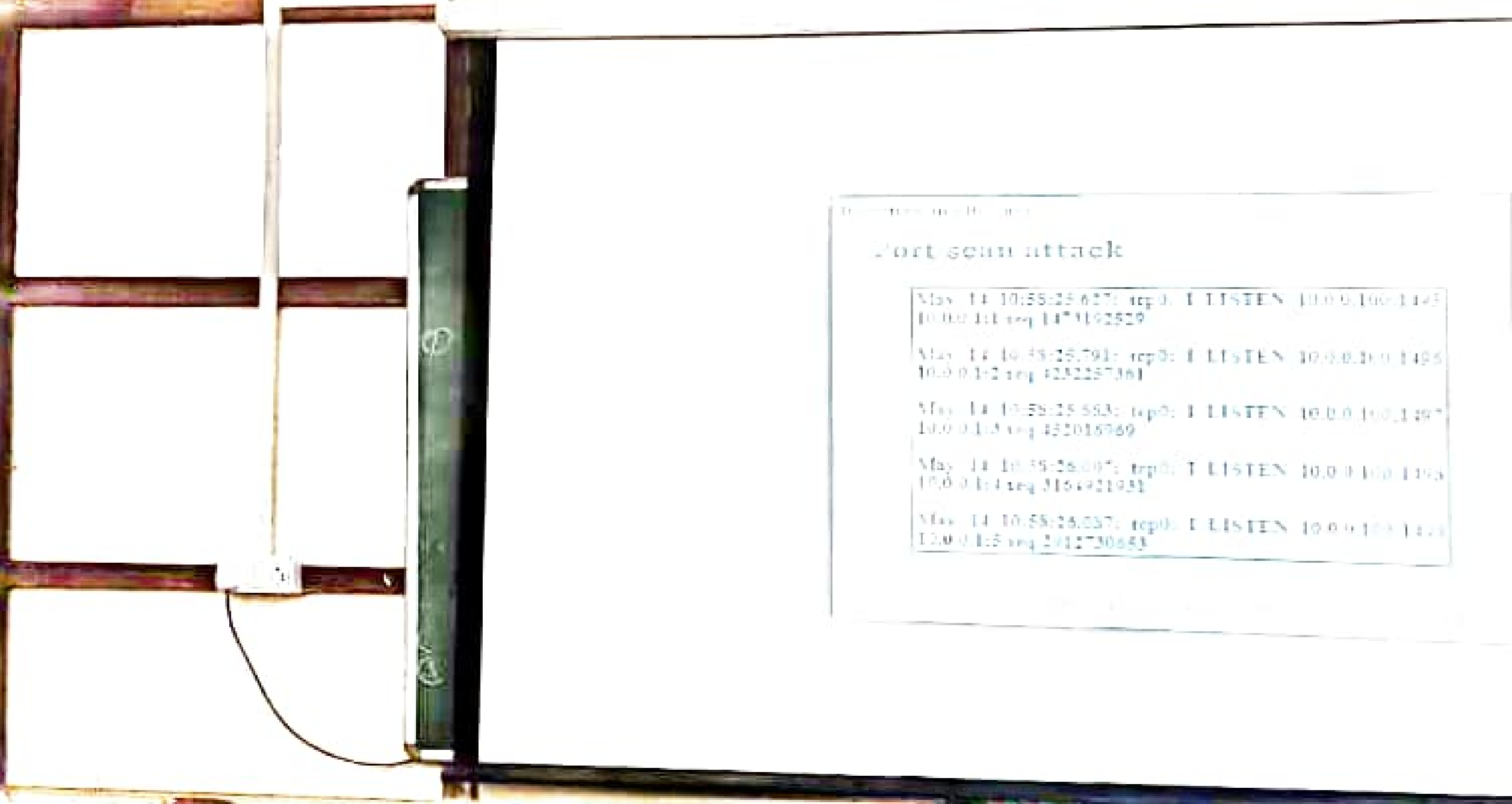
```
May 14 10:58:25.627: tcp0: I LISTEN 10.0.0.100:1495
10.0.0.1:1 seq 1473192529

May 14 10:58:25.791: tcp0: I LISTEN 10.0.0.100:1496
10.0.0.1:2 seq 4232257361

May 14 10:55:25.853: tcp0: I LISTEN 10.0.0.100:1497
10.0.0.1:3 seq 452016969

May 14 10:58:26.007: tcp0: I LISTEN 10.0.0.100:1498
10.0.0.1:4 seq 3164921931

May 14 10:58:26.057: tcp0: I LISTEN 10.0.0.100:1499
10.0.0.1:5 seq 2912730653
```



Port scan attack

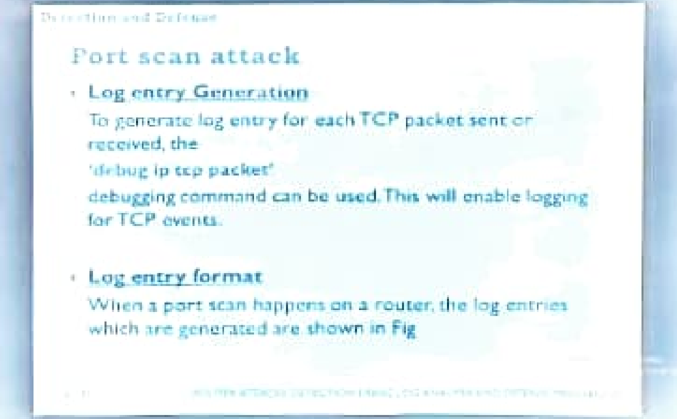
```
May 14 10:55:25.627: tcp0: I LISTEN 10.0.0.100:1443
10.0.0.1:1 seq 1473192529

May 14 10:55:25.791: tcp0: I LISTEN 10.0.0.100:1495
10.0.0.1:2 seq 4232257361

May 14 10:55:25.553: tcp0: I LISTEN 10.0.0.100:1497
10.0.0.1:3 seq 452016969

May 14 10:55:26.007: tcp0: I LISTEN 10.0.0.100:1193
10.0.0.1:4 seq 3164921931

May 14 10:55:26.037: tcp0: I LISTEN 10.0.0.100:1473
10.0.0.1:5 seq 2912730453
```



