

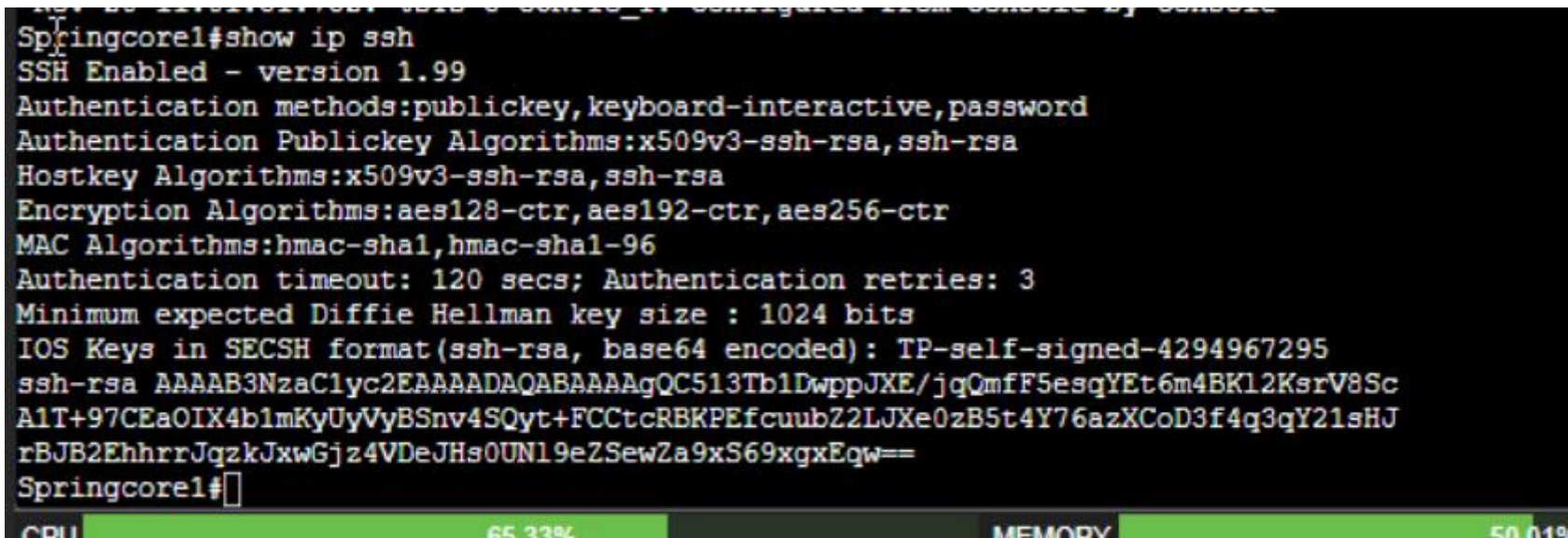
Technical Project

Task 3

Advanced Security and Acl setup

SpringCore1

```
Springcore1#show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha1,hmac-sha1-96
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): TP-self-signed-4294967295
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQC513Tb1DwppJXE/jqQmfF5esqYEt6m4BK12KsrV8Sc
A1T+97CEaOIX4b1mKyUyVyBSnv4SQyt+FCctcRBKPEfcuubZ2LJXe0zB5t4Y76azXCoD3f4q3qY21sHJ
rBJB2EhhrrJqzkJxwGjz4VDeJHs0UN19eZSewZa9xS69xgxEqw==
Springcore1#
```



SpringCore2

```
Springcore2#show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha1,hmac-sha1-96
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): TP-self-signed-4294967295
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDTof6RAKxbbUkD9mTBceQBhLqtq2PBQv5/RgZuwJzJ
1frHjE6uWCld/0UVjcZetl8drtXA8pzkas8+GdnKHrYIxp6eWqBzbs2sezatygt9+DPkf0FuAnezEbP7
12lsv0DlezmxXLh38dFQ5AyxXwdX4aGp6zHlpN8HHwFeu6k6aw==
Springcore2#
```

CPU

49.38%

MEMORY

50

Floor1-Acc1

```
password:
Floor1-Acc1#show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha1,hmac-sha1-96
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): TP-self-signed-4294967295
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCjhGTShU9SnEP7WceWu09QoslV+f6EozW48d5kJwn6
mli5IOb5Q4f7g9uK7ya677Sp7KAs/5+v+7Mpa5ZVCk1S0uUZVBm+DYuwrKMwM4TcVBnSF4JCVOq58sVR
ncU4X4sJYkjTIwNr1N/6vrqX+wVXzs2apqmaGHEBIN+7d0Dx8Q==
Floor1-Acc1#
```

