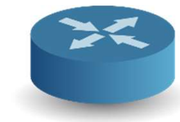


Doruk Arisoy

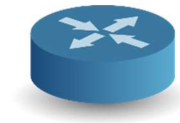
Computer Networking Portfolio

CISCO CERTIFIED
CCNP
ROUTING & SWITCHING

CISCO CERTIFIED
CCNA
SECURITY

CISCO CERTIFIED
CCNA
ROUTING & SWITCHING

Contents



CCNP

Routing & Switching

CISCO CERTIFIED
CCNP
ROUTING & SWITCHING

Multi-Area OSPF

Purpose

The purpose of the lab was to create a topology that includes 6 routers and 2 PCs using multi-area OSPF with 3 areas and establish end-to-end connectivity in both IPv4 and IPv6.

Background Information

Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS).

The OSPF link state routing protocol uses the concept of Areas, which are sub-domains within the OSPF domain. A router within an Area maintains the complete topology information of that Area. By default, an interface can only belong to one OSPF Area. This can not only cause sub-optimal routing in the network, but it can also lead to other issues if the network is not designed correctly.

When Multi-Area Adjacency is configured on an interface, the OSPF speakers form more than one Adjacency (ADJ) over that link. The Multi-Area interface is a logical, point-to-point interface over which the ADJ is formed. This document describes a scenario where Multi-Area OSPF ADJ can be used in order to work around a problem and meet the network requirements.

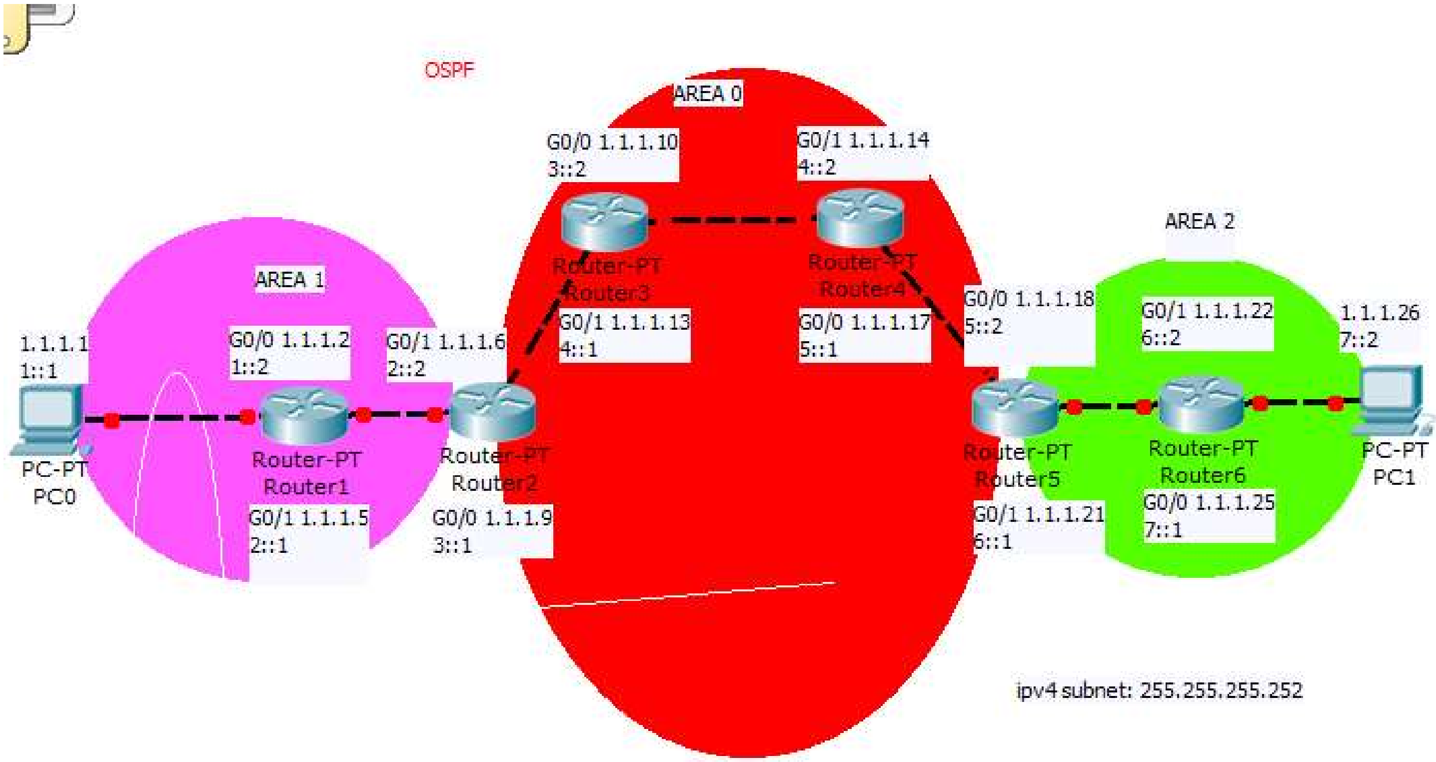
Lab Summary

I first created a topology that has 6 routers and 2 PCs. Then I cabled the topology and configured IPv4 and IPv6 addresses on the PCs and the interfaces on the routers. Once I established connectivity between directly connected routers, I set up OSPFv2 on all of the routers and established IPv4 connectivity between 2 PCs. Then I did the same thing for OSPFv3 and established connectivity in IPv6. The set up the OSPF so that there were 3 areas.

Lab Commands

`router ospf` *`process-id`*	This is used to configure an OSPF routing process, use the router ospf command in global configuration mode.
`network` *`network-address wildcard-mask`* **`area`** *`area-id`*	Network command is used under the router ospf. You enter the network address of the directly connected hop with its wildcard mask and you also enter what area that hop is in. This is only done for IPv4 OSPF routes.
`ipv6 ospf` *`process-id`* `area` *`area-id`*	This is used for IPv6 OSPF routes, to use this command you first have to create router ospf 1 and enter this command under the interface. While entering you have to enter process id of the OSPF group and the area that the port is in.

Network Diagram



Configuration

Router 1
Show run

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
boot-start-marker
boot-end-marker
logging message-counter syslog
no aaa new-model
memory-size iomem 10
no network-clock-participate slot 1
dot11 syslog
ip source-route
ip cef
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
voice-card 0
 no dspfarm
voice-card 1
 no dspfarm
```

```
vtp domain cisco
vtp mode transparent
archive
 log config
  hidekeys
interface FastEthernet0/0
 ip address 1.1.1.2 255.255.255.252
 duplex auto
 speed auto
 ipv6 address 1::2/64
 ipv6 ospf 1 area 1
interface FastEthernet0/1
 ip address 1.1.1.5 255.255.255.252
 duplex auto
 speed auto
 ipv6 address 2::1/64
 ipv6 ospf 1 area 1
interface FastEthernet0/0/0
interface FastEthernet0/0/1
interface FastEthernet0/0/2
interface FastEthernet0/0/3
interface Serial0/1/0
 no ip address
 shutdown
 no fair-queue
interface Serial0/2/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/2/1
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/3/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/3/1
 no ip address
 shutdown
 clock rate 2000000
interface Vlan1
 no ip address
router ospf 1
 log-adjacency-changes
 network 1.1.1.0 0.0.0.3 area 1
 network 1.1.1.4 0.0.0.3 area 1
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
 log-adjacency-changes
```

```
control-plane
voice-port 1/0/0
voice-port 1/0/1
voice-port 1/0/2
voice-port 1/0/3
voice-port 1/1/0
voice-port 1/1/1
line con 0
line aux 0
line vty 0 4
 login
scheduler allocate 20000 1000
end
```

Show IP route

```
     1.0.0.0/30 is subnetted, 7 subnets
C       1.1.1.0 is directly connected, FastEthernet0/0
C       1.1.1.4 is directly connected, FastEthernet0/1
O IA    1.1.1.8 [110/2] via 1.1.1.6, 00:34:50, FastEthernet0/1
O IA    1.1.1.12 [110/3] via 1.1.1.6, 00:29:20, FastEthernet0/1
O IA    1.1.1.16 [110/4] via 1.1.1.6, 00:25:37, FastEthernet0/1
O IA    1.1.1.20 [110/5] via 1.1.1.6, 00:22:32, FastEthernet0/1
O IA    1.1.1.24 [110/6] via 1.1.1.6, 00:22:32, FastEthernet0/1
```

Show ipv6 route

```
C   1::/64 [0/0]
     via FastEthernet0/0, directly connected
L   1::2/128 [0/0]
     via FastEthernet0/0, receive
C   2::/64 [0/0]
     via FastEthernet0/1, directly connected
L   2::1/128 [0/0]
     via FastEthernet0/1, receive
OI  3::/64 [110/2]
     via FE80::21E:F7FF:FE5E:F129, FastEthernet0/1
OI  4::/64 [110/3]
     via FE80::21E:F7FF:FE5E:F129, FastEthernet0/1
OI  5::/64 [110/4]
     via FE80::21E:F7FF:FE5E:F129, FastEthernet0/1
OI  6::/64 [110/5]
     via FE80::21E:F7FF:FE5E:F129, FastEthernet0/1
L   FF00::/8 [0/0]
     via Null0, receive
```

Router 2
Show run

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R2
```

```
boot-start-marker
boot-end-marker
logging message-counter syslog
no aaa new-model
memory-size iomem 10
dot11 syslog
ip source-route
ip cef
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
voice-card 0
 no dspfarm
archive
 log config
  hidekeys
interface FastEthernet0/0
 ip address 1.1.1.9 255.255.255.252
 duplex auto
 speed auto
 ipv6 address 3::1/64
 ipv6 ospf 1 area 0
interface FastEthernet0/1
 ip address 1.1.1.6 255.255.255.252
 duplex auto
 speed auto
 ipv6 address 2::2/64
 ipv6 ospf 1 area 1
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router ospf 1
 log-adjacency-changes
 network 1.1.1.4 0.0.0.3 area 1
 network 1.1.1.8 0.0.0.3 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
control-plane
line con 0
line aux 0
line vty 0 4
 login
```

```
scheduler allocate 20000 1000
end
```

Show ip route

```
     1.0.0.0/30 is subnetted, 7 subnets
O       1.1.1.0 [110/2] via 1.1.1.5, 00:37:35, FastEthernet0/1
C       1.1.1.4 is directly connected, FastEthernet0/1
C       1.1.1.8 is directly connected, FastEthernet0/0
O       1.1.1.12 [110/2] via 1.1.1.10, 00:32:15, FastEthernet0/0
O       1.1.1.16 [110/3] via 1.1.1.10, 00:28:33, FastEthernet0/0
O IA    1.1.1.20 [110/4] via 1.1.1.10, 00:25:27, FastEthernet0/0
O IA    1.1.1.24 [110/5] via 1.1.1.10, 00:25:27, FastEthernet0/0
```

Show ipv6 route

```
O   1::/64 [110/2]
     via FE80::218:19FF:FE69:A2E1, FastEthernet0/1
C   2::/64 [0/0]
     via FastEthernet0/1, directly connected
L   2::2/128 [0/0]
     via FastEthernet0/1, receive
C   3::/64 [0/0]
     via FastEthernet0/0, directly connected
L   3::1/128 [0/0]
     via FastEthernet0/0, receive
O   4::/64 [110/2]
     via FE80::7ADA:6EFF:FE99:AA00, FastEthernet0/0
O   5::/64 [110/3]
     via FE80::7ADA:6EFF:FE99:AA00, FastEthernet0/0
OI  6::/64 [110/4]
     via FE80::7ADA:6EFF:FE99:AA00, FastEthernet0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

Router 3
Show run

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R3
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180M8
license accept end user agreement
```

```
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 1.1.1.10 255.255.255.252
 duplex auto
 speed auto
 ipv6 address 3::2/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/1
 ip address 1.1.1.13 255.255.255.252
 duplex auto
 speed auto
 ipv6 address 4::1/64
 ipv6 ospf 1 area 0
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router ospf 1
 network 1.1.1.8 0.0.0.3 area 0
 network 1.1.1.12 0.0.0.3 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route:

```
     1.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O IA    1.1.1.0/30 [110/3] via 1.1.1.9, 00:40:05, GigabitEthernet0/0
O IA    1.1.1.4/30 [110/2] via 1.1.1.9, 00:40:56, GigabitEthernet0/0
C       1.1.1.8/30 is directly connected, GigabitEthernet0/0
L       1.1.1.10/32 is directly connected, GigabitEthernet0/0
C       1.1.1.12/30 is directly connected, GigabitEthernet0/1
L       1.1.1.13/32 is directly connected, GigabitEthernet0/1
O       1.1.1.16/30 [110/2] via 1.1.1.14, 00:31:03, GigabitEthernet0/1
O IA    1.1.1.20/30 [110/3] via 1.1.1.14, 00:27:57, GigabitEthernet0/1
O IA    1.1.1.24/30 [110/4] via 1.1.1.14, 00:27:57, GigabitEthernet0/1
```

Show ipv6 route:

```
OI  1::/64 [110/3]
     via FE80::21E:F7FF:FE5E:F128, GigabitEthernet0/0
OI  2::/64 [110/2]
     via FE80::21E:F7FF:FE5E:F128, GigabitEthernet0/0
C   3::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   3::2/128 [0/0]
     via GigabitEthernet0/0, receive
C   4::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   4::1/128 [0/0]
     via GigabitEthernet0/1, receive
O   5::/64 [110/2]
     via FE80::26E9:B3FF:FE3C:1949, GigabitEthernet0/1
OI  6::/64 [110/3]
     via FE80::26E9:B3FF:FE3C:1949, GigabitEthernet0/1
L   FF00::/8 [0/0]
     via Null0, receive
```

Router 4
Show run:

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R4
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180M5
license accept end user agreement
```

```
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 1.1.1.17 255.255.255.252
 duplex auto
 speed auto
 ipv6 address 5::1/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/1
 ip address 1.1.1.14 255.255.255.252
 duplex auto
 speed auto
 ipv6 address 4::2/64
 ipv6 ospf 1 area 0
interface Serial0/0/0
 no ip address
 shutdown
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router ospf 1
 network 1.1.1.12 0.0.0.3 area 0
 network 1.1.1.16 0.0.0.3 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
 router-id 4.4.4.4
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
 login
 transport input all
scheduler allocate 20000 1000
```

```
End
```

Show ip route

```
      1.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O IA     1.1.1.0/30 [110/4] via 1.1.1.13, 00:35:09, GigabitEthernet0/1
O IA     1.1.1.4/30 [110/3] via 1.1.1.13, 00:35:09, GigabitEthernet0/1
O        1.1.1.8/30 [110/2] via 1.1.1.13, 00:35:09, GigabitEthernet0/1
C        1.1.1.12/30 is directly connected, GigabitEthernet0/1
L        1.1.1.14/32 is directly connected, GigabitEthernet0/1
C        1.1.1.16/30 is directly connected, GigabitEthernet0/0
L        1.1.1.17/32 is directly connected, GigabitEthernet0/0
O IA     1.1.1.20/30 [110/2] via 1.1.1.18, 00:29:45,
GigabitEthernet0/0
O IA     1.1.1.24/30 [110/3] via 1.1.1.18, 00:29:46,
GigabitEthernet0/0
```

Show ipv6 route

```
OI  1::/64 [110/4]
     via FE80::7ADA:6EFF:FE99:AA01, GigabitEthernet0/1
OI  2::/64 [110/3]
     via FE80::7ADA:6EFF:FE99:AA01, GigabitEthernet0/1
O   3::/64 [110/2]
     via FE80::7ADA:6EFF:FE99:AA01, GigabitEthernet0/1
C   4::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   4::2/128 [0/0]
     via GigabitEthernet0/1, receive
C   5::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   5::1/128 [0/0]
     via GigabitEthernet0/0, receive
OI  6::/64 [110/2]
     via FE80::EAB7:48FF:FE6E:88, GigabitEthernet0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

Router 5
Show run

```
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R5
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ipv6 unicast-routing
ipv6 cef
ip source-route
ip cef
```

```
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX15208074
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
redundancy
interface GigabitEthernet0/0
 ip address 1.1.1.18 255.255.255.252
 duplex auto
 speed auto
 ipv6 address 5::2/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/1
 ip address 1.1.1.21 255.255.255.252
 duplex auto
 speed auto
 ipv6 address 6::1/64
 ipv6 ospf 1 area 2
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
router ospf 1
 log-adjacency-changes
 network 1.1.1.16 0.0.0.3 area 0
 network 1.1.1.20 0.0.0.3 area 2
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
 log-adjacency-changes
control-plane
gatekeeper
 shutdown
line con 0
line aux 0
line vty 0 4
 login
scheduler allocate 20000 1000
end
```

Show ip route

```
      1.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O IA     1.1.1.0/30 [110/5] via 1.1.1.17, 00:31:27, GigabitEthernet0/0
O IA     1.1.1.4/30 [110/4] via 1.1.1.17, 00:31:27, GigabitEthernet0/0
O        1.1.1.8/30 [110/3] via 1.1.1.17, 00:31:27, GigabitEthernet0/0
```

```
O        1.1.1.12/30 [110/2] via 1.1.1.17, 00:31:27,
GigabitEthernet0/0
C        1.1.1.16/30 is directly connected, GigabitEthernet0/0
L        1.1.1.18/32 is directly connected, GigabitEthernet0/0
C        1.1.1.20/30 is directly connected, GigabitEthernet0/1
L        1.1.1.21/32 is directly connected, GigabitEthernet0/1
O        1.1.1.24/30 [110/2] via 1.1.1.22, 00:31:17,
GigabitEthernet0/1
```

Show ipv6 route:

```
OI  1::/64 [110/5]
     via FE80::26E9:B3FF:FE3C:1948, GigabitEthernet0/0
OI  2::/64 [110/4]
     via FE80::26E9:B3FF:FE3C:1948, GigabitEthernet0/0
O   3::/64 [110/3]
     via FE80::26E9:B3FF:FE3C:1948, GigabitEthernet0/0
O   4::/64 [110/2]
     via FE80::26E9:B3FF:FE3C:1948, GigabitEthernet0/0
C   5::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   5::2/128 [0/0]
     via GigabitEthernet0/0, receive
C   6::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   6::1/128 [0/0]
     via GigabitEthernet0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

Router 6

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R6
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX1520806E
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
vtp mode transparent
redundancy
```

```
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 1.1.1.25 255.255.255.252
 duplex auto
 speed auto
 ipv6 address 7::1/64
 ipv6 ospf 1 area 2
interface GigabitEthernet0/1
 ip address 1.1.1.22 255.255.255.252
 duplex auto
 speed auto
 ipv6 address 6::2/64
 ipv6 ospf 1 area 2
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 duplex auto
 speed auto
router ospf 1
 network 1.1.1.20 0.0.0.3 area 2
 network 1.1.1.24 0.0.0.3 area 2
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
 router-id 6.6.6.6
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
```

```
end
```

Show ip route

```
      1.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O IA     1.1.1.0/30 [110/6] via 1.1.1.21, 00:33:36, GigabitEthernet0/1
O IA     1.1.1.4/30 [110/5] via 1.1.1.21, 00:33:36, GigabitEthernet0/1
O IA     1.1.1.8/30 [110/4] via 1.1.1.21, 00:33:36, GigabitEthernet0/1
O IA     1.1.1.12/30 [110/3] via 1.1.1.21, 00:33:36,
GigabitEthernet0/1
O IA     1.1.1.16/30 [110/2] via 1.1.1.21, 00:33:36,
GigabitEthernet0/1
C        1.1.1.20/30 is directly connected, GigabitEthernet0/1
L        1.1.1.22/32 is directly connected, GigabitEthernet0/1
C        1.1.1.24/30 is directly connected, GigabitEthernet0/0
L        1.1.1.25/32 is directly connected, GigabitEthernet0/0
```

Show ipv6 route:

```
OI  1::/64 [110/6]
     via FE80::EAB7:48FF:FE6E:89, GigabitEthernet0/1
OI  2::/64 [110/5]
     via FE80::EAB7:48FF:FE6E:89, GigabitEthernet0/1
OI  3::/64 [110/4]
     via FE80::EAB7:48FF:FE6E:89, GigabitEthernet0/1
OI  4::/64 [110/3]
     via FE80::EAB7:48FF:FE6E:89, GigabitEthernet0/1
OI  5::/64 [110/2]
     via FE80::EAB7:48FF:FE6E:89, GigabitEthernet0/1
C   6::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   6::2/128 [0/0]
     via GigabitEthernet0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

Problems

In our topology, PC0 is connected to Router1 and PC1 is connected to Router6. We configured the routers like that too. However while cabling, we connect PC0 to Router6 and PC1 to Router1. To solve the problem, we only had to switch the cables that were going to PC1 and PC0 from Router1 and Router6. That was the only problem we had.

Conclusion

This was a pretty straight up lab, reviewing the skills I learned from the CCNA Routing and Switching course. Beside the simple cabling error we did not have any other problems. The lab was easy to set up and configure. At the end we were able to establish connectivity between all the different areas of ospf and devices.

End-to-End Pings from PCs

```
Pinging 7::2 with 32 bytes of data:
Reply from 7::2: time=6ms
Reply from 7::2: time=1ms
Reply from 7::2: time=1ms
Reply from 7::2: time=1ms

Ping statistics for 7::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 6ms, Average = 2ms
```

```
Pinging 1.1.1.1 with 32 bytes of data:
Reply from 1.1.1.1: bytes=32 time=3ms TTL=122
Reply from 1.1.1.1: bytes=32 time=1ms TTL=122
Reply from 1.1.1.1: bytes=32 time=1ms TTL=122
Reply from 1.1.1.1: bytes=32 time=1ms TTL=122

Ping statistics for 1.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

```
Pinging 1::1 with 32 bytes of data:
Reply from 1::1: time=3ms
Reply from 1::1: time=1ms
Reply from 1::1: time=1ms
Reply from 1::1: time=1ms

Ping statistics for 1::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

```
Pinging 1.1.1.26 with 32 bytes of data:
Reply from 1.1.1.26: bytes=32 time=3ms TTL=122
Reply from 1.1.1.26: bytes=32 time=1ms TTL=122
Reply from 1.1.1.26: bytes=32 time=1ms TTL=122
Reply from 1.1.1.26: bytes=32 time=1ms TTL=122

Ping statistics for 1.1.1.26:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

Identifying OSPF

Purpose

The purpose of this lab is to understand link state messages that OSPF implemented routers send and the different type of areas in an OSPF implemented network.

Background

Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS).

Routers connect networks using OSPF. Routers that are using OSPF talk and share information between them. So when a router gets a packet it knows which path to send it from.
An OSPF network is divided into areas that are logical groupings of hosts and networks. An area includes its router having interfaces connected to the network. Each area maintains a separate link state database whose information may be summarized towards the rest of the network by the connecting router. Thus, the topology of an area is unknown outside of the area. This reduces the routing traffic between parts of an autonomous system.
Types of Routers in OSPF:

- Internal Router (IR): all interfaces in single area
- Backbone Router (BR): at least 1 interface in area 0 (backbone area)
- Area Border Router (ABR): has interfaces in multiple areas
- Autonomous System Border Router (ASBR): act as gateways between OSPF and other routing protocols

The OSPF protocol is a link-state routing protocol, which means that the routers exchange topology information with their nearest neighbors. The OSPF link state routing protocol uses the concept of Areas, which are sub-domains within the OSPF domain. A router within an Area maintains the complete topology information of that Area. By default, an interface can only belong to one OSPF Area. This can not only cause sub-optimal routing in the network, but it can also lead to other issues if the network is not designed correctly.

The main advantage of a link state routing protocol like OSPF is that the complete knowledge of topology allows routers to calculate routes that satisfy particular criteria. This can be useful for traffic engineering purposes, where routes can be constrained to meet particular quality of service requirements. The main disadvantage of a link state routing protocol is that it does not scale well as more routers are added to the routing domain. Increasing the number of routers increases the size and frequency of the topology updates, and also the length of time it takes to calculate end-to-end routes.

Link State Advertisement (LSA) is a basic communication means of the OSPF routing protocol and is used advertise information about to network.

There are 7 types of LSAs:

- Type 1 – Router LSA: Router LSAs are sent from a router to other routers in the same area. It contains information regarding the routers interfaces in the same area, relevant interfaces IPs, its adjacent routers on those interfaces and sub networks. The router announces its presence and lists the links to other routers or networks in the same area, together with the metrics to them. Type 1 LSAs are flooded across their own area only. The link-state ID of the type 1 LSA is the originating router ID.

- Type 2 – Network LSA: Network LSAs are generated by the DR (Designated Router), which lists which routers are joined together by the segment and looks after all the initial contact and other routing administration, on a multi access segment, and provides similar information to an LSA type 1 for the multi access segment and subnet which it belongs. Type 2 LSAs are flooded across their own area only. The link-state ID of the type 2 LSA is the IP interface address of the DR.

- Type 3 – Summary LSA: An Area Border Router (ABR) takes information it has learned on one of its attached areas and summarizes it before sending it out on other areas it is connected to. This summarization helps provide scalability by removing detailed topology information for other areas, because their routing information is summarized into just an address prefix and metric. The summarization process can also be configured to remove a lot of detailed address prefixes and replace them with a single summary prefix, helping scalability. The link-state ID is the destination network number for type 3 LSAs.

- Type 4 – Summary ASBR LSA: Other routers need to know where to find the ASBR. This is why the ABR will generate a summary ASBR LSA which will include the router ID of the ASBR in the link-state ID field and sent when crossing an AS (Autonomous System) boundary. This is needed because Type 5 External LSAs are flooded to all areas and the detailed next-hop information may not be available in those other areas because it may be using a different routing protocol. This is solved by an Area Border Router flooding the information for the router (i.e. the Autonomous System Boundary Router) where the type 5 originated. The link-state ID is the router ID of the described ASBR for type 4 LSAs.

- Type 5 – External LSA: They are AS external LSAs which are originated by ASBRs and describe external networks. These LSAs contain information imported into OSPF from other routing processes. They are flooded to all areas unchanged (except stub and NSSA areas). For "External Metric Type 1" LSAs routing decisions are made using the Type 1 metric cost sent, as the total cost to get to the external destination and includes the cost to the ASBR; while for "External Type 2" LSAs the metric sent is the cost from the ASBR to the External destination network and must be added to the OSPF cost to the ASBR advertising the Type 5. The link-state ID of the type 5 LSA is the external network number.

- Type 6 – Multicast LSA: Is defined as a Group Membership LSA but not used in Cisco devices. This was defined for Multicast extensions to OSPF (MOSPF), a multicast OSPF routing protocol which was not in general use. MOSPF has been deprecated since OSPFv3 and is not currently used. It may be reassigned in the future.

- Type 7 – External LSA: NSSA (not-so-stubby-area) External LSAs are generated by the ASBR in an NSSA area and do not receive external LSAs from Area Border Routers, but are allowed to send external routing information for redistribution. They use type 7 LSAs to tell the ABRs about these external routes, which the Area Border Router then translates to type 5 external LSAs and floods as normal to the rest of the OSPF network.

4 types of areas of OSPF link state:

Standard Area:

Standard area ensures optimal routing since all routers know about all routes and it is the default area. It permits LSA 1, 2, 3, 4 and 5.

Stub Areas:

A stub area is the most basic form of the “stubbie” area types. It prevents any external route that are coming from outside of the network, from entering into the area’s database. Not only does it block external routes originating in other area’s but also prevents any local redistribution. LSA 4 and 5 are blocked however LSA 1, 2 and 3 are permitted.

Totally Stubby Area:

Totally stub areas not only block any external route (LSA 4 and 5) from entering into the database but they also block any inter-area (LSA 3) routes from entering the area. This reduces the size of the database even further. Local redistribution is not supported.

Not-So-Stubby-Area (NSSA):

Not so stubby areas (NSSA) are very similar to stub areas with 1 major addition. NSSA area’s only block external routes from other area’s from entering into the database (LSA 5). The NSSA areas however do allow for local redistribution using the special NSSA external route type (LSA 7).

Totally-Stubby NSSA:

Totally NSSA areas not only block external routes (LSA 4 and 5) from other areas but also inter-area routes (LSA 3) from other areas. So, it will reduce the size of the database again while still allowing local redistribution using NSSA (LSA 7).

Conclusion

This information will help to define the types of areas in the next lab using Wireshark. We will capture network packets with Wireshark and looking at the LSA types on the packets, we will define the type of area.

OSPF Stubbiness

Purpose

The purpose of this lab was to create multi-area OSPF with 4 areas which were backbone, stub, totally stubby and not-so-stubby in both IPv4 and IPv6. It was also to capture packets from different areas and identify the area based on the LSA messages packets had.

Background information

In this lab we used a normal OSPF area, stubby area, totally stubby area and not-so-stubby. The difference comes from the different types of LSA packets that are generated in each area. A normal area allows LSA types 1 through 5. A stubby area allows LSA types 1, 2 and 3. A totally stubby area is just like a stubby area, the only difference is a totally stubby area does not allow type 3 LSAs which summarizes the information of a given area. A not-so-stubby only allows LSA types 1, 2, 3 and 7 which tells the border routers about the external route.

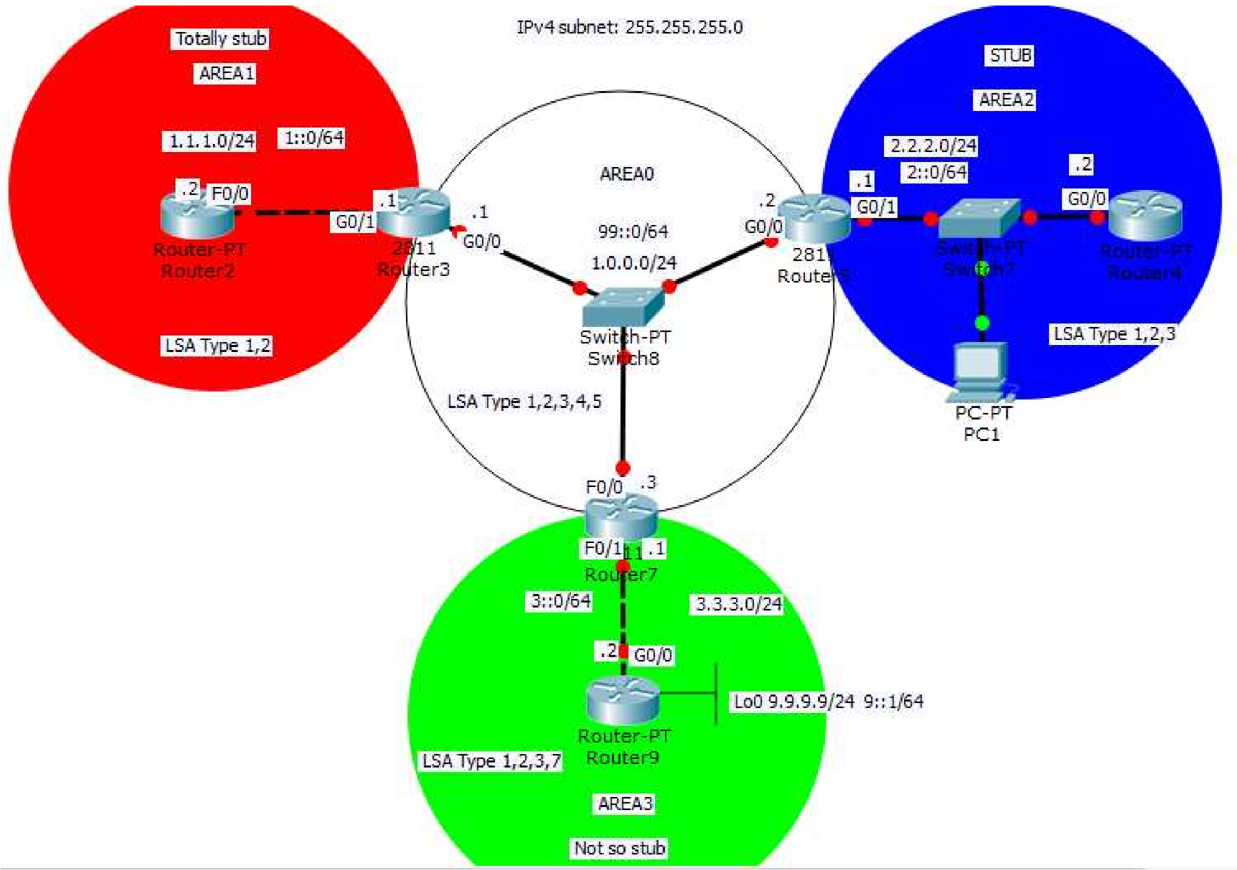
Lab Summary

We set up multi-area OSPF with 4 areas. One area is backbone, one is stubby, one is totally stubby and the last one is not-so-stubby. We first created the network and established connectivity between all the routers in the network. Then we created an external route. Assigned the external router to EIGRP and distributed EIGRP in OSPF. Then we assigned every area a stubbiness. We wired a switch into each area and used Wireshark to capture the packets that were going through. We analyzed the packets and verified that they had the right LSA messages.

Lab Commands

Area *area-id* **stub no-summary**	This command makes area 1 a totally stubby area which only allows LSA type 1 and 2 packets.
area *area-id* **stub**	This command makes the standard area, area 2 in this case, a stubby area which only allows LSA type 1, 2 and 3 packets.
area *area-id* **nssa**	This command makes area 3 a not-so-stubby area which only allows LSA types 1, 2, 3 and 7.
redistribute eigrp *process-id*	This command is used under “router ospf 1”. It distributes the hosts in the EIGRP network to the hosts in OSPF network.

Network Diagram



Configurations

R2:
Show run:

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R2
boot-start-marker
boot-end-marker
logging message-counter syslog
no aaa new-model
memory-size iomem 10
dot11 syslog
ip source-route
ip cef
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
```

```
voice-card 0
 no dspfarm
vtp domain cisco
vtp mode transparent
archive
 log config
  hidekeys
interface FastEthernet0/0
 ip address 1.1.1.2 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 1::2/64
 ipv6 ospf 1 area 1
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router ospf 1
 log-adjacency-changes
 area 1 stub no-summary
 network 1.1.1.0 0.0.0.255 area 1
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
 log-adjacency-changes
control-plane
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
scheduler allocate 20000 1000
end
```

Show ip route

```
     1.0.0.0/24 is subnetted, 1 subnets
C       1.1.1.0 is directly connected, FastEthernet0/0
O*IA 0.0.0.0/0 [110/2] via 1.1.1.1, 00:03:33, FastEthernet0/0
```

Show ipv6 route:

```
C   1::/64 [0/0]
     via FastEthernet0/0, directly connected
L   1::2/128 [0/0]
     via FastEthernet0/0, receive
OI  2::/64 [110/3]
     via FE80::7ADA:6EFF:FE99:AA01, FastEthernet0/0
OI  3::/64 [110/3]
     via FE80::7ADA:6EFF:FE99:AA01, FastEthernet0/0
OE2 9::/64 [110/20]
     via FE80::7ADA:6EFF:FE99:AA01, FastEthernet0/0
OI  99::/64 [110/2]
     via FE80::7ADA:6EFF:FE99:AA01, FastEthernet0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

R3
Show run

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R3
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180M8
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 1.0.0.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 99::1/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/1
 ip address 1.1.1.1 255.255.255.0
 duplex auto
```

```
 speed auto
 ipv6 address 1::1/64
 ipv6 ospf 1 area 1
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router ospf 1
 area 1 stub no-summary
 network 1.0.0.0 0.0.0.255 area 0
 network 1.1.1.0 0.0.0.255 area 1
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route:

```
   1.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        1.0.0.0/24 is directly connected, GigabitEthernet0/0
L        1.0.0.1/32 is directly connected, GigabitEthernet0/0
C        1.1.1.0/24 is directly connected, GigabitEthernet0/1
L        1.1.1.1/32 is directly connected, GigabitEthernet0/1
      2.0.0.0/24 is subnetted, 1 subnets
O IA     2.2.2.0 [110/2] via 1.0.0.2, 00:04:10, GigabitEthernet0/0
      3.0.0.0/24 is subnetted, 1 subnets
O IA     3.3.3.0 [110/2] via 1.0.0.3, 00:05:09, GigabitEthernet0/0
      9.0.0.0/24 is subnetted, 1 subnets
O E2     9.9.9.0 [110/20] via 1.0.0.3, 00:04:26, GigabitEthernet0/0
```

Show ipv6 route:

```
C   1::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   1::1/128 [0/0]
     via GigabitEthernet0/1, receive
OI  2::/64 [110/2]
     via FE80::EAB7:48FF:FE6E:88, GigabitEthernet0/0
OI  3::/64 [110/2]
     via FE80::218:19FF:FECD:92C8, GigabitEthernet0/0
OE2 9::/64 [110/20]
     via FE80::218:19FF:FECD:92C8, GigabitEthernet0/0
C   99::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   99::1/128 [0/0]
     via GigabitEthernet0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

R4:
Show run:

