Cisco.com

Securing Network Devices

Topic 6

Objectives

- Discussion of “The Three Planes”
- Banners/MOTD
- Logging
- Enable/Secret
- Line/Console
- Access-List control of remote access

The Three Planes

Three Planes

- Management Plan
- Control Plane
- Data Plane

Control Plane Example: CDP

Discovering Neighbors with CDP

- Runs on routers with Cisco IOS 10.3 or later and Cisco switches and hubs
- Summary information includes:

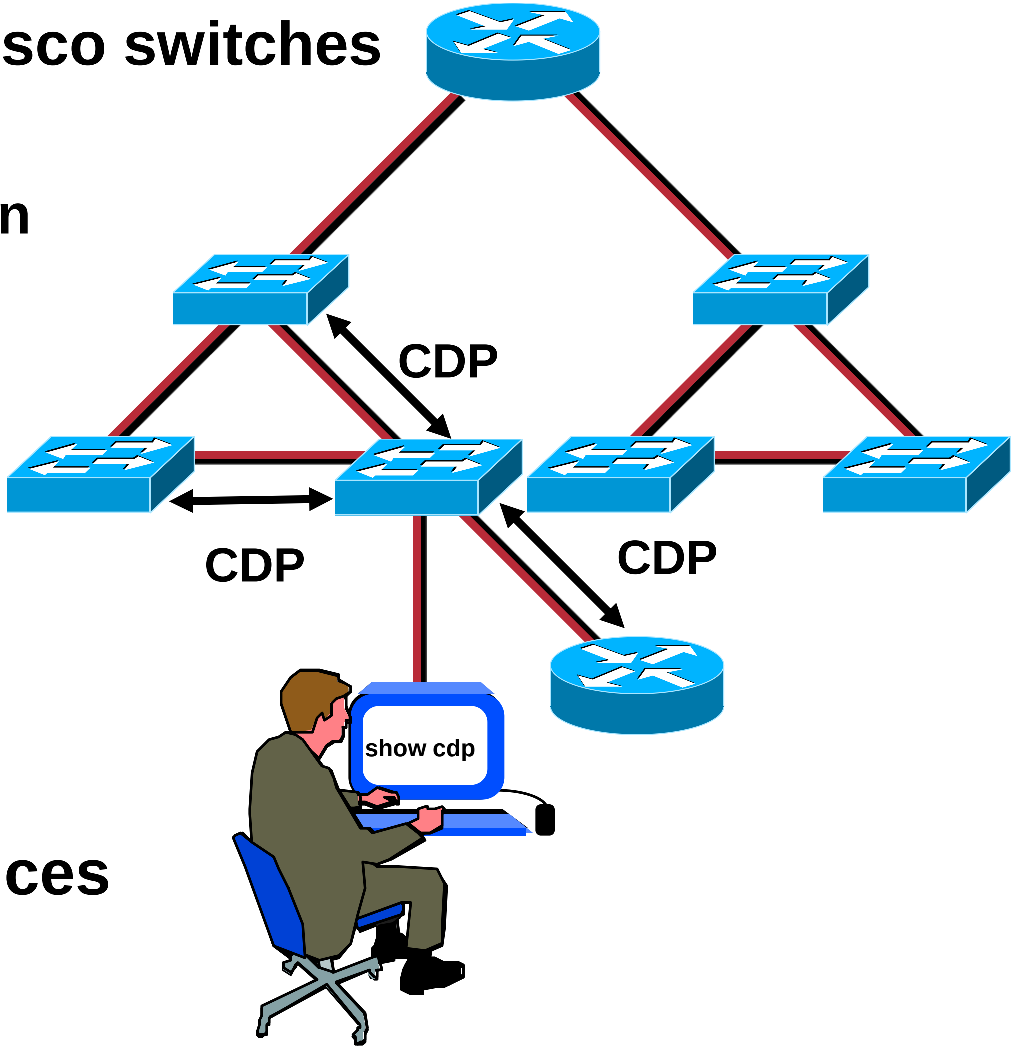
  Device identifiers

  Address list

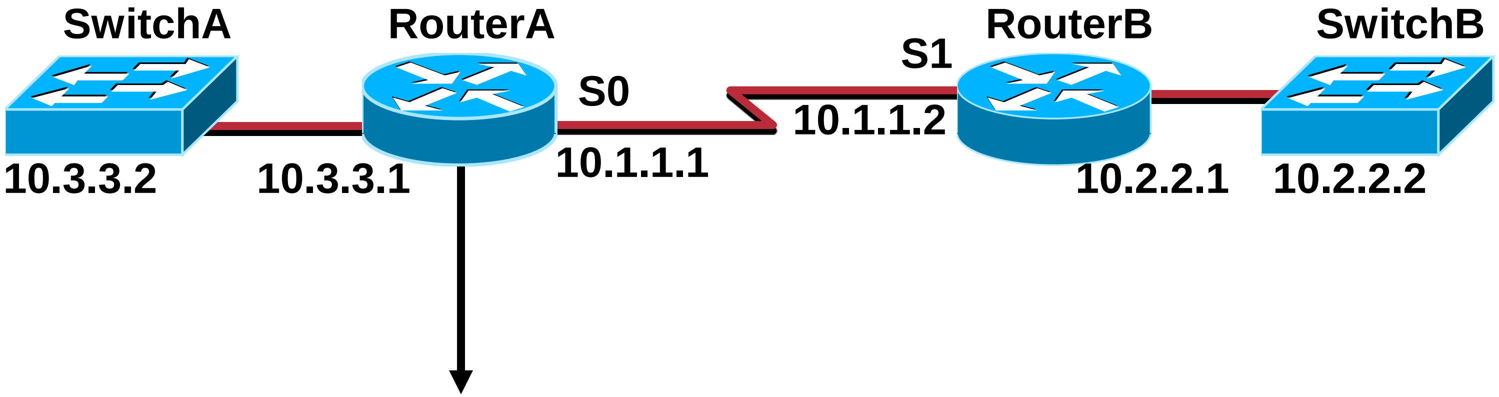
  Port identifier

  Capabilities list

  Platform
- 95% of Cisco Devices

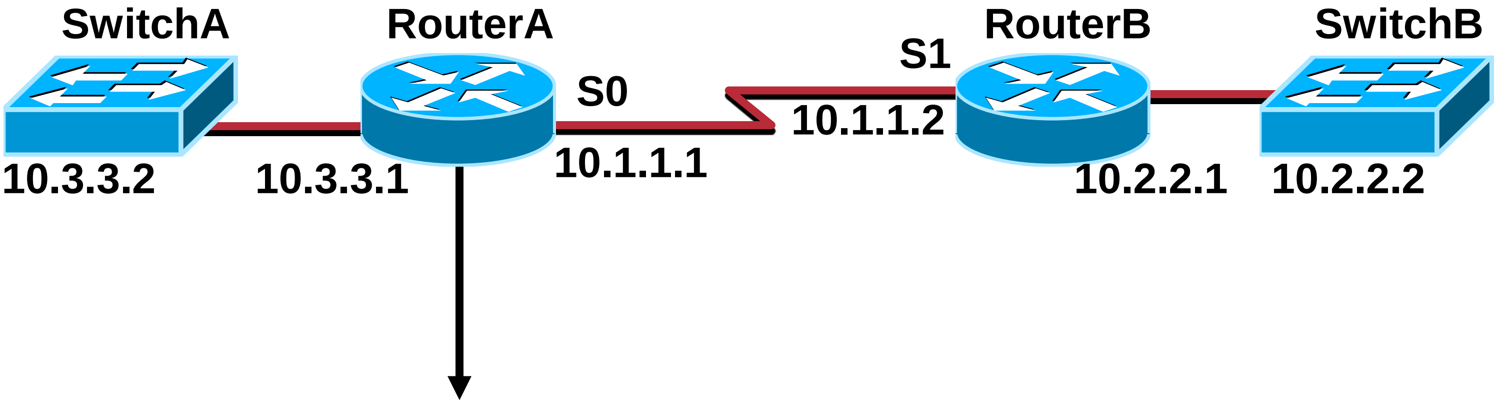


Using CDP



```
RouterA#sh cdp ?
  entry      Information for specific neighbor entry
  interface  CDP interface status and configuration
  neighbors  CDP neighbor entries
  traffic    CDP statistics
  <cr>
RouterA(config)#no cdp run
RouterA(config)#interface serial0
RouterA(config-if)#no cdp enable
```