Port scan attack

- **Log entry Generation**

  To generate log entry for each TCP packet sent or received, the

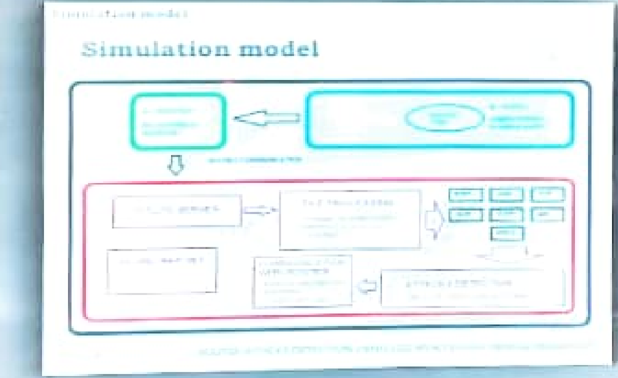
  'debug ip tcp packet'

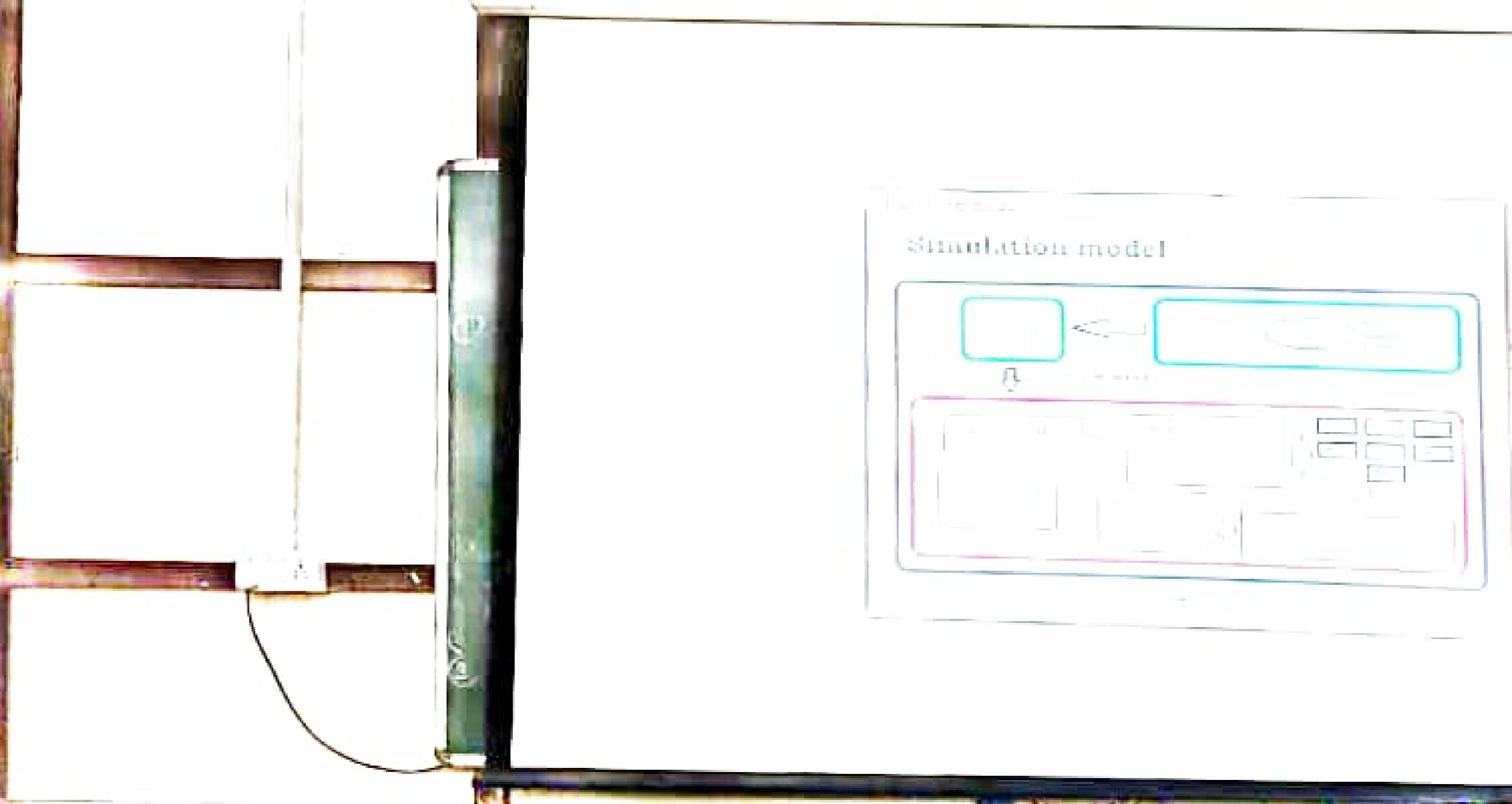
  debugging command can be used. This will enable logging for TCP events.

- **Log entry format**

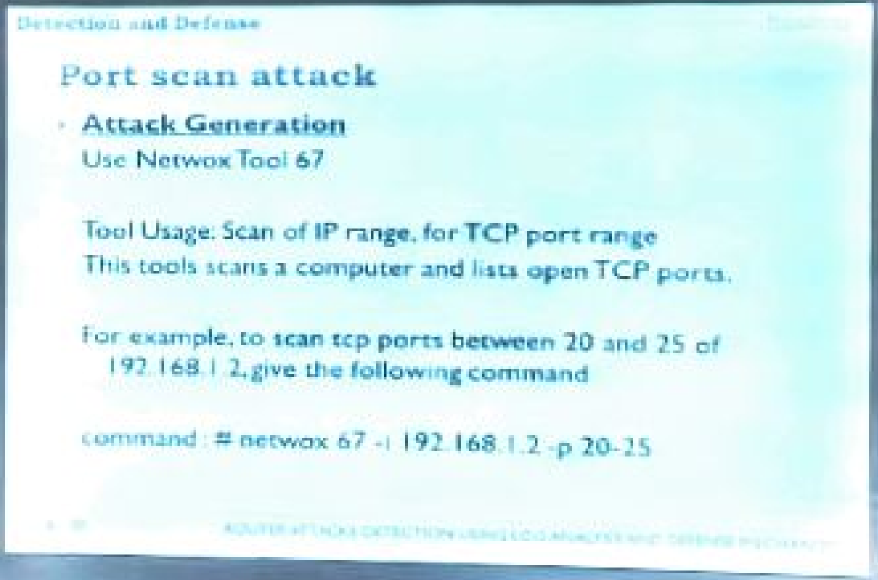
  When a port scan happens on a router, the log entries which are generated are shown in Fig