Floor2-Acc1

```
Floor2-Acc1#show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha1,hmac-sha1-96
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): TP-self-signed-4294967295
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQCNRApL5y+vH6BvsvdIRTL7/YSaACAK0spxZiOYVDb1
wc+V7tex9byqBXv0/xyN/Pg651c2NgVkyUbaN5DeCJRRXh/yfqJnZoPQdYorS5oWiQOAG9wnqgjk4Cpm
rTcXEBO2XYRu4BA7wl8Rj7w7alIMcA0Aq8zhqafNqDvIxrLTdQ==
Floor2-Acc1#
```


Floor3-Acc1

```
Floor3-Acc1#show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha1,hmac-sha1-96
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): TP-self-signed-4294967295
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQCmhf6tTwo5/GQVzOmt2PDOC16m2TL6XvyUHfTGpcjG
70/EiI/7HIZ/q2U3/nI8FIVD2Au+pR0Xowuayc7S6laJQPXgchDglq0eRrJkDrrAzT0EdIJRjw37Sc+N
eghUCFQi5ewE+SZtzOGCff0tNklNBguUcYnfE1QhI3IH35N1nQ==
Floor3-Acc1#
```

DataCentre

```
Datacentre#show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha1,hmac-sha1-96
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): TP-self-signed-4294967295
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQC56ev6EAcEKuB2NAexcI+KBhodub6/vwIuPQs9qKef
bGcNRXIXYLxTd9MV1dyu2DBmVUSC69gs66YEV5rJix3iXL6Eawnymk7uYiOQr8W6P7zIr8xDrem8lINl
nv4RrtBhlC8pEM2Vt/JhRW36LREiqv1FIhneXBD3KkK/+UXXAQ==
Datacentre#
```

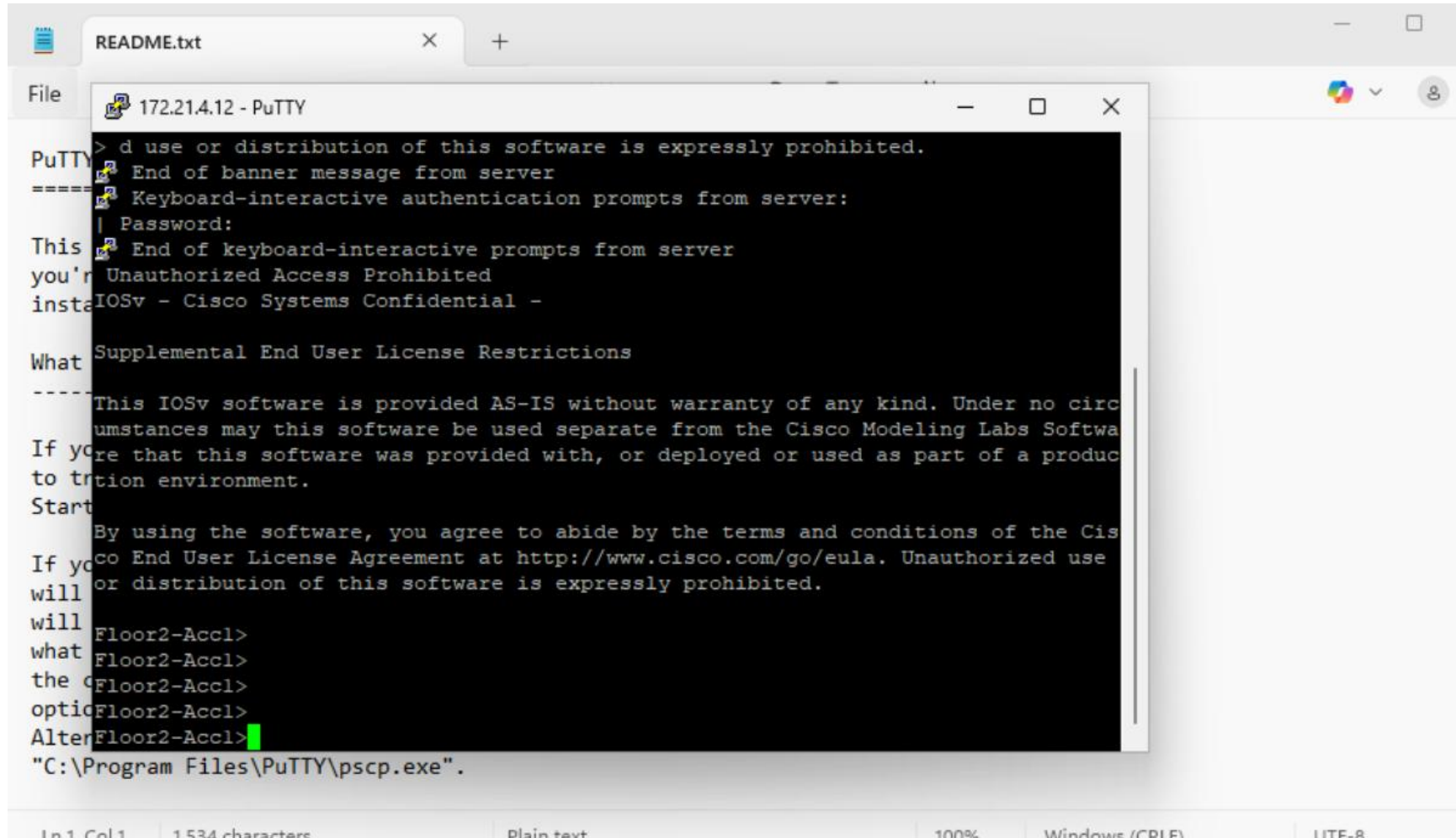
SpringR1

```
SpringR1#show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-96
KEX Algorithms:diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 2048 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): SpringR1.shmc.local
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC7ljpI6Zqg7CJOSz5AY4ZTi5FhJDOmouZeYPALZZPq
ZhAvzM/E3ybQi+f6dJG7RgDsyYZTi0+za/2EWxrU0hMssQozJA8vhj4bnRbVZW0RwVt8mrU+2+Qbvr7r
/R/Z1gyWHQLLXpQRizrIU80eYZqf28PTbpp70HfzsswEQzfbNw==
SpringR1#
```