Using the *show cdp neighbor* Command

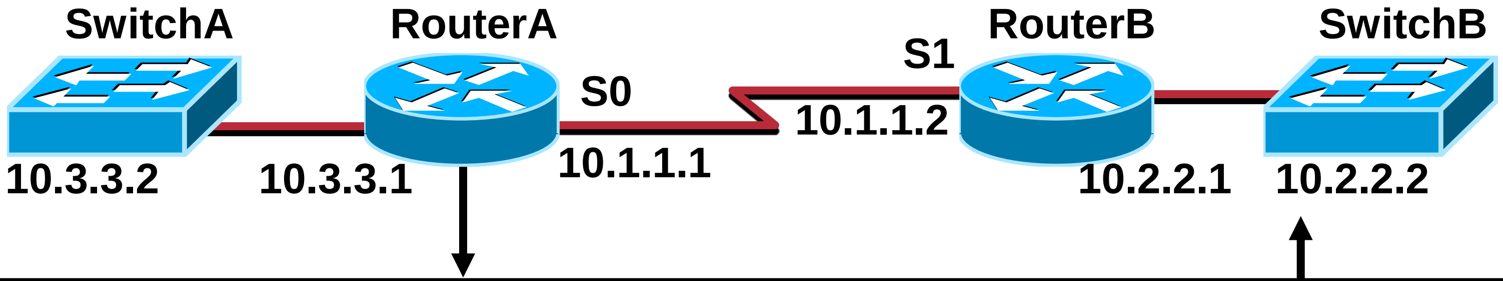


```
RouterA#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce    Holdtme    Capability  Platform  Port ID
RouterB            Ser 0        148          R       2522      Ser 1
SwitchA0050BD855780 Eth 0          167          T S       1900      2
```

SwitchA also provides its Mac address

Management Plane Example: Telnet

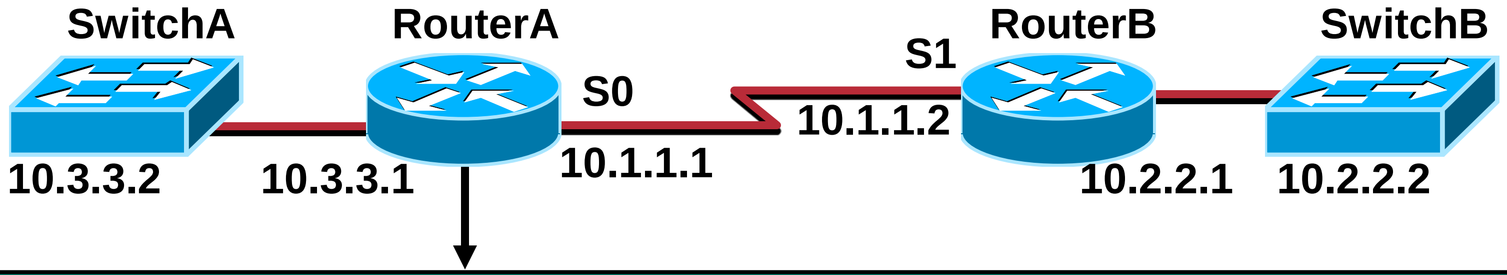
Using Telnet to Connect to Remote Devices



```
RouterA#telnet 10.2.2.2
Trying 10.2.2.2 ... Open
-----------------------------------------------
Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc.  1993-1998
All rights reserved.
Enterprise Edition Software
Ethernet Address:      00-90-86-73-33-40
PCA Number:            73-2239-06
PCA Serial Number:     FAA02359H8K
Model Number:          WS-C1924-EN
System Serial Number:  FAA0237X0FQ
.
.
SwitchB>
```

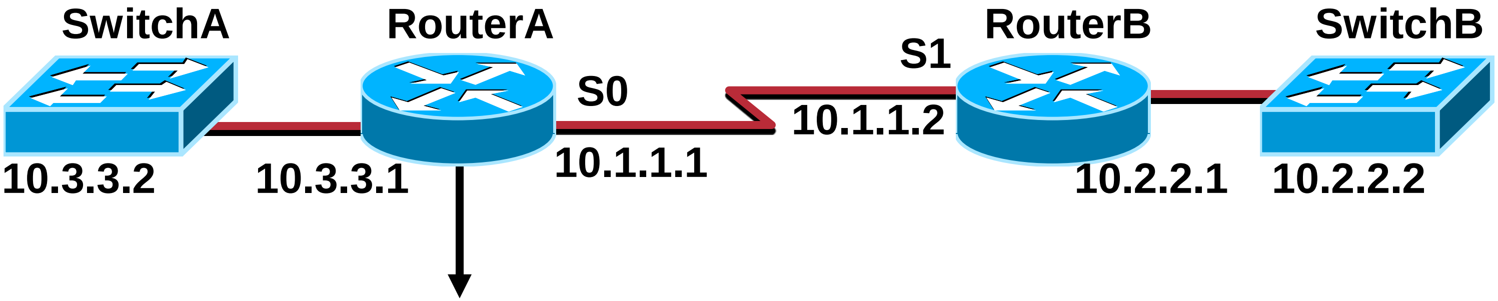
Remote device

Viewing Telnet Connections



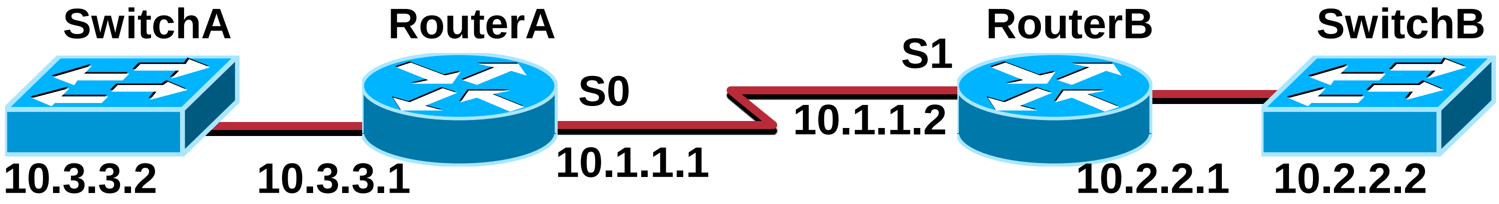
```
RouterA#sh session
Conn Host              Address          Byte  Idle Conn Name
   1 10.1.1.2          10.1.1.2            0     1 10.1.1.2
*  2 10.3.3.2          10.3.3.2            0     0 10.3.3.2



RouterA#sh user
    Line     User      Host(s)              Idle Location
*  0 con 0             10.1.1.2                3
                  10.3.3.2                2
  11 vty 0             idle                  1 10.1.1.2
```

Suspending a Telnet Session



```
RouterB#<Ctrl-Shift-6>x
RouterA#sh session
Conn Host                Address            Byte  Idle Conn Name
   1 10.1.1.2          10.1.1.2              0     1 10.1.1.2
RouterA#resume 1
RouterB#
```

Closing a Telnet Session



```
RouterA#disconnect
Closing connection to 10.3.3.2 [confirm]
```

Closing the current session opened by you

```
RouterA#clear line 11
[confirm]
 [OK]
```

Closing a session opened by a remote device

Objectives

- Discussion of “The Three Planes”
- Banners/MOTD
- Logging
- Enable/Secret
- Line/Console
- Access-List control of remote access

Banner or MOTD [Message of the day]

```
!
banner motd &
------------------------------------------------------------
!!!!!! Warning!!!!!!!!!
Unauthorized users must disconnect now.
All source IP-Addresses and activities are logged.
-
We will prosecute, unauthorized access, to the
Full extent of the law!
------------------------------------------------------------
&
!
!
line con 0
 location SITE-X
 exec-timeout 0 0
 privilege level 15
 logging synchronous
!
line aux 0
!
line vty 0 4
 login
!
```