Simulation model





Simulation model



Port scan attack

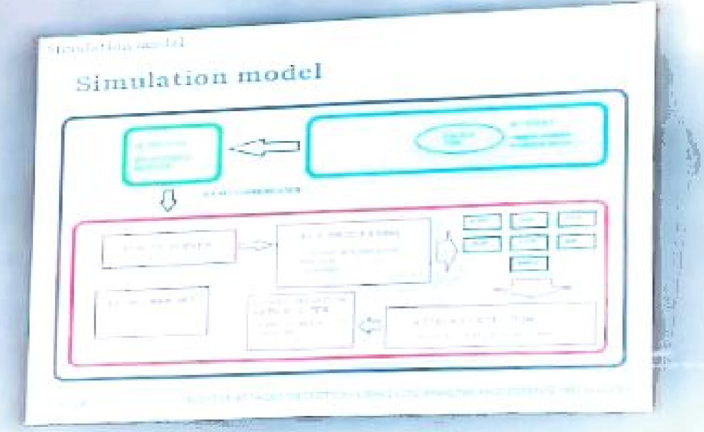
- **Attack Generation**

  Use Netwox Tool 67

  Tool Usage: Scan of IP range, for TCP port range
  This tools scans a computer and lists open TCP ports.

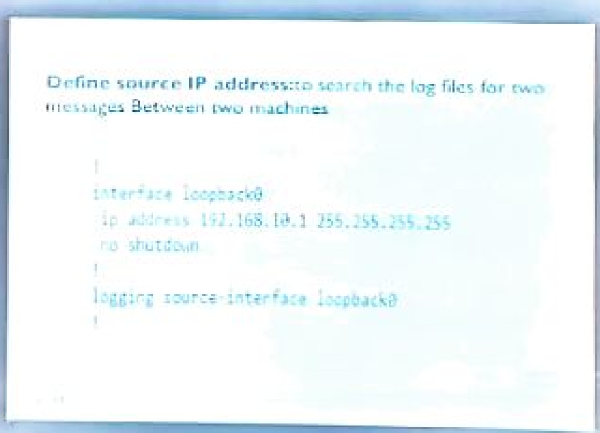
  For example, to scan tcp ports between 20 and 25 of 192.168.1.2,give the following command

  command : # netwox 67 -i 192.168.1.2 -p 20-25



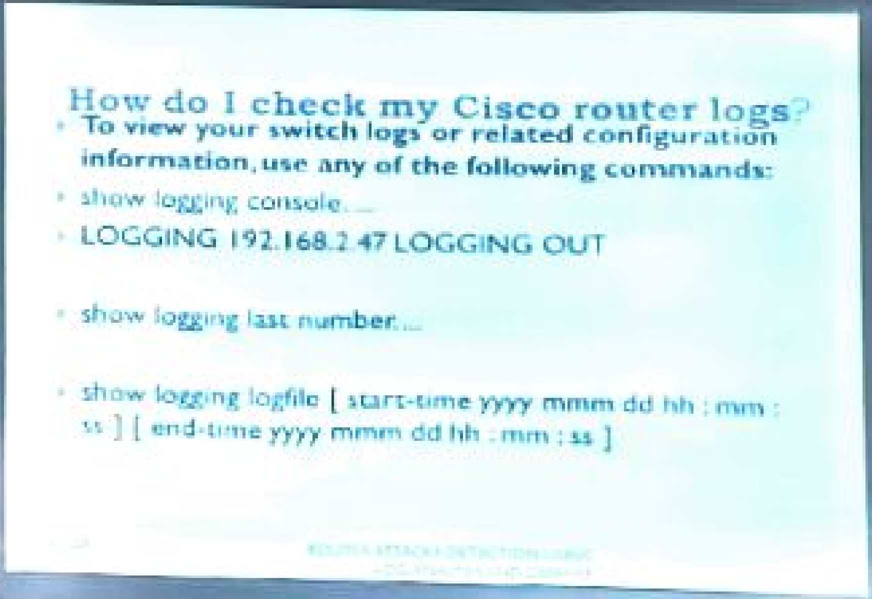
Simulation model

Simulation model



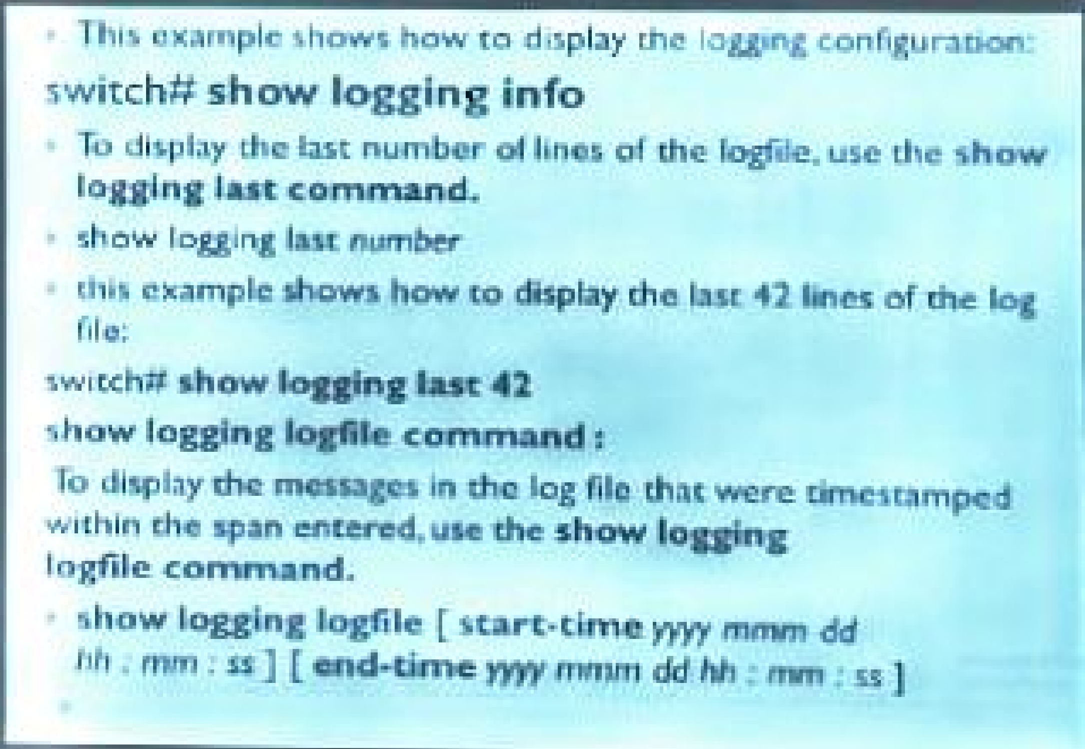
Define source IP address::to search the log files for two messages Between two machines

```
!
interface loopback0
 ip address 192.168.10.1 255.255.255.255
 no shutdown
!
logging source-interface loopback0
!
```