SpringR2

```
SpringR2#show ip ssh
SSH Enabled - version 1.99
Authentication methods:publickey,keyboard-interactive,password
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Encryption Algorithms:aes128-ctr,aes192-ctr,aes256-ctr
MAC Algorithms:hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-96
KEX Algorithms:diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 2048 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded): SpringR2.shmc.local
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDN/Ow+Tgh45mSefd2Xf8KnjiKgaRLcAlria97mPE81
N/XmGVf56tnBGJuZzCRTqTp32JrRTKdCrAMCLZrl7uhZn0jjhBuMTLBX2rf4qR/CDc7/mXnJX44E3lKA
vRh6bzKNP1O4Ma+SDKtwJRkWshh/qBXxYFRzRaKml+5WlvnNJQ==
SpringR2#
```

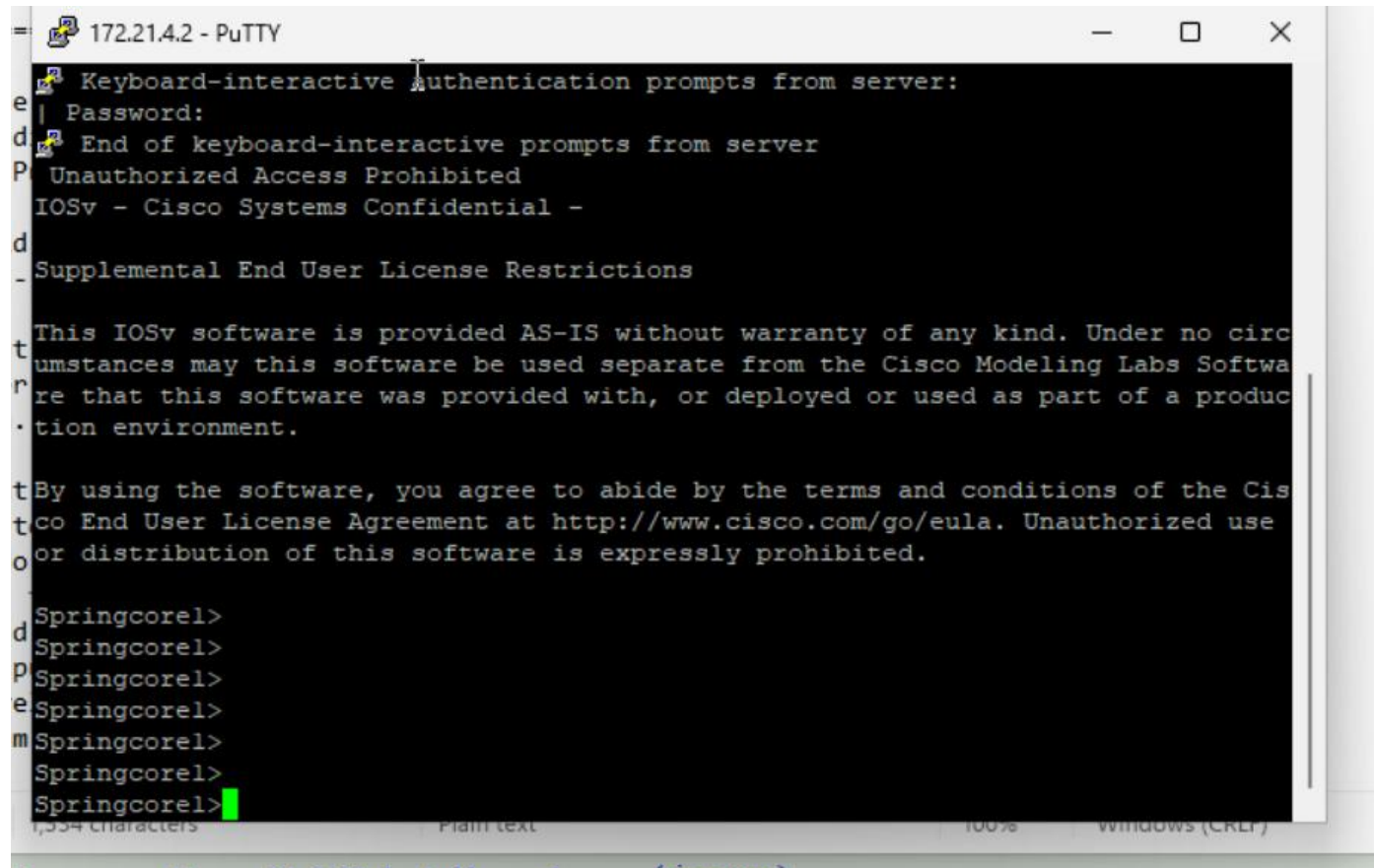
SSH from Client2 > Floor2-Acc1



```
172.21.4.12 - PuTTY
> d use or distribution of this software is expressly prohibited.
PuTTY End of banner message from server
==== Keyboard-interactive authentication prompts from server:
| Password:
This End of keyboard-interactive prompts from server
you'r Unauthorized Access Prohibited
insta IOSv - Cisco Systems Confidential -

What Supplemental End User License Restrictions
-----
This IOSv software is provided AS-IS without warranty of any kind. Under no circ
umstances may this software be used separate from the Cisco Modeling Labs Softwa
If yo re that this software was provided with, or deployed or used as part of a produc
to tr tion environment.
Start