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R4
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180M5
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 2.2.2.2 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2::2/64
 ipv6 ospf 1 area 2
```

```
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router ospf 1
 area 2 stub
 network 2.2.2.0 0.0.0.255 area 2
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
O*IA  0.0.0.0/0 [110/2] via 2.2.2.1, 00:04:32, GigabitEthernet0/0
      1.0.0.0/24 is subnetted, 2 subnets
O IA     1.0.0.0 [110/2] via 2.2.2.1, 00:04:32, GigabitEthernet0/0
O IA     1.1.1.0 [110/3] via 2.2.2.1, 00:04:32, GigabitEthernet0/0
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, GigabitEthernet0/0
L        2.2.2.2/32 is directly connected, GigabitEthernet0/0
      3.0.0.0/24 is subnetted, 1 subnets
O IA     3.3.3.0 [110/3] via 2.2.2.1, 00:04:32, GigabitEthernet0/0
```

Show ipv6 route

```
OI  1::/64 [110/3]
```

```
     via FE80::EAB7:48FF:FE6E:89, GigabitEthernet0/0
C   2::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2::2/128 [0/0]
     via GigabitEthernet0/0, receive
OI  3::/64 [110/3]
     via FE80::EAB7:48FF:FE6E:89, GigabitEthernet0/0
OE2 9::/64 [110/20]
     via FE80::EAB7:48FF:FE6E:89, GigabitEthernet0/0
OI  99::/64 [110/2]
     via FE80::EAB7:48FF:FE6E:89, GigabitEthernet0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

R5
Show run

```
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R5
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ipv6 unicast-routing
ipv6 cef
ip source-route
ip cef
no ip domain lookup
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX15208074
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
redundancy
interface GigabitEthernet0/0
 ip address 1.0.0.2 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 99::2/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/1
 ip address 2.2.2.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2::1/64
 ipv6 ospf 1 area 2
```

```
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
router ospf 1
 log-adjacency-changes
 area 2 stub
 network 1.0.0.0 0.0.0.255 area 0
 network 2.2.2.0 0.0.0.255 area 2
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
control-plane
gatekeeper
 shutdown
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
scheduler allocate 20000 1000
end
```

Show ip route

```
      1.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        1.0.0.0/24 is directly connected, GigabitEthernet0/0
L        1.0.0.2/32 is directly connected, GigabitEthernet0/0
O IA     1.1.1.0/24 [110/2] via 1.0.0.1, 00:08:00, GigabitEthernet0/0
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, GigabitEthernet0/1
L        2.2.2.1/32 is directly connected, GigabitEthernet0/1
      3.0.0.0/24 is subnetted, 1 subnets
O IA     3.3.3.0 [110/2] via 1.0.0.3, 00:08:01, GigabitEthernet0/0
      9.0.0.0/24 is subnetted, 1 subnets
O E2     9.9.9.0 [110/20] via 1.0.0.3, 00:08:01, GigabitEthernet0/0
```

Show ipv6 route

```
OI  1::/64 [110/2]
     via FE80::7ADA:6EFF:FE99:AA00, GigabitEthernet0/0
C   2::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2::1/128 [0/0]
     via GigabitEthernet0/1, receive
OI  3::/64 [110/2]
```

```
     via FE80::218:19FF:FECD:92C8, GigabitEthernet0/0
OE2 9::/64 [110/20]
     via FE80::218:19FF:FECD:92C8, GigabitEthernet0/0
C   99::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   99::2/128 [0/0]
     via GigabitEthernet0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

R7
Show run

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R7
boot-start-marker
boot-end-marker
logging message-counter syslog
no aaa new-model
memory-size iomem 10
dot11 syslog
ip source-route
ip cef
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
voice-card 0
 no dspfarm
vtp domain cisco
vtp mode transparent
archive
 log config
  hidekeys
interface FastEthernet0/0
 ip address 1.0.0.3 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 99::3/64
 ipv6 ospf 1 area 0
interface FastEthernet0/1
 ip address 3.3.3.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 3::1/64
 ipv6 ospf 1 area 3
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
```

```
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/1/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
router ospf 1
 log-adjacency-changes
 area 3 nssa
 network 1.0.0.0 0.0.0.255 area 0
 network 3.3.3.0 0.0.0.255 area 3
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
 router-id 2.32.1.2
 log-adjacency-changes
control-plane
line con 0
line aux 0
line vty 0 4
 login
scheduler allocate 20000 1000
end
```

Show ip route

```
     1.0.0.0/24 is subnetted, 2 subnets
O IA    1.1.1.0 [110/2] via 1.0.0.1, 00:12:02, FastEthernet0/0
C       1.0.0.0 is directly connected, FastEthernet0/0
     2.0.0.0/24 is subnetted, 1 subnets
O IA    2.2.2.0 [110/2] via 1.0.0.2, 00:10:56, FastEthernet0/0
     3.0.0.0/24 is subnetted, 1 subnets
C       3.3.3.0 is directly connected, FastEthernet0/1
     9.0.0.0/24 is subnetted, 1 subnets
O N2    9.9.9.0 [110/20] via 3.3.3.2, 00:11:13, FastEthernet0/1
```

Show ipv6 route

```
OI  1::/64 [110/2]
     via FE80::7ADA:6EFF:FE99:AA00, FastEthernet0/0
OI  2::/64 [110/2]
     via FE80::EAB7:48FF:FE6E:88, FastEthernet0/0
C   3::/64 [0/0]
     via FastEthernet0/1, directly connected
L   3::1/128 [0/0]
```

```
     via FastEthernet0/1, receive
OE2 9::/64 [110/20]
     via FE80::AEF2:C5FF:FE55:9788, FastEthernet0/1
C   99::/64 [0/0]
     via FastEthernet0/0, directly connected
L   99::3/128 [0/0]
     via FastEthernet0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

R9
Show run

```
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R9
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ipv6 unicast-routing
ipv6 cef
ip source-route
ip cef
no ip domain lookup
multilink bundle-name authenticated
crypto pki token default removal timeout 0
voice-card 0
license udi pid CISCO2901/K9 sn FTX1704Y03B
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
license boot module c2900 technology-package datak9
vtp domain cisco
vtp mode transparent
redundancy
interface Loopback0
 ip address 9.9.9.9 255.255.255.0
 ipv6 address 9::1/64
 ipv6 enable
 ipv6 eigrp 1
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 3.3.3.2 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 3::2/64
 ipv6 ospf 1 area 3
```

```
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router eigrp 1
 network 9.0.0.0
router ospf 1
 area 3 nssa
 redistribute eigrp 1 subnets
 network 3.3.3.0 0.0.0.255 area 3
 default-information originate
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router eigrp 1
 eigrp router-id 1.1.1.1
ipv6 router ospf 1
 redistribute connected
 redistribute eigrp 1
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

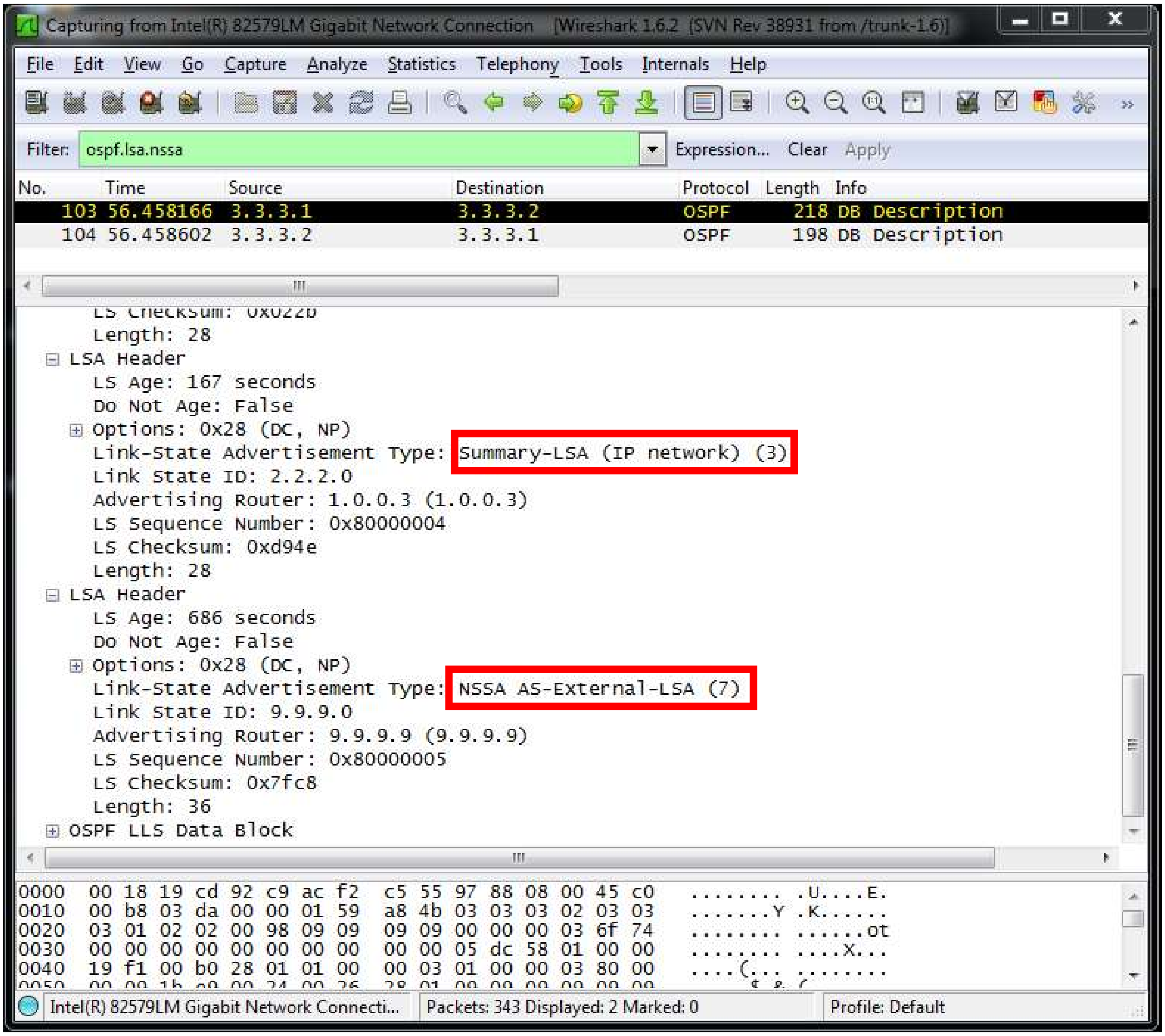
```
   1.0.0.0/24 is subnetted, 2 subnets
```

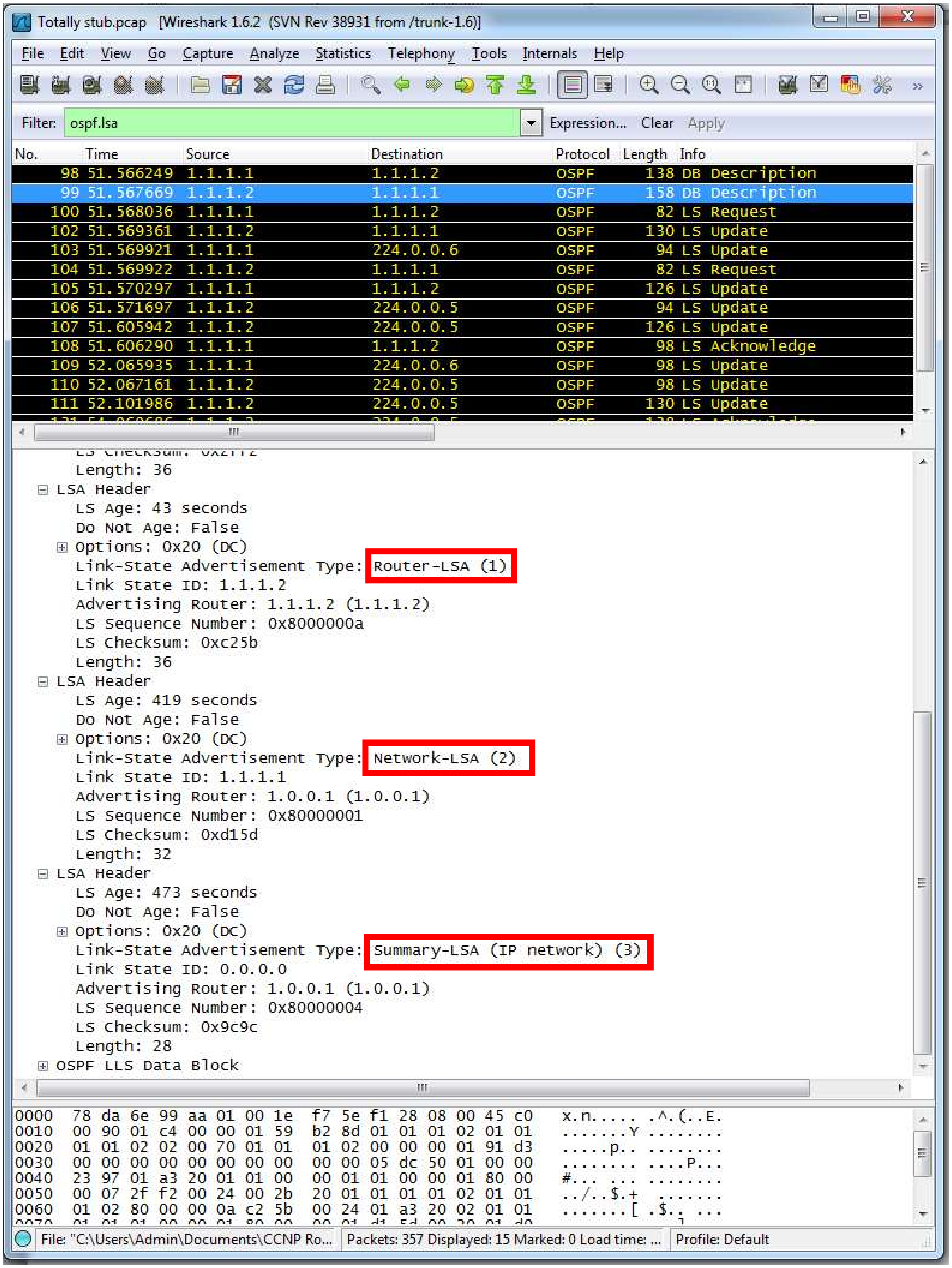
```
O IA     1.0.0.0 [110/2] via 3.3.3.1, 00:12:35, GigabitEthernet0/0
O IA     1.1.1.0 [110/3] via 3.3.3.1, 00:12:35, GigabitEthernet0/0
      2.0.0.0/24 is subnetted, 1 subnets
O IA     2.2.2.0 [110/3] via 3.3.3.1, 00:12:19, GigabitEthernet0/0
      3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        3.3.3.0/24 is directly connected, GigabitEthernet0/0
L        3.3.3.2/32 is directly connected, GigabitEthernet0/0
      9.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        9.9.9.0/24 is directly connected, Loopback0
L        9.9.9.9/32 is directly connected, Loopback0
```

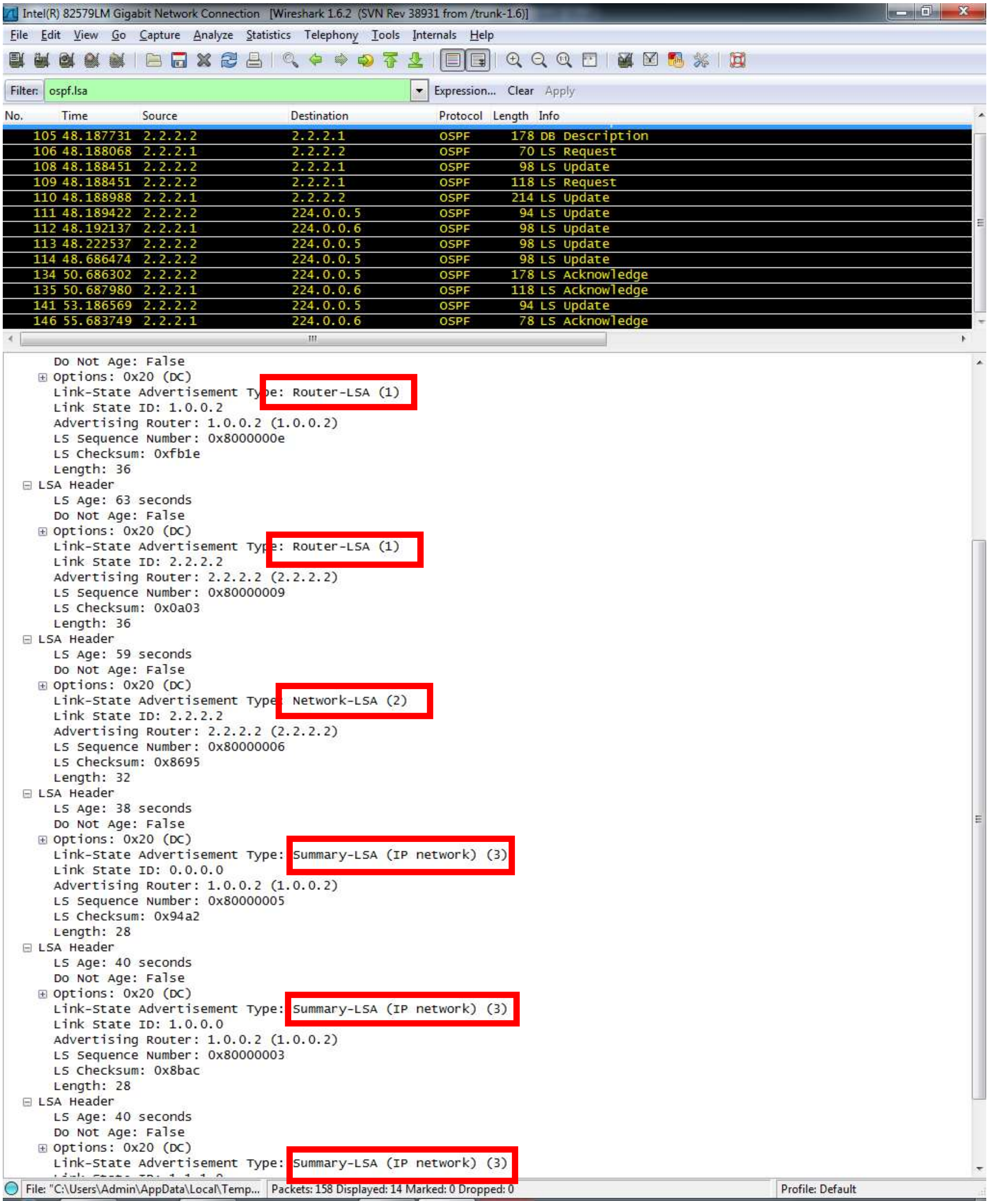
Show ipv6 route

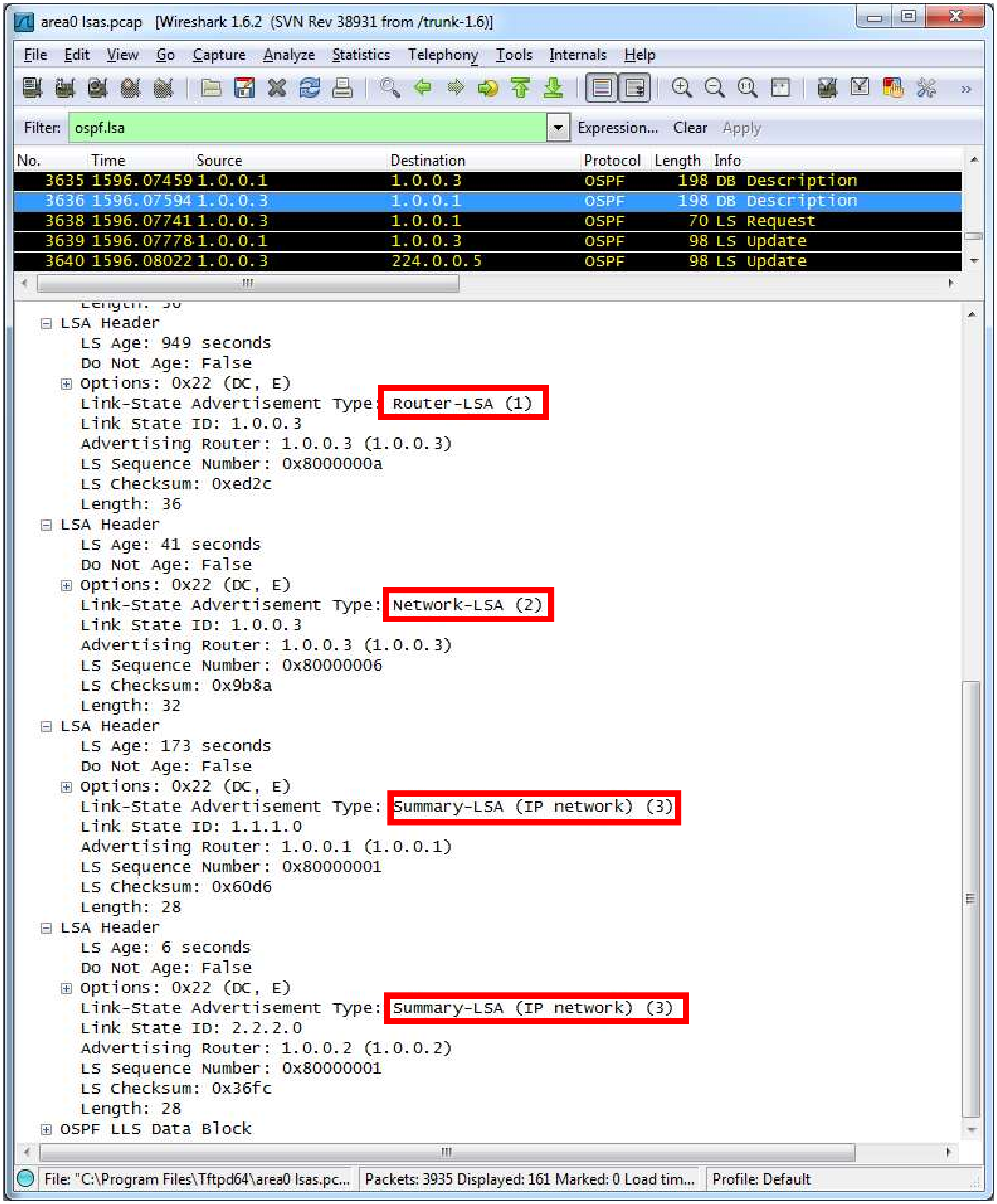
```
OI  1::/64 [110/3]
     via FE80::218:19FF:FECD:92C9, GigabitEthernet0/0
OI  2::/64 [110/3]
     via FE80::218:19FF:FECD:92C9, GigabitEthernet0/0
C   3::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   3::2/128 [0/0]
     via GigabitEthernet0/0, receive
C   9::/64 [0/0]
     via Loopback0, directly connected
L   9::1/128 [0/0]
     via Loopback0, receive
OI  99::/64 [110/2]
     via FE80::218:19FF:FECD:92C9, GigabitEthernet0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

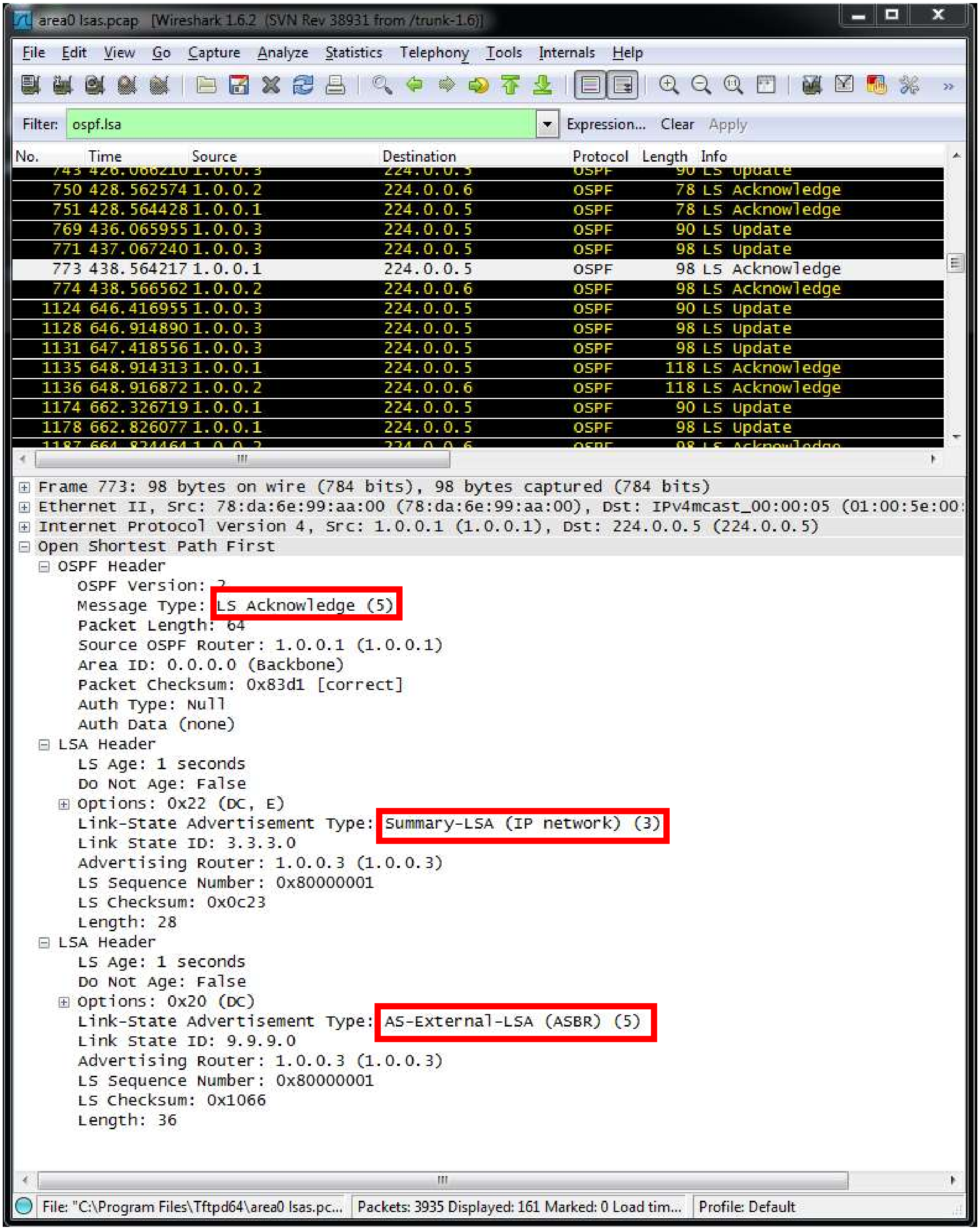
Wireshark Capture of the different area types:




Totally stub.pcap [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ospf.lsa
Expression... Clear Apply
No. Time Source Destination Protocol Length Info
98 51.566249 1.1.1.1 1.1.1.2 OSPF 138 DB Description
99 51.567669 1.1.1.2 1.1.1.1 OSPF 158 DB Description
100 51.568036 1.1.1.1 1.1.1.2 OSPF 82 LS Request
102 51.569361 1.1.1.2 1.1.1.1 OSPF 130 LS Update
103 51.569921 1.1.1.1 224.0.0.6 OSPF 94 LS Update
104 51.569922 1.1.1.2 1.1.1.1 OSPF 82 LS Request
105 51.570297 1.1.1.1 1.1.1.2 OSPF 126 LS Update
106 51.571697 1.1.1.2 224.0.0.5 OSPF 94 LS Update
107 51.605942 1.1.1.2 224.0.0.5 OSPF 126 LS Update
108 51.606290 1.1.1.1 1.1.1.2 OSPF 98 LS Acknowledge
109 52.065935 1.1.1.1 224.0.0.6 OSPF 98 LS Update
110 52.067161 1.1.1.2 224.0.0.5 OSPF 98 LS Update
111 52.101986 1.1.1.2 224.0.0.5 OSPF 130 LS Update
Length: 36
LSA Header
LS Age: 43 seconds
Do Not Age: False
Options: 0x20 (DC)
Link-State Advertisement Type: Router-LSA (1)
Link State ID: 1.1.1.2
Advertising Router: 1.1.1.2 (1.1.1.2)
LS Sequence Number: 0x8000000a
LS Checksum: 0xc25b
Length: 36
LSA Header
LS Age: 419 seconds
Do Not Age: False
Options: 0x20 (DC)
Link-State Advertisement Type: Network-LSA (2)
Link State ID: 1.1.1.1
Advertising Router: 1.0.0.1 (1.0.0.1)
LS Sequence Number: 0x80000001
LS Checksum: 0xd15d
Length: 32
LSA Header
LS Age: 473 seconds
Do Not Age: False
Options: 0x20 (DC)
Link-State Advertisement Type: Summary-LSA (IP network) (3)
Link State ID: 0.0.0.0
Advertising Router: 1.0.0.1 (1.0.0.1)
LS Sequence Number: 0x80000004
LS Checksum: 0x9c9c
Length: 28
OSPF LLS Data Block
0000 78 da 6e 99 aa 01 00 1e f7 5e f1 28 08 00 45 c0 x.n..... .^.(..E.
0010 00 90 01 c4 00 00 01 59 b2 8d 01 01 01 02 01 01 ....Y ....
0020 01 01 02 02 00 70 01 01 01 02 00 00 00 01 91 d3 .....p.. ....
0030 00 00 00 00 00 00 00 00 00 00 05 dc 50 01 00 00 ....P...
0040 23 97 01 a3 20 01 01 00 00 01 01 00 00 01 80 00 #... ... .
0050 00 07 2f f2 00 24 00 2b 20 01 01 01 01 02 01 01 ../..$.+ ....
0060 01 02 80 00 00 0a c2 5b 00 24 01 a3 20 02 01 01 ....[.$.. ...
File: "C:\Users\Admin\Documents\CCNP Ro... Packets: 357 Displayed: 15 Marked: 0 Load time: ... Profile: Default


Intel(R) 82579LM Gigabit Network Connection [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ospf.lsa
Expression... Clear Apply
No. Time Source Destination Protocol Length Info
105 48.187731 2.2.2.2 2.2.2.1 OSPF 178 DB Description
106 48.188068 2.2.2.1 2.2.2.2 OSPF 70 LS Request
108 48.188451 2.2.2.2 2.2.2.1 OSPF 98 LS Update
109 48.188451 2.2.2.2 2.2.2.1 OSPF 118 LS Request
110 48.188988 2.2.2.1 2.2.2.2 OSPF 214 LS Update
111 48.189422 2.2.2.2 224.0.0.5 OSPF 94 LS Update
112 48.192137 2.2.2.1 224.0.0.6 OSPF 98 LS Update
113 48.222537 2.2.2.2 224.0.0.5 OSPF 98 LS Update
114 48.686474 2.2.2.2 224.0.0.5 OSPF 98 LS Update
134 50.686302 2.2.2.2 224.0.0.5 OSPF 178 LS Acknowledge
135 50.687980 2.2.2.1 224.0.0.6 OSPF 118 LS Acknowledge
141 53.186569 2.2.2.2 224.0.0.5 OSPF 94 LS Update
146 55.683749 2.2.2.1 224.0.0.6 OSPF 78 LS Acknowledge
Do Not Age: False
Options: 0x20 (DC)
Link-State Advertisement Type: Router-LSA (1)
Link State ID: 1.0.0.2
Advertising Router: 1.0.0.2 (1.0.0.2)
LS Sequence Number: 0x8000000e
LS Checksum: 0xfb1e
Length: 36
LSA Header
LS Age: 63 seconds
Do Not Age: False
Options: 0x20 (DC)
Link-State Advertisement Type: Router-LSA (1)
Link State ID: 2.2.2.2
Advertising Router: 2.2.2.2 (2.2.2.2)
LS Sequence Number: 0x80000009
LS Checksum: 0x0a03
Length: 36
LSA Header
LS Age: 59 seconds
Do Not Age: False
Options: 0x20 (DC)
Link-State Advertisement Type: Network-LSA (2)
Link State ID: 2.2.2.2
Advertising Router: 2.2.2.2 (2.2.2.2)
LS Sequence Number: 0x80000006
LS Checksum: 0x8695
Length: 32
LSA Header
LS Age: 38 seconds
Do Not Age: False
Options: 0x20 (DC)
Link-State Advertisement Type: Summary-LSA (IP network) (3)
Link State ID: 0.0.0.0
Advertising Router: 1.0.0.2 (1.0.0.2)
LS Sequence Number: 0x80000005
LS Checksum: 0x94a2
Length: 28
LSA Header
LS Age: 40 seconds
Do Not Age: False
Options: 0x20 (DC)
Link-State Advertisement Type: Summary-LSA (IP network) (3)
Link State ID: 1.0.0.0
Advertising Router: 1.0.0.2 (1.0.0.2)
LS Sequence Number: 0x80000003
LS Checksum: 0x8bac
Length: 28
LSA Header
LS Age: 40 seconds
Do Not Age: False
Options: 0x20 (DC)
Link-State Advertisement Type: Summary-LSA (IP network) (3)
File: "C:\Users\Admin\AppData\Local\Temp... Packets: 158 Displayed: 14 Marked: 0 Dropped: 0
Profile: Default


area0 lsas.pcap [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ospf.lsa
Expression... Clear Apply
No. Time Source Destination Protocol Length Info
3635 1596.07459 1.0.0.1 1.0.0.3 OSPF 198 DB Description
3636 1596.07594 1.0.0.3 1.0.0.1 OSPF 198 DB Description
3638 1596.07741 1.0.0.3 1.0.0.1 OSPF 70 LS Request
3639 1596.07778 1.0.0.1 1.0.0.3 OSPF 98 LS Update
3640 1596.08022 1.0.0.3 224.0.0.5 OSPF 98 LS Update
LSA Header
LS Age: 949 seconds
Do Not Age: False
Options: 0x22 (DC, E)
Link-State Advertisement Type: Router-LSA (1)
Link State ID: 1.0.0.3
Advertising Router: 1.0.0.3 (1.0.0.3)
LS Sequence Number: 0x8000000a
LS Checksum: 0xed2c
Length: 36
LSA Header
LS Age: 41 seconds
Do Not Age: False
Options: 0x22 (DC, E)
Link-State Advertisement Type: Network-LSA (2)
Link State ID: 1.0.0.3
Advertising Router: 1.0.0.3 (1.0.0.3)
LS Sequence Number: 0x80000006
LS Checksum: 0x9b8a
Length: 32
LSA Header
LS Age: 173 seconds
Do Not Age: False
Options: 0x22 (DC, E)
Link-State Advertisement Type: Summary-LSA (IP network) (3)
Link State ID: 1.1.1.0
Advertising Router: 1.0.0.1 (1.0.0.1)
LS Sequence Number: 0x80000001
LS Checksum: 0x60d6
Length: 28
LSA Header
LS Age: 6 seconds
Do Not Age: False
Options: 0x22 (DC, E)
Link-State Advertisement Type: Summary-LSA (IP network) (3)
Link State ID: 2.2.2.0
Advertising Router: 1.0.0.2 (1.0.0.2)
LS Sequence Number: 0x80000001
LS Checksum: 0x36fc
Length: 28
OSPF LLS Data Block
File: "C:\Program Files\Tftpd64\area0 lsas.pc...
Packets: 3935 Displayed: 161 Marked: 0 Load tim...
Profile: Default


area0 lsas.pcap [Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ospf.lsa
Expression... Clear Apply
No. Time Source Destination Protocol Length Info
750 428.562574 1.0.0.2 224.0.0.6 OSPF 78 LS Acknowledge
751 428.564428 1.0.0.1 224.0.0.5 OSPF 78 LS Acknowledge
769 436.065955 1.0.0.3 224.0.0.5 OSPF 90 LS Update
771 437.067240 1.0.0.3 224.0.0.5 OSPF 98 LS Update
773 438.564217 1.0.0.1 224.0.0.5 OSPF 98 LS Acknowledge
774 438.566562 1.0.0.2 224.0.0.6 OSPF 98 LS Acknowledge
1124 646.416955 1.0.0.3 224.0.0.5 OSPF 90 LS Update
1128 646.914890 1.0.0.3 224.0.0.5 OSPF 98 LS Update
1131 647.418556 1.0.0.3 224.0.0.5 OSPF 98 LS Update
1135 648.914313 1.0.0.1 224.0.0.5 OSPF 118 LS Acknowledge
1136 648.916872 1.0.0.2 224.0.0.6 OSPF 118 LS Acknowledge
1174 662.326719 1.0.0.1 224.0.0.5 OSPF 90 LS Update
1178 662.826077 1.0.0.1 224.0.0.5 OSPF 98 LS Update
Frame 773: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: 78:da:6e:99:aa:00 (78:da:6e:99:aa:00), Dst: IPv4mcast_00:00:05 (01:00:5e:00:
Internet Protocol Version 4, Src: 1.0.0.1 (1.0.0.1), Dst: 224.0.0.5 (224.0.0.5)
Open Shortest Path First
OSPF Header
OSPF Version: 2
Message Type: LS Acknowledge (5)
Packet Length: 64
Source OSPF Router: 1.0.0.1 (1.0.0.1)
Area ID: 0.0.0.0 (Backbone)
Packet Checksum: 0x83d1 [correct]
Auth Type: Null
Auth Data (none)
LSA Header
LS Age: 1 seconds
Do Not Age: False
Options: 0x22 (DC, E)
Link-State Advertisement Type: Summary-LSA (IP network) (3)
Link State ID: 3.3.3.0
Advertising Router: 1.0.0.3 (1.0.0.3)
LS Sequence Number: 0x80000001
LS Checksum: 0x0c23
Length: 28
LSA Header
LS Age: 1 seconds
Do Not Age: False
Options: 0x20 (DC)
Link-State Advertisement Type: AS-External-LSA (ASBR) (5)
Link State ID: 9.9.9.0
Advertising Router: 1.0.0.3 (1.0.0.3)
LS Sequence Number: 0x80000001
LS Checksum: 0x1066
Length: 36
File: "C:\Program Files\Tftpd64\area0 lsas.pc... Packets: 3935 Displayed: 161 Marked: 0 Load tim... Profile: Default

Problems

When we were using Wireshark to capture OSPF packets, we couldn't find any packet that had LSAs in it. We had to make the routers send the LSA packets again so we unplugged and plugged a cable in the area we were capturing packets from.

After capturing packets from all areas, we realized that the totally stubby area had LSA type 1, 2 and 3 like the stub area. However, it only had to have LSA type 1 and 2. We later compared the LSA type 3 packets from both areas and saw that the link state id was different in the totally stub area.

We could not get the border routers to see the external route. They did not have the external route on their routing tables. So, we decided to use EIGRP on the external route and distribute it on the OSPF protocol. That way we were able to get the external route on all of the border routers.

Conclusion

We created another multi-area OSPF network but this time every area had a different stubbiness type. After we configured everything, we used Wireshark to capture packets and look at the types of LSAs each area had. It was easy to configure the areas to a specific stubbiness since it required only 1 command. It took a while to figure out where the LSA types were in a Wireshark captured packet.

Internal BGP

Purpose

The purpose of this lab is to connect a pre-configured network to another network by configuring internal BGP in that other network and letting the traffic of the pre-configured network go through.

Background Information

BGP uses two primary modes of information exchange, internal BGP (IBGP) and external BGP (EBGP), to communicate with internal and external peers, respectively. In this lab we configured both types of BGP but we configured iBGP for the first time and it was the main point of this lab. Internal BGP is a mechanism to provide more information to your internal routers.

BGP is another routing protocol like EIGRP and OSPF. The main goal of BGP and all other routing protocols is to establish connectivity between destinations that are more than a hop away. This can be any instance where there are one or more routers between the source and the destination. BGP works with different autonomous systems which is common to most routing protocols however, unlike other routing protocols, there are two different types of BGPs: Internal and external.

Internal BGP is when the routers, that are using BGP, are all in the same autonomous system. On the other hand external BGP uses multiple autonomous systems to establish connectivity between networks that use different autonomous systems.

We can view every autonomous system like a country. In internal BGP everyone is inside one country, speaking the same language and following the same rules and laws. In external BGP there are a lot of countries and packets that travel between them who are like tourists with visas. The embassies of tourists' home nations in other countries are like the external BGP, they do pretty much the same job. They help their citizens with legal help and protect them in foreign countries. Overall, they handle the legal transition between the two countries and ensure that tourists are safe and get to wherever they want to go to, just like BGP. And if a tourist has a layover in a country, they can go through a country to get to another. This is just like packets from an outside network going through the iBGP network to get to a network on the other end of the iBGP network.

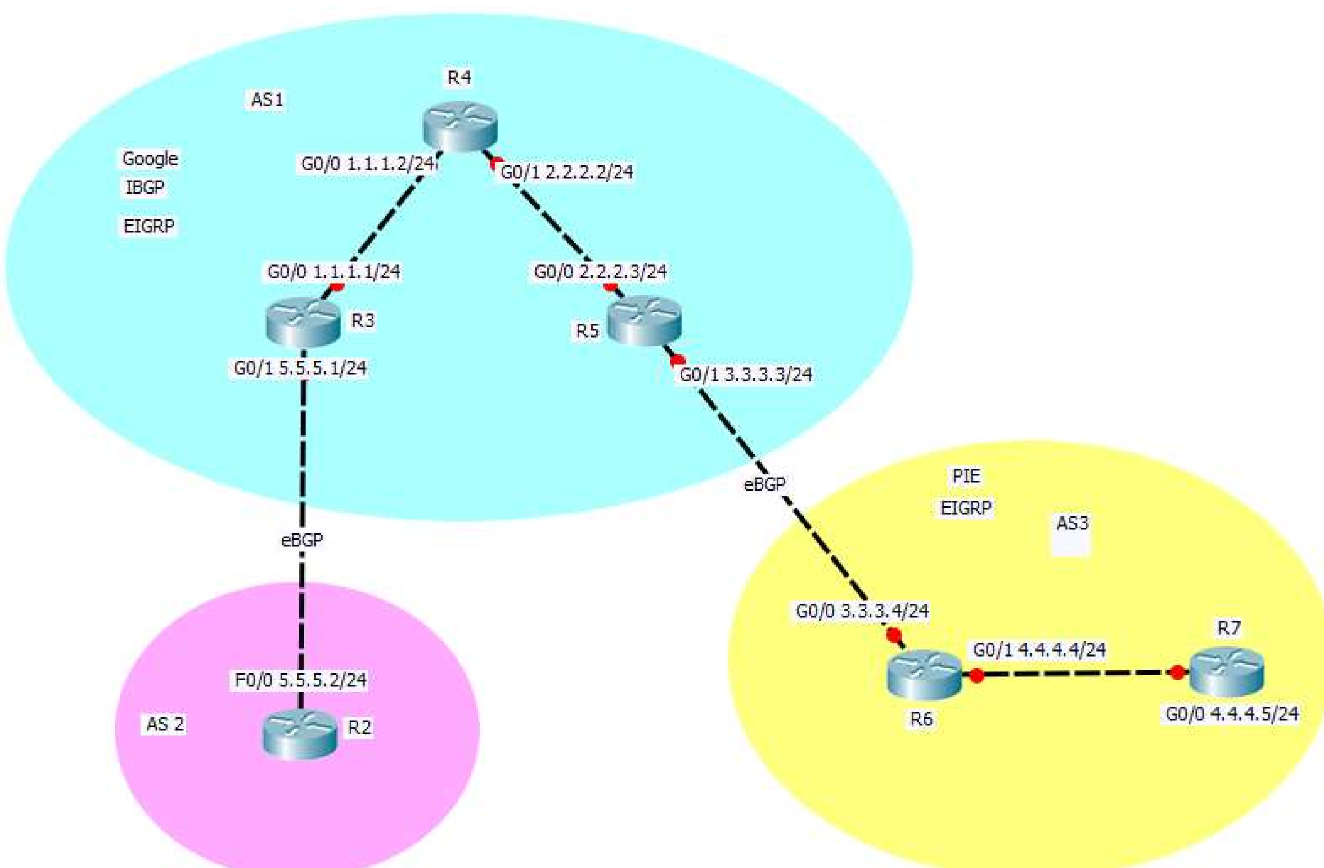
Lab Summary

In this lab, we had a scenario. The scenario was that Google bought a start-up company called PIE and Google wanted to add PIE's network without making any changes in the internal routers of PIE's existing network. PIE was internally using EIGRP (in our scenario) and every router in PIE's network should be able to connect to the internet connection of Google's network which is on the other end of the topology. So PIE's traffic had to go through all the routers in Google's existing network which was also using EIGRP originally. The connection between the internet and Google and the connection between Google and PIE networks are using external BGP to establish connectivity. For the packets coming from the PIE network to go through Google and access the internet, we configured iBGP on the routers of the Google network. While we configured iBGP, we used the same commands as we used on eBGP but the only difference was that the autonomous system numbers of a network that uses iBGP are the same. So we connected the two networks, configured eBGP between two existing networks and configured iBGP in the Google network to create end to end connectivity. To prove that we are running iBGP, on R4 which is an internal router for Google, we entered the command "show ip bgp neighbors" and as a result of the command, we saw that the R4 only has 2 internal BGP routes and no external BGP route. This means that R4 is only running only iBGP and no eBGP just like it's supposed to be. At the end of the lab the router that was at the end of PIE was able to connect to the router that represented the internet on the other end.

Lab Commands

router bgp *1*	This command creates and configures the BGP routing process.
redistribute connected	This command is entered under router eigrp, router ospf or router bgp and advertises the connected routes to the routing protocol that it is configured under.
redistribute bgp *1* **metric** *100 1 255 2 1500*	This command changes the metrics of the routing protocol that it is configured under and also advertises BGP 1 to the same routing protocol so that it can have connectivity with BGP.
neighbor *1.1.1.2* **remote-as** *1*	This command is used under router bgp and it advertises an external bgp network and its autonomous system number to the BGP on the router where this command is entered.
neighbor *1.1.1.2* **activate**	This command enables the exchange of information with a BGP neighbor which is the destination with IP address 1.1.1.2 in this case.

Network Diagram



Configurations

R2
Show run:
```
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R2
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
dot11 syslog
ip source-route
ip cef
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
crypto pki token default removal timeout 0
license udi pid CISCO2811 sn FTX1026A30U
interface FastEthernet0/0
 ip address 5.5.5.2 255.255.255.0
 duplex auto
 speed auto
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router bgp 2
 bgp log-neighbor-changes
 neighbor 5.5.5.1 remote-as 1
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
mgcp profile default
line con 0
line aux 0
line vty 0 4
 login
 transport input all
```