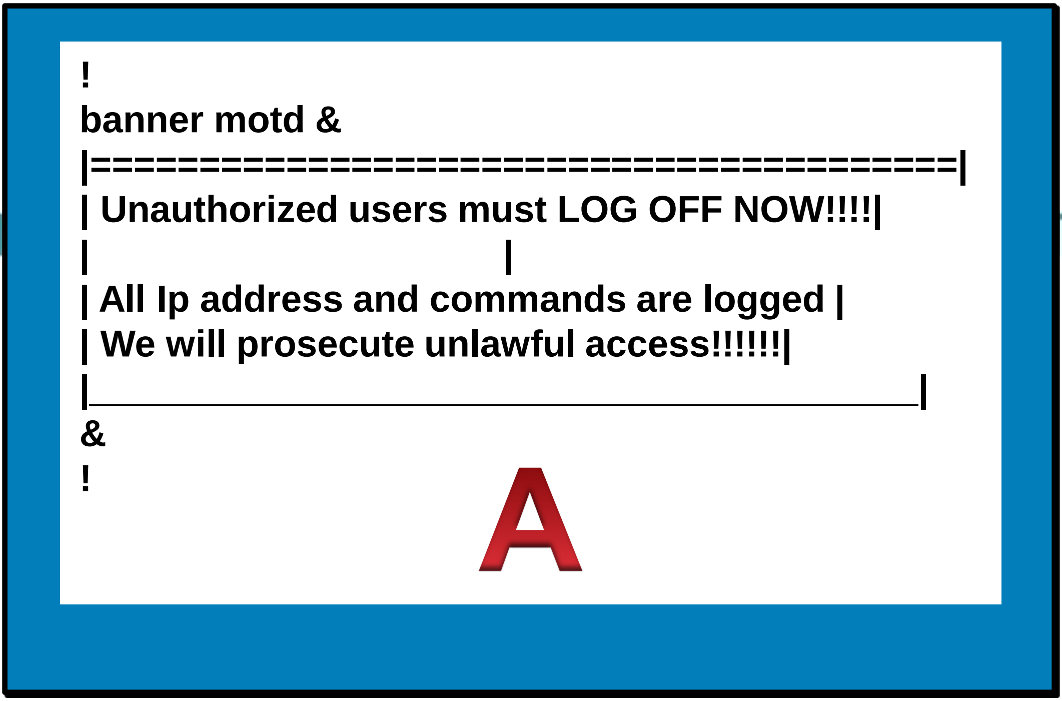
Legal Notification Banners

- Notification that system access and use is permitted only by specifically authorized personnel, and perhaps information about who may authorize use.

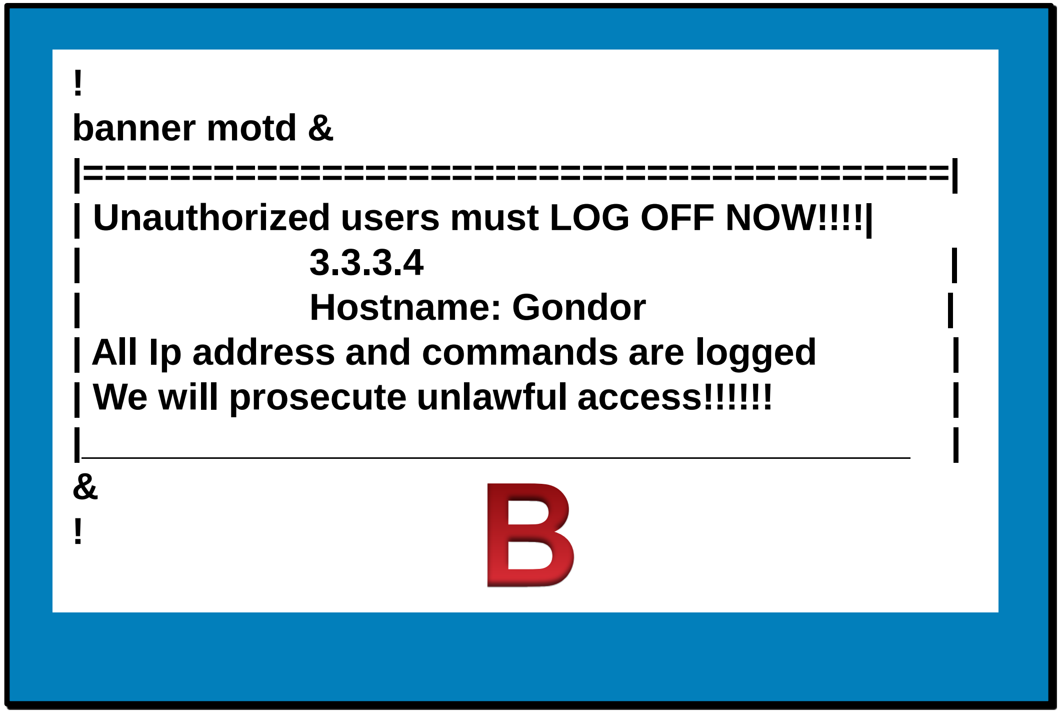
- Notification that unauthorized access and use of the system is unlawful, and may be subject to civil and/or criminal penalties.

- Notification that access and use of the system may be logged or monitored without further notice, and the resulting logs may be used as evidence in court.

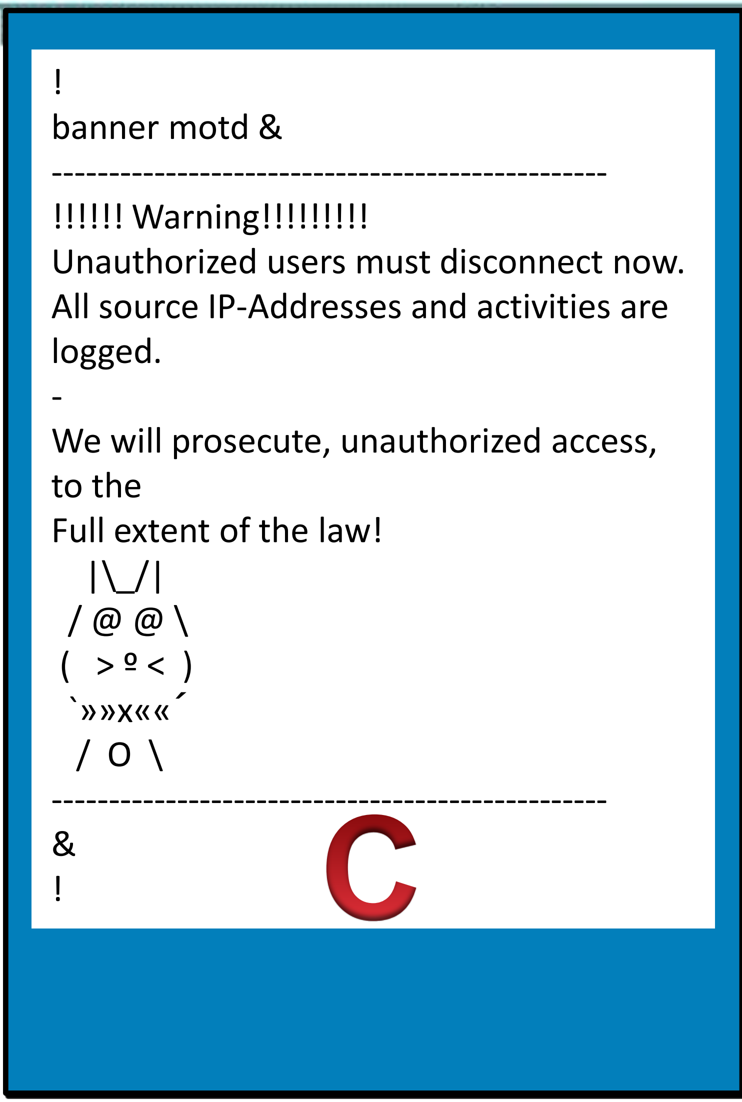
- Additional specific notices required by specific local laws.



```
!
banner motd &
|========================================|
| Unauthorized users must LOG OFF NOW!!!!|
|                                  |
| All Ip address and commands are logged |
| We will prosecute unlawful access!!!!!!|
|________________________________________|
&
!
```



```
!
banner motd &
|========================================|
| Unauthorized users must LOG OFF NOW!!!!|
|                   3.3.3.4                  |
|                   Hostname: Gondor         |
| All Ip address and commands are logged     |
| We will prosecute unlawful access!!!!!!    |
|_______________________________________     |
&
!
```



```
!
banner motd &
-------------------------------------------------
!!!!!! Warning!!!!!!!!!
Unauthorized users must disconnect now.
All source IP-Addresses and activities are
logged.
-
We will prosecute, unauthorized access,
to the
Full extent of the law!
   |\_/|
  / @ @ \
 (  > º < )
  `»»x««´
   /  O  \
-------------------------------------------------
&
!
```

Objectives

- Discussion of “The Three Planes”
- Banners/MOTD
- Logging
- Enable/Secret
- Line/Console
- Access-List control of remote access

Infrastructure Device Management Access Logging

It is critical to ensure that infrastructure device access and configuration changes are logged to record the following information:

- Who accessed a device
- When a user logged in
- What a user did
- When a user logged off
- Failed access attempts
- Failed authentication requests
- Failed authorization requests

Logging Example: “Who’s logging on”

```
Router(config)# login on-success log
Router(config)# login on-failure log
```

A sample syslog message for a successful login is shown below:

```
Sep 25 12:49:32.465 UTC: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success
[user: admin2
] [Source: 172.26.158.234] [localport: 22] at 12:49:32 UTC Thu Sep 25 2003
```

A sample syslog message for a failed login attempt is shown below:

```
Sep 25 13:19:46.864 UTC: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: ]
[Sourc
e: 172.26.158.234] [localport: 22] [Reason: Login Authentication Failed] at 13:1
9:46 UTC Thu Sep 25 2003
```

Objectives

- Discussion of “The Three Planes”
- Banners/MOTD
- Logging
- Enable/Secret
- Line/Console
- Access-List control of remote access

Basic IOS Modes and Commands

- **User EXEC Mode**

  The default command mode for the CLI is user EXEC mode. The EXEC commands available at the user EXEC level are a subset of those available at the privileged EXEC level. In general, the user EXEC commands allow you to connect to remote devices, change terminal settings on a temporary basis, perform basic tests, and list system information. The prompt for user EXEC mode is the name of the device followed by an angle bracket: Router>.