By using the software, you agree to abide by the terms and conditions of the Cis
If yo co End User License Agreement at http://www.cisco.com/go/eula. Unauthorized use
will or distribution of this software is expressly prohibited.
will Floor2-Acc1>
what Floor2-Acc1>
the Floor2-Acc1>
optic Floor2-Acc1>
Alter Floor2-Acc1>
"C:\Program Files\PuTTY\pscp.exe".
```

SSH from Client2 > SpringCore 1



The image shows a PuTTY terminal window titled "172.21.4.2 - PuTTY". The terminal output displays the following sequence of events:

- Keyboard-interactive authentication prompts from server:
- End of keyboard-interactive prompts from server
- Unauthorized Access Prohibited
- IOSv - Cisco Systems Confidential -
- Supplemental End User License Restrictions
- A detailed disclaimer: "This IOSv software is provided AS-IS without warranty of any kind. Under no circumstances may this software be used separate from the Cisco Modeling Labs Software that this software was provided with, or deployed or used as part of a production environment."
- A statement of agreement: "By using the software, you agree to abide by the terms and conditions of the Cisco End User License Agreement at <http://www.cisco.com/go/eula>. Unauthorized use or distribution of this software is expressly prohibited."
- A series of seven "Springcore1>" prompts, with the last one having a green cursor.

The status bar at the bottom indicates "1,554 Characters", "Plain text", "100%", and "Windows (CRLF)".