```
scheduler allocate 20000 1000
end
```

Show ip route

```
      1.0.0.0/24 is subnetted, 1 subnets
B        1.1.1.0 [20/0] via 5.5.5.1, 00:34:08
      2.0.0.0/24 is subnetted, 1 subnets
B        2.2.2.0 [20/28416] via 5.5.5.1, 00:34:08
      3.0.0.0/24 is subnetted, 1 subnets
B        3.3.3.0 [20/28672] via 5.5.5.1, 00:34:08
      4.0.0.0/24 is subnetted, 1 subnets
B        4.4.4.0 [20/25603072] via 5.5.5.1, 00:33:37
      5.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        5.5.5.0/24 is directly connected, FastEthernet0/0
L        5.5.5.2/32 is directly connected, FastEthernet0/0
```

R3

Show run

```
Current configuration : 1653 bytes
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R3
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180LH
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 1.1.1.1 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 5.5.5.1 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
```

```
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router eigrp 1
 network 1.1.1.0 0.0.0.255
 redistribute connected
 redistribute bgp 1 metric 100 1 255 2 1500
router bgp 1
 bgp log-neighbor-changes
 bgp redistribute-internal
 redistribute connected
 redistribute eigrp 1
 neighbor 1.1.1.2 remote-as 1
 neighbor 5.5.5.2 remote-as 2
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
End
```

Show ip route

```
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, GigabitEthernet0/0
L        1.1.1.1/32 is directly connected, GigabitEthernet0/0
      2.0.0.0/24 is subnetted, 1 subnets
D        2.2.2.0 [90/28416] via 1.1.1.2, 00:35:17, GigabitEthernet0/0
      3.0.0.0/24 is subnetted, 1 subnets
D EX     3.3.3.0 [170/28672] via 1.1.1.2, 00:35:17, GigabitEthernet0/0
      4.0.0.0/24 is subnetted, 1 subnets
D EX     4.4.4.0 [170/25603072] via 1.1.1.2, 00:35:11,
GigabitEthernet0/0
      5.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        5.5.5.0/24 is directly connected, GigabitEthernet0/1
L        5.5.5.1/32 is directly connected, GigabitEthernet0/1
```

R4
Show ip bgp neighbors

```
BGP neighbor is 1.1.1.1,  remote AS 1, internal link
  BGP version 4, remote router ID 5.5.5.1
  BGP state = Established, up for 00:39:06
  Last read 00:00:24, last write 00:00:22, hold time is 180, keepalive
interval is 60 seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          5
    Keepalives:            44         44
    Route Refresh:          0          0
    Total:                 46         50
  Default minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  Session: 1.1.1.1
  BGP table version 6, neighbor version 6/0
  Output queue size : 0
  Index 2, Advertise bit 0
  2 update-group member
  Slow-peer detection is disabled
  Slow-peer split-update-group dynamic is disabled
                                 Sent       Rcvd
  Prefix activity:               ----       ----
    Prefixes Current:               0          5 (Consumes 320 bytes)
    Prefixes Total:                 0          5
    Implicit Withdraw:              0          0
    Explicit Withdraw:              0          0
    Used as bestpath:             n/a          3
    Used as multipath:            n/a          0

                                   Outbound    Inbound
  Local Policy Denied Prefixes:    --------    -------
    Bestpath from this peer:              3        n/a
```

```
    Bestpath from iBGP peer:              2        n/a
    Total:                                5          0
  Number of NLRIs in the update sent: max 0, min 0
  Last detected as dynamic slow peer: never
  Dynamic slow peer recovered: never
  Refresh Epoch: 1
  Last Sent Refresh Start-of-rib: never
  Last Sent Refresh End-of-rib: never
  Last Received Refresh Start-of-rib: never
  Last Received Refresh End-of-rib: never
                                     Sent       Rcvd
        Refresh activity:            ----       ----
          Refresh Start-of-RIB         0          0
          Refresh End-of-RIB           0          0

  Address tracking is enabled, the RIB does have a route to 1.1.1.1
  Connections established 2; dropped 1
  Last reset 00:39:07, due to User reset of session 1
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is disabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 255
Local host: 1.1.1.2, Local port: 41901
Foreign host: 1.1.1.1, Foreign port: 179
Connection tableid (VRF): 0
Maximum output segment queue size: 50

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x358880):
Timer          Starts    Wakeups            Next
Retrans            46          0             0x0
TimeWait            0          0             0x0
AckHold            45         42             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger         1464       1463        0x358AD0
DeadWait            0          0             0x0
Linger              0          0             0x0
ProcessQ            0          0             0x0

iss: 3017468227  snduna: 3017469144  sndnxt: 3017469144
irs:  123885278  rcvnxt:  123886419

sndwnd:  15468  scale:      0  maxrcvwnd:  16384
rcvwnd:  15244  scale:      0  delrcvwnd:   1140

SRTT: 998 ms, RTTO: 1016 ms, RTV: 18 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 1000 ms, ACK hold: 200 ms
Status Flags: active open
Option Flags: nagle, path mtu capable
```

```
IP Precedence value : 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 91 (out of order: 0), with data: 46, total data bytes: 1140
Sent: 92 (retransmit: 0, fastretransmit: 0, partialack: 0, Second
Congestion: 0), with data: 46, total data bytes: 916

 Packets received in fast path: 0, fast processed: 0, slow path: 0
 fast lock acquisition failures: 0, slow path: 0
TCP Semaphore      0x3DA8A3A4  FREE

BGP neighbor is 2.2.2.3,  remote AS 1, internal link
  BGP version 4, remote router ID 3.3.3.3
  BGP state = Established, up for 00:39:06
  Last read 00:00:48, last write 00:00:32, hold time is 180, keepalive
interval is 60 seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                1          5
    Keepalives:            45         44
    Route Refresh:          0          0
    Total:                 47         50
  Default minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  Session: 2.2.2.3
  BGP table version 6, neighbor version 6/0
  Output queue size : 0
  Index 2, Advertise bit 0
  2 update-group member
  Slow-peer detection is disabled
  Slow-peer split-update-group dynamic is disabled
                                 Sent       Rcvd
  Prefix activity:               ----       ----
    Prefixes Current:               0          5 (Consumes 320 bytes)
    Prefixes Total:                 0          5
    Implicit Withdraw:              0          0
    Explicit Withdraw:              0          0
```

```
    Used as bestpath:             n/a         2
    Used as multipath:            n/a         0

                                   Outbound    Inbound
  Local Policy Denied Prefixes:    --------    -------
    Bestpath from this peer:              3        n/a
    Bestpath from iBGP peer:              2        n/a
    Total:                                5          0
  Number of NLRIs in the update sent: max 0, min 0
  Last detected as dynamic slow peer: never
  Dynamic slow peer recovered: never
  Refresh Epoch: 1
  Last Sent Refresh Start-of-rib: never
  Last Sent Refresh End-of-rib: never
  Last Received Refresh Start-of-rib: never
  Last Received Refresh End-of-rib: never
                                       Sent       Rcvd
        Refresh activity:              ----       ----
          Refresh Start-of-RIB          0          0
          Refresh End-of-RIB            0          0

  Address tracking is enabled, the RIB does have a route to 2.2.2.3
  Connections established 2; dropped 1
  Last reset 00:39:07, due to User reset of session 1
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is disabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 255
Local host: 2.2.2.2, Local port: 31353
Foreign host: 2.2.2.3, Foreign port: 179
Connection tableid (VRF): 0
Maximum output segment queue size: 50

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x358884):
Timer          Starts    Wakeups            Next
Retrans            47          0             0x0
TimeWait            0          0             0x0
AckHold            45         42             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger         1475       1474        0x358A4E
DeadWait            0          0             0x0
Linger              0          0             0x0
ProcessQ            0          0             0x0

iss: 2566081609  snduna: 2566082545  sndnxt: 2566082545
irs: 3589633439  rcvnxt: 3589634586

sndwnd:  15449  scale:      0  maxrcvwnd:  16384
```

```
rcvwnd:  15238  scale:      0  delrcvwnd:   1146

SRTT: 998 ms, RTTO: 1014 ms, RTV: 16 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 1000 ms, ACK hold: 200 ms
Status Flags: active open
Option Flags: nagle, path mtu capable
IP Precedence value : 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 92 (out of order: 0), with data: 46, total data bytes: 1146
Sent: 93 (retransmit: 0, fastretransmit: 0, partialack: 0, Second
Congestion: 0), with data: 47, total data bytes: 935

 Packets received in fast path: 0, fast processed: 0, slow path: 0
 fast lock acquisition failures: 0, slow path: 0
TCP Semaphore      0x3DA8A334  FREE
```

Show run

```
Current configuration : 1637 bytes Last configuration change at
19:20:51 UTC Wed Feb 24 2016
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R4
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180LN
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 1.1.1.2 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 2.2.2.2 255.255.255.0
 duplex auto
 speed auto
```

```
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router eigrp 1
 network 1.1.1.0 0.0.0.255
 network 2.2.2.0 0.0.0.255
router bgp 1
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 1
 neighbor 2.2.2.3 remote-as 1
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, GigabitEthernet0/0
L        1.1.1.2/32 is directly connected, GigabitEthernet0/0
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, GigabitEthernet0/1
L        2.2.2.2/32 is directly connected, GigabitEthernet0/1
      3.0.0.0/24 is subnetted, 1 subnets
D EX     3.3.3.0 [170/3072] via 2.2.2.3, 00:38:01, GigabitEthernet0/1
      4.0.0.0/24 is subnetted, 1 subnets
D EX     4.4.4.0 [170/25600512] via 2.2.2.3, 00:37:54,
GigabitEthernet0/1
      5.0.0.0/24 is subnetted, 1 subnets
D EX     5.5.5.0 [170/30720] via 1.1.1.1, 00:38:00, GigabitEthernet0/0
```

R5
Show run

```
Current configuration : 1772 bytes Last configuration change at
19:46:56 UTC Wed Feb 24 2016
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R5
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX1520806Y
license accept end user agreement
license boot module c2900 technology-package uck9
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 2.2.2.3 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 3.3.3.3 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 duplex auto
 speed auto
router eigrp 1
 network 2.2.2.0 0.0.0.255
 redistribute connected
 redistribute bgp 3 metric 100 1 255 2 1500
 redistribute bgp 1 metric 100 1 255 2 1500
router bgp 1
```

```
 bgp log-neighbor-changes
 bgp redistribute-internal
 redistribute connected
 redistribute eigrp 1
 neighbor 2.2.2.2 remote-as 1
 neighbor 3.3.3.4 remote-as 3
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
End
```

Show ip route

```
      1.0.0.0/24 is subnetted, 1 subnets
D        1.1.1.0 [90/28416] via 2.2.2.2, 00:39:18, GigabitEthernet0/0
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, GigabitEthernet0/0
L        2.2.2.3/32 is directly connected, GigabitEthernet0/0
      3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        3.3.3.0/24 is directly connected, GigabitEthernet0/1
L        3.3.3.3/32 is directly connected, GigabitEthernet0/1
      4.0.0.0/24 is subnetted, 1 subnets
B        4.4.4.0 [20/0] via 3.3.3.4, 00:39:11
      5.0.0.0/24 is subnetted, 1 subnets
D EX     5.5.5.0 [170/30976] via 2.2.2.2, 00:39:17, GigabitEthernet0/0
```

R6

Show run

```
Current configuration : 1766 bytes Last configuration change at
19:47:54 UTC Wed Feb 24 2016
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R6
boot-start-marker
```

```
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX1520806Z
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 3.3.3.4 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 4.4.4.4 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 duplex auto
 speed auto
router eigrp 1
 network 4.4.4.0 0.0.0.255
 redistribute connected
 redistribute bgp 3 metric 100 1 255 2 1500
router bgp 3
 bgp log-neighbor-changes
 bgp redistribute-internal
 redistribute connected
 redistribute eigrp 1
 neighbor 3.3.3.3 remote-as 1
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
mgcp profile default
gatekeeper
```

```
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
End
```

Show ip route

```
      1.0.0.0/24 is subnetted, 1 subnets
B        1.1.1.0 [20/28416] via 3.3.3.3, 00:40:06
      2.0.0.0/24 is subnetted, 1 subnets
B        2.2.2.0 [20/0] via 3.3.3.3, 00:40:06
      3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        3.3.3.0/24 is directly connected, GigabitEthernet0/0
L        3.3.3.4/32 is directly connected, GigabitEthernet0/0
      4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        4.4.4.0/24 is directly connected, GigabitEthernet0/1
L        4.4.4.4/32 is directly connected, GigabitEthernet0/1
      5.0.0.0/24 is subnetted, 1 subnets
B        5.5.5.0 [20/30976] via 3.3.3.3, 00:40:06
```

R7

Show run

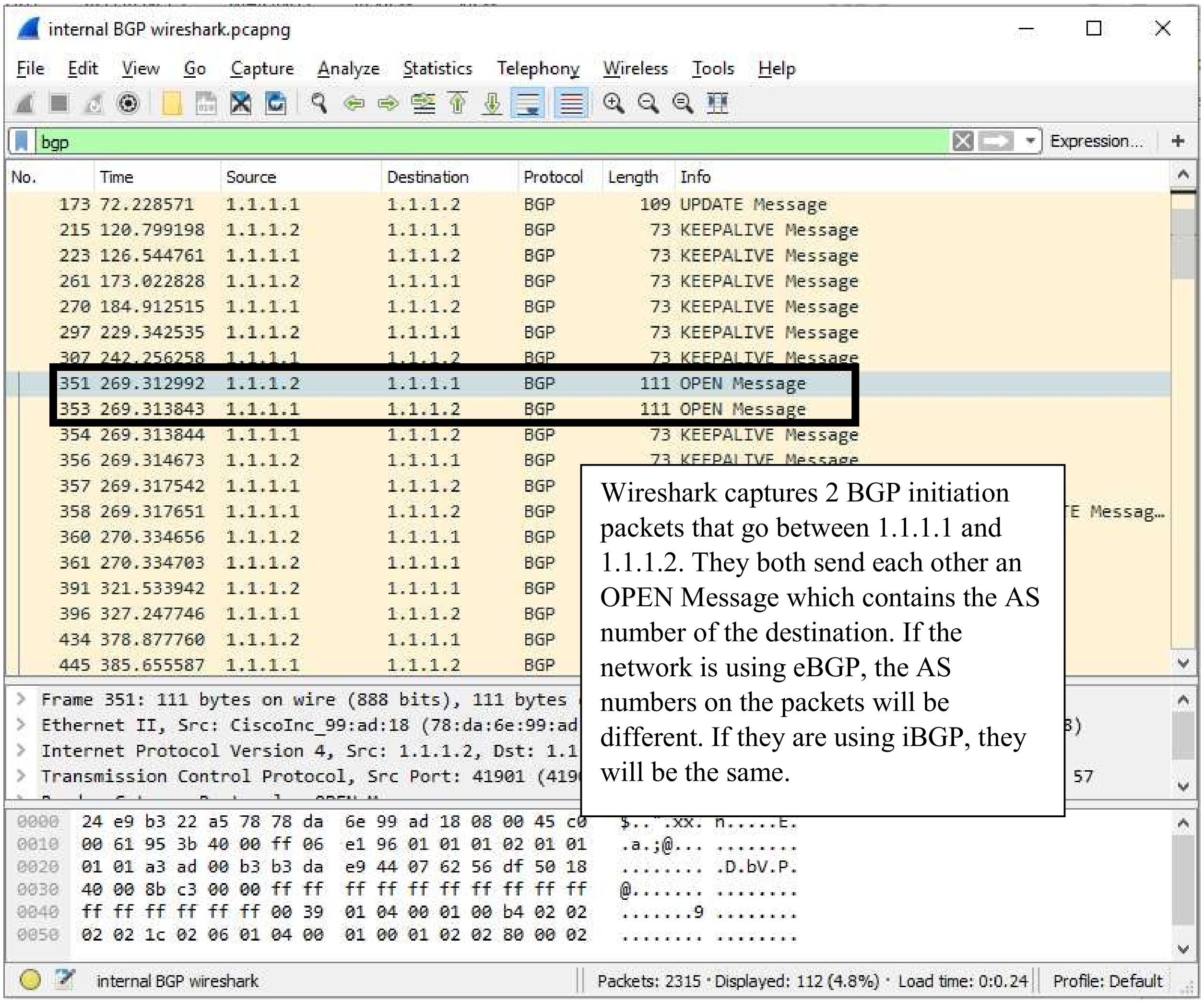
```
Current configuration : 1632 bytes Last configuration change at
19:38:36 UTC Wed Feb 24 2016
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R7
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX152885RE
license accept end user agreement
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
```

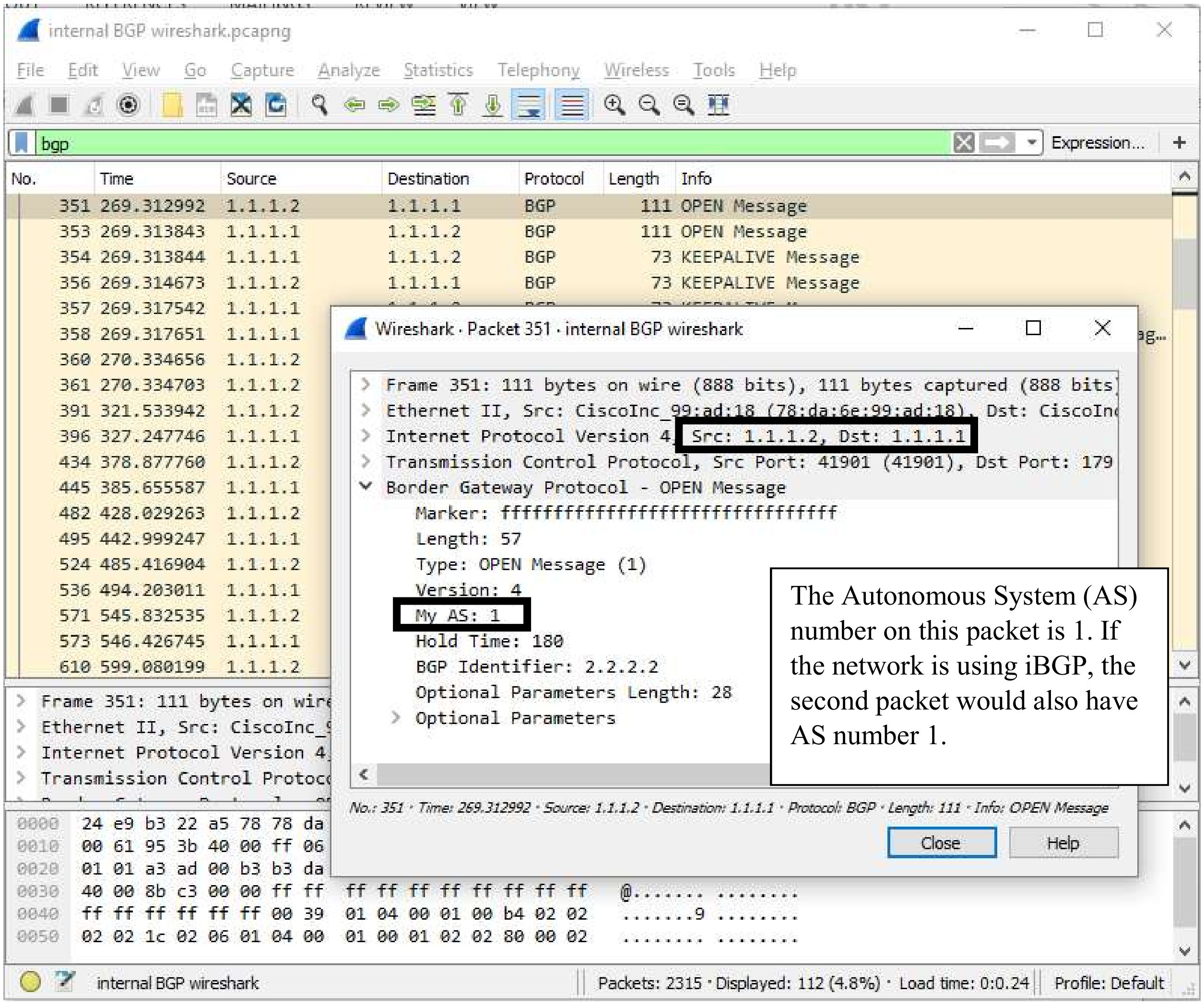
```
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 4.4.4.5 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 192.168.2.2 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 duplex auto
 speed auto
router eigrp 1
 network 4.4.4.0 0.0.0.255
router ospf 1
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.3.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
End
```

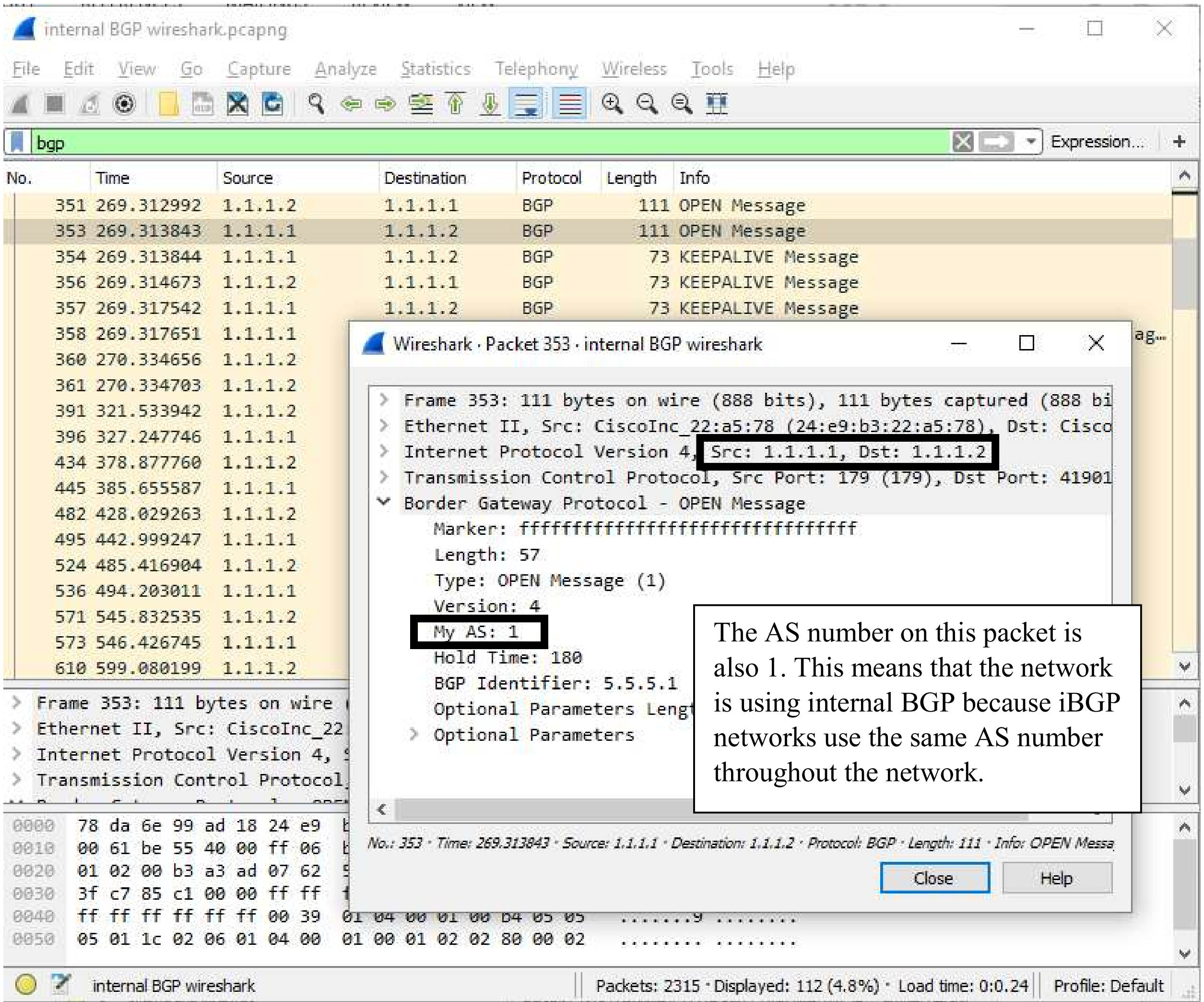
Show ip route