- **Privileged EXEC Mode**

  Privileged EXEC mode is password protected, and allows the use of all EXEC mode commands available on the system. To enter privileged EXEC mode from user EXEC mode, use the **enable** command. Privileged EXEC mode allows access to global configuration mode through the use of the enable command. The privileged EXEC mode prompt consists of the devices's host name followed by the pound sign: Router# .

- **Global Configuration Mode**

  Global configuration commands generally apply to features that affect the system as a whole, rather than just one protocol or interface. You can also enter any of the specific configuration modes listed in the following section from global configuration mode.

  To enter global configuration mode, use the **configure terminal** privileged EXEC command. The router prompt for global configuration mode is indicated by the term config in parenthesis: Router(config)#

- **?** – View available commands
- **enable** – Privileged EXEC Mode
- **configure terminal** – Global Configuration Mode
- **enable password** – Set privileged password
- **show** – View information about specific things on router
- **exit** – Back up one level
- **end** – Exit back to global command line
- **write memory** – Save your configurations
- **logout**

Commands to master!

- enable password
- enable secret
- service password-encryption

Secret or Password?

"If" you were asked, "was the weak or strong scheme used for password/credential?"

To determine which scheme has been used to encrypt a specific password, check the digit preceding the encrypted string in the configuration file.

If that digit is a 7, the password has been encrypted using the weak algorithm. If the digit is a 5, the password has been hashed using the stronger MD5 algorithm.

For example, in the configuration command:

```
enable secret 5 $1$iUjJ$cDZ03KKGh7mHfX2RSbDqP.
```

The enable secret has been hashed with MD5, whereas in the command:

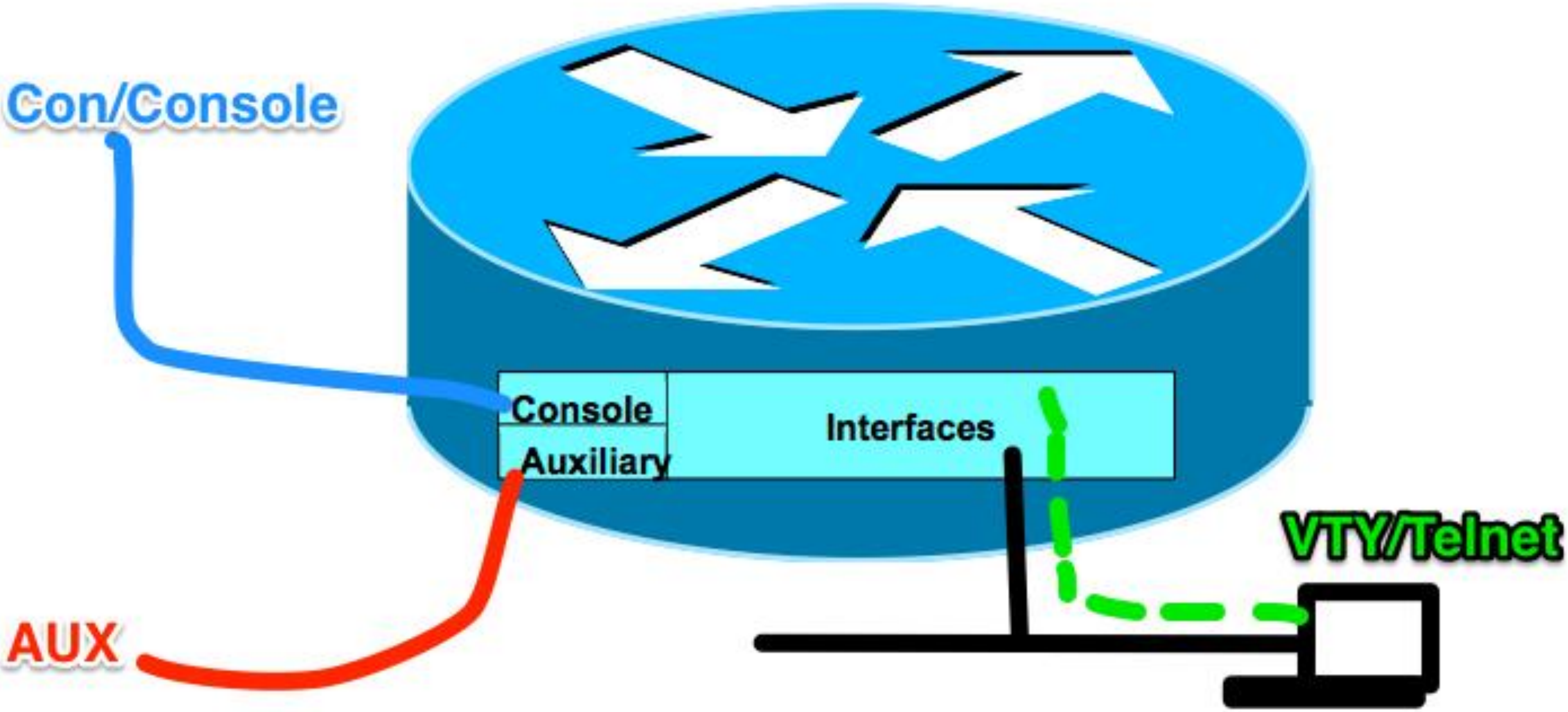
```
username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D
```

The password has been encrypted using the weak reversible algorithm.

Objectives

- Discussion of “The Three Planes”
- Banners/MOTD
- Logging
- Enable/Secret
- Line/Console
- Access-List control of remote access

Router Internal Components



Snippet: Telnet (VTY) and Console

```
line con 0
exec-timeout <minutes> [seconds]
Login
Password insecure
line vty 0 4
Login
Password insecure
exec-timeout <minutes> [seconds]
!
```

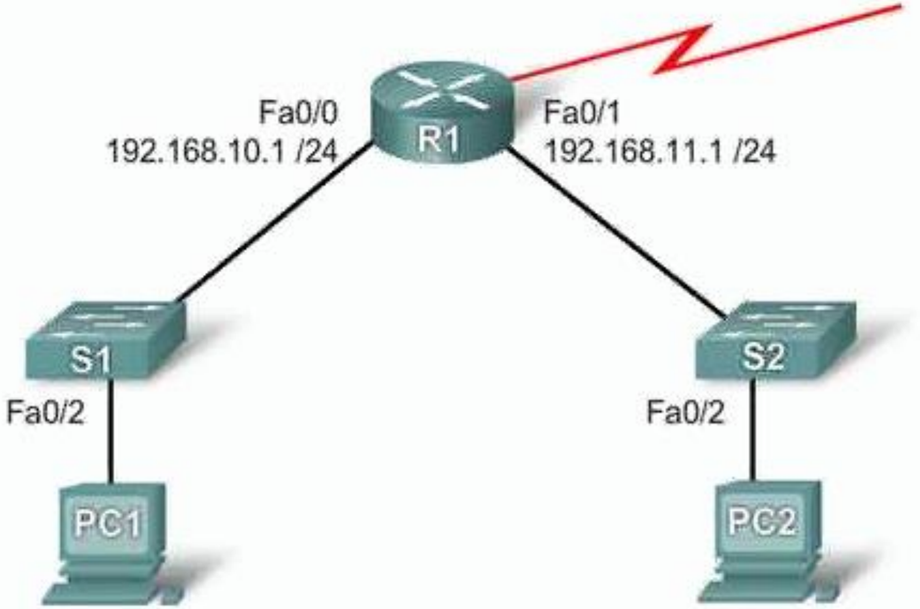
Allow Console and Telnet access with a password