Allowed Vlan on Trunk Interfaces of Switches

Floor1-ACC1

```
NOV 20 14:27:31.194: %SYS-5-CONFIG_1: Configured from console by console
Floor1-Acc1#show interfaces trunk

Port      Mode      Encapsulation  Status        Native vlan
Gi0/0     on        802.1q         trunking      999
Gi0/1     on        802.1q         trunking      999

Port      Vlans allowed on trunk
Gi0/0     110,120,130,140,150,160,716
Gi0/1     110,120,130,140,150,160,716

Port      Vlans allowed and active in management domain
Gi0/0     110,120,130,140,150,160,716
Gi0/1     110,120,130,140,150,160,716

Port      Vlans in spanning tree forwarding state and not pruned
Gi0/0     110,120,130,140,150,160,716
Gi0/1     110,120,130,140,150,160,716
Floor1-Acc1#
```


Floor2-Acc1

```
Floor2-Acc1#show int trunk
```

| Port | Mode | Encapsulation | Status | Native vlan |
|-------|------|---------------|----------|-------------|
| Gi0/0 | on | 802.1q | trunking | 999 |
| Gi0/1 | on | 802.1q | trunking | 999 |

| Port | Vlans allowed on trunk |
|-------|-------------------------|
| Gi0/0 | 210,220,230,240,250,716 |
| Gi0/1 | 210,220,230,240,250,716 |

| Port | Vlans allowed and active in management domain |
|-------|---|
| Gi0/0 | 210,220,230,240,250,716 |
| Gi0/1 | 210,220,230,240,250,716 |

| Port | Vlans in spanning tree forwarding state and not pruned |
|-------|--|
| Gi0/0 | 210,220,230,240,250,716 |
| Gi0/1 | 210,220,230,240,250,716 |

```
Floor2-Acc1#
```

Floor3-Acc1

```
Floor3-Acc1#show int trunk
```

| Port | Mode | Encapsulation | Status | Native vlan |
|-------|------|---------------|----------|-------------|
| Gi0/0 | on | 802.1q | trunking | 999 |
| Gi0/1 | on | 802.1q | trunking | 999 |

| Port | Vlans allowed on trunk |
|-------|-------------------------|
| Gi0/0 | 310,320,330,340,350,716 |
| Gi0/1 | 310,320,330,340,350,716 |

| Port | Vlans allowed and active in management domain |
|-------|---|
| Gi0/0 | 310,320,330,340,350,716 |
| Gi0/1 | 310,320,330,340,350,716 |

| Port | Vlans in spanning tree forwarding state and not pruned |
|-------|--|
| Gi0/0 | 310,320,330,340,350,716 |
| Gi0/1 | 310,320,330,340,350,716 |

```
Floor3-Acc1#
```

DataCentre

```
Datacentre#show int trunk
```

| Port | Mode | Encapsulation | Status | Native vlan |
|------|------|---------------|----------|-------------|
| Po1 | on | 802.1q | trunking | 999 |
| Po2 | on | 802.1q | trunking | 999 |

```
Port      Vlans allowed on trunk
```

```
Po1      716,916,999
```

```
Po2      716,916,999
```

```
Port      Vlans allowed and active in management domain
```

```
Po1      716,916,999
```

```
Po2      716,916,999
```

```
Port      Vlans in spanning tree forwarding state and not pruned
```

```
Po1      716,916,999
```

```
Po2      716,916,999
```

```
Datacentre#
```

Acl to allow visitors restricting access to sql & tftp servers

Spring Core1

```
Springcore1#show access-list
Standard IP access list SSH_ONLY
 10 permit 172.21.4.0, wildcard bits 0.0.0.255 (2 matches)
 20 deny any
Extended IP access list CISCO-CWA-URL-REDIRECT-ACL
 100 deny udp any any eq domain
 101 deny tcp any any eq domain
 102 deny udp any eq bootps any
 103 deny udp any any eq bootpc
 104 deny udp any eq bootpc any
 105 permit tcp any any eq www
Extended IP access list VISITOR_DC_PROTECT
 10 permit udp 172.21.5.0 0.0.0.255 172.21.0.0 0.0.0.255 eq bootps
 20 permit udp 172.21.6.0 0.0.0.255 172.21.0.0 0.0.0.255 eq bootps (31 matches)
 30 permit udp 172.21.7.0 0.0.0.255 172.21.0.0 0.0.0.255 eq bootps
 40 permit udp 172.21.5.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
 50 permit udp 172.21.6.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain (381 matches)
 60 permit udp 172.21.7.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
 70 permit tcp 172.21.5.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
 80 permit tcp 172.21.6.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
 90 permit tcp 172.21.7.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
100 deny ip 172.21.5.0 0.0.0.255 host 172.21.0.30
110 deny ip 172.21.6.0 0.0.0.255 host 172.21.0.30 (4 matches)
120 deny ip 172.21.7.0 0.0.0.255 host 172.21.0.30
130 deny ip 172.21.5.0 0.0.0.255 host 172.21.0.40
140 deny ip 172.21.6.0 0.0.0.255 host 172.21.0.40 (4 matches)
150 deny ip 172.21.7.0 0.0.0.255 host 172.21.0.40
160 permit ip any any (6779 matches)
```