```
      1.0.0.0/24 is subnetted, 1 subnets
D EX     1.1.1.0 [170/25600512] via 4.4.4.4, 00:40:52,
GigabitEthernet0/0
      2.0.0.0/24 is subnetted, 1 subnets
D EX     2.2.2.0 [170/25600512] via 4.4.4.4, 00:40:52,
GigabitEthernet0/0
      3.0.0.0/24 is subnetted, 1 subnets
D EX     3.3.3.0 [170/3072] via 4.4.4.4, 00:40:57, GigabitEthernet0/0
      4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        4.4.4.0/24 is directly connected, GigabitEthernet0/0
L        4.4.4.5/32 is directly connected, GigabitEthernet0/0
      5.0.0.0/24 is subnetted, 1 subnets
D EX     5.5.5.0 [170/25600512] via 4.4.4.4, 00:40:52,
GigabitEthernet0/0
```

Proof of the BGP packets using Wireshark




internal BGP wireshark.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
bgp
Expression...
No. Time Source Destination Protocol Length Info
351 269.312992 1.1.1.2 1.1.1.1 BGP 111 OPEN Message
353 269.313843 1.1.1.1 1.1.1.2 BGP 111 OPEN Message
354 269.313844 1.1.1.1 1.1.1.2 BGP 73 KEEPALIVE Message
356 269.314673 1.1.1.2 1.1.1.1 BGP 73 KEEPALIVE Message
Wireshark · Packet 351 · internal BGP wireshark
Frame 351: 111 bytes on wire (888 bits), 111 bytes captured (888 bits)
Ethernet II, Src: CiscoInc_99:ad:18 (78:da:6e:99:ad:18), Dst: CiscoInc
Internet Protocol Version 4, Src: 1.1.1.2, Dst: 1.1.1.1
Transmission Control Protocol, Src Port: 41901 (41901), Dst Port: 179
Border Gateway Protocol - OPEN Message
Marker: ffffffffffffffffffffffffffffffff
Length: 57
Type: OPEN Message (1)
Version: 4
My AS: 1
Hold Time: 180
BGP Identifier: 2.2.2.2
Optional Parameters Length: 28
Optional Parameters
The Autonomous System (AS) number on this packet is 1. If the network is using iBGP, the second packet would also have AS number 1.
No.: 351 · Time: 269.312992 · Source: 1.1.1.2 · Destination: 1.1.1.1 · Protocol: BGP · Length: 111 · Info: OPEN Message
Close
Help
internal BGP wireshark
Packets: 2315 · Displayed: 112 (4.8%) · Load time: 0:0.24
Profile: Default



internal BGP wireshark.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
bgp
Expression...
No. Time Source Destination Protocol Length Info
351 269.312992 1.1.1.2 1.1.1.1 BGP 111 OPEN Message
353 269.313843 1.1.1.1 1.1.1.2 BGP 111 OPEN Message
354 269.313844 1.1.1.1 1.1.1.2 BGP 73 KEEPALIVE Message
356 269.314673 1.1.1.2 1.1.1.1 BGP 73 KEEPALIVE Message
357 269.317542 1.1.1.1 1.1.1.2 BGP 73 KEEPALIVE Message
Wireshark · Packet 353 · internal BGP wireshark
Frame 353: 111 bytes on wire (888 bits), 111 bytes captured (888 bi
Ethernet II, Src: CiscoInc_22:a5:78 (24:e9:b3:22:a5:78), Dst: Cisco
Internet Protocol Version 4, Src: 1.1.1.1, Dst: 1.1.1.2
Transmission Control Protocol, Src Port: 179 (179), Dst Port: 41901
Border Gateway Protocol - OPEN Message
Marker: ffffffffffffffffffffffffffffffff
Length: 57
Type: OPEN Message (1)
Version: 4
My AS: 1
Hold Time: 180
BGP Identifier: 5.5.5.1
Optional Parameters Lengt
Optional Parameters
The AS number on this packet is also 1. This means that the network is using internal BGP because iBGP networks use the same AS number throughout the network.
No.: 353 · Time: 269.313843 · Source: 1.1.1.1 · Destination: 1.1.1.2 · Protocol: BGP · Length: 111 · Info: OPEN Messa
Close
Help
internal BGP wireshark
Packets: 2315 · Displayed: 112 (4.8%) · Load time: 0:0.24
Profile: Default

Problems

When we first created our topology, we only had two routers in the Google's network and both of them were border routers. We later learned that we need a third router that is not a border router to prove that iBGP was working. But before figuring that problem out, we made another mistake.

Google's network is connected to the internet on one end and to PIE's network on the other. Those two connections are both using eBGP to establish connectivity. PIE and Google were just using EIGRP as their routing protocol. We knew that the only difference between iBGP and eBGP is that iBGP uses the same autonomous system numbers and eBGP uses different. We thought while configuring BGP on the two connections, we could just configure them with the same AS number, distribute BGP onto EIGRP and we will be good. We created end to end connectivity but that wasn't the point of the lab. We were not using iBGP. Google was using only using EIGRP and the other connections were in fact eBGP connections.

We realized that we were configuring eBGP and that the Google's network has to have both EIGRP and iBGP running, not just EIGRP by itself and EIGRP is not supposed to be distributed into eBGP. So we configured the two eBGP connections with different autonomous system numbers, and configured iBGP inside the Google's network as well as EIGRP with the same AS numbers. We finally configured iBGP successfully but now we needed to prove that we were running iBGP inside Google. To do that, we needed a router that wasn't a border router and only had internal BGP connections. However we only had two routers in Google and both of them were bordering an eBGP network.

We realized that we needed to add a new router to our topology, into the Google network that is not bordering a network with another protocol. So we added that router which required configuration and addressing changes throughout our network. At the end, all Google routers were running both iBGP and EIGRP, we had end to end connectivity in our network and we could prove that our network was using iBGP.

The last problem we had was a minor problem that we came across while fixing the topology and configuration problems we had. After we fixed the topology and entered the new configuration, we were able to prove that we were running iBGP but we did not have end to end connectivity. The routers in Google's network were not able to ping the routers in PIE's network. Before we started troubleshooting for a solution, we ran out of time that day. When we came back the other day, there were other configurations on the router from other people's labs so we reloaded the routers to get rid of their configurations. Then we entered our commands in and everything was working perfectly fine. We had the end to end connectivity and we were done with the lab. We are not totally sure on why we didn't have end to end connectivity the day before, but my guess is that we might have forgotten to erase the redistribution commands between eBGP and EIGRP networks. When we reloaded the routers, every command was erased including the redistribution commands, and we did not enter them again while entering the other commands to the network. I think they caused the problem that we fixed without realizing.

Conclusion

This lab was a rather easy and quick lab even though the topology caused a little confusion in the beginning. We first created two different networks, Google and PIE. Google had internet access and we were supposed to connect the two networks so PIE was able to connect to the internet. We configured iBGP on the Google to do that. Before this lab, I knew what eBGP and iBGP was, I knew the different and the commands to configure it but I have only configured eBGP before. This was first time configuring iBGP and it was almost the same as eBGP configurations and for that reason our configuration went fairly smoothly. It is a useful tool to connect two networks without changing configurations on all routers.

External BGP

Purpose

The purpose of this lab was to configure BGP and redistribute it to OSPF and EIGRP configured networks both in IPv4 and IPv6.

Background Information

Border Gateway Protocol (BGP) is another routing protocol like EIGRP and OSPF. The main goal of BGP and all other routing protocols is to establish connectivity between destinations that are more than a hop away. This can be any instance where there are one or more routers between the source and the destination. BGP works with different autonomous systems which is common to most routing protocols however, unlike other routing protocols, there are two different types of BGPs: Internal and external. Internal BGP is when the routers, that are using BGP, are all in the same autonomous system. On the other hand, external BGP uses multiple autonomous systems to establish connectivity between networks that use different autonomous systems.

We can view every autonomous system like a country. In internal BGP everyone is inside one country, speaking the same language and following the same rules and laws. In external BGP there are a lot of countries and packets that travel between them who are like tourists with visas. The embassies of tourists' home nations in other countries are like the external BGP, they do pretty much the same job. They help their citizens with legal help and protect them in foreign countries. Overall, they handle the legal transition between the two countries and ensure that tourists are safe and get to wherever they want to go to, just like BGP.

In this lab we also configured EIGRP and OSPF and unfortunately OSPF, EIGRP and BGP don't magically work with each other. In order for routing protocols to work with each other they have to be redistributed. By default, routers only advertise and share routes with other routers that are running the same routing protocol. So if there are 2 routers and one runs OSPF or EIGRP and the other runs BGP and they are supposed to know about each other's routes, by default, they won't share routing information because they are not running the same protocol. To fix this problem, route redistribution can be used so that 2 different protocols can still share and advertise routes to each other.

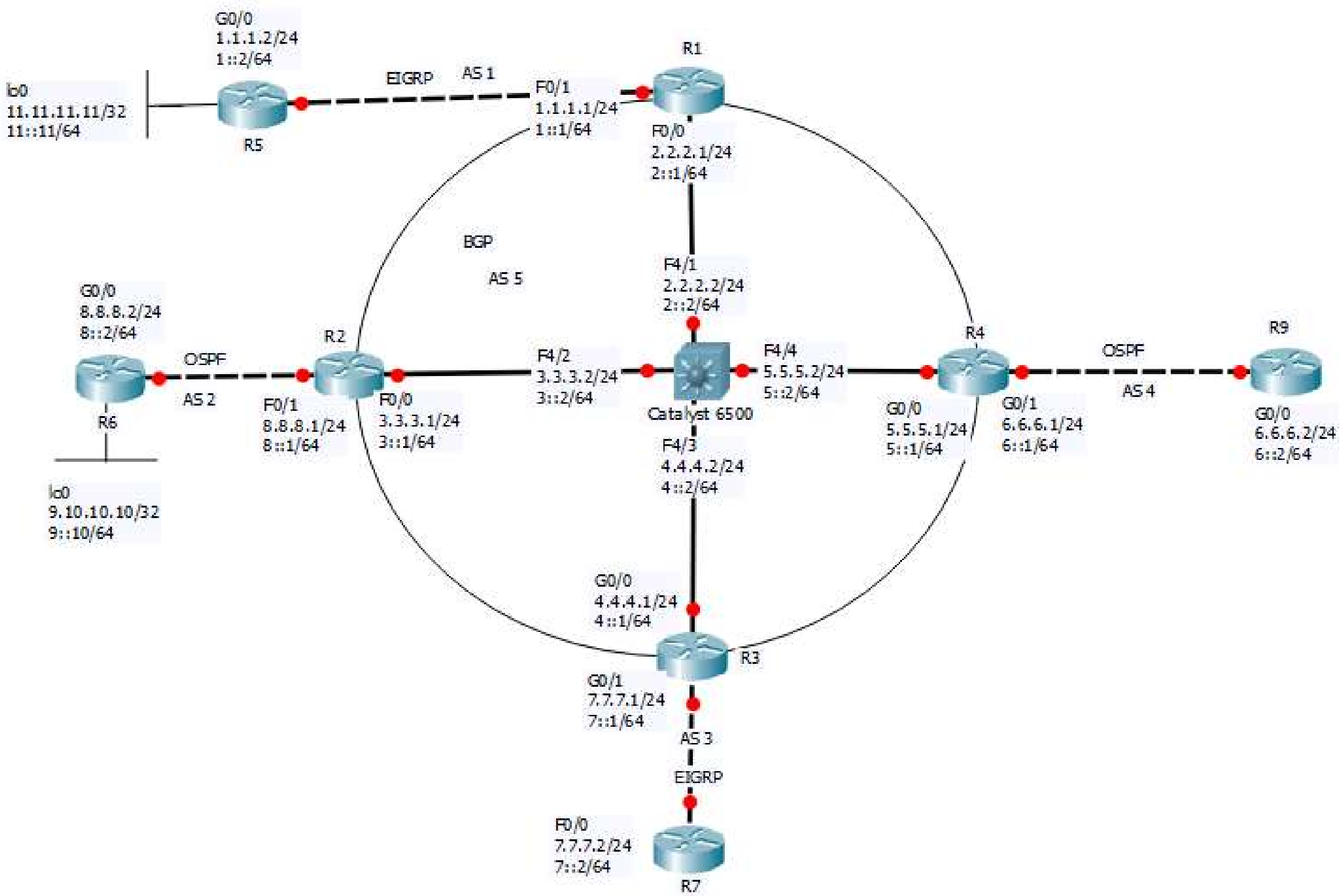
Lab Summary

We started with IPv4 first, we first configured EIGRP on R1, R5, R3 and R7 with the autonomous system number 1. Then we configured OSPF on R2, R6, R4 and R9 with the autonomous system number 1 and area 0. After checking the connectivity between EIGRP and OSPF router we moved onto configuring BGP on R1, R2, R3, R4 and catalyst 6500. These are also the border routers because they run more than one routing protocol except for the catalyst. We used different autonomous system numbers for all the border routers and the catalyst. Then we configured BGP on the catalyst 6500. We used the “neighbor” command to advertise the connected routes on a router to other routers that were using BGP. Once we configured BGP on the border routers and the catalyst, we checked the connectivity between all the border routers. To establish connectivity between the end users such as R5, R6, R7, R9 we had to let EIGRP, OSPF and BGP exchange information with each other. In order to do that we had to redistribute those routing protocols between each other. We used the “redistribute” command to do that and after that we had connectivity between every router in the topology in IPv4.
We then moved onto IPv6. The configuration was pretty much the same as the IPv4 configuration except IPv6 commands had to be done under the IPv6 address family instead of IPv4 address family. After that we also established IPv6 connectivity between every router in the topology.

Lab Commands

router bgp *1*	This command creates and configures the BGP routing process.
redistribute connected	This command is entered under router eigrp, router ospf or router bgp and advertises the connected routes to the routing protocol that it is configured under.
redistribute bgp *1* **metric** *100 1 255 2 1500*	This command changes the metrics of the routing protocol that it is configured under and also advertises BGP 1 to the same routing protocol so that it can have connectivity with BGP.
neighbor *1.1.1.2* **remote-as** *1*	This command is used under router bgp and it advertises an external bgp network and its autonomous system number to the BGP on the router where this command is entered.
address-family ipv4	This command places the router in address family configuration mode from which you can configure routing sessions that use IPv4. This command also keeps the IPv4 commands together in one place.
neighbor *1.1.1.2* **activate**	This command enables the exchange of information with a BGP neighbor which is the destination with IP address 1.1.1.2 in this case.
redistribute ospf *1* **match internal external** *1* **external** *2*	This command redistributes OSPF on external 1 and 2 routes.
redistribute bgp *2* **subnets**	This command is used when pulling routes into OSPF, without “subnets” keyword, only the classful address will be redistributed, not the subnets.

Network Diagram



Configurations

R1

Show run

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
boot-start-marker
boot system flash:
boot-end-marker
logging message-counter syslog
no aaa new-model
memory-size iomem 10
no network-clock-participate slot 1
dot11 syslog
ip source-route
ip cef
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
voice-card 0
 no dspfarm
voice-card 1
 no dspfarm
vtp domain cisco
vtp mode transparent
archive
 log config
  hidekeys
vlan 2
interface FastEthernet0/0
 ip address 2.2.2.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2::1/64
 ipv6 eigrp 1
interface FastEthernet0/1
 ip address 1.1.1.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 1::1/64
 ipv6 eigrp 1
interface FastEthernet0/0/0
interface FastEthernet0/0/1
interface FastEthernet0/0/2
interface FastEthernet0/0/3
interface Serial0/1/0
 no ip address
```

```
 shutdown
interface Serial0/2/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/2/1
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/3/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/3/1
 no ip address
 shutdown
 clock rate 2000000
interface Vlan1
 no ip address
router eigrp 1
 redistribute connected
 redistribute bgp 1 metric 100 1 255 2 1500
 network 1.1.1.0 0.0.0.255
 network 2.2.2.0 0.0.0.255
 no auto-summary
 eigrp router-id 1.1.1.1
router bgp 1
 bgp log-neighbor-changes
 neighbor 1::2 remote-as 1
 neighbor 2::2 remote-as 5
 neighbor 1.1.1.2 remote-as 1
 neighbor 2.2.2.2 remote-as 5
  address-family ipv4
  redistribute connected
  redistribute eigrp 1
  no neighbor 1::2 activate
  no neighbor 2::2 activate
  neighbor 1.1.1.2 activate
  neighbor 2.2.2.2 activate
  no auto-summary
  no synchronization
 exit-address-family
 address-family ipv6
  neighbor 1::2 activate
  neighbor 2::2 activate
  redistribute connected
  redistribute eigrp 1
  no synchronization
 exit-address-family
ip forward-protocol nd
no ip http server
no ip http secure-server
```

```
ipv6 router eigrp 1
 eigrp router-id 3.3.3.3
 no shutdown
 redistribute bgp 1 metric 100 1 255 2 1500
control-plane
voice-port 1/0/0
voice-port 1/0/1
voice-port 1/0/2
voice-port 1/0/3
voice-port 1/1/0
voice-port 1/1/1
line con 0
line aux 0
line vty 0 4
 login
scheduler allocate 20000 1000
end
```

Show ip route

```
Gateway of last resort is not set
     1.0.0.0/24 is subnetted, 1 subnets
C       1.1.1.0 is directly connected, FastEthernet0/1
     2.0.0.0/24 is subnetted, 1 subnets
C       2.2.2.0 is directly connected, FastEthernet0/0
     3.0.0.0/24 is subnetted, 1 subnets
B       3.3.3.0 [20/0] via 2.2.2.2, 00:33:07
     4.0.0.0/24 is subnetted, 1 subnets
B       4.4.4.0 [20/0] via 2.2.2.2, 00:33:07
     5.0.0.0/24 is subnetted, 1 subnets
B       5.5.5.0 [20/0] via 2.2.2.2, 00:33:07
     6.0.0.0/24 is subnetted, 1 subnets
B       6.6.6.0 [20/0] via 2.2.2.2, 01:05:41
     7.0.0.0/24 is subnetted, 1 subnets
B       7.7.7.0 [20/0] via 2.2.2.2, 01:04:35
     8.0.0.0/24 is subnetted, 1 subnets
B       8.8.8.0 [20/0] via 2.2.2.2, 01:05:10
     9.0.0.0/32 is subnetted, 1 subnets
B       9.10.10.10 [20/0] via 2.2.2.2, 00:01:57
     11.0.0.0/32 is subnetted, 1 subnets
D       11.11.11.11 [90/156160] via 1.1.1.2, 00:00:04, FastEthernet0/1
```

Show ipv6 route

```
C   1::/64 [0/0]
     via FastEthernet0/1, directly connected
L   1::1/128 [0/0]
     via FastEthernet0/1, receive
C   2::/64 [0/0]
     via FastEthernet0/0, directly connected
L   2::1/128 [0/0]
     via FastEthernet0/0, receive
B   3::/64 [20/0]
```

```
     via FE80::2D0:2BFF:FE15:1100, FastEthernet0/0
B   4::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, FastEthernet0/0
B   5::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, FastEthernet0/0
B   6::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, FastEthernet0/0
B   7::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, FastEthernet0/0
B   8::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, FastEthernet0/0
B   9::10/128 [20/0]
     via FE80::2D0:2BFF:FE15:1100, FastEthernet0/0
D   11::/64 [90/156160]
     via FE80::EAB7:48FF:FE6E:88, FastEthernet0/1
L   FF00::/8 [0/0]
     via Null0, receive
```

R2
Show run

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R2
boot-start-marker
boot system flash:
boot-end-marker
logging message-counter syslog
no aaa new-model
memory-size iomem 10
dot11 syslog
ip source-route
ip cef
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
voice-card 0
 no dspfarm
crypto pki token default removal timeout 0
vtp domain cisco
vtp mode transparent
archive
 log config
  hidekeys
interface FastEthernet0/0
 ip address 3.3.3.1 255.255.255.0
 ip ospf network broadcast
 duplex auto
 speed auto
```

```
 ipv6 address 3::1/64
 ipv6 ospf network broadcast
 ipv6 ospf 1 area 0
interface FastEthernet0/1
 ip address 8.8.8.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 8::1/64
 ipv6 ospf 1 area 0
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router ospf 1
 log-adjacency-changes
 no auto-cost
 redistribute connected
 redistribute bgp 2 subnets
 network 3.3.3.0 0.0.0.255 area 0
 network 8.8.8.0 0.0.0.255 area 0
router ospf 2
 log-adjacency-changes
router bgp 2
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 3::2 remote-as 5
 neighbor 8::2 remote-as 2
 neighbor 3.3.3.2 remote-as 5
 neighbor 8.8.8.2 remote-as 2
 address-family ipv4
  redistribute connected
  redistribute ospf 1 match internal external 1 external 2
  neighbor 3.3.3.2 activate
  neighbor 8.8.8.2 activate
  no auto-summary
  synchronization
 exit-address-family
 address-family ipv6
  neighbor 3::2 activate
  neighbor 8::2 activate
  redistribute connected
  redistribute ospf 1 match internal external 1 external 2
  synchronization
 exit-address-family
ip forward-protocol nd
no ip http server
no ip http secure-server
```

```
ipv6 router ospf 1
 log-adjacency-changes
 redistribute connected
 redistribute bgp 2 metric 100
control-plane
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
Gateway of last resort is not set
     1.0.0.0/24 is subnetted, 1 subnets
B       1.1.1.0 [20/0] via 3.3.3.2, 01:07:22
     2.0.0.0/24 is subnetted, 1 subnets
B       2.2.2.0 [20/0] via 3.3.3.2, 00:34:48
     3.0.0.0/24 is subnetted, 1 subnets
C       3.3.3.0 is directly connected, FastEthernet0/0
     4.0.0.0/24 is subnetted, 1 subnets
B       4.4.4.0 [20/0] via 3.3.3.2, 00:34:48
     5.0.0.0/24 is subnetted, 1 subnets
B       5.5.5.0 [20/0] via 3.3.3.2, 00:34:48
     6.0.0.0/24 is subnetted, 1 subnets
B       6.6.6.0 [20/0] via 3.3.3.2, 01:07:23
     7.0.0.0/24 is subnetted, 1 subnets
B       7.7.7.0 [20/0] via 3.3.3.2, 01:06:17
     8.0.0.0/24 is subnetted, 1 subnets
C       8.8.8.0 is directly connected, FastEthernet0/1
     9.0.0.0/32 is subnetted, 1 subnets
O       9.10.10.10 [110/11] via 8.8.8.2, 00:03:39, FastEthernet0/1
     11.0.0.0/32 is subnetted, 1 subnets
B       11.11.11.11 [20/0] via 3.3.3.2, 00:01:46
```

Show ipv6 route

```
B   1::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, FastEthernet0/0
B   2::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, FastEthernet0/0
C   3::/64 [0/0]
     via FastEthernet0/0, directly connected
L   3::1/128 [0/0]
     via FastEthernet0/0, receive
B   4::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, FastEthernet0/0
B   5::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, FastEthernet0/0
B   6::/64 [20/0]
```

```
     via FE80::2D0:2BFF:FE15:1100, FastEthernet0/0
B   7::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, FastEthernet0/0
C   8::/64 [0/0]
     via FastEthernet0/1, directly connected
L   8::1/128 [0/0]
     via FastEthernet0/1, receive
O   9::10/128 [110/1]
     via FE80::4255:39FF:FEB7:61E8, FastEthernet0/1
B   11::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, FastEthernet0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

R3
Show run

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R3
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180M8
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
archive
 log config
  hidekeys
vtp domain cisco
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 4.4.4.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 4::1/64
 ipv6 eigrp 1
interface GigabitEthernet0/1
```

```
 ip address 7.7.7.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 7::1/64
 ipv6 eigrp 1
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router eigrp 1
 network 4.4.4.0 0.0.0.255
 network 7.7.7.0 0.0.0.255
 redistribute bgp 3 metric 100 1 255 1 1500
 redistribute connected
router bgp 3
 bgp log-neighbor-changes
 neighbor 4::2 remote-as 5
 neighbor 7::2 remote-as 3
 neighbor 4.4.4.2 remote-as 5
 neighbor 7.7.7.2 remote-as 3
 address-family ipv4
  redistribute connected
  redistribute eigrp 1
  no neighbor 4::2 activate
  no neighbor 7::2 activate
  neighbor 4.4.4.2 activate
  neighbor 7.7.7.2 activate
 exit-address-family
 address-family ipv6
  redistribute connected
  redistribute eigrp 1
  neighbor 4::2 activate
  neighbor 7::2 activate
 exit-address-family
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router eigrp 1
 eigrp router-id 2.2.2.2
 redistribute bgp 3 metric 100 1 255 1 1500
control-plane
mgcp fax t38 ecm
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
```

```
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
      1.0.0.0/24 is subnetted, 1 subnets
B        1.1.1.0 [20/0] via 4.4.4.2, 01:07:56
      2.0.0.0/24 is subnetted, 1 subnets
B        2.2.2.0 [20/0] via 4.4.4.2, 00:35:22
      3.0.0.0/24 is subnetted, 1 subnets
B        3.3.3.0 [20/0] via 4.4.4.2, 00:35:22
      4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        4.4.4.0/24 is directly connected, GigabitEthernet0/0
L        4.4.4.1/32 is directly connected, GigabitEthernet0/0
      5.0.0.0/24 is subnetted, 1 subnets
B        5.5.5.0 [20/0] via 4.4.4.2, 00:35:22
      6.0.0.0/24 is subnetted, 1 subnets
B        6.6.6.0 [20/0] via 4.4.4.2, 01:07:56
      7.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        7.7.7.0/24 is directly connected, GigabitEthernet0/1
L        7.7.7.1/32 is directly connected, GigabitEthernet0/1
      8.0.0.0/24 is subnetted, 1 subnets
B        8.8.8.0 [20/0] via 4.4.4.2, 01:07:25
      9.0.0.0/32 is subnetted, 1 subnets
B        9.10.10.10 [20/0] via 4.4.4.2, 00:04:12
      11.0.0.0/32 is subnetted, 1 subnets
B        11.11.11.11 [20/0] via 4.4.4.2, 00:02:19
```

Show ipv6 route

```
B   1::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, GigabitEthernet0/0
B   2::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, GigabitEthernet0/0
B   3::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, GigabitEthernet0/0
C   4::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   4::1/128 [0/0]
     via GigabitEthernet0/0, receive
B   5::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, GigabitEthernet0/0
B   6::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, GigabitEthernet0/0
```

```
C   7::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   7::1/128 [0/0]
     via GigabitEthernet0/1, receive
B   8::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, GigabitEthernet0/0
B   9::10/128 [20/0]
     via FE80::2D0:2BFF:FE15:1100, GigabitEthernet0/0
B   11::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, GigabitEthernet0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

R4
Show run

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R4
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180M5
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
archive
 log config
  hidekeys
vtp domain cisco
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 5.5.5.1 255.255.255.0
 ip ospf network broadcast
 duplex auto
 speed auto
 ipv6 address 5::1/64
 ipv6 ospf 1 area 0
 ipv6 ospf network broadcast
```

```
interface GigabitEthernet0/1
 ip address 6.6.6.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 6::1/64
 ipv6 ospf 1 area 0
interface Serial0/0/0
 no ip address
 shutdown
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router ospf 1
 no auto-cost
 redistribute connected
 redistribute bgp 4 subnets
 network 5.5.5.0 0.0.0.255 area 0
 network 6.6.6.0 0.0.0.255 area 0
router bgp 4
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 5::2 remote-as 5
 neighbor 6::2 remote-as 4
 neighbor 5.5.5.2 remote-as 5
 neighbor 6.6.6.2 remote-as 4
 address-family ipv4
  redistribute connected
  redistribute ospf 1 match internal external 1 external 2
  neighbor 5.5.5.2 activate
  neighbor 6.6.6.2 activate
 exit-address-family
 address-family ipv6
  redistribute connected
  redistribute ospf 1 match internal external 1 external 2
  neighbor 5::2 activate
  neighbor 6::2 activate
 exit-address-family
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
 redistribute connected
 redistribute bgp 4 metric 100
control-plane
mgcp fax t38 ecm
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
```

```
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
      1.0.0.0/24 is subnetted, 1 subnets
B        1.1.1.0 [20/0] via 5.5.5.2, 01:08:30
      2.0.0.0/24 is subnetted, 1 subnets
B        2.2.2.0 [20/0] via 5.5.5.2, 00:35:56
      3.0.0.0/24 is subnetted, 1 subnets
B        3.3.3.0 [20/0] via 5.5.5.2, 00:35:56
      4.0.0.0/24 is subnetted, 1 subnets
B        4.4.4.0 [20/0] via 5.5.5.2, 00:35:56
      5.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        5.5.5.0/24 is directly connected, GigabitEthernet0/0
L        5.5.5.1/32 is directly connected, GigabitEthernet0/0
      6.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        6.6.6.0/24 is directly connected, GigabitEthernet0/1
L        6.6.6.1/32 is directly connected, GigabitEthernet0/1
      7.0.0.0/24 is subnetted, 1 subnets
B        7.7.7.0 [20/0] via 5.5.5.2, 01:07:24
      8.0.0.0/24 is subnetted, 1 subnets
B        8.8.8.0 [20/0] via 5.5.5.2, 01:07:58
      9.0.0.0/32 is subnetted, 1 subnets
B        9.10.10.10 [20/0] via 5.5.5.2, 00:04:46
      11.0.0.0/32 is subnetted, 1 subnets
B        11.11.11.11 [20/0] via 5.5.5.2, 00:02:53
```

Show ipv6 route

```
B   1::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, GigabitEthernet0/0
B   2::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, GigabitEthernet0/0
B   3::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, GigabitEthernet0/0
B   4::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, GigabitEthernet0/0
C   5::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   5::1/128 [0/0]
     via GigabitEthernet0/0, receive
C   6::/64 [0/0]
     via GigabitEthernet0/1, directly connected
```

```
L   6::1/128 [0/0]
     via GigabitEthernet0/1, receive
B   7::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, GigabitEthernet0/0
B   8::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, GigabitEthernet0/0
B   9::10/128 [20/0]
     via FE80::2D0:2BFF:FE15:1100, GigabitEthernet0/0
B   11::/64 [20/0]
     via FE80::2D0:2BFF:FE15:1100, GigabitEthernet0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

R5
Show run

```
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R5
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ipv6 unicast-routing
ipv6 cef
ip source-route
ip cef
no ip domain lookup
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX15208074
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
archive
 log config
  hidekeys
vtp domain cisco
vtp mode transparent
redundancy
interface Loopback0
 ip address 11.11.11.11 255.255.255.255
 ipv6 address 11::11/64
 ipv6 eigrp 1
interface GigabitEthernet0/0
 ip address 1.1.1.2 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 1::2/64
 ipv6 eigrp 1
```

```
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 router eigrp 1
 network 1.1.1.0 0.0.0.255
 network 11.11.11.11 0.0.0.0
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router eigrp 1
 eigrp router-id 4.4.4.4
control-plane
mgcp fax t38 ecm
gatekeeper
 shutdown
line con 0
line aux 0
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, GigabitEthernet0/0
L        1.1.1.2/32 is directly connected, GigabitEthernet0/0
      2.0.0.0/24 is subnetted, 1 subnets
D        2.2.2.0 [90/30720] via 1.1.1.1, 00:33:32, GigabitEthernet0/0
      3.0.0.0/24 is subnetted, 1 subnets
D EX     3.3.3.0 [170/25602816] via 1.1.1.1, 00:22:19,
GigabitEthernet0/0
      4.0.0.0/24 is subnetted, 1 subnets
D EX     4.4.4.0 [170/25602816] via 1.1.1.1, 00:22:20,
GigabitEthernet0/0
      5.0.0.0/24 is subnetted, 1 subnets
D EX     5.5.5.0 [170/25602816] via 1.1.1.1, 00:22:20,
GigabitEthernet0/0
      6.0.0.0/24 is subnetted, 1 subnets
D EX     6.6.6.0 [170/25602816] via 1.1.1.1, 00:22:20,
GigabitEthernet0/0
      7.0.0.0/24 is subnetted, 1 subnets
```

```
D EX     7.7.7.0 [170/25602816] via 1.1.1.1, 00:22:21,
GigabitEthernet0/0
      8.0.0.0/24 is subnetted, 1 subnets
D EX     8.8.8.0 [170/25602816] via 1.1.1.1, 00:22:21,
GigabitEthernet0/0
      9.0.0.0/32 is subnetted, 1 subnets
D EX     9.10.10.10 [170/25602816] via 1.1.1.1, 00:05:33,
GigabitEthernet0/0
      11.0.0.0/32 is subnetted, 1 subnets
C        11.11.11.11 is directly connected, Loopback0
```

Show ipv6 route

```
C   1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   1::2/128 [0/0]
     via GigabitEthernet0/0, receive
D   2::/64 [90/30720]
     via FE80::218:19FF:FE69:A2E1, GigabitEthernet0/0
EX  3::/64 [170/25605376]
     via FE80::218:19FF:FE69:A2E1, GigabitEthernet0/0
EX  4::/64 [170/25605376]
     via FE80::218:19FF:FE69:A2E1, GigabitEthernet0/0
EX  5::/64 [170/25605376]
     via FE80::218:19FF:FE69:A2E1, GigabitEthernet0/0
EX  6::/64 [170/25605376]
     via FE80::218:19FF:FE69:A2E1, GigabitEthernet0/0
EX  7::/64 [170/25605376]
     via FE80::218:19FF:FE69:A2E1, GigabitEthernet0/0
EX  8::/64 [170/25605376]
     via FE80::218:19FF:FE69:A2E1, GigabitEthernet0/0
EX  9::10/128 [170/25605376]
     via FE80::218:19FF:FE69:A2E1, GigabitEthernet0/0
C   11::/64 [0/0]
     via Loopback0, directly connected
L   11::11/128 [0/0]
     via Loopback0, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

IPv4 Pings

```
R5#ping 6.6.6.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R5#ping 7.7.7.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7.7.7.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R5#ping 9.10.10.10
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 9.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

R6
Show run

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R6
boot-start-marker
boot-end-marker
logging snmp-authfail
no aaa new-model
memory-size iomem 10
ip cef
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX1520806E
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
vtp mode transparent
redundancy
interface Loopback0
 ip address 9.10.10.10 255.255.255.255
 ipv6 address 9::10/64
 ipv6 ospf 1 area 0
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 8.8.8.2 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 8::2/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
```

```
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 duplex auto
 speed auto
router ospf 1
 no auto-cost
 network 8.8.8.0 0.0.0.255 area 0
 network 9.10.10.10 0.0.0.0 area 0
router ospf 2
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
control-plane
 mgcp profile default
gatekeeper
 shutdown
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
      1.0.0.0/24 is subnetted, 1 subnets
O E2     1.1.1.0 [110/1] via 8.8.8.1, 01:08:46, GigabitEthernet0/0
      2.0.0.0/24 is subnetted, 1 subnets
O E2     2.2.2.0 [110/1] via 8.8.8.1, 01:08:46, GigabitEthernet0/0
      3.0.0.0/24 is subnetted, 1 subnets
O        3.3.3.0 [110/20] via 8.8.8.1, 00:49:33, GigabitEthernet0/0
      4.0.0.0/24 is subnetted, 1 subnets
O E2     4.4.4.0 [110/1] via 8.8.8.1, 01:08:46, GigabitEthernet0/0
      5.0.0.0/24 is subnetted, 1 subnets
O E2     5.5.5.0 [110/1] via 8.8.8.1, 01:08:46, GigabitEthernet0/0
      6.0.0.0/24 is subnetted, 1 subnets
O E2     6.6.6.0 [110/1] via 8.8.8.1, 01:08:46, GigabitEthernet0/0
      7.0.0.0/24 is subnetted, 1 subnets
```

```
O E2     7.7.7.0 [110/1] via 8.8.8.1, 01:08:45, GigabitEthernet0/0
      8.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        8.8.8.0/24 is directly connected, GigabitEthernet0/0
L        8.8.8.2/32 is directly connected, GigabitEthernet0/0
      9.0.0.0/32 is subnetted, 1 subnets
C        9.10.10.10 is directly connected, Loopback0
      11.0.0.0/32 is subnetted, 1 subnets
O E2     11.11.11.11 [110/1] via 8.8.8.1, 00:04:14, GigabitEthernet0/0
```

Show ipv6 route

```
OE2 1::/64 [110/100]
     via FE80::21E:F7FF:FE5E:F129, GigabitEthernet0/0
OE2 2::/64 [110/100]
     via FE80::21E:F7FF:FE5E:F129, GigabitEthernet0/0
O   3::/64 [110/2]
     via FE80::21E:F7FF:FE5E:F129, GigabitEthernet0/0
OE2 4::/64 [110/100]
     via FE80::21E:F7FF:FE5E:F129, GigabitEthernet0/0
OE2 5::/64 [110/100]
     via FE80::21E:F7FF:FE5E:F129, GigabitEthernet0/0
OE2 6::/64 [110/100]
     via FE80::21E:F7FF:FE5E:F129, GigabitEthernet0/0
OE2 7::/64 [110/100]
     via FE80::21E:F7FF:FE5E:F129, GigabitEthernet0/0
C   8::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   8::2/128 [0/0]
     via GigabitEthernet0/0, receive
C   9::/64 [0/0]
     via Loopback0, directly connected
L   9::10/128 [0/0]
     via Loopback0, receive
OE2 11::/64 [110/100]
     via FE80::21E:F7FF:FE5E:F129, GigabitEthernet0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

IPv4 Pings

```
R6#ping 11.11.11.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.11.11.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R6#ping 6.6.6.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R6#ping 7.7.7.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7.7.7.2, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

R7
Show run

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R7
boot-start-marker
boot-end-marker
logging message-counter syslog
no aaa new-model
memory-size iomem 10
dot11 syslog
ip source-route
ip cef
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
voice-card 0
 no dspfarm
vtp domain cisco
vtp mode transparent
archive
 log config
  hidekeys
interface FastEthernet0/0
 ip address 7.7.7.2 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 7::2/64
 ipv6 eigrp 1
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/1/0
 no ip address
 shutdown
```

```
 clock rate 2000000
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
router eigrp 1
 network 7.7.7.0 0.0.0.255
 no auto-summary
router bgp 3
 no synchronization
 bgp log-neighbor-changes
 no auto-summary
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router eigrp 1
 eigrp router-id 1.1.1.1
 no shutdown
control-plane
mgcp behavior g729-variants static-pt
line con 0
line aux 0
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
     1.0.0.0/24 is subnetted, 1 subnets
D EX    1.1.1.0 [170/25602816] via 7.7.7.1, 00:24:15, FastEthernet0/0
     2.0.0.0/24 is subnetted, 1 subnets
D EX    2.2.2.0 [170/25602816] via 7.7.7.1, 00:24:15, FastEthernet0/0
     3.0.0.0/24 is subnetted, 1 subnets
D EX    3.3.3.0 [170/25602816] via 7.7.7.1, 00:24:15, FastEthernet0/0
     4.0.0.0/24 is subnetted, 1 subnets
D       4.4.4.0 [90/30720] via 7.7.7.1, 00:51:51, FastEthernet0/0
     5.0.0.0/24 is subnetted, 1 subnets
D EX    5.5.5.0 [170/25602816] via 7.7.7.1, 00:24:17, FastEthernet0/0
     6.0.0.0/24 is subnetted, 1 subnets
D EX    6.6.6.0 [170/25602816] via 7.7.7.1, 00:24:17, FastEthernet0/0
     7.0.0.0/24 is subnetted, 1 subnets
C       7.7.7.0 is directly connected, FastEthernet0/0
     8.0.0.0/24 is subnetted, 1 subnets
D EX    8.8.8.0 [170/25602816] via 7.7.7.1, 00:24:17, FastEthernet0/0
     9.0.0.0/32 is subnetted, 1 subnets
D EX    9.10.10.10 [170/25602816] via 7.7.7.1, 00:06:41,
FastEthernet0/0
     11.0.0.0/32 is subnetted, 1 subnets
D EX    11.11.11.11 [170/25602816] via 7.7.7.1, 00:04:48,
FastEthernet0/0
```