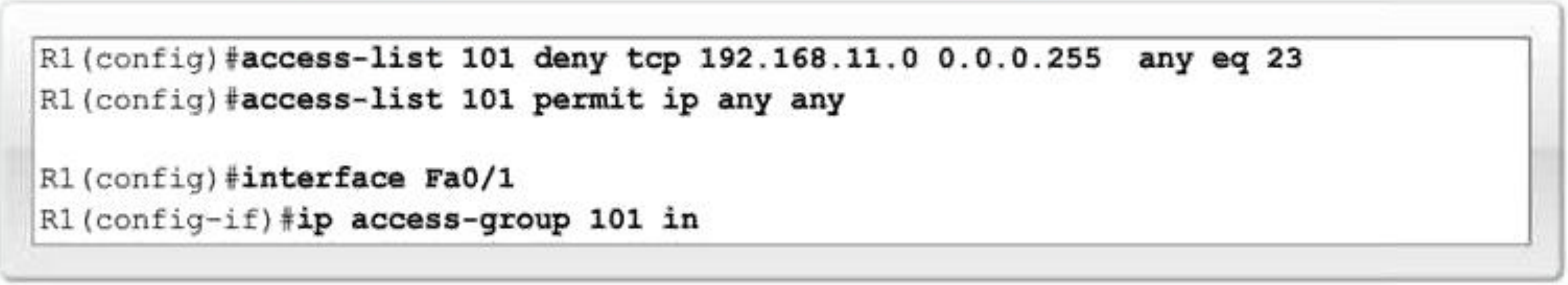
```
! Disable access to VTY
line vty 1
 login
 no exec
!
! Disable access to Console
line con 0
  login
  no exec
!
```

Disable Console and Telnet access, key command is “no exec”

Deny Telnet

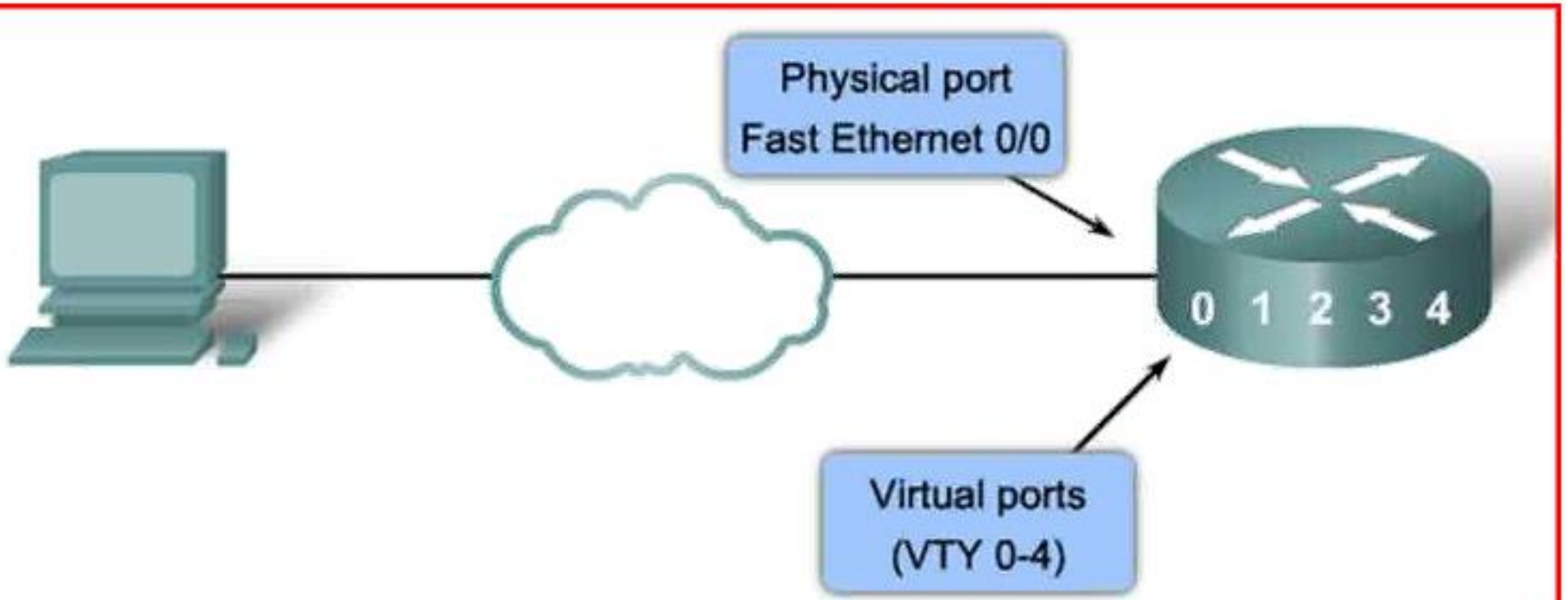
Extended ACL to Deny Only Telnet from Subnet





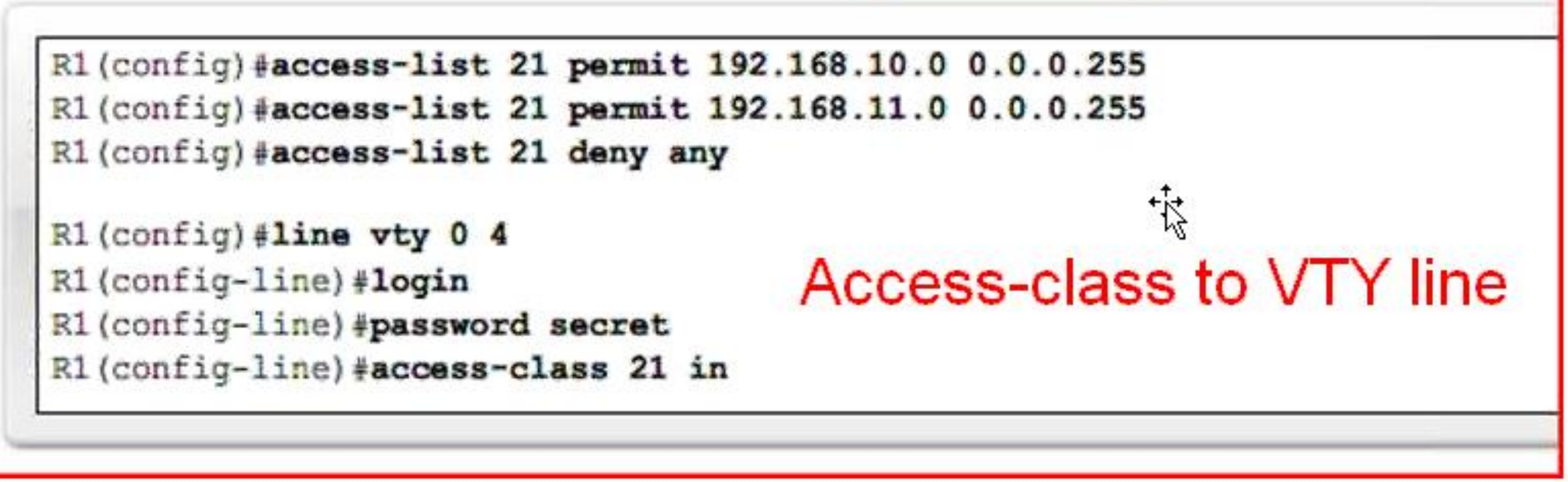
```
R1(config)#access-list 101 deny tcp 192.168.11.0 0.0.0.255  any eq 23
R1(config)#access-list 101 permit ip any any

R1(config)#interface Fa0/1
R1(config-if)#ip access-group 101 in
```

Control VTY Access



Physical port
Fast Ethernet 0/0

Virtual ports
(VTY 0-4)



```
R1(config)#access-list 21 permit 192.168.10.0 0.0.0.255
R1(config)#access-list 21 permit 192.168.11.0 0.0.0.255
R1(config)#access-list 21 deny any

R1(config)#line vty 0 4
R1(config-line)#login
R1(config-line)#password secret
R1(config-line)#access-class 21 in
```

Access-class to VTY line

Switch Configuration

- **enable** Privileged EXEC Mode
- **configure terminal**
- **enable password** (ex. Cisco)
- **hostname** (ex. MFHS_Switch) no spaces allowed in hostname
- **interface** (ex. fastethernet 0/1)
- **description** (ex. Connection MFHS Laptop1) any description you wish
- **ip address** (ex. 10.1.2.2 255.255.255.0) ip address and subnet mask
- **switchport access vlan 2** (ex. Sets port to access only vlan 2) or…
- **switchport mode trunk** (ex. Sets port to trunk all Vlans)
- **end**
- **write memory** **(ALAWAYS, ALWAYS, ALWAYS SAVE YOUR WORK)**