How do I check my Cisco router logs?

- **To view your switch logs or related configuration information, use any of the following commands:**
- show logging console. ...
- LOGGING 192.168.2.47 LOGGING OUT
- show logging last number. ...
- show logging logfile [start-time yyyy mmm dd hh : mm : ss] [end-time yyyy mmm dd hh : mm : ss]



- This example shows how to display the logging configuration:

```
switch# show logging info
```

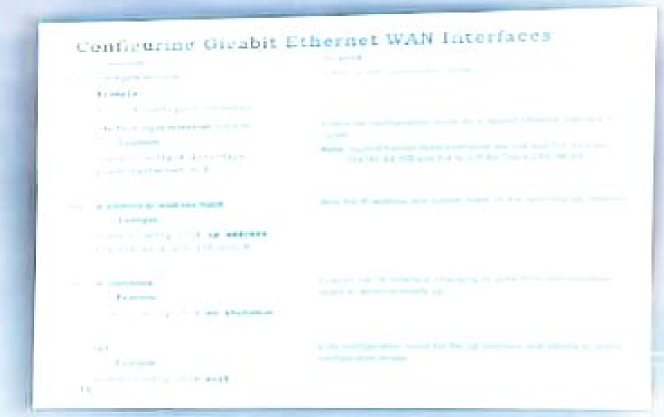
- To display the last number of lines of the logfile, use the **show logging last command.**
- show logging last *number*
- this example shows how to display the last 42 lines of the log file:

```
switch# show logging last 42
```

show logging logfile command :

To display the messages in the log file that were timestamped within the span entered, use the **show logging logfile command.**

- **show logging logfile** [**start-time** *yyyy mmm dd hh* : *mm* : *ss*] [**end-time** *yyyy mmm dd hh* : *mm* : *ss*]



Configuring Gigabit Ethernet WAN Interfaces

```
[illegible]
Example:
[illegible]
```

[illegible]

Note: [illegible]

```
[illegible]
Example:
[illegible] ip address
[illegible]
```

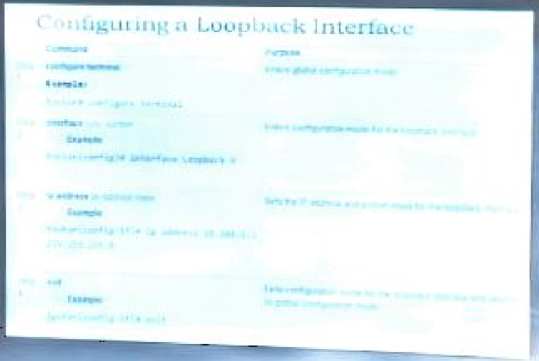
[illegible]

```
no shutdown
Example:
[illegible] no shutdown
```

[illegible]

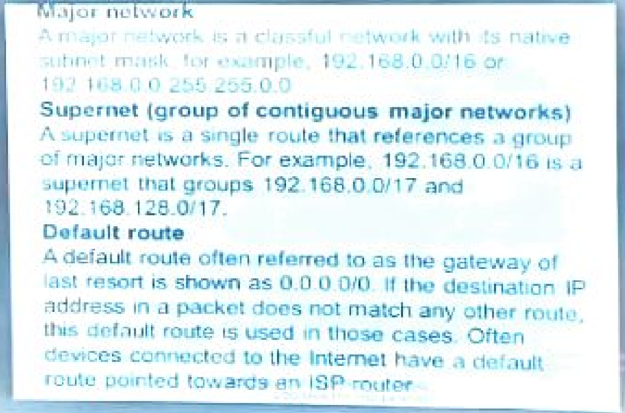
```
exit
Example:
[illegible] exit
```

[illegible]



Configuring a Loopback Interface

	Command	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**interface** *type number* **Example:** `Router(config)# interface Loopback 0`	Enters configuration mode for the loopback interface.
Step 3	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.108.1.1 255.255.255.0`	Sets the IP address and subnet mask for the loopback interface.
Step 4	**exit** **Example:** `Router(config-if)# exit`	Exits configuration mode for the loopback interface and returns to global configuration mode.



Major network

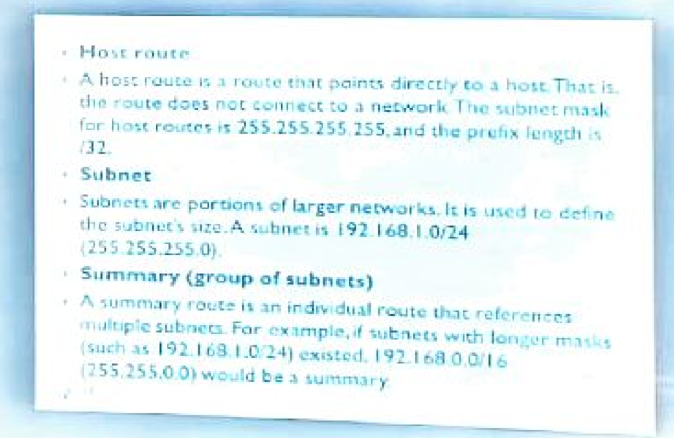
A major network is a classful network with its native subnet mask, for example, 192.168.0.0/16 or 192.168.0.0 255.255.0.0

Supernet (group of contiguous major networks)

A supernet is a single route that references a group of major networks. For example, 192.168.0.0/16 is a supernet that groups 192.168.0.0/17 and 192.168.128.0/17.