Show ipv6 route

```
EX  1::/64 [170/25602816]
     via FE80::7ADA:6EFF:FE99:AA01, FastEthernet0/0
EX  2::/64 [170/25602816]
     via FE80::7ADA:6EFF:FE99:AA01, FastEthernet0/0
EX  3::/64 [170/25602816]
     via FE80::7ADA:6EFF:FE99:AA01, FastEthernet0/0
D   4::/64 [90/30720]
     via FE80::7ADA:6EFF:FE99:AA01, FastEthernet0/0
EX  5::/64 [170/25602816]
     via FE80::7ADA:6EFF:FE99:AA01, FastEthernet0/0
EX  6::/64 [170/25602816]
     via FE80::7ADA:6EFF:FE99:AA01, FastEthernet0/0
C   7::/64 [0/0]
     via FastEthernet0/0, directly connected
L   7::2/128 [0/0]
     via FastEthernet0/0, receive
EX  8::/64 [170/25602816]
     via FE80::7ADA:6EFF:FE99:AA01, FastEthernet0/0
EX  9::10/128 [170/25602816]
     via FE80::7ADA:6EFF:FE99:AA01, FastEthernet0/0
EX  11::/64 [170/25602816]
     via FE80::7ADA:6EFF:FE99:AA01, FastEthernet0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

IPv4 Pings

```
R7#ping 11.11.11.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.11.11.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R7#ping 9.10.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 9.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R7#ping 6.6.6.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

IPv6 Pings

```
R7#ping 9::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 9::10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
R7#ping 11::11
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11::11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
R7#ping 6::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms
```

R9
Show run

```
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R9
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ipv6 unicast-routing
ipv6 cef
ip source-route
ip cef
no ip domain lookup
multilink bundle-name authenticated
crypto pki token default removal timeout 0
voice-card 0
license udi pid CISCO2901/K9 sn FTX1704Y03B
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
license boot module c2900 technology-package datak9
vtp domain cisco
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 6.6.6.2 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 6::2/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
interface Serial0/0/0
```

```
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router ospf 1
 no auto-cost
 network 6.6.6.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
      1.0.0.0/24 is subnetted, 1 subnets
O E2     1.1.1.0 [110/1] via 6.6.6.1, 01:10:47, GigabitEthernet0/0
      2.0.0.0/24 is subnetted, 1 subnets
O E2     2.2.2.0 [110/1] via 6.6.6.1, 01:10:47, GigabitEthernet0/0
      3.0.0.0/24 is subnetted, 1 subnets
O E2     3.3.3.0 [110/1] via 6.6.6.1, 01:10:47, GigabitEthernet0/0
      4.0.0.0/24 is subnetted, 1 subnets
O E2     4.4.4.0 [110/1] via 6.6.6.1, 01:10:47, GigabitEthernet0/0
      5.0.0.0/24 is subnetted, 1 subnets
O        5.5.5.0 [110/20] via 6.6.6.1, 00:50:02, GigabitEthernet0/0
      6.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        6.6.6.0/24 is directly connected, GigabitEthernet0/0
L        6.6.6.2/32 is directly connected, GigabitEthernet0/0
      7.0.0.0/24 is subnetted, 1 subnets
O E2     7.7.7.0 [110/1] via 6.6.6.1, 01:09:56, GigabitEthernet0/0
      8.0.0.0/24 is subnetted, 1 subnets
```

```
O E2     8.8.8.0 [110/1] via 6.6.6.1, 01:10:31, GigabitEthernet0/0
      9.0.0.0/32 is subnetted, 1 subnets
O E2     9.10.10.10 [110/1] via 6.6.6.1, 00:07:18, GigabitEthernet0/0
      11.0.0.0/32 is subnetted, 1 subnets
O E2     11.11.11.11 [110/1] via 6.6.6.1, 00:05:25, GigabitEthernet0/0
```

Show ipv6 route:

```
OE2 1::/64 [110/100]
     via FE80::26E9:B3FF:FE3C:1949, GigabitEthernet0/0
OE2 2::/64 [110/100]
     via FE80::26E9:B3FF:FE3C:1949, GigabitEthernet0/0
OE2 3::/64 [110/100]
     via FE80::26E9:B3FF:FE3C:1949, GigabitEthernet0/0
OE2 4::/64 [110/100]
     via FE80::26E9:B3FF:FE3C:1949, GigabitEthernet0/0
O   5::/64 [110/2]
     via FE80::26E9:B3FF:FE3C:1949, GigabitEthernet0/0
C   6::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   6::2/128 [0/0]
     via GigabitEthernet0/0, receive
OE2 7::/64 [110/100]
     via FE80::26E9:B3FF:FE3C:1949, GigabitEthernet0/0
OE2 8::/64 [110/100]
     via FE80::26E9:B3FF:FE3C:1949, GigabitEthernet0/0
OE2 9::10/128 [110/100]
     via FE80::26E9:B3FF:FE3C:1949, GigabitEthernet0/0
OE2 11::/64 [110/100]
     via FE80::26E9:B3FF:FE3C:1949, GigabitEthernet0/0
L   FF00::/8 [0/0]
     via Null0, receiveIPv4 Pings:
```

IPv4 Pings:

```
R9#ping 11.11.11.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.11.11.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R9#ping 9.10.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 9.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R9#ping 7.7.7.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7.7.7.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

IPv6 Pings:

```
R9#ping 7::2
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
R9#ping 9::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 9::10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
R9#ping 11::11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11::11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
```

Catalyst 6500:
Show run:

```
upgrade fpd auto
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service counters max age 5
hostname catalyst
boot-start-marker
boot system sup-bootdisk:s3223-advipservicesk9_wan-mz.122-33.SXH4.bin
boot-end-marker
no aaa new-model
call-home
  alert-group configuration
  alert-group diagnostic
  alert-group environment
  alert-group inventory
  alert-group syslog
 profile "CiscoTAC-1"
   no active
   no destination transport-method http
   destination transport-method email
   destination address email callhome@cisco.com
   destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
   subscribe-to-alert-group diagnostic severity minor
   subscribe-to-alert-group environment severity minor
   subscribe-to-alert-group syslog severity major pattern ".*"
   subscribe-to-alert-group configuration periodic monthly 25 13:19
   subscribe-to-alert-group inventory periodic monthly 25 13:04
ip subnet-zero
ipv6 unicast-routing
mls ip slb purge global
mls netflow interface
no mls flow ip
```

```
no mls flow ipv6
mls cef error action reset
redundancy
 keepalive-enable
 mode sso
 main-cpu
  auto-sync running-config
spanning-tree mode pvst
spanning-tree extend system-id
system flowcontrol bus auto
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
interface FastEthernet4/1
 ip address 2.2.2.2 255.255.255.0
 shutdown
 ipv6 address 2::2/64
interface FastEthernet4/2
 ip address 3.3.3.2 255.255.255.0
 shutdown
 ipv6 address 3::2/64
interface FastEthernet4/3
 ip address 4.4.4.2 255.255.255.0
 shutdown
 ipv6 address 4::2/64
interface FastEthernet4/4
 ip address 5.5.5.2 255.255.255.0
 shutdown
 ipv6 address 5::2/64
router bgp 5
 bgp log-neighbor-changes
 neighbor 2::1 remote-as 1
 neighbor 3::1 remote-as 2
 neighbor 4::1 remote-as 3
 neighbor 5::1 remote-as 4
 neighbor 2.2.2.1 remote-as 1
 neighbor 3.3.3.1 remote-as 2
 neighbor 4.4.4.1 remote-as 3
 neighbor 5.5.5.1 remote-as 4
 address-family ipv4
  redistribute connected
  redistribute eigrp 1
  redistribute ospf 1
  no neighbor 2::1 activate
  no neighbor 3::1 activate
  no neighbor 4::1 activate
  no neighbor 5::1 activate
  neighbor 2.2.2.1 activate
  neighbor 3.3.3.1 activate
  neighbor 4.4.4.1 activate
  neighbor 5.5.5.1 activate
```

```
  no auto-summary
  synchronization
 exit-address-family
 address-family ipv6
  neighbor 2::1 activate
  neighbor 3::1 activate
  neighbor 4::1 activate
  neighbor 5::1 activate
 exit-address-family
ip classless
no ip http server
no ip http secure-server
control-plane
dial-peer cor custom
line con 0
 logging synchronous
line vty 0 4
 login
line vty 5 15
 login
monitor session 1 source interface Fa4/1
monitor session 1 destination interface Fa4/11
end
```

Show ip route:

```
Gateway of last resort is not set
     1.0.0.0/24 is subnetted, 1 subnets
B       1.1.1.0 [20/0] via 2.2.2.1, 01:11:27
     2.0.0.0/24 is subnetted, 1 subnets
C       2.2.2.0 is directly connected, FastEthernet4/1
     3.0.0.0/24 is subnetted, 1 subnets
C       3.3.3.0 is directly connected, FastEthernet4/2
     4.0.0.0/24 is subnetted, 1 subnets
C       4.4.4.0 is directly connected, FastEthernet4/3
     5.0.0.0/24 is subnetted, 1 subnets
C       5.5.5.0 is directly connected, FastEthernet4/4
     6.0.0.0/24 is subnetted, 1 subnets
B       6.6.6.0 [20/0] via 5.5.5.1, 01:11:55
     7.0.0.0/24 is subnetted, 1 subnets
B       7.7.7.0 [20/0] via 4.4.4.1, 01:10:22
     8.0.0.0/24 is subnetted, 1 subnets
B       8.8.8.0 [20/0] via 3.3.3.1, 01:10:57
     9.0.0.0/32 is subnetted, 1 subnets
B       9.10.10.10 [20/11] via 3.3.3.1, 00:07:44
     11.0.0.0/32 is subnetted, 1 subnets
B       11.11.11.11 [20/156160] via 2.2.2.1, 00:05:51
```

Show ipv6 route:

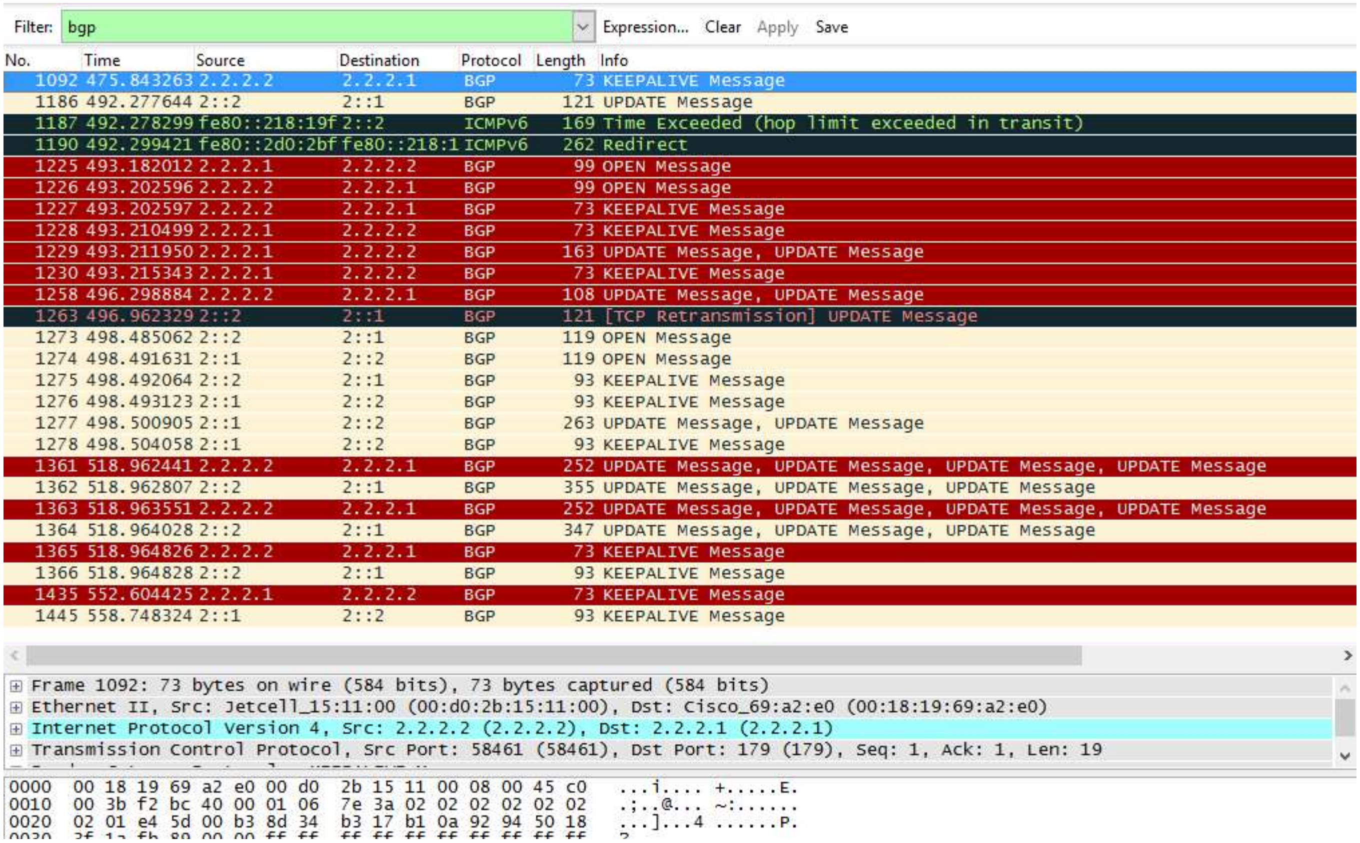
```
B   1::/64 [20/0]
     via FE80::218:19FF:FE69:A2E0, FastEthernet4/1
C   2::/64 [0/0]
```

```
     via FastEthernet4/1, directly connected
L   2::2/128 [0/0]
     via FastEthernet4/1, receive
C   3::/64 [0/0]
     via FastEthernet4/2, directly connected
L   3::2/128 [0/0]
     via FastEthernet4/2, receive
C   4::/64 [0/0]
     via FastEthernet4/3, directly connected
L   4::2/128 [0/0]
     via FastEthernet4/3, receive
C   5::/64 [0/0]
     via FastEthernet4/4, directly connected
L   5::2/128 [0/0]
     via FastEthernet4/4, receive
B   6::/64 [20/0]
     via FE80::26E9:B3FF:FE3C:1948, FastEthernet4/4
B   7::/64 [20/0]
     via FE80::7ADA:6EFF:FE99:AA00, FastEthernet4/3
B   8::/64 [20/0]
     via FE80::21E:F7FF:FE5E:F128, FastEthernet4/2
B   9::10/128 [20/1]
     via FE80::21E:F7FF:FE5E:F128, FastEthernet4/2
B   11::/64 [20/156160]
     via FE80::218:19FF:FE69:A2E0, FastEthernet4/1
L   FF00::/8 [0/0]
     via Null0, receive
```

IPv4 Pings:

```
catalyst#ping 11.11.11.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.11.11.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
catalyst#ping 9.10.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 9.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
catalyst#ping 7.7.7.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7.7.7.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
catalyst#ping 6.6.6.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

BGP Wireshark Capture:



Filter: bgp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1092	475.843263	2.2.2.2	2.2.2.1	BGP	73	KEEPALIVE Message
1186	492.277644	2::2	2::1	BGP	121	UPDATE Message
1187	492.278299	fe80::218:19f	2::2	ICMPv6	169	Time Exceeded (hop limit exceeded in transit)
1190	492.299421	fe80::2d0:2bf	fe80::218:1	ICMPv6	262	Redirect
1225	493.182012	2.2.2.1	2.2.2.2	BGP	99	OPEN Message
1226	493.202596	2.2.2.2	2.2.2.1	BGP	99	OPEN Message
1227	493.202597	2.2.2.2	2.2.2.1	BGP	73	KEEPALIVE Message
1228	493.210499	2.2.2.1	2.2.2.2	BGP	73	KEEPALIVE Message
1229	493.211950	2.2.2.1	2.2.2.2	BGP	163	UPDATE Message, UPDATE Message
1230	493.215343	2.2.2.1	2.2.2.2	BGP	73	KEEPALIVE Message
1258	496.298884	2.2.2.2	2.2.2.1	BGP	108	UPDATE Message, UPDATE Message
1263	496.962329	2::2	2::1	BGP	121	[TCP Retransmission] UPDATE Message
1273	498.485062	2::2	2::1	BGP	119	OPEN Message
1274	498.491631	2::1	2::2	BGP	119	OPEN Message
1275	498.492064	2::2	2::1	BGP	93	KEEPALIVE Message
1276	498.493123	2::1	2::2	BGP	93	KEEPALIVE Message
1277	498.500905	2::1	2::2	BGP	263	UPDATE Message, UPDATE Message
1278	498.504058	2::1	2::2	BGP	93	KEEPALIVE Message
1361	518.962441	2.2.2.2	2.2.2.1	BGP	252	UPDATE Message, UPDATE Message, UPDATE Message, UPDATE Message
1362	518.962807	2::2	2::1	BGP	355	UPDATE Message, UPDATE Message, UPDATE Message
1363	518.963551	2.2.2.2	2.2.2.1	BGP	252	UPDATE Message, UPDATE Message, UPDATE Message, UPDATE Message
1364	518.964028	2::2	2::1	BGP	347	UPDATE Message, UPDATE Message, UPDATE Message
1365	518.964826	2.2.2.2	2.2.2.1	BGP	73	KEEPALIVE Message
1366	518.964828	2::2	2::1	BGP	93	KEEPALIVE Message
1435	552.604425	2.2.2.1	2.2.2.2	BGP	73	KEEPALIVE Message
1445	558.748324	2::1	2::2	BGP	93	KEEPALIVE Message

Frame 1092: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
Ethernet II, Src: Jetcell_15:11:00 (00:d0:2b:15:11:00), Dst: Cisco_69:a2:e0 (00:18:19:69:a2:e0)
Internet Protocol Version 4, Src: 2.2.2.2 (2.2.2.2), Dst: 2.2.2.1 (2.2.2.1)
Transmission Control Protocol, Src Port: 58461 (58461), Dst Port: 179 (179), Seq: 1, Ack: 1, Len: 19

```
0000  00 18 19 69 a2 e0 00 d0  2b 15 11 00 08 00 45 c0   ...i.... +.....E.
0010  00 3b f2 bc 40 00 01 06  7e 3a 02 02 02 02 02 02   .;..@... ~:......
0020  02 01 e4 5d 00 b3 8d 34  b3 17 b1 0a 92 94 50 18   ...]...4 ......P.
```

Problems

We first configured IPv4 and we were able to ping between border routers with no problems but we were not able get to the routers in the OSPF and EIGRP networks. BGP was not being distributed right on the border routers even though we issued the “redistribute bgp AS” command under OSPF and EIGRP and “redistribute ospf AS” and “redistribute eigrp AS” command under BGP.

To fix the redistribution problem on OSPF we used the “redistribute bgp 2 subnets” and “redistribute connected” commands to redistribute OSPF into the BGP network and by doing that we were able to establish end-to-end connectivity between the OSPF networks.

We tried to do the same thing for the EIGRP networks but it didn’t work. There was something else different and we had a really hard finding it however after long hours of research we figured that we had to change the metrics of the EIGRP because the default metrics of EIGRP does not work with many other routing protocols including BGP. We also found the right metrics in order for the EIGRP to work with BGP and it was “100 1 255 2 1500”. After configuring the “redistribute bgp 1 metric 100 1 255 2 1500” command our IPv4 EIGRP networks established end to end connectivity too.

After we fully configured IPv4 in every network and were able ping any destination from any source we moved onto IPv6 configuration. The problem was we weren’t able to ping any address on the other side of the catalyst from any border router. So, BGP was not working. We went back and looked back at our configurations on the routers and realized that all the commands including IPv4 and IPv6 commands were under the IPv4 address family in BGP. However, IPv4 commands have to be under IPv4 address family and IPv6 commands have to be under IPv6 address family. In order to move the IPv6 command to the IPv6 address family, we first deleted them under the IPv4 address family and entered them under the IPv6 address family.

After fixing the address family problem in the routers that were running BGP, IPv6 BGP was working and we were able to ping any destination from any source.

Conclusion

This was the first time we ever used BGP. The configuration and the idea behind how it works is a little different than the routing protocols we learned to use. It was a little bit challenging to understand the idea on how BGP works but after understanding it, it was easy to configure it on a topology with 8 routers and a catalyst 6500. We had some problems with the redistribution of OSPF first then with EIGRP. The solution was a really easy and simple solution but it took a long time to figure out the problem. Overall it was quicker to configure IPv6 because by the time we were done with IPv4 we learned how BGP worked and knew what we were doing. So we were able to configure IPv6 really fast. There were some address family problems but it was an easy fix. This lab started off harder than I expected but finished easy.

Route Reflectors

Purpose

The purpose of this lab was to configure two route reflectors in a redundant network that was using internal BGP in order to minimize the number of neighbor commands in every router's configuration.

Background Information

While configuring internal BGP, IBGP requires full-mesh which can be a complicated process, so instead most networks use route reflectors to simplify configuration.

A mesh network is a local area network (LAN), wireless local area network (WLAN) or virtual LAN (VLAN) that employs one of two decentralized connection arrangements: full mesh topology or partial mesh topology. In a full mesh topology, each network node (workstation or other device) is connected directly to each of the others. In a partial mesh topology, some nodes are connected to all the others, but others are only connected to those nodes with which they exchange the most data.

In an IBGP network, when IBGP is configured, every directly connected router must be configured as a neighbor. So if the router that is being configured is directly connected to two other routers then it will need to have two different neighbor entries in its configuration. If it is connected to a hundred other routers, then it will have to have a hundred neighbor entries. That is how full mesh relates to IBGP. Going back to the example, every other router will need to have a hundred entrees if they are also connected to every other router. That is a lot of work and that's when route reflectors come into play.

So, a route reflector is a network routing component. It offers an alternative to the logical full-mesh requirement of IBGP. A route reflector acts as a focal point for IBGP sessions. The purpose of the RR is concentration. Multiple BGP routers can peer with a central point, the route reflector, which is acting as a route reflector server, rather than peer with every other router in a full mesh. All the other IBGP routers become route reflector clients.

This approach, similar to OSPF's DR/BDR feature, provides large networks with added IBGP scalability. Just like the previous example, in a fully meshed IBGP network of ten routers, ninety individual CLI statements that are spread throughout all routers in the topology are needed just to define the remote-AS of each peer. This can quickly become a pretty frustrating and boring thing to do for the network administrator and it will take a long time to enter those commands. A route reflector topology could cut these ninety statements down to eighteen, offering a viable solution for the larger networks administered by ISPs.

A route reflector is a single point of failure, therefore a second route reflector may be configured in order to provide redundancy. The additional route reflector would require some commands too but it still would be a lot less than configuring full mesh IBGP.

Route reflectors can be viewed like Google contacts. This is a feature Google offers to android users. The user uploads all of his/her contacts to Google contacts once. Every time he/she gets a new phone, he/she can go to Google contacts and download all of his/her contacts to his/her new phone. If this service Google offered for no charge did not exist, the person would have to enter his/her contacts to his/her new phone every time he/she gets a new phone. That can be really painful if the person has a lot of people in his/her contacts. Route reflectors do what Google contacts does but instead of storing people's contacts, route reflectors store the neighbor information of the routers in the IBGP network they are in.

Lab Summary

This lab had two steps to it. First, we configured a full mesh IBGP topology and created end-to-end connectivity in the network. On the second step, we used two route reflectors in the IBGP network to create end-to-end connectivity.

On the first step we connected five routers, a layer 3 switch and a catalyst 6500 to a layer 2 switch and created a network. We were using IBGP so every router was in the same autonomous system. We entered the IP addresses for the interfaces and created a loopback in every device except for the layer 2 switch. We did not configure anything on the layer 2 switch, it was just connecting every device in the network to each other, creating a full mesh network. On the other devices however, we configured their IP addresses and then we configured IBGP on every router, layer 3 switch and catalyst 6500. Since it was a full mesh network, we entered the addresses of every neighbor under the BGP configuration of every device. Then we redistributed the connected links of the routers with other devices so that the loopbacks could ping each other. After doing those configurations on every device except for the layer 2 switch, we were able to ping every address in the network from any device and we were able to see all the routes in the routing table of the routers.

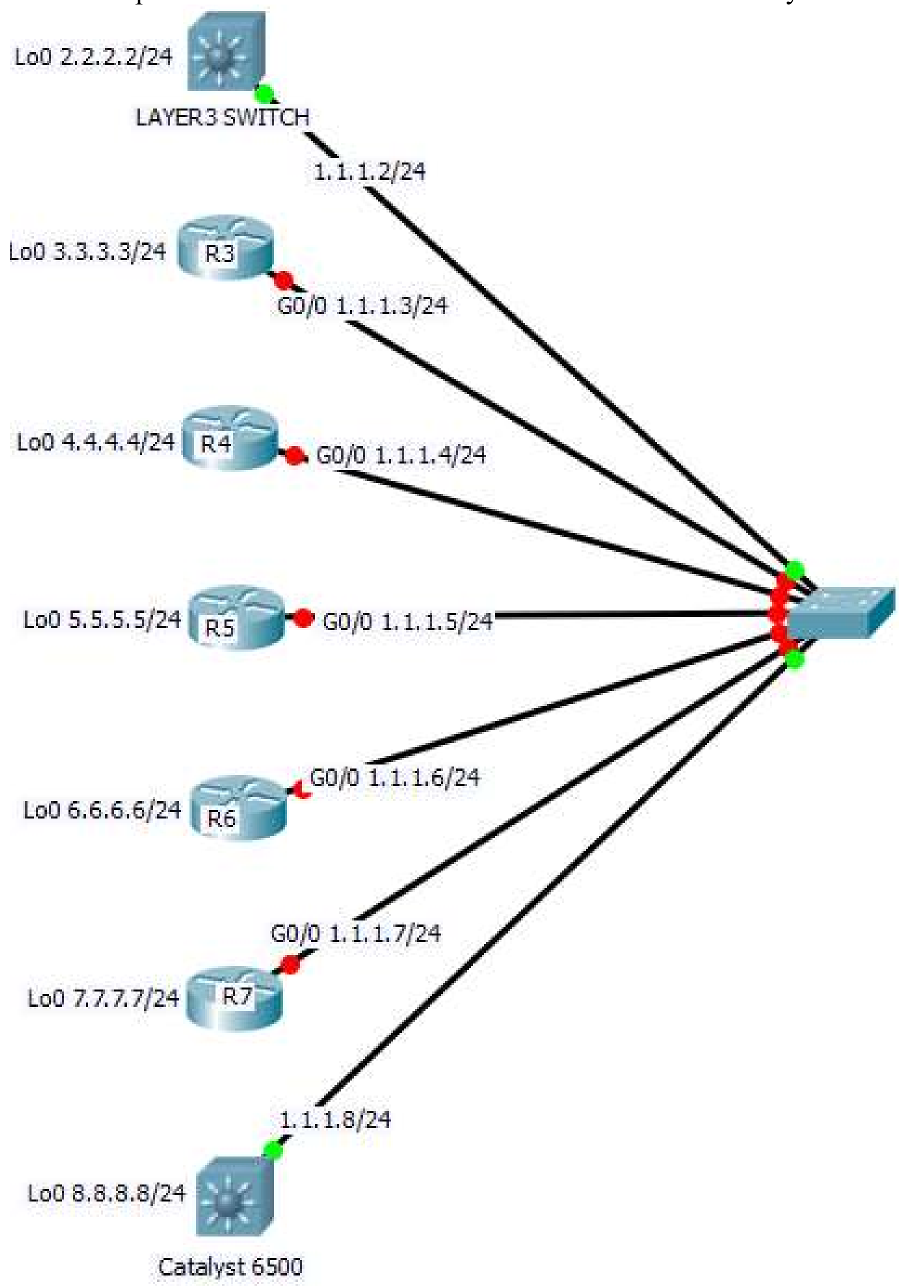
On the second step we changed our topology a little bit. We got rid of the layer 2 switch and we used layer 3 switch and the catalyst to connect the routers together. The layer 3 switch and the catalyst were not directly connected. We were going to configure route reflectors on this step. We decided to have two route reflectors to make the network redundant. This time every link was a different network by itself because we weren't using a layer 2 switch anymore. So we entered the IP address for every port in the topology first. Then we configured BGP in every route reflector client and then we configured the route reflectors. In route reflector clients, we only entered three commands. The first two commands specified the two route reflectors as the neighbors and the third command redistributed the connected links of the routers with other devices. In the route reflectors, we entered every neighbor's address just like we did to every device in the full mesh. In the route reflectors, we also specified who were going to be the clients of that reflector. After doing those things we had a redundant IBGP network that was using two route reflectors. Every router was able to ping every other device even when one of the route reflectors was not working.

Lab Commands

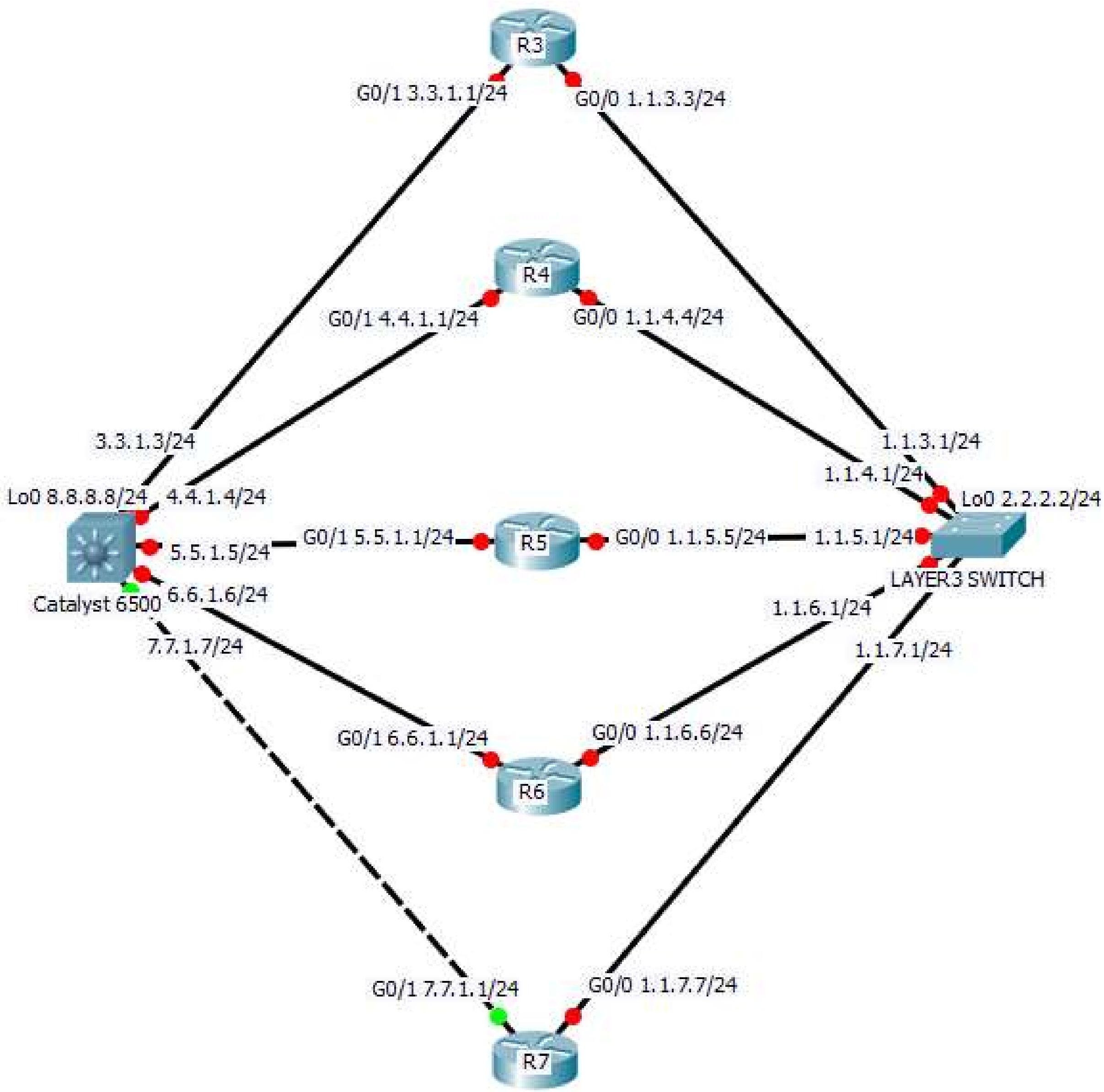
router bgp *1*	This command creates and configures the BGP routing process.
redistribute connected	This command is entered under router eigrp, router ospf or router bgp and advertises the connected routes to the routing protocol that it is configured under.
neighbor *1.1.1.2* **remote-as** *1*	This command is used under router bgp and it advertises an external bgp network and its autonomous system number to the BGP on the router where this command is entered.
neighbor *3.3.1.1* **route-reflector-client**	This command is used to configure the router as a BGP route reflector and configure the specified neighbor as its client. It is the router with the IP address 3.3.1.1 in this case.