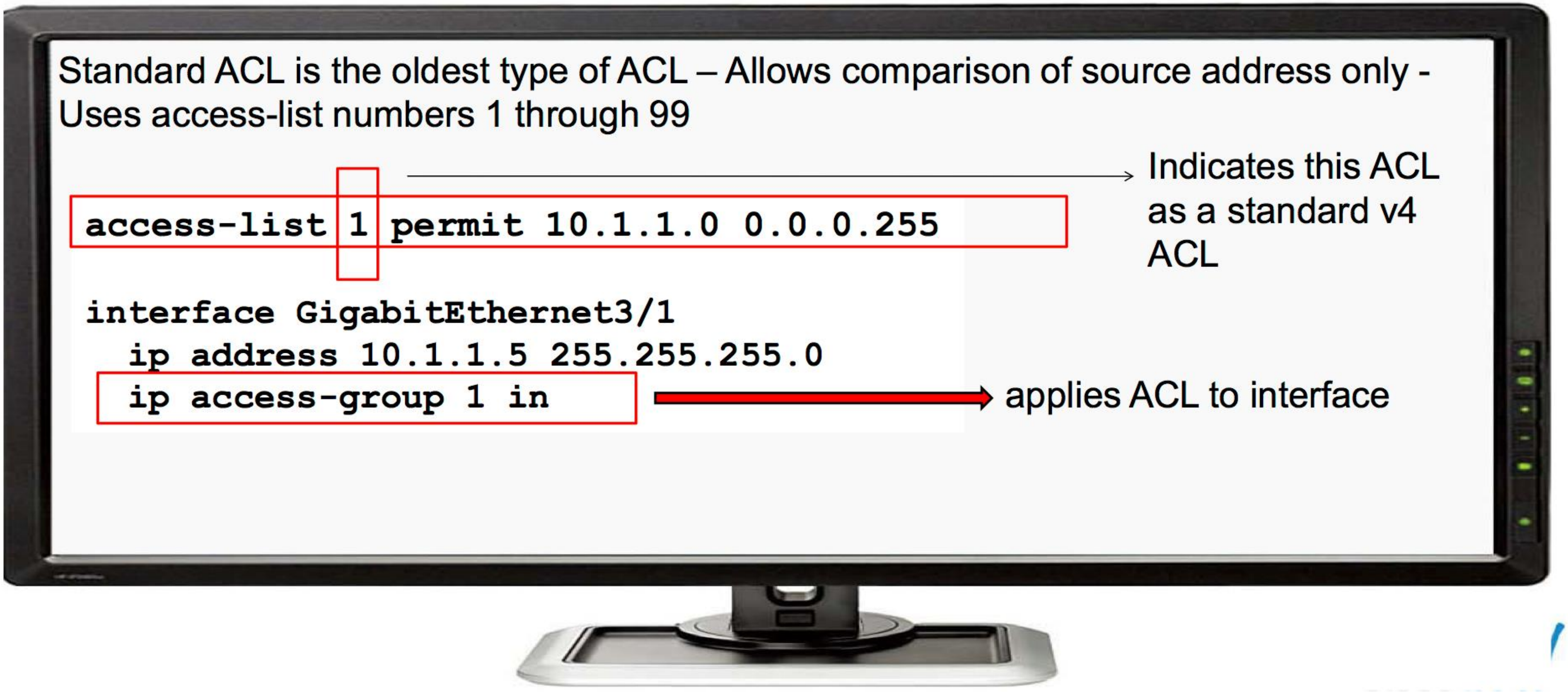
Router Configuration

- **enable** Privileged EXEC Mode
- **configure terminal**
- **hostname** (ex. MFHS_Router) no spaces allowed in hostname
- **interface** (ex. gigabit 0/0) and/or…
- **interface** (ex. gigabit 0/0.2 when setting up Vlan Trunk)
- **description** (ex. Connection HSH Router) any description you wish
- **ip address** (10.1.100.1 255.255.255.0) ip address and subnet mask
- **encapsulation dot1q 2** (ex. Set when trunking vlan 2)
- **end**
- **write memory** **(ALAWAYS, ALWAYS, ALWAYS SAVE YOUR WORK)**

End-Point Configuration

- Name Your Device (ex. HSH iPad)
- IP Address (ex. 10.1.4.100)
- Subnet Mask (ex. 255.255.255.0)
- Default Gateway (ex. 10.1.4.1)

Standard IPv4 ACL



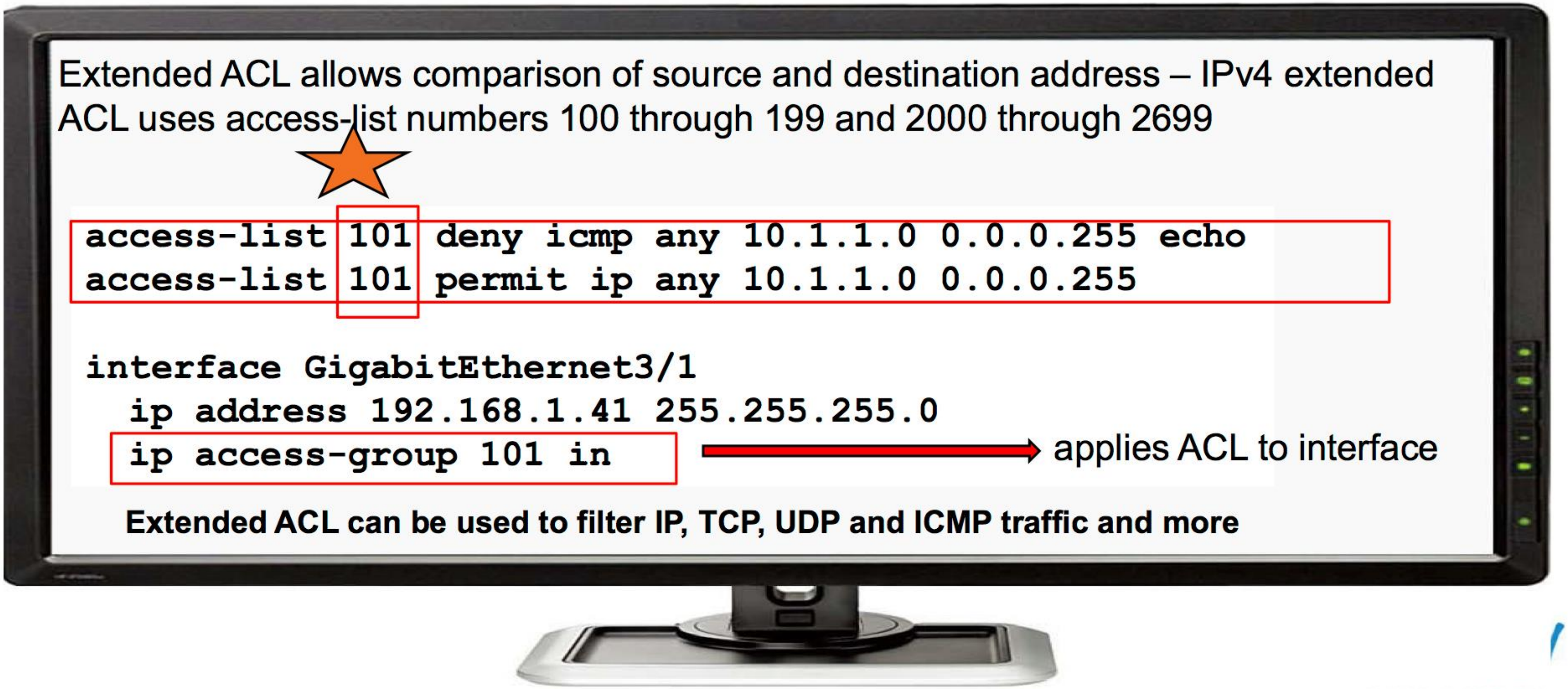
Standard ACL is the oldest type of ACL – Allows comparison of source address only - Uses access-list numbers 1 through 99

```
access-list 1 permit 10.1.1.0 0.0.0.255

interface GigabitEthernet3/1
  ip address 10.1.1.5 255.255.255.0
  ip access-group 1 in
```

Indicates this ACL as a standard v4 ACL

applies ACL to interface

Extended IPv4 ACL



Extended ACL allows comparison of source and destination address – IPv4 extended ACL uses access-list numbers 100 through 199 and 2000 through 2699

```
access-list 101 deny icmp any 10.1.1.0 0.0.0.255 echo
access-list 101 permit ip any 10.1.1.0 0.0.0.255

interface GigabitEthernet3/1
  ip address 192.168.1.41 255.255.255.0
  ip access-group 101 in
```

applies ACL to interface

Extended ACL can be used to filter IP, TCP, UDP and ICMP traffic and more

Router ACL

ACL that is applied to an interface that has a Layer 3 address assigned to it

RACL Example

```
ip access-list extended apply_racl
  permit ip host 10.1.1.2 host 192.168.1.14

interface GigabitEthernet3/1
  ip address 192.168.1.1 255.255.255.0
  ip access-group apply_racl in
```