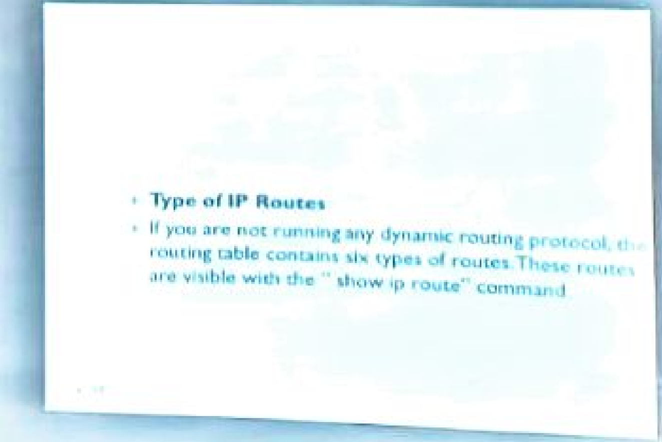
Default route

A default route often referred to as the gateway of last resort is shown as 0.0.0.0/0. If the destination IP address in a packet does not match any other route, this default route is used in those cases. Often devices connected to the Internet have a default route pointed towards an ISP router.

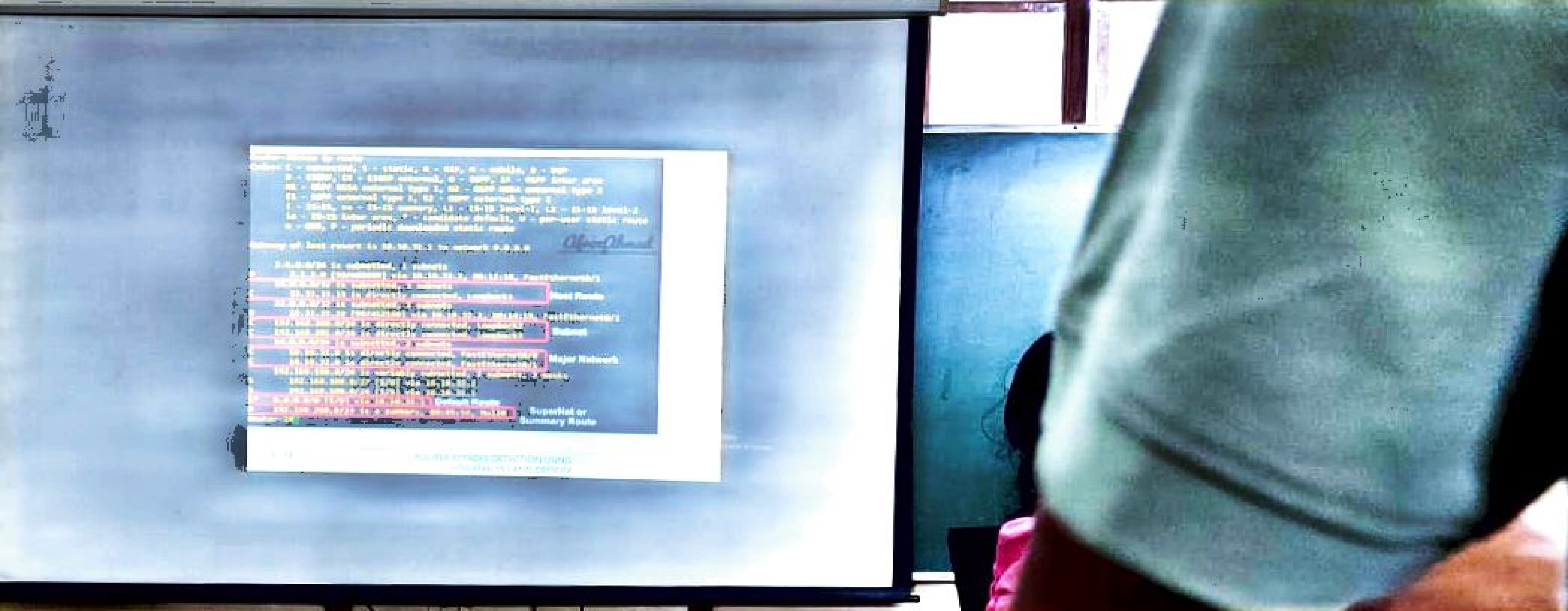


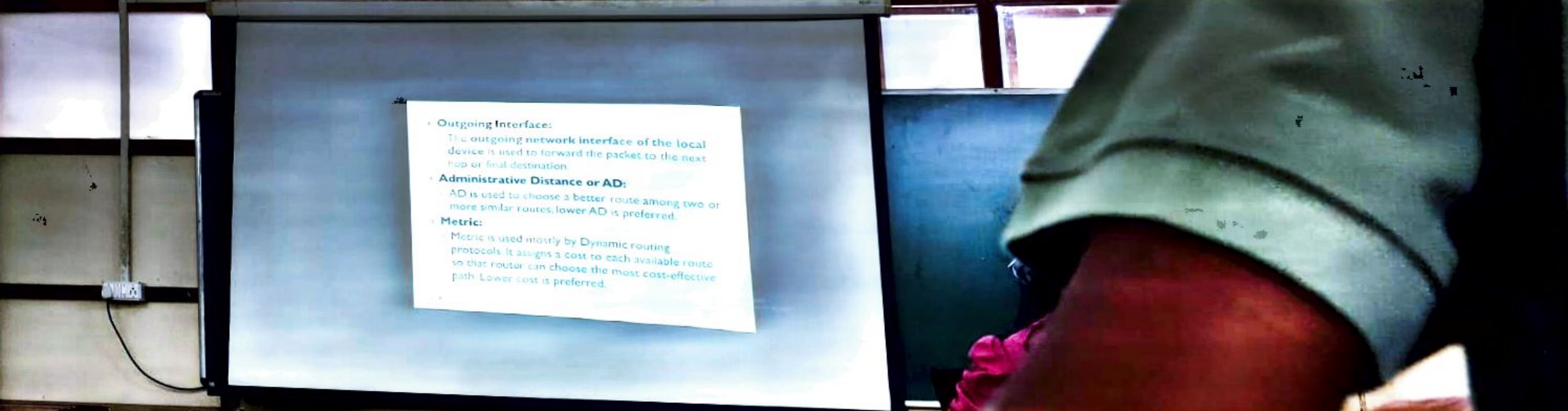
- Host route
- A host route is a route that points directly to a host. That is, the route does not connect to a network. The subnet mask for host routes is 255.255.255.255, and the prefix length is /32.
- **Subnet**
- Subnets are portions of larger networks. It is used to define the subnet's size. A subnet is 192.168.1.0/24 (255.255.255.0).
- **Summary (group of subnets)**
- A summary route is an individual route that references multiple subnets. For example, if subnets with longer masks (such as 192.168.1.0/24) existed, 192.168.0.0/16 (255.255.0.0) would be a summary.