Network Diagram

Topology for the first step of the lab which is to establish end-to-end connectivity via full mesh:



Topology for the second step of the lab which is to create end-to-end connectivity by using two route reflectors:



Configurations

Configurations for the first step of the lab (only from R3 and R4, the other configurations are similar):
R3:
Show run

```
hostname R3
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180LH
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
redundancy
interface Loopback0
 ip address 3.3.3.3 255.255.255.0
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 1.1.1.3 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router bgp 1
 bgp log-neighbor-changes
 network 3.3.3.0 mask 255.255.255.0
 neighbor 1.1.1.2 remote-as 1
 neighbor 1.1.1.4 remote-as 1
 neighbor 1.1.1.5 remote-as 1
 neighbor 1.1.1.6 remote-as 1
 neighbor 1.1.1.7 remote-as 1
```

```
 neighbor 1.1.1.8 remote-as 1
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
   mgcp profile default
gatekeeper
 shutdown
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
End
```

Show ip route

```
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, GigabitEthernet0/0
L        1.1.1.3/32 is directly connected, GigabitEthernet0/0
      2.0.0.0/24 is subnetted, 1 subnets
B        2.2.2.0 [200/0] via 1.1.1.2, 00:01:57
      3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        3.3.3.0/24 is directly connected, Loopback0
L        3.3.3.3/32 is directly connected, Loopback0
      4.0.0.0/24 is subnetted, 1 subnets
B        4.4.4.0 [200/0] via 1.1.1.4, 00:22:05
      5.0.0.0/24 is subnetted, 1 subnets
B        5.5.5.0 [200/0] via 1.1.1.5, 00:21:25
      6.0.0.0/24 is subnetted, 1 subnets
B        6.6.6.0 [200/0] via 1.1.1.6, 00:20:53
      7.0.0.0/24 is subnetted, 1 subnets
B        7.7.7.0 [200/0] via 1.1.1.7, 00:20:01
      8.0.0.0/24 is subnetted, 1 subnets
B        8.8.8.0 [200/0] via 1.1.1.8, 00:10:41
```

Show bgp

```
     Network          Next Hop            Metric LocPrf Weight Path
 *>i 2.2.2.0/24       1.1.1.2                  0    100      0 i
 *>  3.3.3.0/24       0.0.0.0                  0         32768 i
 *>i 4.4.4.0/24       1.1.1.4                  0    100      0 i
 *>i 5.5.5.0/24       1.1.1.5                  0    100      0 i
 *>i 6.6.6.0/24       1.1.1.6                  0    100      0 i
 *>i 7.7.7.0/24       1.1.1.7                  0    100      0 i
```

```
 *>i 8.8.8.0/24       1.1.1.8                  0    100      0 i
```

R4
Show run

```
hostname R4
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180LN
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
redundancy
interface Loopback0
 ip address 4.4.4.4 255.255.255.0
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 1.1.1.4 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router bgp 1
 bgp log-neighbor-changes
 network 4.4.4.0 mask 255.255.255.0
 neighbor 1.1.1.2 remote-as 1
 neighbor 1.1.1.3 remote-as 1
 neighbor 1.1.1.5 remote-as 1
 neighbor 1.1.1.6 remote-as 1
 neighbor 1.1.1.7 remote-as 1
```

```
 neighbor 1.1.1.8 remote-as 1
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
   mgcp profile default
gatekeeper
 shutdown
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, GigabitEthernet0/0
L        1.1.1.4/32 is directly connected, GigabitEthernet0/0
      2.0.0.0/24 is subnetted, 1 subnets
B        2.2.2.0 [200/0] via 1.1.1.2, 00:02:51
      3.0.0.0/24 is subnetted, 1 subnets
B        3.3.3.0 [200/0] via 1.1.1.3, 00:23:05
      4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        4.4.4.0/24 is directly connected, Loopback0
L        4.4.4.4/32 is directly connected, Loopback0
      5.0.0.0/24 is subnetted, 1 subnets
B        5.5.5.0 [200/0] via 1.1.1.5, 00:22:26
      6.0.0.0/24 is subnetted, 1 subnets
B        6.6.6.0 [200/0] via 1.1.1.6, 00:21:54
      7.0.0.0/24 is subnetted, 1 subnets
B        7.7.7.0 [200/0] via 1.1.1.7, 00:21:01
      8.0.0.0/24 is subnetted, 1 subnets
B        8.8.8.0 [200/0] via 1.1.1.8, 00:11:41
```

Show bgp

```
     Network          Next Hop            Metric LocPrf Weight Path
 *>i 2.2.2.0/24       1.1.1.2                  0    100      0 i
 *>i 3.3.3.0/24       1.1.1.3                  0    100      0 i
 *>  4.4.4.0/24       0.0.0.0                  0         32768 i
 *>i 5.5.5.0/24       1.1.1.5                  0    100      0 i
 *>i 6.6.6.0/24       1.1.1.6                  0    100      0 i
 *>i 7.7.7.0/24       1.1.1.7                  0    100      0 i
```

```
 *>i 8.8.8.0/24       1.1.1.8                  0    100      0 iR5
```

Configurations for the second step of the lab:
R3
Show run:

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R3
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180LH
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 1.1.3.3 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 3.3.1.1 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router bgp 1
 bgp log-neighbor-changes
 redistribute connected
 neighbor 1.1.3.1 remote-as 1
 neighbor 3.3.1.3 remote-as 1
ip forward-protocol nd
```

```
no ip http server
no ip http secure-server
control-plane
   mgcp profile default
gatekeeper
 shutdown
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
      1.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        1.1.3.0/24 is directly connected, GigabitEthernet0/0
L        1.1.3.3/32 is directly connected, GigabitEthernet0/0
B        1.1.4.0/24 [200/0] via 1.1.3.1, 00:06:07
B        1.1.5.0/24 [200/0] via 1.1.3.1, 00:06:07
B        1.1.6.0/24 [200/0] via 1.1.3.1, 00:06:07
B        1.1.7.0/24 [200/0] via 1.1.3.1, 00:06:07
      2.0.0.0/24 is subnetted, 1 subnets
B        2.2.2.0 [200/0] via 1.1.3.1, 00:06:07
      3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        3.3.1.0/24 is directly connected, GigabitEthernet0/1
L        3.3.1.1/32 is directly connected, GigabitEthernet0/1
      4.0.0.0/24 is subnetted, 1 subnets
B        4.4.1.0 [200/0] via 1.1.4.4, 00:06:07
      5.0.0.0/24 is subnetted, 1 subnets
B        5.5.1.0 [200/0] via 1.1.5.5, 00:06:06
      6.0.0.0/24 is subnetted, 1 subnets
B        6.6.1.0 [200/0] via 1.1.6.6, 00:06:05
      7.0.0.0/24 is subnetted, 1 subnets
B        7.7.1.0 [200/0] via 1.1.7.7, 00:06:05
      8.0.0.0/24 is subnetted, 1 subnets
B        8.8.8.0 [200/0] via 3.3.1.3, 00:39:38
```

Show bgp

```
     Network          Next Hop            Metric LocPrf Weight Path
 * i 1.1.3.0/24       1.1.3.1                  0    100      0 ?
 *>                   0.0.0.0                  0         32768 ?
 *>i 1.1.4.0/24       1.1.3.1                  0    100      0 ?
 * i                  4.4.1.1                  0    100      0 ?
```

```
 *>i 1.1.5.0/24       1.1.3.1                  0    100      0 ?
 * i                  5.5.1.1                  0    100      0 ?
 *>i 1.1.6.0/24       1.1.3.1                  0    100      0 ?
 * i                  6.6.1.1                  0    100      0 ?
 *>i 1.1.7.0/24       1.1.3.1                  0    100      0 ?
 * i                  7.7.1.1                  0    100      0 ?
 *>i 2.2.2.0/24       1.1.3.1                  0    100      0 i
 * i 3.3.1.0/24       3.3.1.3                  0    100      0 ?
 *>                   0.0.0.0                  0         32768 ?
 *>i 4.4.1.0/24       1.1.4.4                  0    100      0 ?
     Network          Next Hop            Metric LocPrf Weight Path
 * i                  3.3.1.3                  0    100      0 ?
 *>i 5.5.1.0/24       1.1.5.5                  0    100      0 ?
 * i                  3.3.1.3                  0    100      0 ?
 *>i 6.6.1.0/24       1.1.6.6                  0    100      0 ?
 * i                  3.3.1.3                  0    100      0 ?
 *>i 7.7.1.0/24       1.1.7.7                  0    100      0 ?
 * i                  3.3.1.3                  0    100      0 ?
 *>i 8.8.8.0/24       3.3.1.3                  0    100      0 i
```

R4
Show run:

```
Current configuration : 1629 bytesLast configuration change at
20:10:06 UTC Thu Apr 28 2016
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R4
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180LN
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 1.1.4.4 255.255.255.0
 duplex auto
```

```
 speed auto
interface GigabitEthernet0/1
 ip address 4.4.1.1 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router bgp 1
 bgp log-neighbor-changes
 redistribute connected
 neighbor 1.1.4.1 remote-as 1
 neighbor 4.4.1.4 remote-as 1
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
   mgcp profile default
gatekeeper
 shutdown
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
      1.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
B        1.1.3.0/24 [200/0] via 1.1.4.1, 00:07:15
C        1.1.4.0/24 is directly connected, GigabitEthernet0/0
L        1.1.4.4/32 is directly connected, GigabitEthernet0/0
B        1.1.5.0/24 [200/0] via 1.1.4.1, 00:07:15
B        1.1.6.0/24 [200/0] via 1.1.4.1, 00:07:15
B        1.1.7.0/24 [200/0] via 1.1.4.1, 00:07:15
      2.0.0.0/24 is subnetted, 1 subnets
B        2.2.2.0 [200/0] via 1.1.4.1, 00:07:15
      3.0.0.0/24 is subnetted, 1 subnets
```

```
B        3.3.1.0 [200/0] via 1.1.3.3, 00:07:15
      4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        4.4.1.0/24 is directly connected, GigabitEthernet0/1
L        4.4.1.1/32 is directly connected, GigabitEthernet0/1
      5.0.0.0/24 is subnetted, 1 subnets
B        5.5.1.0 [200/0] via 1.1.5.5, 00:07:14
      6.0.0.0/24 is subnetted, 1 subnets
B        6.6.1.0 [200/0] via 1.1.6.6, 00:07:14
      7.0.0.0/24 is subnetted, 1 subnets
B        7.7.1.0 [200/0] via 1.1.7.7, 00:07:13
      8.0.0.0/24 is subnetted, 1 subnets
B        8.8.8.0 [200/0] via 4.4.1.4, 00:40:47
```

Show bgp

```
     Network          Next Hop            Metric LocPrf Weight Path
 *>i 1.1.3.0/24       1.1.4.1                  0    100      0 ?
 * i                  3.3.1.1                  0    100      0 ?
 * i 1.1.4.0/24       1.1.4.1                  0    100      0 ?
 *>                   0.0.0.0                  0         32768 ?
 *>i 1.1.5.0/24       1.1.4.1                  0    100      0 ?
 * i                  5.5.1.1                  0    100      0 ?
 *>i 1.1.6.0/24       1.1.4.1                  0    100      0 ?
 * i                  6.6.1.1                  0    100      0 ?
 *>i 1.1.7.0/24       1.1.4.1                  0    100      0 ?
 * i                  7.7.1.1                  0    100      0 ?
 *>i 2.2.2.0/24       1.1.4.1                  0    100      0 i
 *>i 3.3.1.0/24       1.1.3.3                  0    100      0 ?
 * i                  4.4.1.4                  0    100      0 ?
 * i 4.4.1.0/24       4.4.1.4                  0    100      0 ?
     Network          Next Hop            Metric LocPrf Weight Path
 *>                   0.0.0.0                  0         32768 ?
 *>i 5.5.1.0/24       1.1.5.5                  0    100      0 ?
 * i                  4.4.1.4                  0    100      0 ?
 *>i 6.6.1.0/24       1.1.6.6                  0    100      0 ?
 * i                  4.4.1.4                  0    100      0 ?
 *>i 7.7.1.0/24       1.1.7.7                  0    100      0 ?
 * i                  4.4.1.4                  0    100      0 ?
 *>i 8.8.8.0/24       4.4.1.4                  0    100      0 i
```

R5

Show run

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R5
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
```

```
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX1520806Y
license accept end user agreement
license boot module c2900 technology-package uck9
license boot module c2900 technology-package datak9
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 1.1.5.5 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 5.5.1.1 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 duplex auto
 speed auto
router bgp 1
 bgp log-neighbor-changes
 redistribute connected
 neighbor 1.1.5.1 remote-as 1
 neighbor 5.5.1.5 remote-as 1
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
   mgcp profile default
gatekeeper
 shutdown
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
```

```
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
      1.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
B        1.1.3.0/24 [200/0] via 1.1.5.1, 00:08:20
B        1.1.4.0/24 [200/0] via 1.1.5.1, 00:08:20
C        1.1.5.0/24 is directly connected, GigabitEthernet0/0
L        1.1.5.5/32 is directly connected, GigabitEthernet0/0
B        1.1.6.0/24 [200/0] via 1.1.5.1, 00:08:20
B        1.1.7.0/24 [200/0] via 1.1.5.1, 00:08:20
      2.0.0.0/24 is subnetted, 1 subnets
B        2.2.2.0 [200/0] via 1.1.5.1, 00:08:20
      3.0.0.0/24 is subnetted, 1 subnets
B        3.3.1.0 [200/0] via 1.1.3.3, 00:08:20
      4.0.0.0/24 is subnetted, 1 subnets
B        4.4.1.0 [200/0] via 1.1.4.4, 00:08:20
      5.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        5.5.1.0/24 is directly connected, GigabitEthernet0/1
L        5.5.1.1/32 is directly connected, GigabitEthernet0/1
      6.0.0.0/24 is subnetted, 1 subnets
B        6.6.1.0 [200/0] via 1.1.6.6, 00:08:20
      7.0.0.0/24 is subnetted, 1 subnets
B        7.7.1.0 [200/0] via 1.1.7.7, 00:08:20
      8.0.0.0/24 is subnetted, 1 subnets
B        8.8.8.0 [200/0] via 5.5.1.5, 00:41:53
```

Show bgp

```
     Network          Next Hop            Metric LocPrf Weight Path
 *>i 1.1.3.0/24       1.1.5.1                  0    100      0 ?
 * i                  3.3.1.1                  0    100      0 ?
 *>i 1.1.4.0/24       1.1.5.1                  0    100      0 ?
 * i                  4.4.1.1                  0    100      0 ?
 * i 1.1.5.0/24       1.1.5.1                  0    100      0 ?
 *>                   0.0.0.0                  0         32768 ?
 *>i 1.1.6.0/24       1.1.5.1                  0    100      0 ?
 * i                  6.6.1.1                  0    100      0 ?
 *>i 1.1.7.0/24       1.1.5.1                  0    100      0 ?
 * i                  7.7.1.1                  0    100      0 ?
 *>i 2.2.2.0/24       1.1.5.1                  0    100      0 i
 *>i 3.3.1.0/24       1.1.3.3                  0    100      0 ?
 * i                  5.5.1.5                  0    100      0 ?
 *>i 4.4.1.0/24       1.1.4.4                  0    100      0 ?
     Network          Next Hop            Metric LocPrf Weight Path
 * i                  5.5.1.5                  0    100      0 ?
 * i 5.5.1.0/24       5.5.1.5                  0    100      0 ?
```

```
 *>                  0.0.0.0                  0         32768 ?
 *>i 6.6.1.0/24      1.1.6.6                  0    100      0 ?
 * i                 5.5.1.5                  0    100      0 ?
 *>i 7.7.1.0/24      1.1.7.7                  0    100      0 ?
 * i                 5.5.1.5                  0    100      0 ?
 *>i 8.8.8.0/24      5.5.1.5                  0    100      0 i
```

R6
Show run:

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R6
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX1520806Z
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 1.1.6.6 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 6.6.1.1 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 duplex auto
```

```
 speed auto
router bgp 1
 bgp log-neighbor-changes
 redistribute connected
 neighbor 1.1.6.1 remote-as 1
 neighbor 6.6.1.6 remote-as 1
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
   mgcp profile default
gatekeeper
 shutdown
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
      1.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
B        1.1.3.0/24 [200/0] via 1.1.6.1, 00:09:01
B        1.1.4.0/24 [200/0] via 1.1.6.1, 00:09:01
B        1.1.5.0/24 [200/0] via 1.1.6.1, 00:09:01
C        1.1.6.0/24 is directly connected, GigabitEthernet0/0
L        1.1.6.6/32 is directly connected, GigabitEthernet0/0
B        1.1.7.0/24 [200/0] via 1.1.6.1, 00:09:01
      2.0.0.0/24 is subnetted, 1 subnets
B        2.2.2.0 [200/0] via 1.1.6.1, 00:09:01
      3.0.0.0/24 is subnetted, 1 subnets
B        3.3.1.0 [200/0] via 1.1.3.3, 00:09:01
      4.0.0.0/24 is subnetted, 1 subnets
B        4.4.1.0 [200/0] via 1.1.4.4, 00:09:01
      5.0.0.0/24 is subnetted, 1 subnets
B        5.5.1.0 [200/0] via 1.1.5.5, 00:09:01
      6.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        6.6.1.0/24 is directly connected, GigabitEthernet0/1
L        6.6.1.1/32 is directly connected, GigabitEthernet0/1
      7.0.0.0/24 is subnetted, 1 subnets
B        7.7.1.0 [200/0] via 1.1.7.7, 00:09:01
      8.0.0.0/24 is subnetted, 1 subnets
B        8.8.8.0 [200/0] via 6.6.1.6, 00:42:34
```

Show bgp

```
     Network          Next Hop            Metric LocPrf Weight Path
 *>i 1.1.3.0/24       1.1.6.1                  0    100      0 ?
 * i                  3.3.1.1                  0    100      0 ?
 *>i 1.1.4.0/24       1.1.6.1                  0    100      0 ?
 * i                  4.4.1.1                  0    100      0 ?
 *>i 1.1.5.0/24       1.1.6.1                  0    100      0 ?
 * i                  5.5.1.1                  0    100      0 ?
 * i 1.1.6.0/24       1.1.6.1                  0    100      0 ?
 *>                   0.0.0.0                  0         32768 ?
 *>i 1.1.7.0/24       1.1.6.1                  0    100      0 ?
 * i                  7.7.1.1                  0    100      0 ?
 *>i 2.2.2.0/24       1.1.6.1                  0    100      0 i
 *>i 3.3.1.0/24       1.1.3.3                  0    100      0 ?
 * i                  6.6.1.6                  0    100      0 ?
 *>i 4.4.1.0/24       1.1.4.4                  0    100      0 ?
     Network          Next Hop            Metric LocPrf Weight Path
 * i                  6.6.1.6                  0    100      0 ?
 *>i 5.5.1.0/24       1.1.5.5                  0    100      0 ?
 * i                  6.6.1.6                  0    100      0 ?
 * i 6.6.1.0/24       6.6.1.6                  0    100      0 ?
 *>                   0.0.0.0                  0         32768 ?
 *>i 7.7.1.0/24       1.1.7.7                  0    100      0 ?
 * i                  6.6.1.6                  0    100      0 ?
 *>i 8.8.8.0/24       6.6.1.6                  0    100      0 i
```

R7

Show run:

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R7
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ip domain lookup
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX152885RE
license accept end user agreement
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
```

```
 shutdown
interface GigabitEthernet0/0
 ip address 1.1.7.7 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 7.7.1.1 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 duplex auto
 speed auto
router bgp 1
 bgp log-neighbor-changes
 redistribute connected
 neighbor 1.1.7.1 remote-as 1
 neighbor 7.7.1.7 remote-as 1
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
   mgcp profile default
gatekeeper
 shutdown
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
      1.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
```

```
B        1.1.3.0/24 [200/0] via 1.1.7.1, 00:10:54
B        1.1.4.0/24 [200/0] via 1.1.7.1, 00:10:54
B        1.1.5.0/24 [200/0] via 1.1.7.1, 00:10:54
B        1.1.6.0/24 [200/0] via 1.1.7.1, 00:10:54
C        1.1.7.0/24 is directly connected, GigabitEthernet0/0
L        1.1.7.7/32 is directly connected, GigabitEthernet0/0
      2.0.0.0/24 is subnetted, 1 subnets
B        2.2.2.0 [200/0] via 1.1.7.1, 00:10:54
      3.0.0.0/24 is subnetted, 1 subnets
B        3.3.1.0 [200/0] via 1.1.3.3, 00:10:54
      4.0.0.0/24 is subnetted, 1 subnets
B        4.4.1.0 [200/0] via 1.1.4.4, 00:10:54
      5.0.0.0/24 is subnetted, 1 subnets
B        5.5.1.0 [200/0] via 1.1.5.5, 00:10:54
      6.0.0.0/24 is subnetted, 1 subnets
B        6.6.1.0 [200/0] via 1.1.6.6, 00:10:54
      7.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        7.7.1.0/24 is directly connected, GigabitEthernet0/1
L        7.7.1.1/32 is directly connected, GigabitEthernet0/1
      8.0.0.0/24 is subnetted, 1 subnets
B        8.8.8.0 [200/0] via 7.7.1.7, 00:44:27
```

Show bgp

```
     Network          Next Hop            Metric LocPrf Weight Path
 *>i 1.1.3.0/24       1.1.7.1                  0    100      0 ?
 * i                  3.3.1.1                  0    100      0 ?
 *>i 1.1.4.0/24       1.1.7.1                  0    100      0 ?
 * i                  4.4.1.1                  0    100      0 ?
 *>i 1.1.5.0/24       1.1.7.1                  0    100      0 ?
 * i                  5.5.1.1                  0    100      0 ?
 *>i 1.1.6.0/24       1.1.7.1                  0    100      0 ?
 * i                  6.6.1.1                  0    100      0 ?
 * i 1.1.7.0/24       1.1.7.1                  0    100      0 ?
 *>                   0.0.0.0                  0         32768 ?
 *>i 2.2.2.0/24       1.1.7.1                  0    100      0 i
 *>i 3.3.1.0/24       1.1.3.3                  0    100      0 ?
 * i                  7.7.1.7                  0    100      0 ?
 *>i 4.4.1.0/24       1.1.4.4                  0    100      0 ?
     Network          Next Hop            Metric LocPrf Weight Path
 * i                  7.7.1.7                  0    100      0 ?
 *>i 5.5.1.0/24       1.1.5.5                  0    100      0 ?
 * i                  7.7.1.7                  0    100      0 ?
 *>i 6.6.1.0/24       1.1.6.6                  0    100      0 ?
 * i                  7.7.1.7                  0    100      0 ?
 * i 7.7.1.0/24       7.7.1.7                  0    100      0 ?
 *>                   0.0.0.0                  0         32768 ?
 *>i 8.8.8.0/24       7.7.1.7                  0    100      0 i
```

Layer 3 switch
Show run

```
version 12.2
```

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Layer3Switch
boot-start-marker
boot-end-marker
no aaa new-model
system mtu routing 1500
ip routing
no ip domain-lookup
vtp mode transparent
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
vlan 996
 name CUSTOMER_NATIVE
interface Loopback0
 ip address 2.2.2.2 255.255.255.0
interface FastEthernet1/0/1
interface FastEthernet1/0/2
interface FastEthernet1/0/3
 no switchport
 ip address 1.1.3.1 255.255.255.0
interface FastEthernet1/0/4
 no switchport
 ip address 1.1.4.1 255.255.255.0
interface FastEthernet1/0/5
 no switchport
 ip address 1.1.5.1 255.255.255.0
interface FastEthernet1/0/6
 no switchport
 ip address 1.1.6.1 255.255.255.0
interface FastEthernet1/0/7
 no switchport
 ip address 1.1.7.1 255.255.255.0
interface FastEthernet1/0/8
interface FastEthernet1/0/9
interface FastEthernet1/0/10
interface FastEthernet1/0/11
interface FastEthernet1/0/12
interface FastEthernet1/0/13
interface FastEthernet1/0/14
interface FastEthernet1/0/15
interface FastEthernet1/0/16
interface FastEthernet1/0/17
interface FastEthernet1/0/18
interface FastEthernet1/0/19
interface FastEthernet1/0/20
interface FastEthernet1/0/21
interface FastEthernet1/0/22
interface FastEthernet1/0/23
```

```
interface FastEthernet1/0/24
interface GigabitEthernet1/0/1
interface GigabitEthernet1/0/2
interface GigabitEthernet1/1/1
interface GigabitEthernet1/1/2
interface Vlan1
 no ip address
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 network 2.2.2.0 mask 255.255.255.0
 redistribute connected
 neighbor 1.1.3.3 remote-as 1
 neighbor 1.1.3.3 route-reflector-client
 neighbor 1.1.4.4 remote-as 1
 neighbor 1.1.4.4 route-reflector-client
 neighbor 1.1.5.5 remote-as 1
 neighbor 1.1.5.5 route-reflector-client
 neighbor 1.1.6.6 remote-as 1
 neighbor 1.1.6.6 route-reflector-client
 neighbor 1.1.7.7 remote-as 1
 neighbor 1.1.7.7 route-reflector-client
 no auto-summary
ip classless
ip http server
ip http secure-server
ip sla enable reaction-alerts
line con 0
 logging synchronous
line vty 0 4
 login
line vty 5 15
 login
end
```

Show ip route

```
     1.0.0.0/24 is subnetted, 5 subnets
C       1.1.3.0 is directly connected, FastEthernet1/0/3
C       1.1.4.0 is directly connected, FastEthernet1/0/4
C       1.1.5.0 is directly connected, FastEthernet1/0/5
C       1.1.6.0 is directly connected, FastEthernet1/0/6
C       1.1.7.0 is directly connected, FastEthernet1/0/7
     2.0.0.0/24 is subnetted, 1 subnets
C       2.2.2.0 is directly connected, Loopback0
     3.0.0.0/24 is subnetted, 1 subnets
B       3.3.1.0 [200/0] via 1.1.3.3, 00:11:53
     4.0.0.0/24 is subnetted, 1 subnets
B       4.4.1.0 [200/0] via 1.1.4.4, 00:11:53
     5.0.0.0/24 is subnetted, 1 subnets
B       5.5.1.0 [200/0] via 1.1.5.5, 00:11:53
     6.0.0.0/24 is subnetted, 1 subnets
```

```
B       6.6.1.0 [200/0] via 1.1.6.6, 00:11:52
     7.0.0.0/24 is subnetted, 1 subnets
B       7.7.1.0 [200/0] via 1.1.7.7, 00:11:52
```

Show bgp

```
   Network          Next Hop            Metric LocPrf Weight Path
* i1.1.3.0/24       1.1.3.3                  0    100      0 ?
*>                  0.0.0.0                  0         32768 ?
* i1.1.4.0/24       1.1.4.4                  0    100      0 ?
*>                  0.0.0.0                  0         32768 ?
* i1.1.5.0/24       1.1.5.5                  0    100      0 ?
*>                  0.0.0.0                  0         32768 ?
* i1.1.6.0/24       1.1.6.6                  0    100      0 ?
*>                  0.0.0.0                  0         32768 ?
* i1.1.7.0/24       1.1.7.7                  0    100      0 ?
*>                  0.0.0.0                  0         32768 ?
*> 2.2.2.0/24       0.0.0.0                  0         32768 i
*>i3.3.1.0/24       1.1.3.3                  0    100      0 ?
*>i4.4.1.0/24       1.1.4.4                  0    100      0 ?
*>i5.5.1.0/24       1.1.5.5                  0    100      0 ?
*>i6.6.1.0/24       1.1.6.6                  0    100      0 ?
*>i7.7.1.0/24       1.1.7.7                  0    100      0 ?
```

Catalyst 6500
Show run:

```
Current configuration : 17260 bytes
upgrade fpd auto
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service counters max age 5
hostname CatalystRouter
boot-start-marker
boot system sup-bootdisk:s3223-advipservicesk9_wan-mz.122-33.SXH4.bin
boot-end-marker
no aaa new-model
call-home
  alert-group configuration
  alert-group diagnostic
  alert-group environment
  alert-group inventory
  alert-group syslog
 profile "CiscoTAC-1"
   no active
   no destination transport-method http
   destination transport-method email
   destination address email callhome@cisco.com
   destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
   subscribe-to-alert-group diagnostic severity minor
```

```
   subscribe-to-alert-group environment severity minor
   subscribe-to-alert-group syslog severity major pattern ".*"
   subscribe-to-alert-group configuration periodic monthly 26 14:28
   subscribe-to-alert-group inventory periodic monthly 26 14:13
ip subnet-zero
no ip domain-lookup
ipv6 mfib hardware-switching replication-mode ingress
vtp domain Houston_Greenway
vtp mode transparent
mls ip slb purge global
no mls acl tcam share-global
mls netflow interface
no mls flow ip
no mls flow ipv6
mls cef error action freeze
redundancy
 keepalive-enable
 mode sso
 main-cpu
  auto-sync running-config
spanning-tree mode pvst
system flowcontrol bus auto
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
vlan 2
 name Office
vlan 54,100
interface Loopback0
 ip address 8.8.8.8 255.255.255.0
interface FastEthernet4/3
 ip address 3.3.1.3 255.255.255.0
interface FastEthernet4/4
 ip address 4.4.1.4 255.255.255.0
interface FastEthernet4/5
 ip address 5.5.1.5 255.255.255.0
interface FastEthernet4/6
 ip address 6.6.1.6 255.255.255.0
interface FastEthernet4/7
 ip address 7.7.1.7 255.255.255.0
interface Vlan1
 no ip address
 shutdown
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 network 8.8.8.0 mask 255.255.255.0
 redistribute connected
 neighbor 3.3.1.1 remote-as 1
 neighbor 3.3.1.1 route-reflector-client
 neighbor 4.4.1.1 remote-as 1
```

```
 neighbor 4.4.1.1 route-reflector-client
 neighbor 5.5.1.1 remote-as 1
 neighbor 5.5.1.1 route-reflector-client
 neighbor 6.6.1.1 remote-as 1
 neighbor 6.6.1.1 route-reflector-client
 neighbor 7.7.1.1 remote-as 1
 neighbor 7.7.1.1 route-reflector-client
 no auto-summary
ip classless
no ip http server
no ip http secure-server
control-plane
dial-peer cor custom
line con 0
 logging synchronous
line vty 0 4
 login
line vty 5 5
 login
End
```

Show ip route

```
     1.0.0.0/24 is subnetted, 5 subnets
B       1.1.3.0 [200/0] via 3.3.1.1, 00:14:57
B       1.1.5.0 [200/0] via 5.5.1.1, 00:14:55
B       1.1.7.0 [200/0] via 7.7.1.1, 00:14:54
B       1.1.4.0 [200/0] via 4.4.1.1, 00:14:56
B       1.1.6.0 [200/0] via 6.6.1.1, 00:14:55
     3.0.0.0/24 is subnetted, 1 subnets
C       3.3.1.0 is directly connected, FastEthernet4/3
     4.0.0.0/24 is subnetted, 1 subnets
C       4.4.1.0 is directly connected, FastEthernet4/4
     5.0.0.0/24 is subnetted, 1 subnets
C       5.5.1.0 is directly connected, FastEthernet4/5
     6.0.0.0/24 is subnetted, 1 subnets
C       6.6.1.0 is directly connected, FastEthernet4/6
     7.0.0.0/24 is subnetted, 1 subnets
C       7.7.1.0 is directly connected, FastEthernet4/7
     8.0.0.0/24 is subnetted, 1 subnets
C       8.8.8.0 is directly connected, Loopback0
```

Show bgp

```
   Network          Next Hop            Metric LocPrf Weight Path
*>i1.1.3.0/24       3.3.1.1                  0    100      0 ?
*>i1.1.4.0/24       4.4.1.1                  0    100      0 ?
*>i1.1.5.0/24       5.5.1.1                  0    100      0 ?
*>i1.1.6.0/24       6.6.1.1                  0    100      0 ?
*>i1.1.7.0/24       7.7.1.1                  0    100      0 ?
*> 3.3.1.0/24       0.0.0.0                  0         32768 ?
* i                 3.3.1.1                  0    100      0 ?
*> 4.4.1.0/24       0.0.0.0                  0         32768 ?
```

```
* i                 4.4.1.1                  0    100      0 ?
*> 5.5.1.0/24       0.0.0.0                  0         32768 ?
* i                 5.5.1.1                  0    100      0 ?
*> 6.6.1.0/24       0.0.0.0                  0         32768 ?
* i                 6.6.1.1                  0    100      0 ?
*> 7.7.1.0/24       0.0.0.0                  0         32768 ?
* i                 7.7.1.1                  0    100      0 ?
*> 8.8.8.0/       0.0.0.0                  0         32768 i
```

Problems

In this lab we had a plenty of problem in both of the steps. Starting with the full mesh, we had many problems we faced every day. The first problem we had was related with the layer 3 switch. We were supposed to configure one of the layer 2 switches in our rack to function as a layer 3 switch. However, we weren't able to enter any IP address to the switch, it was acting like a layer 2 switch no matter what we did. Finding the solution to this simple problem was easy though. We learned that we had to enter the command "ip routing" in the switch and enter the "no switchport" command in the interfaces that we wanted to configure IP address to. Then we moved onto configuring IBGP. While configuring IBGP for the full mesh portion of the lab, we first configured IBGP however we couldn't get anything to ping. No router was able to ping the other, our IBGP configuration was clearly not working. To solve the problem, we thought we needed to use another routing protocol along with IBGP. So we decided to also configure OSPF in the routers. We configured the OSPF and we were able to ping everything now, however IBGP was still not working. We knew that we didn't solve the problem in the IBGP, we just covered it up with a different way. So it wasn't the actual solution. We kept looking at the configurations of IBGP and tried to find the problem. After a while we realized that we put the wrong neighbor addresses in the IBGP commands. We needed to put the addresses that are on the other end of the link, not the addresses from the other networks. So we made the change so the IP addresses under the BGP were the actual neighbors' addresses and removed OSPF from our network. However even after that change we weren't able to establish end-to-end connectivity. We kept troubleshooting and looking at our configurations for a problem and after a long time, we realize that we didn't distributed the connected links of the routers. We entered the "redistribute connected" command under the IBGP configurations mode in every router and device and after doing that we were able to ping every router and our first step of the lab was complete.

The other day, when we entered the same configurations, nothing was working. We weren't expecting that because we did everything just fine the day before and we had established end-to-end connectivity. We didn't know what was going on until we took our troubleshooting to the physical level and started look at our cabling. We realized that we switched the places of the layer 2 and layer 3 switches in our topology. It was a super simple mistake and everything was working just fine after we fixed the cabling and we finally finished the first step of the lab.

After the first step of the lab was successful we moved on to the second step. In the second step where we were going to use route reflectors, we first tried to do them on the same topology we used from the first step but that did not work. We learned that the clients of the route reflector had to be directly connected to the route reflector with their own link and not through a layer 2 switch because every connection from the route reflector has to be on a different network. When we used a layer 2 switch, all the clients were in the same network and that didn't allow the route reflector to fully function. In order to fix this problem, we had to change our topology. So we got rid of the layer 2 switch, replaced it with the layer 3 switch we already had in the topology. Since our previous topology didn't have redundancy, we decided to make the catalyst 6500 a router reflector too and we placed it on the opposite side of the layer 3 switch. Instead heaving on interface and a loopback, the routers had two interfaces in the new topology. Both layer 3 switch and the catalyst 6500 were connected to every router. We fixed the topology problem like that and we were ready to configure the route reflectors and their clients.

When we were configuring the layer 3 switch, we came across a really small problem comparing to the ones we had before. The switch was not functioning like we wanted it to be, so we looked at the running configuration and we saw that there was an IP address that wasn't in our topology. We didn't put it in there. It probably was there because somebody else was using that layer 3 switch before and saved their running configuration to also be their start-up configuration. This was a fairly simple problem and we just deleted the old IP address and entered the one for our lab.

After the small IP addressing problem, we configured the route reflectors and their clients but we came across a huge problem that we had on the first step of the lab too. We weren't able to ping anything. Using our experience form the first step, we did troubleshooting on our configurations and quickly realized that we forgot the "redistribute connected" command again. The routers were not sharing the connected links they had with the other routers and that was why we did not have any connectivity.

The big problem we had that took us almost two full days to fix happened right before we were about to finish the second step and eventually the lab. We configured everything, all the routers, catalyst, layer 3 switch. The route reflectors were working fine; every device was able to ping one another then we decided to check our redundancy. We first shut down the catalyst to see if we would still have connectivity throughout the network. We shut it down and everything was working just fine. All the routers were still able to ping every other router. Then we turned the catalyst back on again and this time we shut down layer 3 switch. After shutting the layer 3 switch down, we lost all the connectivity in the network. No router was able to ping any other router. This meant that our catalyst was not working right, it was functioning correctly as a route reflector. We thought we did something wrong in the configuration of the interfaces that faced the catalyst or we forgot to include catalyst as a neighbor in the IBGP configurations of the router. But those things were all correct, nothing was wrong with the IBGP configurations on the routers or the interfaces. We then realized that the problem was with the IBGP configuration of the catalyst. In the catalyst's IBGP configuration, we first entered the IP addresses of the clients that were facing the layer 3 switch. However, we were supposed to enter the IP address of the interfaces on the clients that were facing the catalyst. We fixed that big addressing mistake and after fixing that our second step of the lab was finally complete. Both of the route reflectors were working just fine. We had connectivity throughout our topology and our network was redundant.

Conclusion

I have to start by saying that this lab was a challenging lab. It took a long time to finish and we came across too many problems. We had a plenty of difficult problems in both steps of the lab. While the first step of the lab was a revision of what we have done in one of the previous labs, the second step was a new topic. Route reflectors are like a different feature of the routing protocol BGP and I learned that they can save so much time from a busy network administrator. It is easier to troubleshoot a network that is using route reflectors because most of the configuration is in one place and the administrator doesn't have to look through a bunch of routers and go back and forth between them. I think it is a really useful feature BGP has. Even though we came across many problems, it is easy to set it up once you know how it works and what you need to configure and the command that are needed to configure route reflectors is only a couple too. So the configuration is not complicated at all. With this lab I learned a useful skill that can save a lot of time and effort.

MPLS

Purpose

The purpose of this lab was to create two separate areas in a network while implementing MPLS and it was also to capture the two different MPLS packets for the two areas.

Background Information

Multiprotocol Label Switching (MPLS) is a type of data-carrying technique for high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table.

The fundamental concept behind MPLS is that of labeling packets. In a traditional routed IP network, each router makes an independent forwarding decision for each packet based solely on the packet's network-layer header. Thus, every time a packet arrives at a router, the router has to "think through" where to send the packet next.

With MPLS, the first time the packet enters a network, it's assigned to a specific forwarding equivalence class (FEC), indicated by adding a short bit sequence (the label) to the end of the packet. Each router in the network has a table indicating how to handle packets of a specific FEC type, so once the packet has entered the network, routers don't need to perform header analysis. Instead, subsequent routers use the label as an index into a table that provides them with a new FEC for that packet.

This gives the MPLS network the ability to handle packets with particular characteristics, such as coming from particular ports or carrying traffic of particular application types, in a consistent fashion. Packets carrying real-time traffic, such as voice or video, can easily be mapped to low-latency routes across the network. This is something that's really challenging to do with conventional routing. The key point with all this is that the labels provide a way to add additional information to each packet, information above and beyond what the routers previously had. Besides faster routing, MPLS also has some other benefits. MPLS networks achieve greater Quality of Service for their customers. In addition, MPLS networks are able to assign priorities to the different packets based on what the labels say about that packet. MPLS networks are also able to restore interrupted connections at a faster speed than typical networks. Finally MPLS offers greater security and are often required for companies which need enhanced privacy and security for their network needs.

There's been a lot of confusion over the years about whether MPLS is a Layer 2 or Layer 3 service. But MPLS doesn't fit neatly into the OSI seven-layer hierarchy. In fact, one of the key benefits of MPLS is that it separates forwarding mechanisms from the underlying data-link service.

One can think of MPLS as the express lane on the highway. When someone is using the express lane, they don't bother with the people who are entering or exiting the highway and most of the time, even doing high traffic, express lane goes the fastest. This is just like the benefit MPLS brings to a network. It makes the packets travel faster. In this express lane case, the highway can be viewed as a traditional network, the express as a route that is using MPLS on a traditional network and the cars are the packets that are going through the network. The ones that use the express lane tend to travel faster than the cars that use the other, traditional lanes. Just like an MPLS network.

Lab Summary

In this lab, we had seven routers, three in the middle creating a core to the network and two on each end of the core network. This core network also supported MPLS. We had two different areas that were separate from each other in this lab. One area included routers R5 and R9, and the other area included routers R4 and R8. These routers were not allowed to connect to the routers on the other area.

We started off by cabling the topology, we set the IP address on every interface and then to create end to end connectivity in the network, we used OSPF. After all the IP addresses were entered and OSPF was configured in every router, we had end to end connectivity between every router. After that we needed to create the two separate areas and configure the core three routers so that they did MPLS.

To create the separate areas in the network, we used access lists. On the end routers R4, R5, R8 and R9 we created extended access lists that would block the traffic from the other area. Every end router needed three access list entries. Two of them to deny traffic coming from the two routers that belong to the other area and the last entry allowed every other traffic through the routers. After creating theses access lists, we assigned them to the interfaces of those four routers in order for the access lists to work. After we configured the access lists, the two areas were created and the routers on one area could only ping the router on the same area. The ping did not work when a router in one area tried to ping a router from the other area.

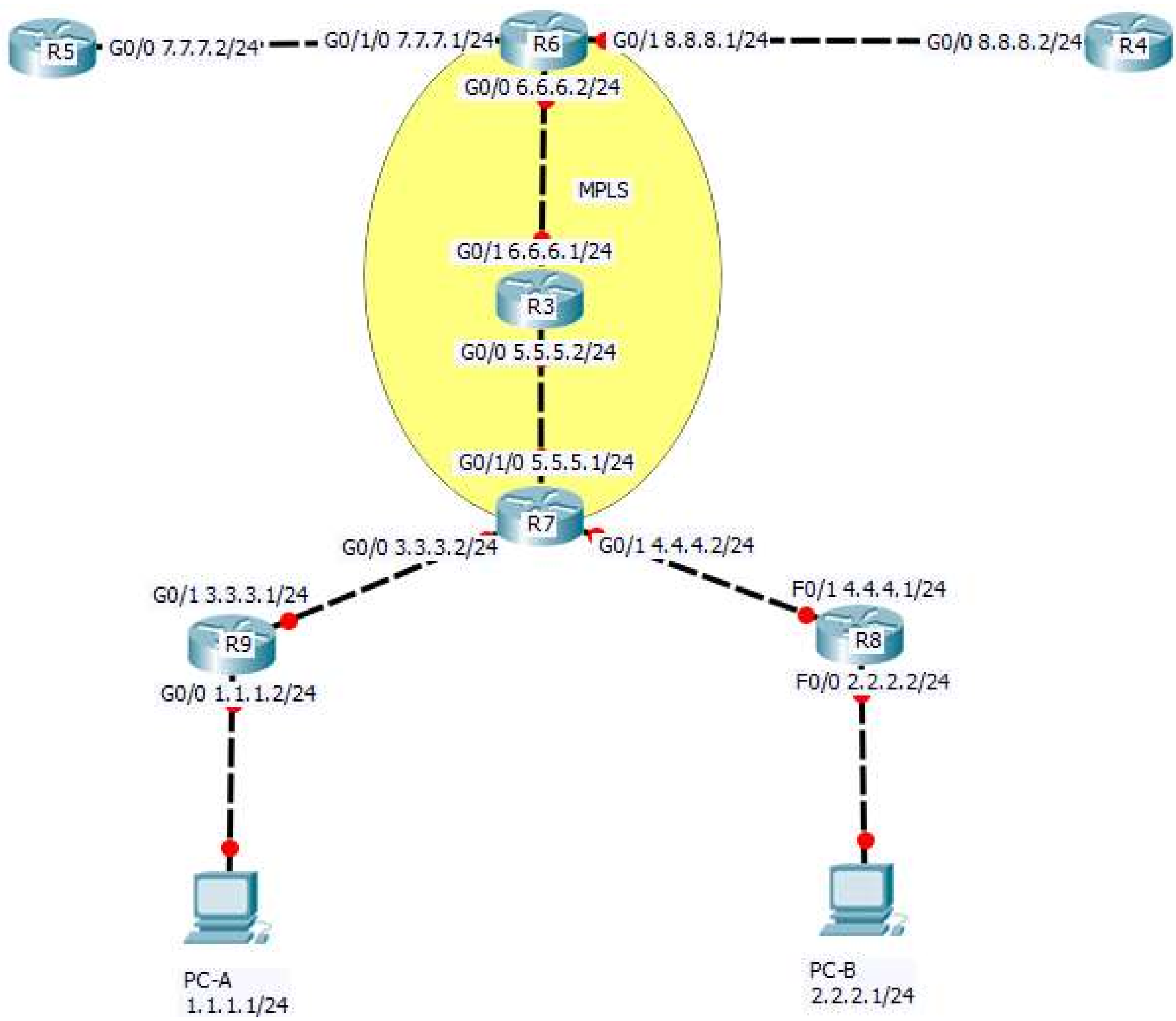
After creating the areas, only thing that was left to do was to configure MPLS on the three core routers, R3, R6 and R7. To do that we configured two simple MPLS commands on the routers and the interfaces that were going to use MPLS. On routers R6 and R7, only one interface used MPLS. On the interfaces that were going to use MPLS, we entered the command "mpls ip" to enable MPLS in that interface. We also wanted MPLS to route with different tags, so we entered the command "mpls label protocol ldp" on the routers that had one or more interfaces using MPLS. After entering those two simple commands in the needed places, we successfully configured MPLS in the three core routers.

To verify that MPLS was working, we did a Wireshark capture from a link between two core routers that were using MPLS. After we started capturing packets, we first made a ping between the two end routers on one area, then we also did another ping between the end routers of the other area. We then went back to the Wireshark capture and looked at the ICMP packets which are the pings we did between end routers of the two different areas. We analyzed the ICMP packets and the packets from one area had the MPLS tag number 16 and the packets from the other area had the tag number 17. This showed us that there the MPLS was working and it was assigning different tags to the packets from different areas.

Lab Commands

`ip cef`	This command enables Cisco Express Forwarding on the router.
`mpls label protocol ldp`	This command configures the use of LDP on all interfaces.
`mpls ip`	This command enables MPLS on a specific interface.
access-list *100* **deny ip 3.***3.3.0 0.0.0.255* **any**	This command is used to create an extended access list on the router. In this case the command is blocking any IP address in the 3.3.3.0 network form getting through the router.
ip access-group *100* **in**	This command is entered under the interface configuration mode and tells which way the access list is going to work through the router.

Network Diagram



Configurations

R3
Show run

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R3
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ipv6 cef
multilink bundle-name authenticated
mpls label protocol ldp
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180LH
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 5.5.5.2 255.255.255.0
 duplex auto
 speed auto
 mpls ip
interface GigabitEthernet0/1
 ip address 6.6.6.1 255.255.255.0
 duplex auto
 speed auto
 mpls ip
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router ospf 1
 network 5.5.5.0 0.0.0.255 area 0
 network 6.6.6.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
```

```
   mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
End
```