Security Boundary

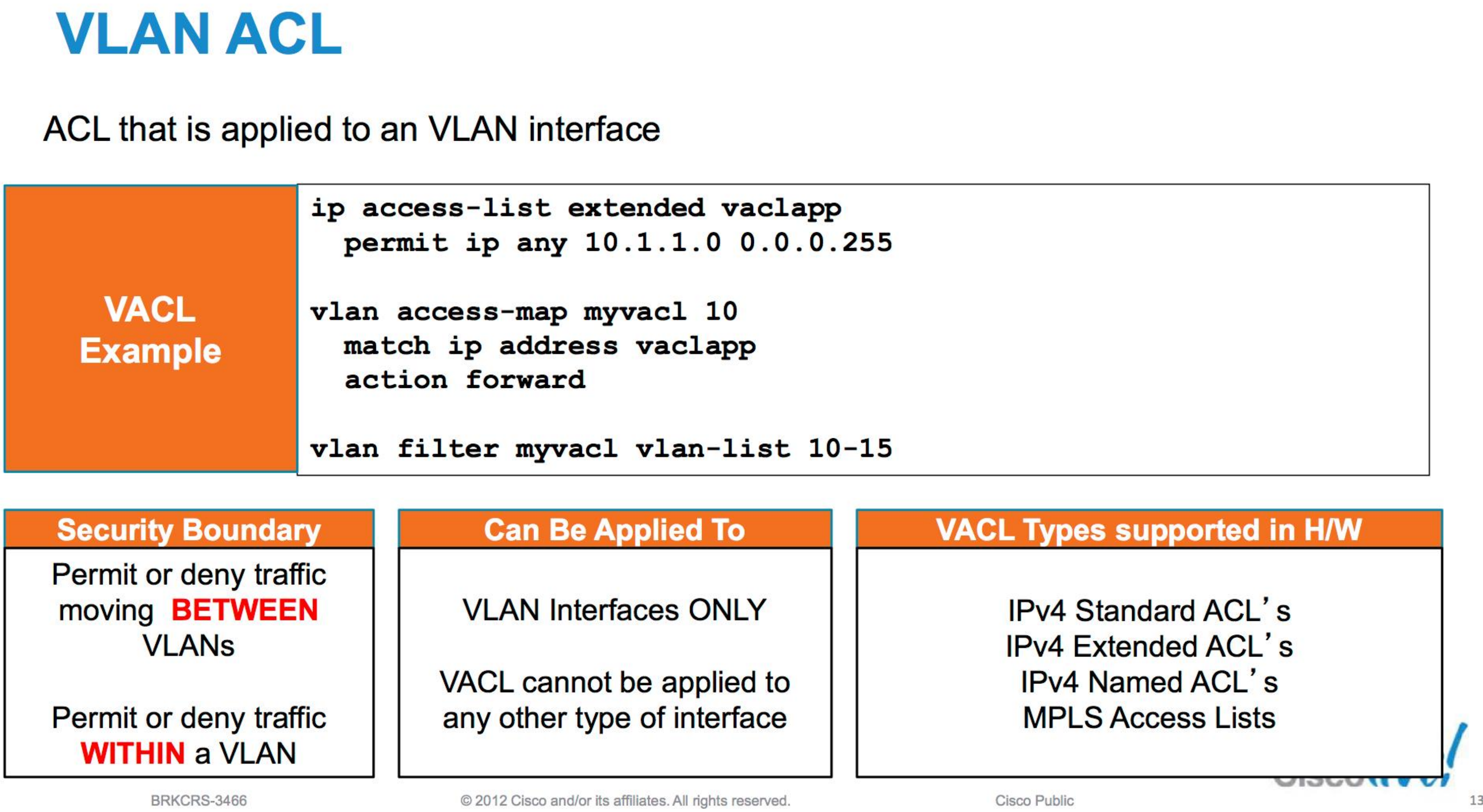
Permit or deny traffic moving **BETWEEN** subnets or networks

Can Be Applied To

ANY PORT WITH AN IP ADDRESS
Routed Interfaces
Tunnel Interfaces
Loopback Interfaces
WAN Interfaces
VLAN Interfaces, etc

RACL Types supported in H/W

IPv4 Standard and Extended ACL’s
IPv4 Named ACL’s
IPv6 Access Lists
MPLS Access Lists



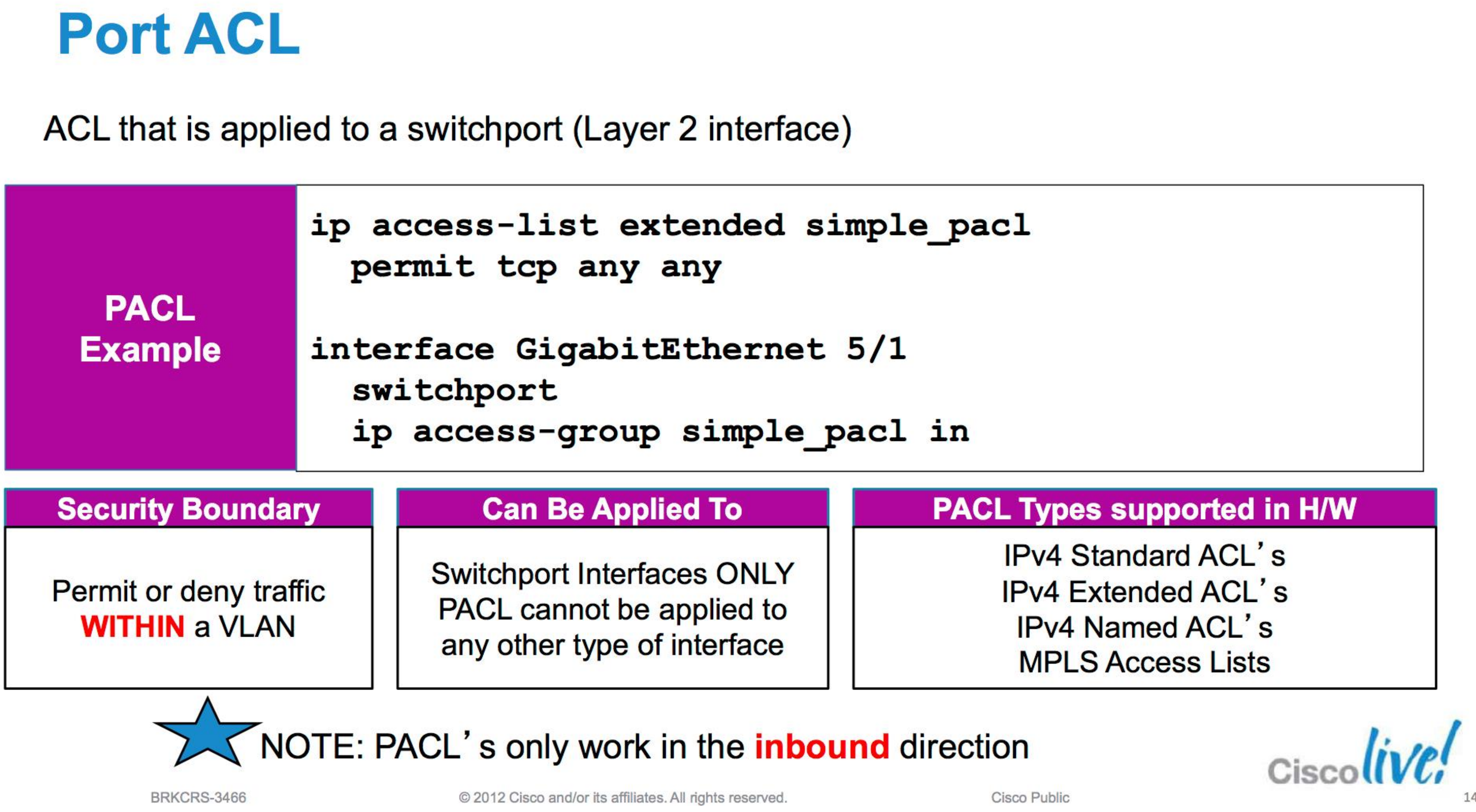
VLAN ACL

ACL that is applied to an VLAN interface

VACL Example

```
ip access-list extended vaclapp
  permit ip any 10.1.1.0 0.0.0.255

vlan access-map myvacl 10
  match ip address vaclapp
  action forward

vlan filter myvacl vlan-list 10-15
```

Security Boundary	Can Be Applied To	VACL Types supported in H/W
Permit or deny traffic moving **BETWEEN** VLANs Permit or deny traffic **WITHIN** a VLAN	VLAN Interfaces ONLY VACL cannot be applied to any other type of interface	IPv4 Standard ACL's IPv4 Extended ACL's IPv4 Named ACL's MPLS Access Lists



Port ACL

ACL that is applied to a switchport (Layer 2 interface)