SpringCore2

```
Springcore2#show access-list
Standard IP access list SSH_ONLY
 10 permit 172.21.4.0, wildcard bits 0.0.0.255
 20 deny any
Extended IP access list CISCO-CWA-URL-REDIRECT-ACL
 100 deny udp any any eq domain
 101 deny tcp any any eq domain
 102 deny udp any eq bootps any
 103 deny udp any any eq bootpc
 104 deny udp any eq bootpc any
 105 permit tcp any any eq www
Extended IP access list VISITOR_DC_PROTECT
 10 permit udp 172.21.5.0 0.0.0.255 172.21.0.0 0.0.0.255 eq bootps
 20 permit udp 172.21.6.0 0.0.0.255 172.21.0.0 0.0.0.255 eq bootps
 30 permit udp 172.21.7.0 0.0.0.255 172.21.0.0 0.0.0.255 eq bootps
 40 permit udp 172.21.5.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
 50 permit udp 172.21.6.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
 60 permit udp 172.21.7.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
 70 permit tcp 172.21.5.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
 80 permit tcp 172.21.6.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
 90 permit tcp 172.21.7.0 0.0.0.255 172.21.0.0 0.0.0.255 eq domain
100 deny ip 172.21.5.0 0.0.0.255 host 172.21.0.30
110 deny ip 172.21.6.0 0.0.0.255 host 172.21.0.30
120 deny ip 172.21.7.0 0.0.0.255 host 172.21.0.30
130 deny ip 172.21.5.0 0.0.0.255 host 172.21.0.40
140 deny ip 172.21.6.0 0.0.0.255 host 172.21.0.40
150 deny ip 172.21.7.0 0.0.0.255 host 172.21.0.40
160 permit ip any any (4412 matches)
```

ACL to only allow HTTP/HTTPS from the MN
visitor network to the ISP public internet

SpringCore1

```
Extended IP access list VISITOR_WEB_ONLY
 10 permit tcp 172.21.5.0 0.0.0.255 any eq www
 20 permit tcp 172.21.5.0 0.0.0.255 any eq 443
 30 permit tcp 172.21.6.0 0.0.0.255 any eq www (217890 matches)
 40 permit tcp 172.21.6.0 0.0.0.255 any eq 443 (76424 matches)
 50 permit tcp 172.21.7.0 0.0.0.255 any eq www
 60 permit tcp 172.21.7.0 0.0.0.255 any eq 443
 70 deny ip 172.21.5.0 0.0.0.255 any (351 matches)
 80 deny ip 172.21.6.0 0.0.0.255 any (77387 matches)
 90 deny ip 172.21.7.0 0.0.0.255 any (349 matches)
100 permit ip any any (553660 matches)
110 permit udp any any eq domain
120 permit tcp any any eq domain
```

SpringCore 2

```
Extended IP access list VISITOR_WEB_ONLY
 10 permit tcp 172.21.5.0 0.0.0.255 any eq www
 20 permit tcp 172.21.5.0 0.0.0.255 any eq 443
 30 permit tcp 172.21.6.0 0.0.0.255 any eq www (1 match)
 40 permit tcp 172.21.6.0 0.0.0.255 any eq 443
 50 permit tcp 172.21.7.0 0.0.0.255 any eq www
 60 permit tcp 172.21.7.0 0.0.0.255 any eq 443
 70 deny ip 172.21.5.0 0.0.0.255 any (337 matches)
 80 deny ip 172.21.6.0 0.0.0.255 any (3180 matches)
 90 deny ip 172.21.7.0 0.0.0.255 any (339 matches)
100 permit ip any any (61254 matches)
110 permit udp any any eq domain
120 permit tcp any any eq domain
```