Show mpls forwarding-table

```
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next
Hop
Label      Label      or Tunnel Id     Switched      interface
16         16         1.1.1.0/24       312           Gi0/0
5.5.5.1
17         Pop Label  3.3.3.0/24       0             Gi0/0
5.5.5.1
18         Pop Label  4.4.4.0/24       0             Gi0/0
5.5.5.1
19         Pop Label  8.8.8.0/24       0             Gi0/1
6.6.6.2
20         Pop Label  7.7.7.0/24       296           Gi0/1
6.6.6.2
```

Show ip route

```
Gateway of last resort is not set

      1.0.0.0/24 is subnetted, 1 subnets
O        1.1.1.0 [110/3] via 5.5.5.1, 00:10:18, GigabitEthernet0/0
      3.0.0.0/24 is subnetted, 1 subnets
O        3.3.3.0 [110/2] via 5.5.5.1, 00:10:18, GigabitEthernet0/0
      4.0.0.0/24 is subnetted, 1 subnets
O        4.4.4.0 [110/2] via 5.5.5.1, 00:10:18, GigabitEthernet0/0
      5.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        5.5.5.0/24 is directly connected, GigabitEthernet0/0
L        5.5.5.2/32 is directly connected, GigabitEthernet0/0
      6.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        6.6.6.0/24 is directly connected, GigabitEthernet0/1
L        6.6.6.1/32 is directly connected, GigabitEthernet0/1
      7.0.0.0/24 is subnetted, 1 subnets
O        7.7.7.0 [110/2] via 6.6.6.2, 00:02:29, GigabitEthernet0/1
      8.0.0.0/24 is subnetted, 1 subnets
O        8.8.8.0 [110/2] via 6.6.6.2, 00:02:29, GigabitEthernet0/1
```

R4
Show run

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R4
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180LN
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 8.8.8.2 255.255.255.0
 ip access-group 100 in
 duplex auto
 speed auto
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router ospf 1
 network 8.8.8.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
access-list 100 deny   ip 3.3.3.0 0.0.0.255 any
```

```
access-list 100 deny   ip 7.7.7.0 0.0.0.255 any
access-list 100 permit ip any any
control-plane
   mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
End
```

Show ip route

```
Gateway of last resort is not set
      1.0.0.0/24 is subnetted, 1 subnets
O        1.1.1.0 [110/5] via 8.8.8.1, 00:03:25, GigabitEthernet0/0
      3.0.0.0/24 is subnetted, 1 subnets
O        3.3.3.0 [110/4] via 8.8.8.1, 00:03:25, GigabitEthernet0/0
      4.0.0.0/24 is subnetted, 1 subnets
O        4.4.4.0 [110/4] via 8.8.8.1, 00:03:25, GigabitEthernet0/0
      5.0.0.0/24 is subnetted, 1 subnets
O        5.5.5.0 [110/3] via 8.8.8.1, 00:03:25, GigabitEthernet0/0
      6.0.0.0/24 is subnetted, 1 subnets
O        6.6.6.0 [110/2] via 8.8.8.1, 00:06:46, GigabitEthernet0/0
      7.0.0.0/24 is subnetted, 1 subnets
O        7.7.7.0 [110/2] via 8.8.8.1, 00:10:48, GigabitEthernet0/0
      8.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        8.8.8.0/24 is directly connected, GigabitEthernet0/0
L        8.8.8.2/32 is directly connected, GigabitEthernet0/0
```

R5

Show run

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R5
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ipv6 cef
```

```
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX1520806Y
license accept end user agreement
license boot module c2900 technology-package uck9
license boot module c2900 technology-package datak9
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 7.7.7.2 255.255.255.0
 ip access-group 100 in
 duplex auto
 speed auto
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 duplex auto
 speed auto
router ospf 1
 network 7.7.7.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
access-list 100 deny   ip 4.4.4.0 0.0.0.255 any
access-list 100 deny   ip 8.8.8.0 0.0.0.255 any
access-list 100 permit ip any any
control-plane
   mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
```

```
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
Gateway of last resort is not set
      1.0.0.0/24 is subnetted, 1 subnets
O        1.1.1.0 [110/5] via 7.7.7.1, 00:06:16, GigabitEthernet0/0
      3.0.0.0/24 is subnetted, 1 subnets
O        3.3.3.0 [110/4] via 7.7.7.1, 00:06:16, GigabitEthernet0/0
      4.0.0.0/24 is subnetted, 1 subnets
O        4.4.4.0 [110/4] via 7.7.7.1, 00:06:16, GigabitEthernet0/0
      5.0.0.0/24 is subnetted, 1 subnets
O        5.5.5.0 [110/3] via 7.7.7.1, 00:06:16, GigabitEthernet0/0
      6.0.0.0/24 is subnetted, 1 subnets
O        6.6.6.0 [110/2] via 7.7.7.1, 00:09:36, GigabitEthernet0/0
      7.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        7.7.7.0/24 is directly connected, GigabitEthernet0/0
L        7.7.7.2/32 is directly connected, GigabitEthernet0/0
      8.0.0.0/24 is subnetted, 1 subnets
O        8.8.8.0 [110/2] via 7.7.7.1, 00:13:11, GigabitEthernet0/0
```

R6

Show run

```
Current configuration : 1668 bytes
! Last configuration change at 19:07:26 UTC Wed Apr 13 2016
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R6
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ipv6 cef
multilink bundle-name authenticated
mpls label protocol ldp
voice-card 0
license udi pid CISCO2901/K9 sn FTX1520806Z
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
```

```
interface GigabitEthernet0/0
 ip address 6.6.6.2 255.255.255.0
 duplex auto
 speed auto
 mpls ip
interface GigabitEthernet0/1
 ip address 8.8.8.1 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 ip address 7.7.7.1 255.255.255.0
 duplex auto
 speed auto
router ospf 1
 network 6.6.6.0 0.0.0.255 area 0
 network 7.7.7.0 0.0.0.255 area 0
 network 8.8.8.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
   mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
Gateway of last resort is not set
      1.0.0.0/24 is subnetted, 1 subnets
O        1.1.1.0 [110/4] via 6.6.6.1, 00:04:39, GigabitEthernet0/0
      3.0.0.0/24 is subnetted, 1 subnets
```

```
O        3.3.3.0 [110/3] via 6.6.6.1, 00:04:39, GigabitEthernet0/0
      4.0.0.0/24 is subnetted, 1 subnets
O        4.4.4.0 [110/3] via 6.6.6.1, 00:04:39, GigabitEthernet0/0
      5.0.0.0/24 is subnetted, 1 subnets
O        5.5.5.0 [110/2] via 6.6.6.1, 00:04:39, GigabitEthernet0/0
      6.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        6.6.6.0/24 is directly connected, GigabitEthernet0/0
L        6.6.6.2/32 is directly connected, GigabitEthernet0/0
      7.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        7.7.7.0/24 is directly connected, GigabitEthernet0/1/0
L        7.7.7.1/32 is directly connected, GigabitEthernet0/1/0
      8.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        8.8.8.0/24 is directly connected, GigabitEthernet0/1
L        8.8.8.1/32 is directly connected, GigabitEthernet0/1
```

R7
Show run

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R7
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ipv6 cef
multilink bundle-name authenticated
mpls label protocol ldp
voice-card 0
license udi pid CISCO2901/K9 sn FTX152885RE
license accept end user agreement
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 3.3.3.2 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 4.4.4.2 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
```

```
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 ip address 5.5.5.1 255.255.255.0
 duplex auto
 speed auto
 mpls ip
router ospf 1
 network 3.3.3.0 0.0.0.255 area 0
 network 4.4.4.0 0.0.0.255 area 0
 network 5.5.5.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
   mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
Gateway of last resort is not set
      1.0.0.0/24 is subnetted, 1 subnets
O        1.1.1.0 [110/2] via 3.3.3.1, 00:15:48, GigabitEthernet0/0
      3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        3.3.3.0/24 is directly connected, GigabitEthernet0/0
L        3.3.3.2/32 is directly connected, GigabitEthernet0/0
      4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        4.4.4.0/24 is directly connected, GigabitEthernet0/1
L        4.4.4.2/32 is directly connected, GigabitEthernet0/1
      5.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        5.5.5.0/24 is directly connected, GigabitEthernet0/1/0
L        5.5.5.1/32 is directly connected, GigabitEthernet0/1/0
      6.0.0.0/24 is subnetted, 1 subnets
O        6.6.6.0 [110/2] via 5.5.5.2, 00:07:30, GigabitEthernet0/1/0
      7.0.0.0/24 is subnetted, 1 subnets
```

```
O        7.7.7.0 [110/3] via 5.5.5.2, 00:07:20, GigabitEthernet0/1/0
      8.0.0.0/24 is subnetted, 1 subnets
O        8.8.8.0 [110/3] via 5.5.5.2, 00:07:20, GigabitEthernet0/1/0
```

R8

Show run

```
Current configuration : 1320 bytes
! Last configuration change at 19:11:00 UTC Wed Apr 13 2016
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R8
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
dot11 syslog
ip source-route
ip cef
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
crypto pki token default removal timeout 0
license udi pid CISCO2811 sn FTX1346A0XG
interface FastEthernet0/0
 ip address 2.2.2.2 255.255.255.0
 ip access-group 100 in
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 4.4.4.1 255.255.255.0
 ip access-group 100 in
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router ospf 1
 network 2.2.2.0 0.0.0.255 area 0
 network 4.4.4.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
access-list 100 deny   ip 3.3.3.0 0.0.0.255 any
```

```
access-list 100 deny   ip 7.7.7.0 0.0.0.255 any
access-list 100 permit ip any any
control-plane
mgcp profile default
line con 0
line aux 0
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
Gateway of last resort is not set
      1.0.0.0/24 is subnetted, 1 subnets
O        1.1.1.0 [110/3] via 4.4.4.2, 00:16:23, FastEthernet0/1
      3.0.0.0/24 is subnetted, 1 subnets
O        3.3.3.0 [110/2] via 4.4.4.2, 00:16:23, FastEthernet0/1
      4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        4.4.4.0/24 is directly connected, FastEthernet0/1
L        4.4.4.1/32 is directly connected, FastEthernet0/1
      5.0.0.0/24 is subnetted, 1 subnets
O        5.5.5.0 [110/2] via 4.4.4.2, 00:16:05, FastEthernet0/1
      6.0.0.0/24 is subnetted, 1 subnets
O        6.6.6.0 [110/3] via 4.4.4.2, 00:08:16, FastEthernet0/1
      7.0.0.0/24 is subnetted, 1 subnets
O        7.7.7.0 [110/4] via 4.4.4.2, 00:08:06, FastEthernet0/1
      8.0.0.0/24 is subnetted, 1 subnets
O        8.8.8.0 [110/4] via 4.4.4.2, 00:08:06, FastEthernet0/1
```

R9

Show run

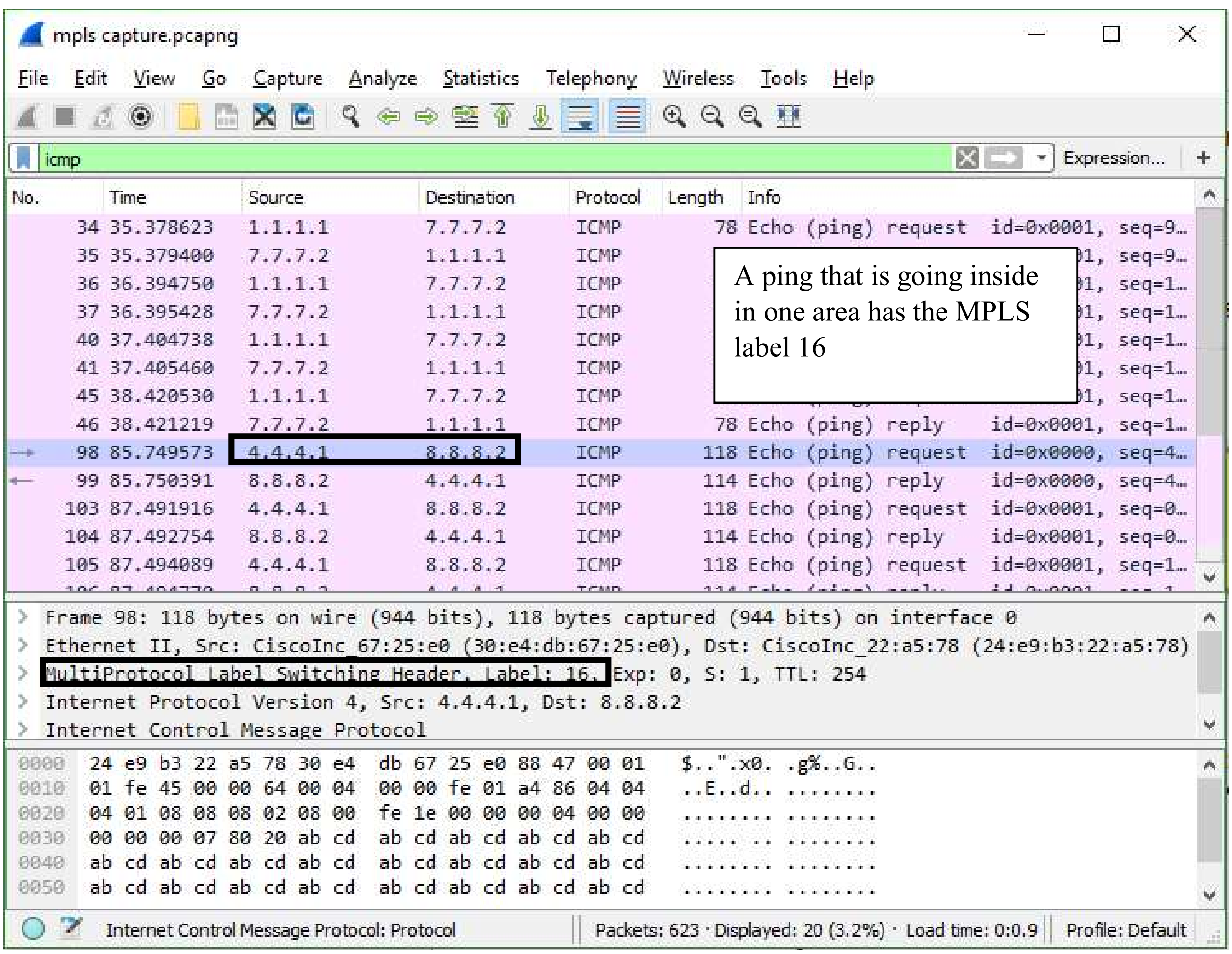
```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R9
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX1704Y03N
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
license boot module c2900 technology-package datak9
```

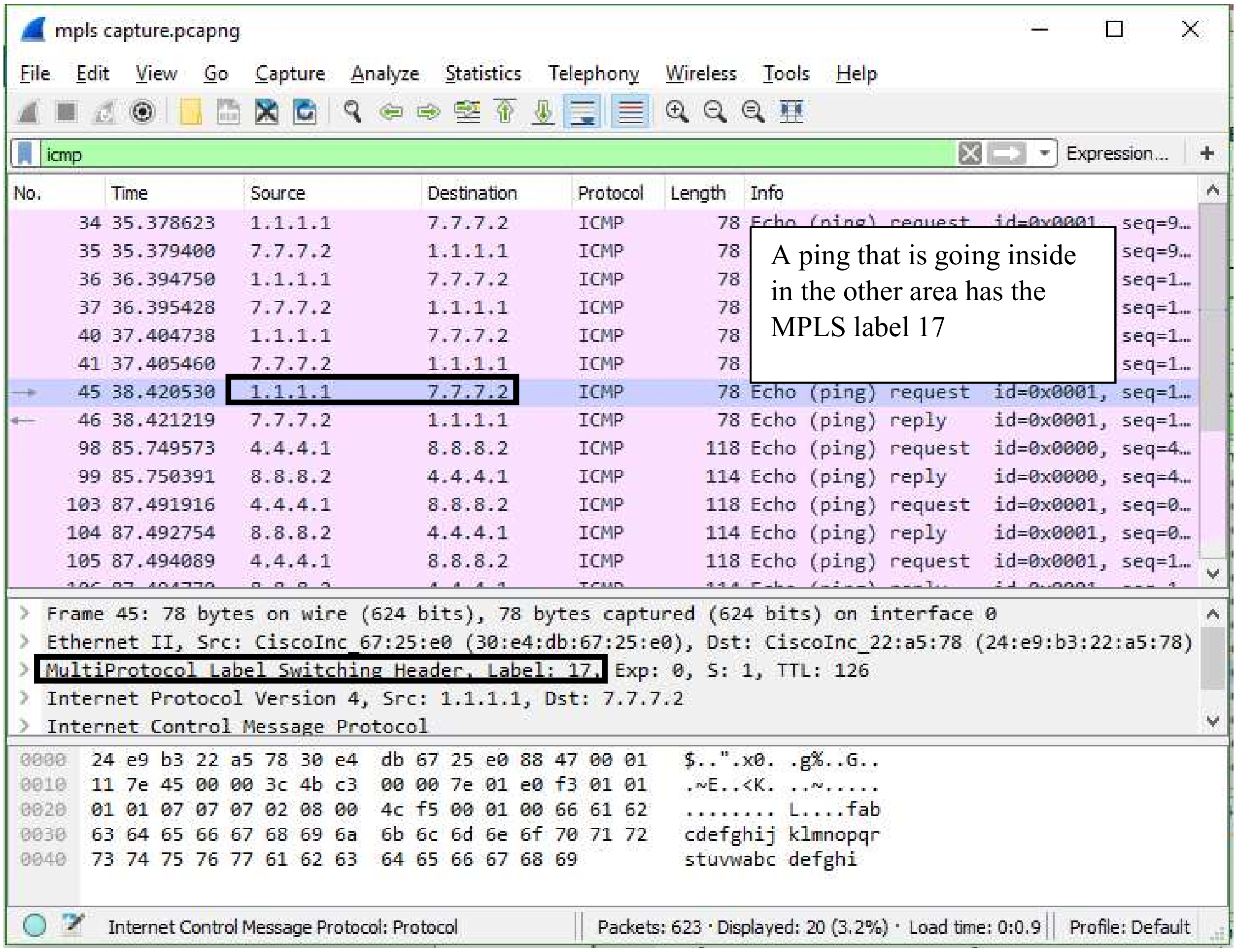
```
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 1.1.1.2 255.255.255.0
 ip access-group 100 in
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 3.3.3.1 255.255.255.0
 ip access-group 100 in
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router ospf 1
 network 1.1.1.0 0.0.0.255 area 0
 network 3.3.3.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
access-list 100 deny   ip 4.4.4.0 0.0.0.255 any
access-list 100 deny   ip 8.8.8.0 0.0.0.255 any
access-list 100 permit ip any any
control-plane
   mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
End
```

Show ip route

```
Gateway of last resort is not set
       1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C         1.1.1.0/24 is directly connected, GigabitEthernet0/0
L         1.1.1.2/32 is directly connected, GigabitEthernet0/0
       3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C         3.3.3.0/24 is directly connected, GigabitEthernet0/1
L         3.3.3.1/32 is directly connected, GigabitEthernet0/1
       4.0.0.0/24 is subnetted, 1 subnets
O         4.4.4.0 [110/2] via 3.3.3.2, 00:17:18, GigabitEthernet0/1
       5.0.0.0/24 is subnetted, 1 subnets
O         5.5.5.0 [110/2] via 3.3.3.2, 00:16:42, GigabitEthernet0/1
       6.0.0.0/24 is subnetted, 1 subnets
O         6.6.6.0 [110/3] via 3.3.3.2, 00:08:55, GigabitEthernet0/1
       7.0.0.0/24 is subnetted, 1 subnets
O         7.7.7.0 [110/4] via 3.3.3.2, 00:08:45, GigabitEthernet0/1
       8.0.0.0/24 is subnetted, 1 subnets
O         8.8.8.0 [110/4] via 3.3.3.2, 00:08:45, GigabitEthernet0/1
```

Wireshark Capture





Problems

In this lab we had some simple problems and some critical problems. The simple problem was about our topology but the critical problems were about configuring extended access lists and configuring the right MPLS commands. The problems that took most of our time as the access-list problems, the other ones were easy to fix once we figured them out.

When we started configuring the lab, we first started by creating a topology. Then we cabled the topology we have created. Our first goal was to create end to end connectivity using OSPF before we configured MPLS in the three core routers. We took our time and configured the IP addresses on every router, then OSPF, then we checked if we had end to end connectivity. We had end to end connectivity so we moved onto configuring MPLS on the interfaces. We entered to comment “mpls ip” in R6 and R7 and it worked. Then we entered the same command on R5 and it gave an error message. It turns out R5 was not capable of doing MPLS. We had a couple of solutions to fix the problem. We were either going to upload an IOS on the router that has MPLS or we were going to change the topology and replace R5 with another router that was capable of doing MPLS. Since we already had other routers that were able to do MPLS, we decided to change the topology. However, we couldn’t not simply switch a router that was able to do MPLS to the core network that was made up off three routers. The router that was supposed replace R5 needed to have three gigabit interfaces. We needed two router that were able to do MPLS and have three gigabit ports at the same time and those were routers R6 and R7. So, we moved R6 and R7 to the border of the core network and used R3 as the middle router of the core since it only had two gigabit interfaces. After we made the topology change, all three routers in the core network were able to do MPLS.

After the simple topology problem, we entered "mpls ip" command to configure MPLS. We first thought that's all we needed to successfully configure MPLS however we did not get any labels for the different paths. Then we realize that we needed to something that would create two different areas. We made research and we realized that we needed to enter the command "mpls label protocol ldp" command first and we since we didn't have the command in there in the first place, we didn't get the tags on the ICMP packets on the Wireshark capture. We entered the command and we also learned that we needed to use extended access lists to specify the two areas.

So, while configuring the extended access lists we came across with several simple problems. The first problem was, when we entered the command, the router didn't accept the command. It said that it was an unrecognized command. We took a closer look at the commands and it turns out, we forgot to specify the protocol in the command. We added the "ip" in to the command and the router accepted it this time. However the problems didn't end there. After we added "ip", we checked if the access lists were working. In order for them to work, they shouldn't have been able to ping the routers from the other area, however, every router was still able to ping every other router regardless of its area. That meant that the access lists we configured were not working. So we went back and started looking at our access lists entries. After a while, we realized that we put the wrong IP addresses on the wrong routers. In order words, we mixed up the commands. We put the commands that were supposed to be on the routers on one area to the routers on the other area. So we changed the IP addresses of the routers on different routers group so they blocked the right IP addresses. Then we also realized that the access lists were blocking only one address instead of a network. We entered a host's address instead of the network address. So we also made that change so that the access lists blocked all the addresses coming from one network, not just one. After we made those changes, we looked at the packets that were going through the network to see if the MPLS was working using Wireshark. We still couldn't see the MPLS packets. The access lists were still not working. We were looking for solutions and were trying to find the problem, then we realized, we did not assign the access lists to the interfaces. Then we went to interface configuration mode and entered the "access-group 100 in" command which specifies the direction the access lists is going to be used in the router. Finally, we tried to look for MPLS packets with different labels again, and we saw the different packets. The access lists and the MPLs configuration was finally working and we successfully completed the lab.

Conclusion

This was somewhat an easy lab. It wasn't the easiest lab but it wasn't super hard either. MPLS was a completely new concept and it was really important skill to learn. We had some problems with the MPLS compatibility in some of the routers and some problems with the configuration of the extended access lists but they weren't super hard problems. We had a lot of easy and small problems. Even though we had problems, we finished the lab on time and at the end of the day we were able to see the different path labels for the different areas in the network using Wireshark. With this lab, I learned how MPLS can improve the speed of a corporate network where speed is really important using services like teleconference, watching videos and voice over IP. MPLS has many benefits and configuring it is fairly simple.

Policy Based Routing

Purpose

The purpose of this lab was to create two different routes in a network. One only allowing HTTP packets and one allowing everything but HTTP packets.

Background Information

Nowadays, organizations need the freedom to implement packet forwarding and routing according to their own defined policies in a way that goes beyond traditional routing protocol concerns. Where administrative issues dictate that traffic be routed through specific paths, policy-based routing (PBR) can provide the solution. By using policy-based routing, companies can implement policies that selectively cause packets to take different paths.

With PBR, a network administrator has the ability to dictate the routing behavior based on a number of different criteria other than destination network, including source or destination network, source or destination address, source or destination port, protocol, packet size, and packet classification among others. PBR would give a network administrator the ability to route higher priority traffic over the high bandwidth or low delay link while sending all other traffic over the low bandwidth or high delay link.

Organizations can achieve cost savings by distributing interactive and batch traffic among low-bandwidth, low-cost permanent paths and high-bandwidth, high-cost, switched paths with implementing PBR on their networks. Internet service providers and other organizations can use policy-based routing to route traffic originating from different sets of users through different Internet connections across the policy routers. Organizations can also provide QOS to differentiated traffic by setting the precedence or type of service values in the IP packet headers at the periphery of the network and leveraging queuing mechanisms to prioritize traffic in the core or backbone of the network.

One can think of PBR as the garbage collecting system. Most people nowadays have two trashcans. One for recycle and one for non-recyclable objects like compost or food. Both recycle and compost take different paths after they leave someone's house or office. This can be thought like the PBR. On a PBR traffic, certain typed of traffic takes different routes to get to their final destination. Just like garbage. If people put recycle and compost in the same garbage, that garbage has to go to processing plant and they have to separate recyclable material from non-recyclables. That takes time and extra money. That is just like not using PBR and using a routing protocol. It might cost more and it will take slightly more time for the packets to travel across a network.

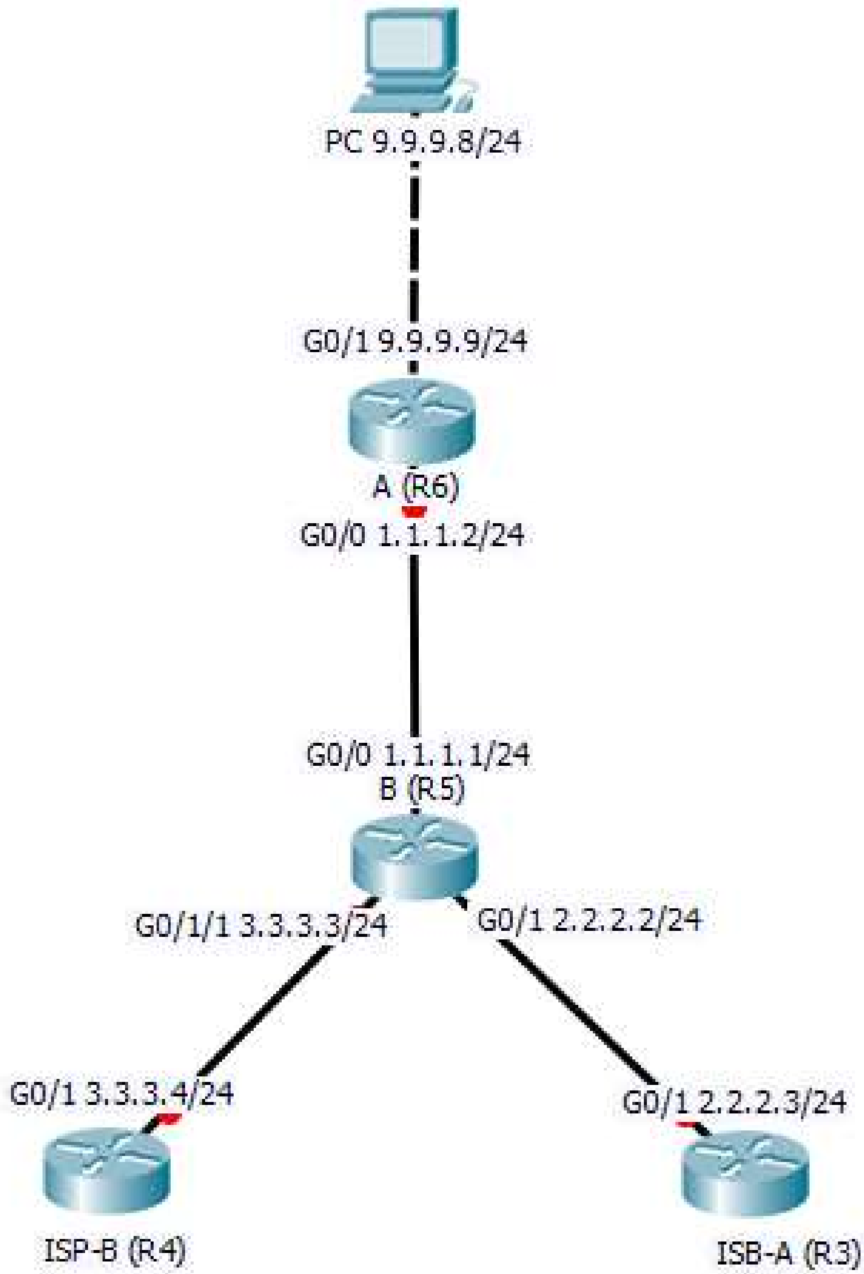
Lab Summary

In this lab we first set the topology with 4 routers. A PC was connected to one of them. One router was in between all three routers and the other two were HTTP and HTTPS servers. To establish connectivity, we did not use any routing protocols. Instead after setting IP addresses we set IP routes to create connectivity. One route going from A to the other routers in the network and routes coming to A from the other routers in the topology. Then we set ISP-B and ISP-A as HTTP and HTTPS servers with usernames and passwords on them. Then we set the policy based routes on the Router B which connects all the other routers. To do that we had to create a route map with two different entrees on that router. One was going to allow only HTTP traffic on one router and the other was going to allow HTTPS and any other kinds of traffic on the other router. On each of the route map entrees we specified which router was going to be the next hop of that route. In other words, which route a certain type of traffic was going to go through. Then we had to specify the types of traffic these route maps were going to allow, and to do that we used extended access lists. We created two extended access lists. One allowed HTTPS and any other traffic besides HTTP traffic and the other only allowed HTTP traffic and denied any other traffic. We then assigned those access lists to a route map entrée and the lab was complete. The route that was going to ISB-B only allowed HTTP traffic and the route that was going to ISB-A allowed every other type of traffic including HTTPS except for HTTP traffic. We then checked if the route maps were working. So, we tried to connect to ISB-B's HTTPS server but it didn't work. However, we were able to connect to the HTTP server of ISB-B since the route that was going to that router only allowed HTTP traffic. The visa versa happened for ISB-A. The HTTPS worked but the HTTP server didn't because the route that was going to ISB-A was not allowing HTTP traffic. After doing this, it proved that our route maps were working properly and that we successfully completed the lab.

Lab Commands

ip http server	This command allows the router to be a HTTP server.
ip http secure-server	This command allows the router to be a HTTPS server.
ip http authentication local	This command allows access to the web server by using a username and password.
ip policy route-map *calvin*	This command identifies the route map to use for PBR. One interface can have only one route map tag, but it can have several route map entries, each with its own sequence number. Entries are evaluated in order of their sequence numbers until the first match occurs. If no match occurs, packets are routed as usual.
access-list *101* **permit tcp any any eq www**	This command is an entry for the access-list. It enters a rule that every HTTP packet is allowed through the router. This command can also be used to block or permit any service or IP addresses which can be both source and/or destination addresses.
route-map *calvin* **permit** *1*	This command defines a route map to control where packets are output. This command puts the router into route-map configuration mode.
match ip address *101*	This command specifies the match criteria. Although there are many route-map matching options, here this command can specify only length and/or IP address.
set ip next-hop *3.3.3.4*	This command specifies the action(s) to take on the packets that match the criteria. This specific command sets next hop to which to route the packet.

Network Diagram



Configurations

ISB-A (R3)
Show run

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R3
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ipv6 cef
multilink bundle-name authenticated
crypto pki trustpoint TP-self-signed-4010493856
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4010493856
 revocation-check none
 rsakeypair TP-self-signed-4010493856
crypto pki certificate chain TP-self-signed-4010493856
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101
05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
43657274
  69666963 6174652D 34303130 34393338 3536301E 170D3136 30333232
31393533
  34385A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D34
30313034
  39333835 3630819F 300D0609 2A864886 F70D0101 01050003 818D0030
81890281
  8100D012 95E2AB20 5876A113 1821AF07 C07227FA 9A5430A4 6AAD673E
BD87DF61
  CB82606F C6F5F25B 00AABEB1 C0AA24BC DDCDD1A7 558916AA 103AC4CA
F3BC8495
  EF741BD4 561E9E3E 74A0BAF5 905E6D18 BF4CA791 DF74B236 5ECCF42A
5D67EE8C
  159A082F 35F96920 E94E6B1D A3E8AB3F 651B2509 C7C4512B F3016F4A
20993CD0
  DC310203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
301F0603
  551D2304 18301680 14D74761 A13B4843 1D9DDF5F 825A62B3 7A36B5F7
C0301D06
  03551D0E 04160414 D74761A1 3B48431D 9DDF5F82 5A62B37A 36B5F7C0
300D0609
  2A864886 F70D0101 05050003 81810051 CC3ED6DE A84BFA86 F20910C2
C995981E
```

```
  E499D7D7 C2F36B01 2DB7CAEB 685DD657 F743D7AC 5DC0A41D 6BC1AC07
C21E294D
  897EEBE2 C9E29A84 0A1C954D 017D8A5C 24C111E9 AF8972DF 1263B430
B88568DC
  9A594E85 C936222E 81F4C6BD 35E96887 7DD33E49 B7BA1649 111E40B2
0E6E5B9D
  1EA71304 9611AD0C 8734D82E D0B7BA
        quit
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180LH
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
username admin privilege 15 password 0 cisco
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 2.2.2.3 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
```

```
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S*    0.0.0.0/0 is directly connected, GigabitEthernet0/1
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, GigabitEthernet0/1
L        2.2.2.3/32 is directly connected, GigabitEthernet0/1
```