Command	Purpose
configure terminal Example: [illegible] Router# configure terminal	Enters global configuration mode, when using the console port.
hostname name Example: Router(config)# hostname Router	Specifies the name for the router.
enable secret password Example: Router(config)# enable secret [illegible]	Specifies an encrypted password to prevent unauthorized access to the router.
no ip domain-lookup Example: Router(config)# no ip domain-lookup	Disables the router from translating unfamiliar words (typos) into IP addresses.

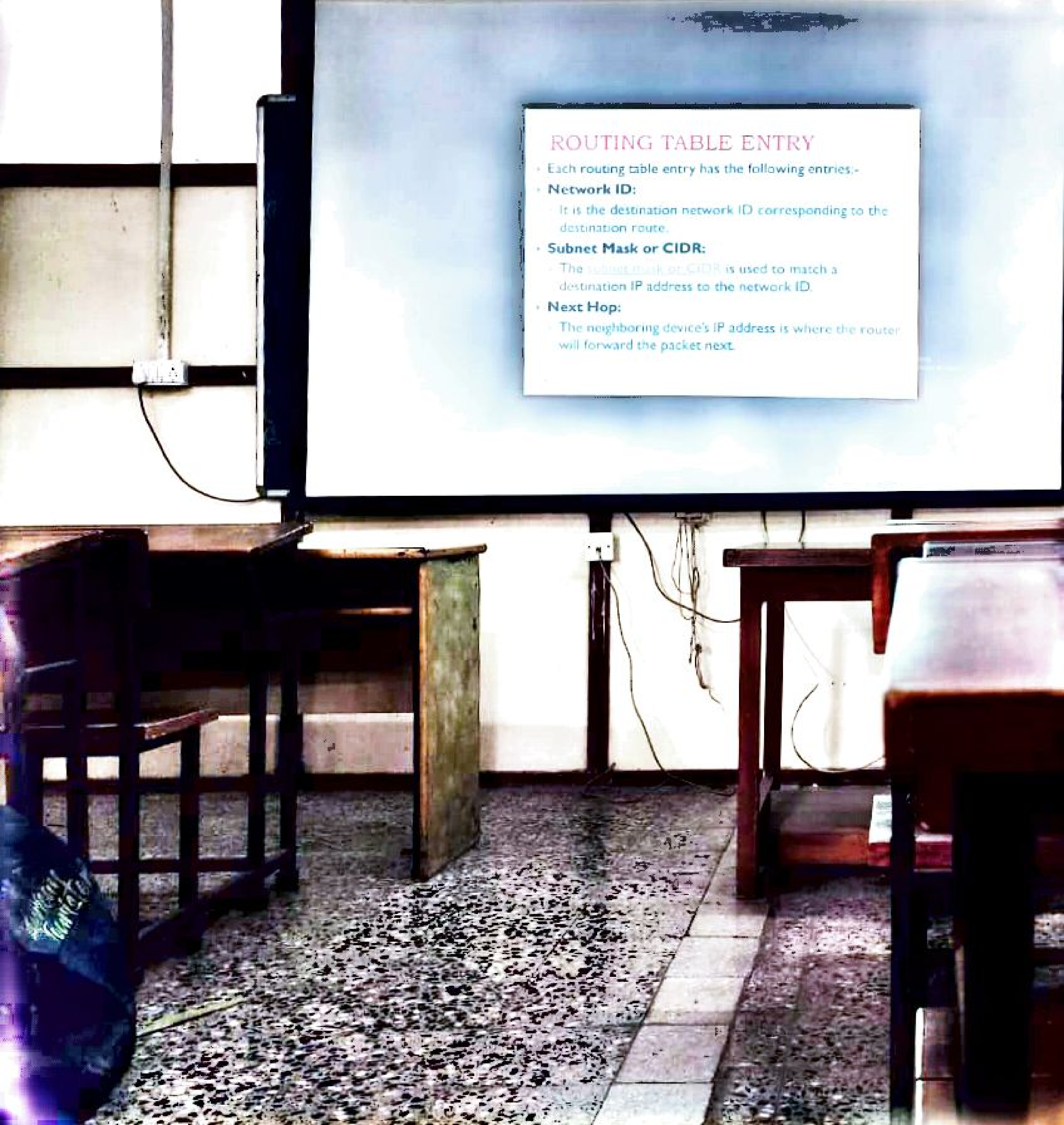


- **Type of IP Routes**
- If you are not running any dynamic routing protocol, the routing table contains six types of routes.These routes are visible with the " show ip route" command.