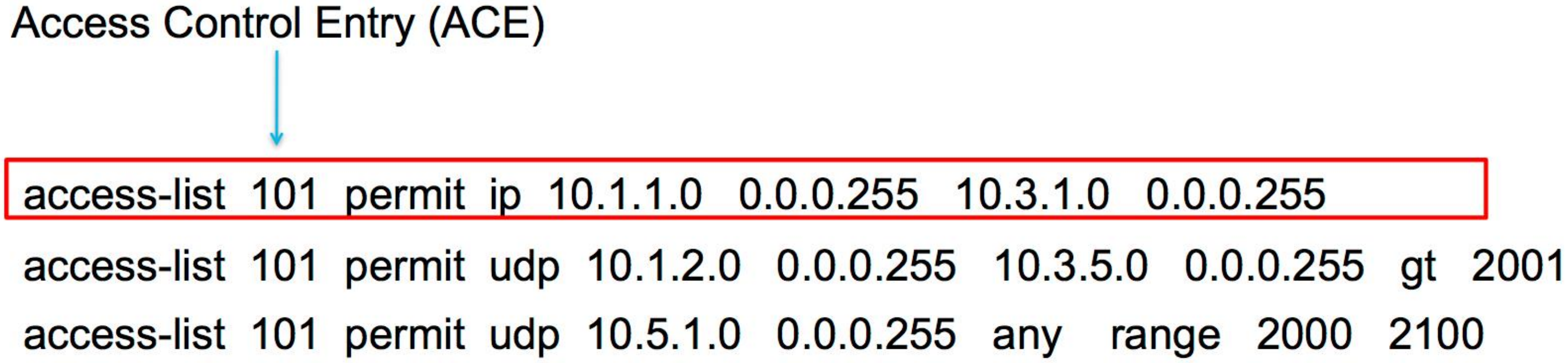
PACL Example

```
ip access-list extended simple_pacl
  permit tcp any any

interface GigabitEthernet 5/1
  switchport
  ip access-group simple_pacl in
```

Security Boundary	Can Be Applied To	PACL Types supported in H/W
Permit or deny traffic **WITHIN** a VLAN	Switchport Interfaces ONLY PACL cannot be applied to any other type of interface	IPv4 Standard ACL's IPv4 Extended ACL's IPv4 Named ACL's MPLS Access Lists

★ NOTE: PACL's only work in the **inbound** direction

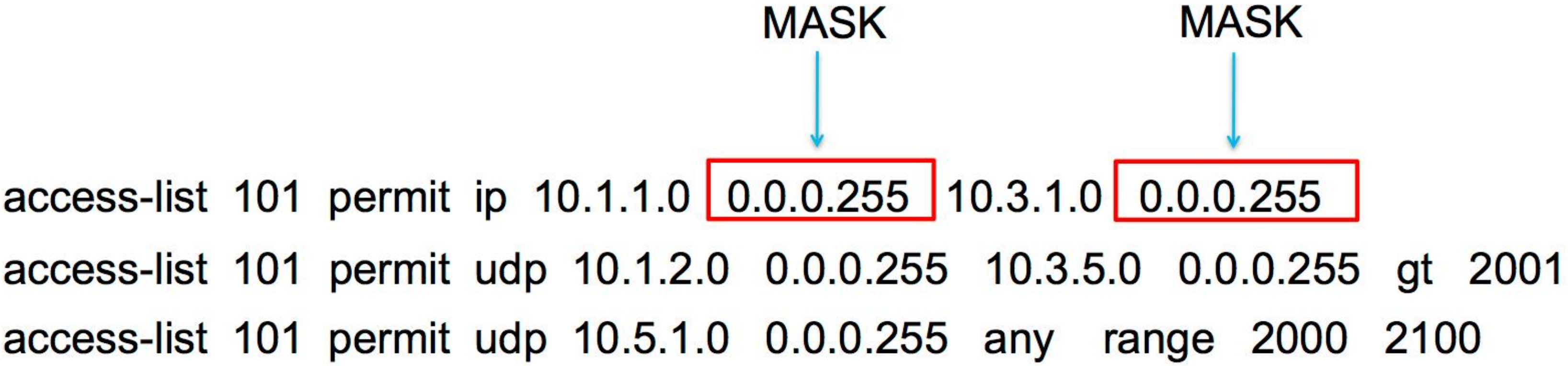
Security Access Control Entries (ACE)



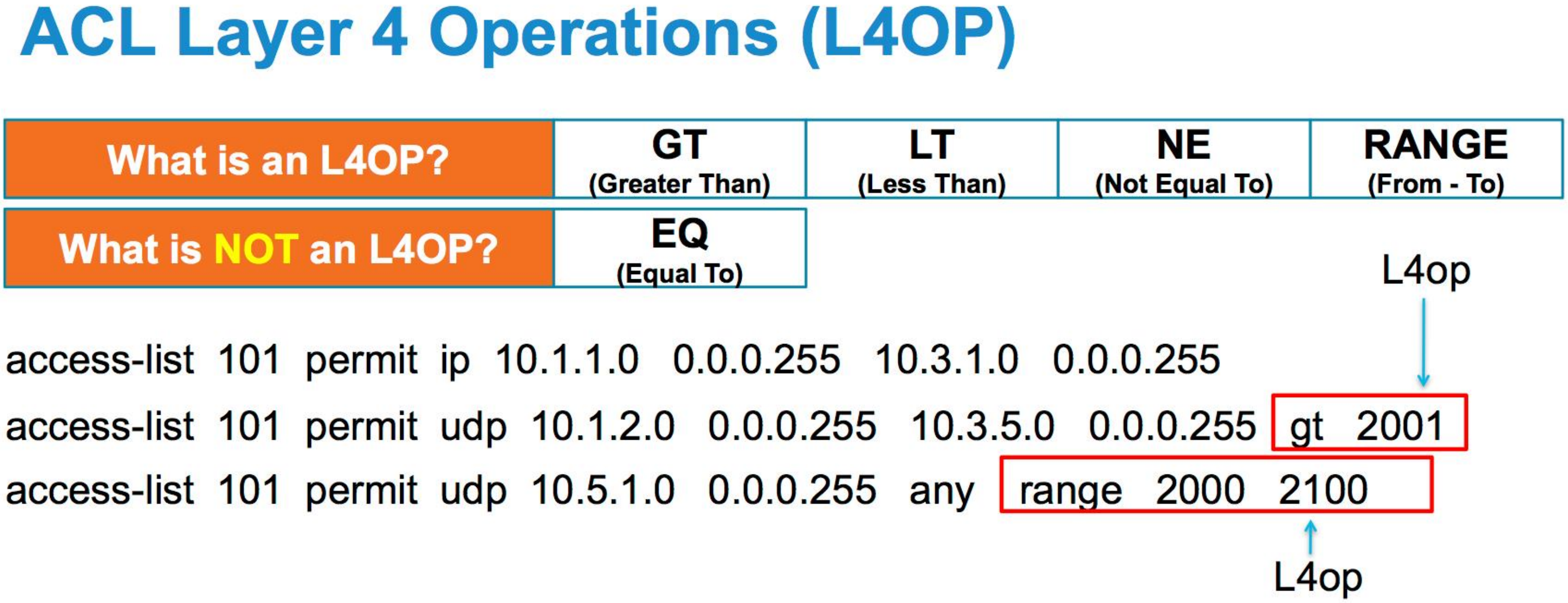
Access Control Entry (ACE)

```
access-list  101  permit  ip  10.1.1.0   0.0.0.255   10.3.1.0   0.0.0.255
access-list  101  permit  udp  10.1.2.0   0.0.0.255   10.3.5.0   0.0.0.255   gt   2001
access-list  101  permit  udp  10.5.1.0   0.0.0.255   any   range   2000   2100
```

ACL Masks



```
access-list 101 permit ip 10.1.1.0 0.0.0.255 10.3.1.0 0.0.0.255
access-list 101 permit udp 10.1.2.0 0.0.0.255 10.3.5.0 0.0.0.255 gt 2001
access-list 101 permit udp 10.5.1.0 0.0.0.255 any range 2000 2100
```



ACL Layer 4 Operations (L4OP)

What is an L4OP?	**GT** (Greater Than)	**LT** (Less Than)	**NE** (Not Equal To)	**RANGE** (From - To)
What is NOT an L4OP?	**EQ** (Equal To)			

L4op

```
access-list  101  permit  ip  10.1.1.0   0.0.0.255   10.3.1.0   0.0.0.255
access-list  101  permit  udp  10.1.2.0   0.0.0.255   10.3.5.0   0.0.0.255  gt   2001
access-list  101  permit  udp  10.5.1.0   0.0.0.255   any   range   2000   2100
```

L4op