Host Route
Subnet
Major Network
Default Route
Supernet or
Summary Route
ROUTER ATTACKS DETECTION USING

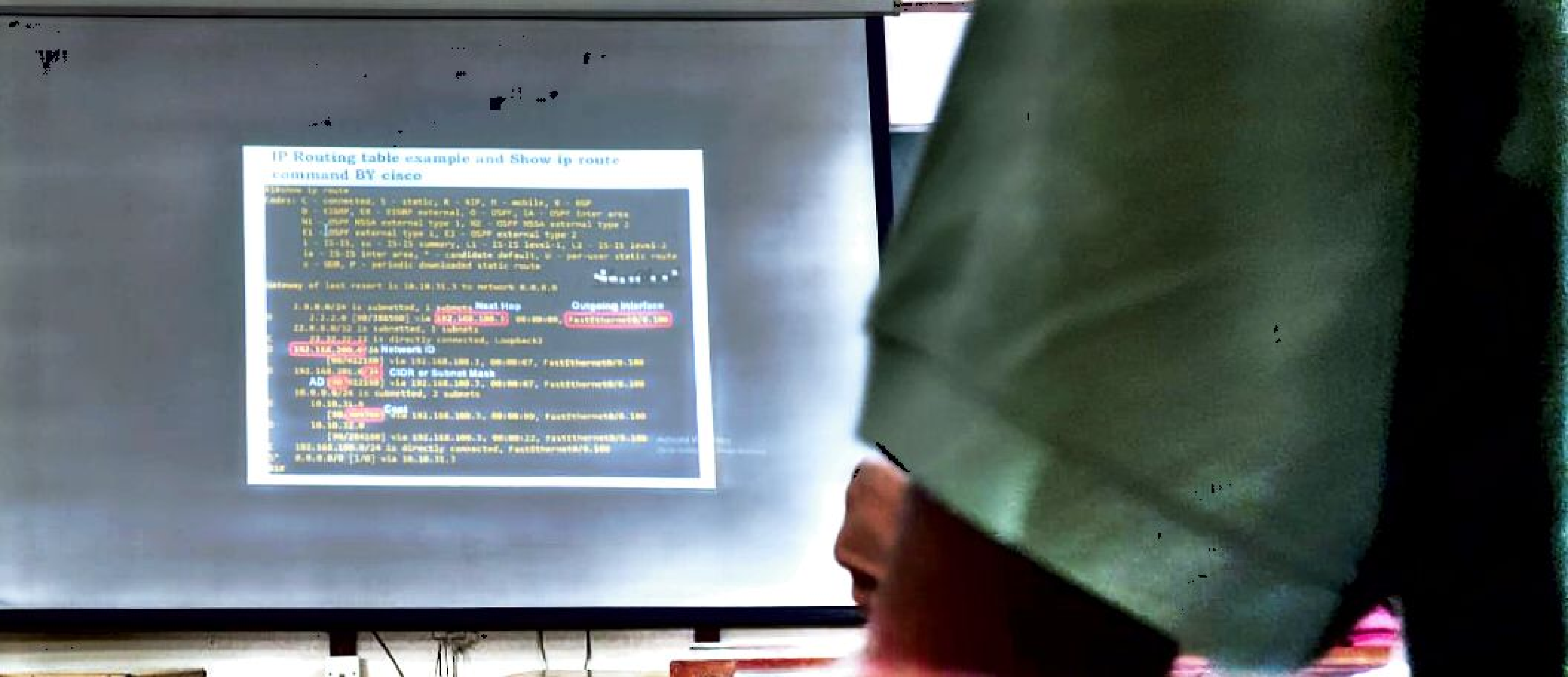


- **Outgoing Interface:**
  - The **outgoing network interface of the local device** is used to forward the packet to the next hop or final destination.
- **Administrative Distance or AD:**
  - AD is used to choose a better route among two or more similar routes; lower AD is preferred.
- **Metric:**
  - Metric is used mostly by Dynamic routing protocols. It assigns a cost to each available route so that router can choose the most cost-effective path. Lower cost is preferred.



ROUTING TABLE ENTRY

- Each routing table entry has the following entries:-
- **Network ID:**
  - It is the destination network ID corresponding to the destination route.
- **Subnet Mask or CIDR:**
  - The subnet mask or CIDR is used to match a destination IP address to the network ID.
- **Next Hop:**
  - The neighboring device's IP address is where the router will forward the packet next.

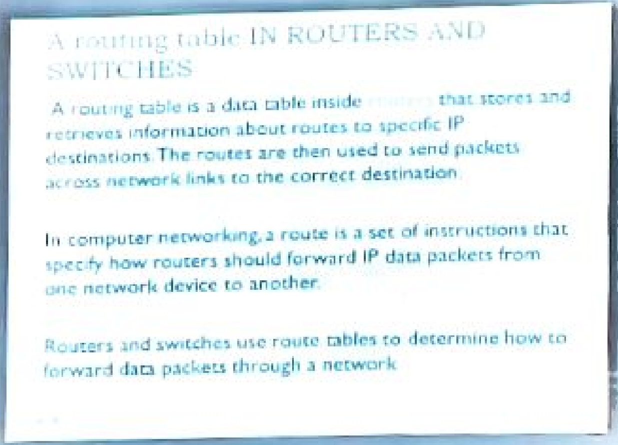


IP Routing table example and Show ip route command BY cisco

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.10.31.3 to network 0.0.0.0

     1.0.0.0/24 is subnetted, 1 subnets
D       2.2.2.0 [90/[illegible]] via 192.168.100.1, 00:00:00, FastEthernet0/0.100
     22.0.0.0/32 is subnetted, 3 subnets
C       22.22.22.22 is directly connected, Loopback2
D    192.168.200.0/24
           [90/412160] via 192.168.100.1, 00:00:47, FastEthernet0/0.100
D    192.168.201.0/24
           [90/412160] via 192.168.100.3, 00:00:47, FastEthernet0/0.100
     10.0.0.0/24 is subnetted, 2 subnets
D       10.10.31.0
           [90/[illegible]] via 192.168.100.3, 00:00:59, FastEthernet0/0.100
D       10.10.32.0
           [90/284160] via 192.168.100.3, 00:00:12, FastEthernet0/0.100
C    192.168.100.0/24 is directly connected, FastEthernet0/0.100
S*   0.0.0.0/0 [1/0] via 10.10.31.3
R1#
```

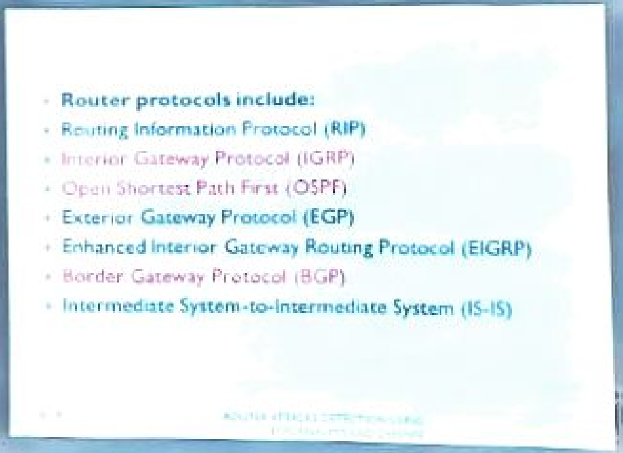


A routing table IN ROUTERS AND SWITCHES

A routing table is a data table inside routers that stores and retrieves information about routes to specific IP destinations. The routes are then used to send packets across network links to the correct destination.

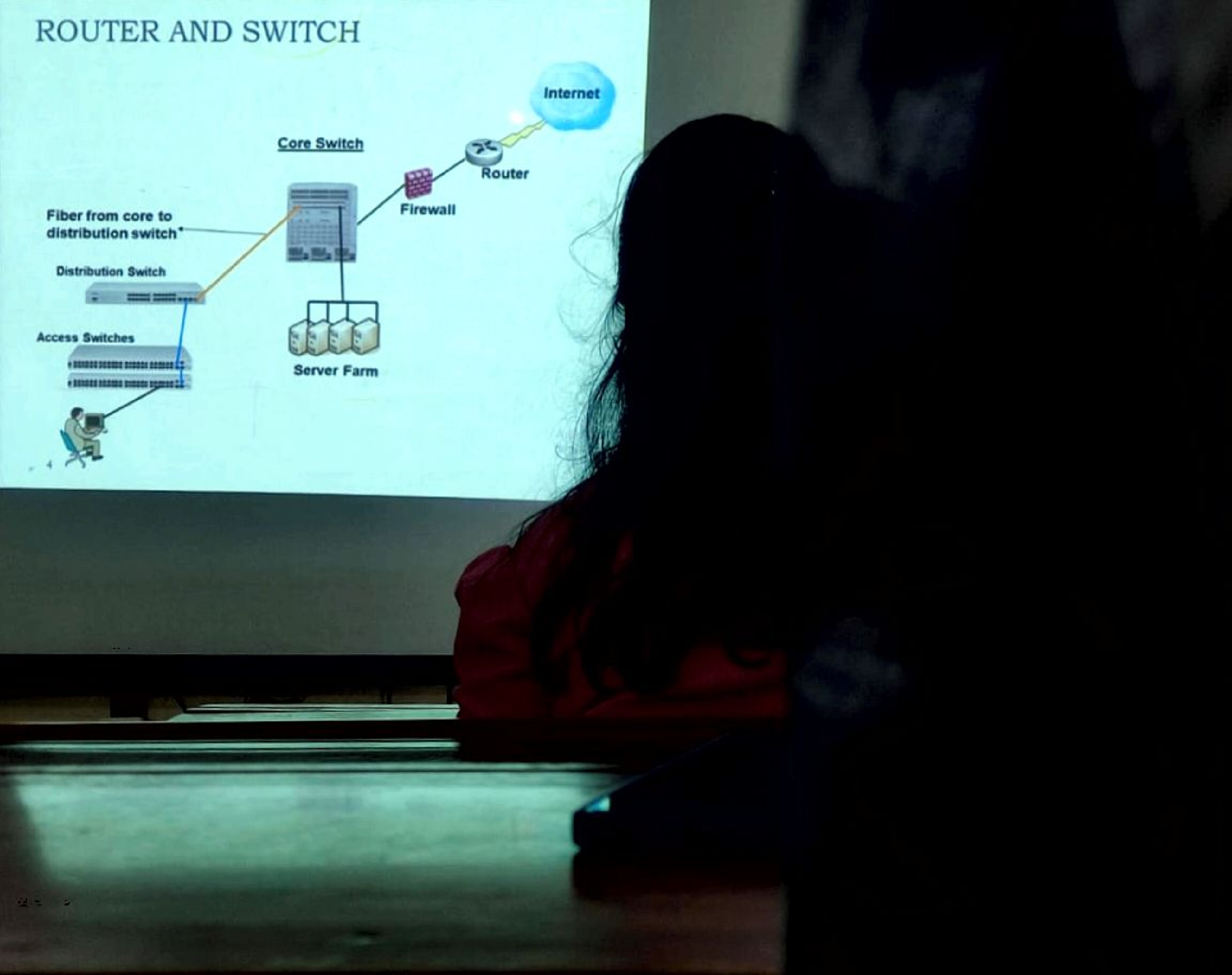
In computer networking, a route is a set of instructions that specify how routers should forward IP data packets from one network device to another.

Routers and switches use route tables to determine how to forward data packets through a network.

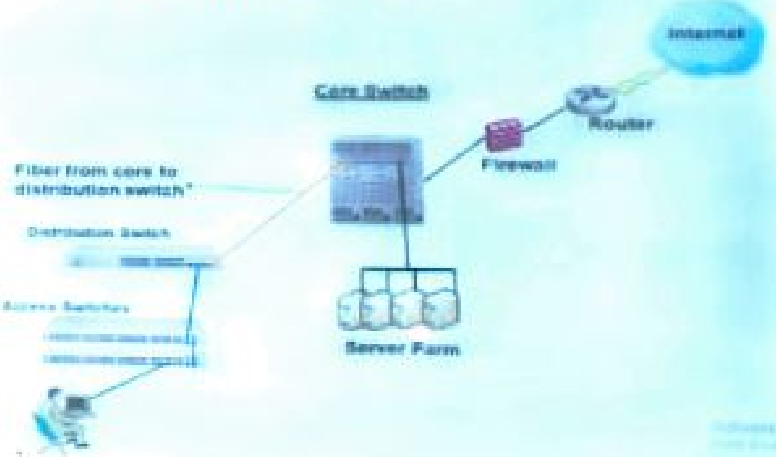


- **Router protocols include:**
- Routing Information Protocol (RIP)
- Interior Gateway Protocol (IGRP)
- Open Shortest Path First (OSPF)
- Exterior Gateway Protocol (EGP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Border Gateway Protocol (BGP)
- Intermediate System-to-Intermediate System (IS-IS)

ROUTER AND SWITCH



ROUTER AND SWITCH



Internet

Core Switch

Router

Firewall

Fiber from core to distribution switch"

Distribution Switch

Access Switches

Server Farm