ISB-B (R4)
Show run

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R4
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ipv6 cef
multilink bundle-name authenticated
crypto pki trustpoint TP-self-signed-2319299287
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2319299287
 revocation-check none
 rsakeypair TP-self-signed-2319299287
crypto pki certificate chain TP-self-signed-2319299287
 certificate self-signed 01
```


```
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101
05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
43657274
  69666963 6174652D 32333139 32393932 3837301E 170D3136 30333232
31393438
  33315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32
33313932
  39393238 3730819F 300D0609 2A864886 F70D0101 01050003 818D0030
81890281
  810098D5 9F375AE5 5CD26F2A A7B00175 7F9309CC 1E72F47C 8AB007AD
691DA2B4
  317BE585 CDD1B00A B36B6126 2D12CCA1 A08FFC19 0E4F497F 6B13DF84
6EB8060A
```

```
  C6F528C3 09A1FC79 65CBD256 DDF82C08 8570FE52 A3EF9817 C0F0F954
D4F5D1A2
  A32A9F04 85FE25B0 C1545351 9970A93C 68FB8A91 31F29430 534C3CB5
AD7E1840
  47030203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
301F0603
  551D2304 18301680 14B4B160 E5AAA592 B97E6569 C8E67CDF 9AD6B045
41301D06
  03551D0E 04160414 B4B160E5 AAA592B9 7E6569C8 E67CDF9A D6B04541
300D0609
  2A864886 F70D0101 05050003 81810017 A7540FF7 FFCAA7B2 C44CE884
7BF4CD4F
  75AAB044 DBBD3DB5 97A22AEC 724E1D55 374E868C A5655DB8 3F6DB748
C92E675F
  BAF1B5D1 325D1E89 950DFF84 E5179846 3F8D750A 4D3D01C0 6627AD01
F612CE9A
  E0DF4E28 5B6F721B 854B95B0 A556FC8C D24E8D58 9818CC6F 0B2A5A91
BDF43748
  6F157AA3 A02CAC7E C4B104D1 C7C6F1
        quit
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180LN
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
username admin privilege 15 password 0 cisco
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 3.3.3.4 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
ip http server
ip http authentication local
```

```
ip http secure-server
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
End
```

Show ip route

```
S*    0.0.0.0/0 is directly connected, GigabitEthernet0/1
      3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        3.3.3.0/24 is directly connected, GigabitEthernet0/1
L        3.3.3.4/32 is directly connected, GigabitEthernet0/1
```

B (R5)

Show run

```
Current configuration : 1887 bytes Last configuration change at
20:17:08 UTC Tue Mar 22 2016
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R5
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX1520806Y
license accept end user agreement
license boot module c2900 technology-package uck9
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
```

```
 ip address 1.1.1.1 255.255.255.0
 ip policy route-map calvin
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 2.2.2.2 255.255.255.0
 ip policy route-map calvin
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 ip address 3.3.3.3 255.255.255.0
 ip policy route-map calvin
 duplex auto
 speed auto
ip forward-protocol nd
no ip http server
no ip http secure-server
ip route 9.9.9.0 255.255.255.0 GigabitEthernet0/0
access-list 101 permit tcp any any eq www
access-list 101 deny   tcp any any
access-list 102 permit tcp any any eq 443
access-list 102 deny   tcp any any
route-map calvin permit 1
 match ip address 101
 set ip next-hop 3.3.3.4
route-map calvin permit 2
 match ip address 102
 set ip next-hop 2.2.2.3
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
```

```
end
```

Show ip route

```
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, GigabitEthernet0/0
L        1.1.1.1/32 is directly connected, GigabitEthernet0/0
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, GigabitEthernet0/1
L        2.2.2.2/32 is directly connected, GigabitEthernet0/1
      3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        3.3.3.0/24 is directly connected, GigabitEthernet0/1/0
L        3.3.3.3/32 is directly connected, GigabitEthernet0/1/0
      9.0.0.0/24 is subnetted, 1 subnets
S        9.9.9.0 is directly connected, GigabitEthernet0/0
```

A (R6)
Show run

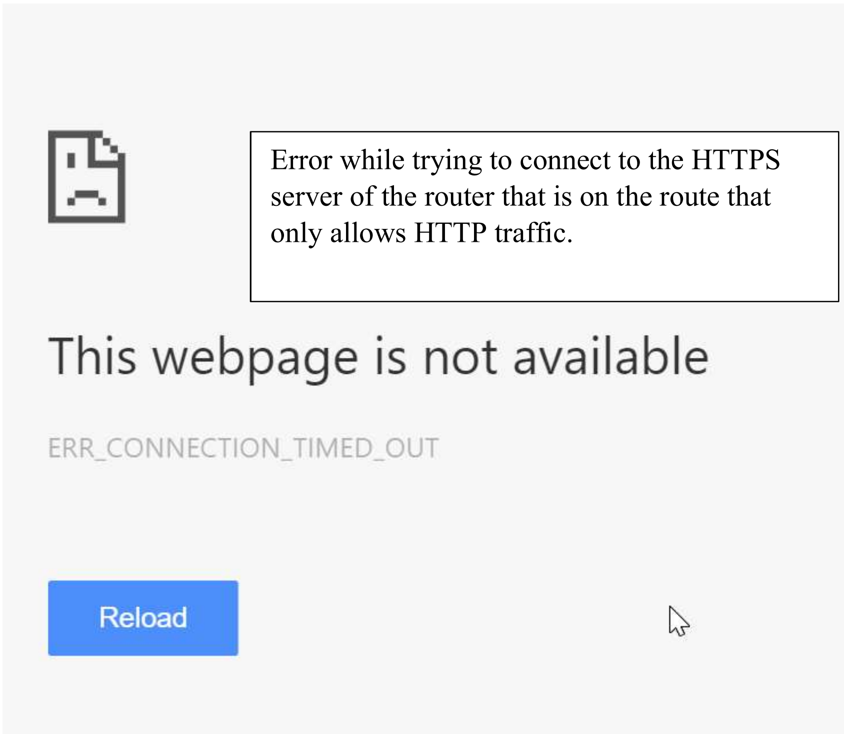
```
Current configuration : 1552 bytes Last configuration change at
20:30:42 UTC Tue Mar 22 2016
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R6
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX1520806Z
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 1.1.1.2 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 9.9.9.9 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
```

```
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 duplex auto
 speed auto
ip forward-protocol nd
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
End
```

Show ip route

```
S*    0.0.0.0/0 is directly connected, GigabitEthernet0/0
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, GigabitEthernet0/0
L        1.1.1.2/32 is directly connected, GigabitEthernet0/0
      9.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        9.9.9.0/24 is directly connected, GigabitEthernet0/1
L        9.9.9.9/32 is directly connected, GigabitEthernet0/1
```

Screenshots



Error while trying to connect to the HTTPS server of the router that is on the route that only allows HTTP traffic.

Successful connection while trying to connect to the HTTP server of the router that is on the route that only allows HTTP traffic.

Problems

As we were configuring this lab, we did not come across with many problems and completed the lab successfully in a short amount of time. The only two problems we had were related with entering commands. We had problems on figuring out which values or words to enter in some part of the commands. We entered wrong variables for those commands and spent some time trying to figure out the problems.

First problem we had, occurred during configuring the access lists. We were trying to allow HTTP on one access list and deny everything else and on the other one we were trying to allow HTTPS and everything except for HTTP. We were trying to specify our access list to do certain things with specific ports and protocols. And we were using the IP protocol while trying to enter the access list commands. However, the router was saying that it was an unrecognized command. So, we were trying to use a command that doesn't exist. The command was wrong and it was pretty challenging to find the solution to the problem, but after research and troubleshooting we realized that the problem was with the protocol we were using. We were using IP, however we needed to use TCP (TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation via which application programs can exchange data.) to allow HTTP and HTTPS ports. So, we changed the IP to TCP on the commands and router finally accepted them and the access lists were working.

The second problem we had was related with implementing the access lists that we created into different routes. We configured the access lists, now we needed to assign them to the routes that are going to HTTP and HTTPS servers. To do that, we have already created the route map "calvin" and we needed to configure two entries for that route map. To create them we used the command "route-map calvin permit 101". We used permit 101 for the number because we thought that number was supposed to match the number of the extended access list we created. However, PBR was not working. After some research, we learned that we didn't need to use the number of access list we were going to use on the route-map. The number didn't matter, but that wasn't causing the main problem. The thing that was causing the problem was the word "permit". We learned that we weren't supposed to use that word while entering the command. So it should just be “route-map calvin 1”. We didn’t need to put the word “permit” in there because the route was putting it in there after we enter it. After we entered the command without the “permit”, we looked at the running configuration on the router and the word “permit” was in the command. It looked just like the first command we entered first. After solving that problem, we did not have any more problems. We finished the configuration, verified that PBR was working and then we completed the lab successfully.

Conclusion

Policy Based Routing was a totally new concept for me. At first, I did not know what PBR was or how to configure it. After some research, I learned that I first needed to configure extended access lists, which I already knew how to do. The only new commands I used in this lab were the commands to create the specific route, route entries and the commands to use the access lists on those entries. It was an easy lab. It didn’t take a lot of commands or research to complete this lab. We had a couple of simple problems but they were mainly about entering certain values to the router. We didn’t have any conceptual problems, or big problems that took us a long time to solve. We solved our problems really fast and completed the lab.

VRF-lite

Purpose

The purpose of this lab is to create two different VRF networks that are sharing the same networks and connect the VRF networks into VLANs.

Background Information

Virtual routing and forwarding (VRF) is a technology included in IP (Internet Protocol) network routers that allows multiple instances of a routing table to exist in a router and work simultaneously. This increases functionality by allowing network paths to be segmented without using multiple devices. Because traffic is automatically segregated, VRF also increases network security and can eliminate the need for encryption and authentication. In addition, VRF requires a forwarding table that designates the next hop for each data packet, a list of devices that may be called upon to forward the packet and a set of rules and routing protocols that govern how the packet is forwarded. These tables prevent traffic from being forwarded outside a specific VRF path and also keep out traffic that should remain outside the VRF path.

The simplest form of VRF implementation is VRF Lite. In this implementation, each router within the network participates in the virtual routing environment in a peer-based fashion. While simple to deploy and appropriate for small to medium enterprises and shared data centers, VRF Lite does not scale to the size required by global enterprises or large carriers, as there is the need to implement each VRF instance on every router, including intermediate routers.

VRF-lite creates subnetworks that are completely separate from each other on the same router. Using two different VRP networks can be like using the I-90 highway bridge. Cars can go from either the normal lanes or the express lanes but they cannot go from express lane to normal lanes or the other way around. The bridge can be viewed as the connection between two routers and the lanes can be viewed as the VRF networks. Normal lanes make up a VRF network and the express lanes make another. Finally, the cars represent the packets that going through those links. The cars can’t change lanes, just like the packets on the two different VRF networks but they are both going between the same two destinations. Those destinations represent the routers.

VRFs are just like VLANs. A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible. The only difference between VFRs and VLANs is that VRFs are used in routing and VLANs are used in switching.

Lab Summery

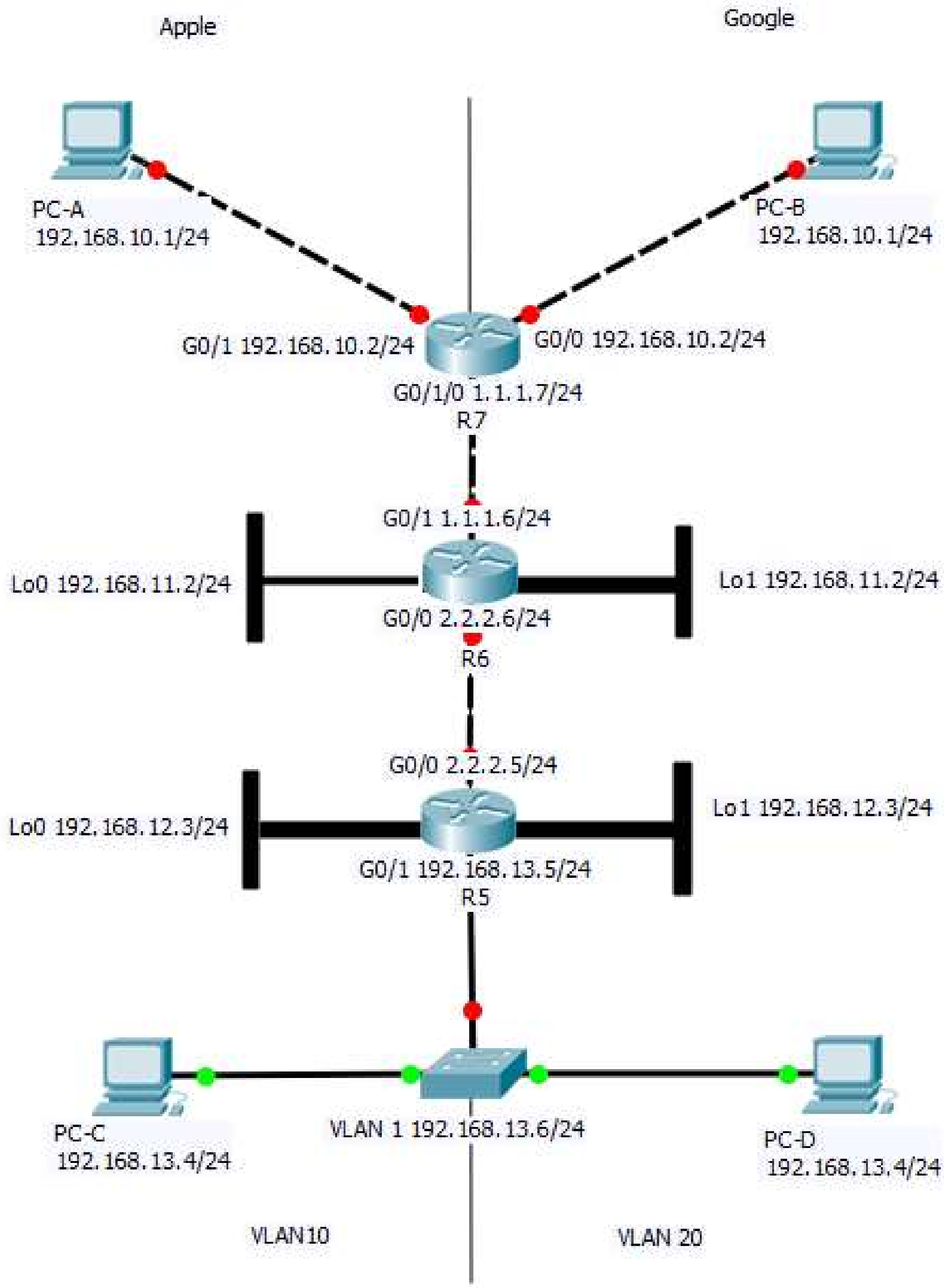
In this lab, we had 3 routers that were using VRF, and a switch using VLANs. We had two VRF networks. One named apple and the other names google. Both apple and google had the same addressing table. PC-A which was in apple and PC-B which was in google had the exact same IP addresses. This was the same case for the PC-C and PC-D and the loopbacks on the routers. They had the same IP addresses but they were still able to work. The reason for that is because they are in two different VRF which are completely different from each other. To do this in the routers we first created the VRFs. Apple and google. Then we assigned interfaces to the VRFs. This way the interface that was going to an end device will be either in apple or google VRF. Then we were able to set the same IP on the two different end devices. If we tried to do it before we created the VRFs, the router would say there is an addressing mismatch and would not let us to set both interfaces with the same IP address. We were able to set both interfaces with the same IP address after configuring VRF on those interfaces. That means that our configuration was successful.

Then, we moved onto the configuration of the links between the routers. They have to allow both apple and google VRFs. To do that, we used sub-interfaces on the interfaces that connect the routers and R5 and the switch. Those interfaces had one sub-interface for each VRF. Then we configured IP addresses and encapsulation in those sub-interfaces. The IP addresses were the same for both sub-interfaces and VRFs but the VLANs were different. We used VLAN 10 for apple and VLAN 20 for google in the encapsulations. After that we configured OSPF for connectivity but we had to configure it for both VRFs in all the routers. One for apple and google. After that, we were able to ping all the loopbacks that are in the same VRF as the PC we were pinging from. Finally, we configured the switch. We had a trunk port that was going to the R5 that allowed both VLAN 10 and 20. The port that was going to PC-C was an access port that only allowed VLAN 10 because it is in apple. The port that was going to PC-D was also an access port and only allowed VLAN 20 because it is in google VRF. After that we had end to end connectivity form PC-A to PC-C and from PC-B to PC-D. The lab was successfully complete.

Lab Commands

`ip vrf` *`apple`*	This command names the VRF, and enters the VRF configuration mode.
`ip vrf forwarding` *`google`*	This command associates the VRF with the Layer 3 interface.
`interface GigabitEthernet0/0.1`	This command enters into the sub-interface configuration mode. In this instance, the user is entering the first sub interface of the interface GigabitEthernet0/0.
`encapsulation dot1Q` *`10`*	This command is used in the sub-interface range configuration mode to apply a VLAN ID to the sub-interface.
`router ospf` *`1`* **`vrf`** *`apple`*	This command enters the OSPF configuration of a specific VRF network.

Network Diagram



Configurations

R7
Show run

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R7
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
ip vrf apple
ip vrf google
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX152885RE
license accept end user agreement
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip vrf forwarding google
 ip address 192.168.10.2 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip vrf forwarding apple
 ip address 192.168.10.2 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 no ip address
 duplex auto
 speed auto
interface GigabitEthernet0/1/0.1
```

```
 encapsulation dot1Q 10
 ip vrf forwarding apple
 ip address 1.1.1.7 255.255.255.0
interface GigabitEthernet0/1/0.2
 encapsulation dot1Q 20
 ip vrf forwarding google
 ip address 1.1.1.7 255.255.255.0
router ospf 1 vrf apple
 network 1.1.1.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
router ospf 2 vrf google
 network 1.1.1.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
End
```

Show ip route vrf apple

```
Routing Table: apple
Gateway of last resort is not set
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, GigabitEthernet0/1/0.1
L        1.1.1.7/32 is directly connected, GigabitEthernet0/1/0.1
      2.0.0.0/24 is subnetted, 1 subnets
O        2.2.2.0 [110/2] via 1.1.1.6, 01:14:01, GigabitEthernet0/1/0.1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/1
L        192.168.10.2/32 is directly connected, GigabitEthernet0/1
      192.168.11.0/32 is subnetted, 1 subnets
O        192.168.11.2 [110/2] via 1.1.1.6, 01:14:38,
GigabitEthernet0/1/0.1
      192.168.12.0/32 is subnetted, 1 subnets
O        192.168.12.3 [110/3] via 1.1.1.6, 01:13:51,
GigabitEthernet0/1/0.1
```

```
O     192.168.13.0/24 [110/3] via 1.1.1.6, 00:20:09,
GigabitEthernet0/1/0.1
```

Show ip route vrf google

```
Routing Table: google
Gateway of last resort is not set
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, GigabitEthernet0/1/0.2
L        1.1.1.7/32 is directly connected, GigabitEthernet0/1/0.2
      2.0.0.0/24 is subnetted, 1 subnets
O        2.2.2.0 [110/2] via 1.1.1.6, 01:15:08, GigabitEthernet0/1/0.2
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0
L        192.168.10.2/32 is directly connected, GigabitEthernet0/0
      192.168.11.0/32 is subnetted, 1 subnets
O        192.168.11.2 [110/2] via 1.1.1.6, 01:15:08,
GigabitEthernet0/1/0.2
      192.168.12.0/32 is subnetted, 1 subnets
O        192.168.12.3 [110/3] via 1.1.1.6, 01:14:25,
GigabitEthernet0/1/0.2
O     192.168.13.0/24 [110/3] via 1.1.1.6, 00:20:39,
GigabitEthernet0/1/0.2
```

R6
Show run

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R6
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
ip vrf apple
ip vrf google
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX1520806Z
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
redundancy
interface Loopback0
 ip vrf forwarding apple
 ip address 192.168.11.2 255.255.255.0
interface Loopback1
 ip vrf forwarding google
 ip address 192.168.11.2 255.255.255.0
```

```
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
interface GigabitEthernet0/0.1
 encapsulation dot1Q 10
 ip vrf forwarding apple
 ip address 2.2.2.6 255.255.255.0
interface GigabitEthernet0/0.2
 encapsulation dot1Q 20
 ip vrf forwarding google
 ip address 2.2.2.6 255.255.255.0
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
interface GigabitEthernet0/1.1
 encapsulation dot1Q 10
 ip vrf forwarding apple
 ip address 1.1.1.6 255.255.255.0
interface GigabitEthernet0/1.2
 encapsulation dot1Q 20
 ip vrf forwarding google
 ip address 1.1.1.6 255.255.255.0
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 duplex auto
 speed auto
router ospf 1 vrf apple
 network 1.1.1.0 0.0.0.255 area 0
 network 2.2.2.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
router ospf 2 vrf google
 network 1.1.1.0 0.0.0.255 area 0
 network 2.2.2.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
```

```
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
End
```

Show ip route vrf apple

```
Routing Table: apple
Gateway of last resort is not set
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, GigabitEthernet0/1.1
L        1.1.1.6/32 is directly connected, GigabitEthernet0/1.1
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, GigabitEthernet0/0.1
L        2.2.2.6/32 is directly connected, GigabitEthernet0/0.1
O     192.168.10.0/24 [110/2] via 1.1.1.7, 01:17:16,
GigabitEthernet0/1.1
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.11.0/24 is directly connected, Loopback0
L        192.168.11.2/32 is directly connected, Loopback0
      192.168.12.0/32 is subnetted, 1 subnets
O        192.168.12.3 [110/2] via 2.2.2.5, 01:16:42,
GigabitEthernet0/0.1
O     192.168.13.0/24 [110/2] via 2.2.2.5, 00:22:50,
GigabitEthernet0/0.1
```

Show ip route vrf google

```
Routing Table: google
Gateway of last resort is not set
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, GigabitEthernet0/1.2
L        1.1.1.6/32 is directly connected, GigabitEthernet0/1.2
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, GigabitEthernet0/0.2
L        2.2.2.6/32 is directly connected, GigabitEthernet0/0.2
O     192.168.10.0/24 [110/2] via 1.1.1.7, 01:17:33,
GigabitEthernet0/1.2
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.11.0/24 is directly connected, Loopback1
L        192.168.11.2/32 is directly connected, Loopback1
```

```
      192.168.12.0/32 is subnetted, 1 subnets
O        192.168.12.3 [110/2] via 2.2.2.5, 01:17:04,
GigabitEthernet0/0.2
O     192.168.13.0/24 [110/2] via 2.2.2.5, 00:23:07,
GigabitEthernet0/0.2
```

R5

Show run

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R5
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
ip vrf apple
ip vrf google
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX1520806Y
license accept end user agreement
license boot module c2900 technology-package uck9
redundancy
interface Loopback0
 ip vrf forwarding apple
 ip address 192.168.12.3 255.255.255.0
interface Loopback1
 ip vrf forwarding google
 ip address 192.168.12.3 255.255.255.0
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
interface GigabitEthernet0/0.1
 encapsulation dot1Q 10
 ip vrf forwarding apple
 ip address 2.2.2.5 255.255.255.0
interface GigabitEthernet0/0.2
 encapsulation dot1Q 20
 ip vrf forwarding google
 ip address 2.2.2.5 255.255.255.0
interface GigabitEthernet0/1
 no ip address
 duplex auto
```

```
 speed auto
interface GigabitEthernet0/1.1
 encapsulation dot1Q 10
 ip vrf forwarding apple
 ip address 192.168.13.5 255.255.255.0
interface GigabitEthernet0/1.2
 encapsulation dot1Q 20
 ip vrf forwarding google
 ip address 192.168.13.5 255.255.255.0
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 duplex auto
 speed auto
router ospf 1 vrf apple
 network 2.2.2.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.255 area 0
 network 192.168.13.0 0.0.0.255 area 0
router ospf 2 vrf google
 network 2.2.2.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.255 area 0
 network 192.168.13.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
End
```

Show ip route vrf apple

```
Routing Table: apple
Gateway of last resort is not set
      1.0.0.0/24 is subnetted, 1 subnets
O        1.1.1.0 [110/2] via 2.2.2.6, 01:18:40, GigabitEthernet0/0.1
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, GigabitEthernet0/0.1
L        2.2.2.5/32 is directly connected, GigabitEthernet0/0.1
O     192.168.10.0/24 [110/3] via 2.2.2.6, 01:18:40,
GigabitEthernet0/0.1
      192.168.11.0/32 is subnetted, 1 subnets
O        192.168.11.2 [110/2] via 2.2.2.6, 01:18:40,
GigabitEthernet0/0.1
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, Loopback0
L        192.168.12.3/32 is directly connected, Loopback0
      192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.13.0/24 is directly connected, GigabitEthernet0/1.1
L        192.168.13.5/32 is directly connected, GigabitEthernet0/1.1
```

Show ip route vrf google

```
Routing Table: google
Gateway of last resort is not set
      1.0.0.0/24 is subnetted, 1 subnets
O        1.1.1.0 [110/2] via 2.2.2.6, 01:19:12, GigabitEthernet0/0.2
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, GigabitEthernet0/0.2
L        2.2.2.5/32 is directly connected, GigabitEthernet0/0.2
O     192.168.10.0/24 [110/3] via 2.2.2.6, 01:19:12,
GigabitEthernet0/0.2
      192.168.11.0/32 is subnetted, 1 subnets
O        192.168.11.2 [110/2] via 2.2.2.6, 01:19:12,
GigabitEthernet0/0.2
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, Loopback1
L        192.168.12.3/32 is directly connected, Loopback1
      192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.13.0/24 is directly connected, GigabitEthernet0/1.2
L        192.168.13.5/32 is directly connected, GigabitEthernet0/1.2
```

Switch
Show run
```
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Switch
boot-start-marker
boot-end-marker
no aaa new-model
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
vlan internal allocation policy ascending
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface FastEthernet0/2
 switchport access vlan 10
interface FastEthernet0/3
 switchport access vlan 20
interface FastEthernet0/4
interface FastEthernet0/5
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface Vlan1
 ip address 192.168.13.6 255.255.255.0
ip classless
ip http server
ip http secure-server
ip sla enable reaction-alerts
line con 0
line vty 5 15
end
```

Switch PC-D
show run
```
Current configuration : 1332 bytes
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname Switch
ip subnet-zero
ip ssh time-out 120
```

```
ip ssh authentication-retries 3
vtp domain HackAttacks
vtp mode transparent
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
vlan 10
 name apple
vlan 20
 name google
interface FastEthernet0/1
 switchport access vlan 20
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
interface Vlan20
 ip address 192.168.13.4 255.255.255.0
ip http server
line con 0
line vty 5 15
end
```

Switch PC-C
Show run

```
Current configuration : 2748 bytes
version 12.1
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname Switch
vlan 10
 name apple
vlan 20
 name google
ip subnet-zero
vtp domain HackAttacks
vtp mode transparent
spanning-tree extend system-id
interface FastEthernet0/1
 switchport access vlan 10
 no ip address
interface FastEthernet0/2
 no ip address
```

```
interface FastEthernet0/3
 no ip address
interface FastEthernet0/4
 no ip address
interface GigabitEthernet0/1
 no ip address
interface GigabitEthernet0/2
 no ip address
interface Vlan1
 no ip address
 shutdown
interface Vlan10
 ip address 192.168.13.4 255.255.255.0
interface Vlan20
 no ip address
ip classless
ip http server
line con 0
line vty 5 15
end
```

Problems

In this lab, we had a couple of issues that were all related with connectivity. The first problem we had was, we weren't able to ping between the routers. It looked like everything was configured right and the ports were on. We couldn't find the problem for a little bit, then we thought that we might have configured VRF or something was missing. We made more research and realized that we needed sub-interfaces. Turns out, we tried to configure both VRFs on the same port, however it doesn't work like that. We needed to configure sub-interfaces and set IP addresses. So we did that but the links were still not working. After researching the details of using sub-interfaces in VRF networks, we learned that we were missing the encapsulation command. This command gives the VLAN or VRF an identification number which was going to be useful later when we configured VLANs on the switch. So then we entered the different VLAN numbers for both VRFs and we were able to ping the first hop now.

Even though we fixed the problem of not being able to ping the first hop from a router, we now had a new problem. We weren't able to ping anything beyond the first hop. That meant that our routing protocol was not working. When we first configured our routers, we used EIGRP as our routing protocol but after doing some research about VRF and routing protocols, we learned that EIGRP is nor compatible with VRF. Since we had two VRFs, we also needed two separate routing tables. EIGRP didn't have any commands to specify different VRFs and therefore was not able to create two routing tables. According to our research the one routing protocol that is compatible with VRF is OSPF. OSPF allows us to identify which VRF were are trying to configure the routing table to unlike EIGRP. So we configured OSPF on all routers and for both VRFs. After configuring that we were able ping every device.

Final problem we had was a simple problem with the VLANs on the switch. We configured the trunk port on the switch which allowed all VLANs to go through but we made a simple mistake on the access ports of that same switch. Since we did not have four PCs, we decided to use two different switches instead of PC-C and PC-D. While setting the IP addresses of these switches that replaced the PCs, we assigned the address under the VLANs they should be in. So the switch that represented PC-C was on VLAN 10 and PC-D was on VLAN 20 but we weren't able to ping the PCs. There was something wrong. After checking the configurations and the topology we realized that the access port that was connect to the PC-C was an access port that only allowed VLAN 20, not 10. For PC-D it was the other was around. The access port that was going to PC-D only allowed VLAN 10 not 20. Fixing this problem was simple. We simply changed the cables on the switch so that PCs were on the VLANs that they belong to. After this change, we were able to ping from PC-A to PC-C and from PC-B to PC-D. We solved all of our problems and completed the lab with the end to end connectivity.

Conclusion

This lab first felt like a completely different lab and nothing like we have ever done before because I have never heard of the term VRF before. However, after doing research on what VRF is, I learned it is just basically VLANs for router and I have done VLANs quite a lot of times before. We configured two different VRFs under the name of google and apple. They were completely separate from each other even though they were using the same routers. We also configured two different VLANs that were connected to the VRFs. We had some problems while configuring the links between the routers that were supposed to allow both VRFs and some simple problems with assigning VLANs to the access ports of the switch. But overall it was an easy lab because the problems were not too difficult to figure out.

FHRP

Purpose

The purpose of this lab is to use 3 different first-hop redundancy protocols which are HSRP, GLBP and VRRP to create a redundant network that can access internet from 2 different routes.

Background Information

Any network should be redundant in today's world. There are a lot of companies who use internet 24/7 and their business relies on remote customers. Those companies want to stay connected to the internet all the time. However, things can go wrong in a network, so in order for those companies to stay connected, they have to have backups in their networks so when one link goes down. End users should be able to talk to each other or access internet without noticing any problem. In order to do that there has to be at least 2 routes that are going to the internet and either GLBP, HSRP or VRRP have to be configured on the routers. So, when the one goes down, the other one can kick in and the network will still have access to the internet. GLBP, HSRP and VRRP are types of first-hop redundancy protocols that can change connection between the 2 routes. It's their job to detect a connectivity problem and change the link to a connection that doesn't have any problems

First-hop redundancy is almost like a long-distance cruise ship. Those ships generally have 2 or 3 engines depending on the size of the ship. The reason for that is because if one engine breaks down in the middle of the ocean, they can use the other engine to go the nearest port and get it fixed. In this case number of engines, the ship has is like the number of routes that are going to internet in a network. The ship staff who detect the problem with the first engine and start using the second engine is like HSRP, GLBP and VRRP. They act like the ship staff for the network, detect problems and change the routes if necessary. They do same job in slightly different ways.

Host Standby Routing Protocol (HSRP) provides default gateway redundancy using one active and one standby router. That means it uses a virtual default gateway instead of an IP address on a router. The traffic can go out to the internet using any route since the routers have a common virtual IP. HSRP is like the ship is going with only 1 engine in full speed and when that engine goes down, the other engine starts working with full power to keep the ship going in the same speed. HSRP uses only 1 route at a time. Virtual Router Redundancy Protocol (VRRP) provides redundancy the same way as HSRP. The only difference is HSRP is licensed by Cisco Systems but VRRP is open source which means the original software code is freely available and maybe redistributed or modified.

Gateway Load Balancing Protocol (GLBP) supports arbitrary load balancing in addition to redundancy across gateways. When both of the routes are working, this protocol sends half of the packets from one route, the other half from the other route. It is just like the cruise ship using half power from both engines and going with full speed without damaging the engines. And when an engine goes down the other engine applies full power to keep the ship going in the same speed. Same with a network using GLBP, when a route goes down, all the packets go through the other route and the network keeps running in the same speed.

These first-hop redundancy protocols determine which router is going to be active and which router is going to be in the standby mode. The active router is the router that the traffic is going through and the standby router is the one for backup. When there is a problem with the active router, the protocol turns the active router into standby and the standby router to active which changes the router where the traffic is flowing through.

Lab Summary

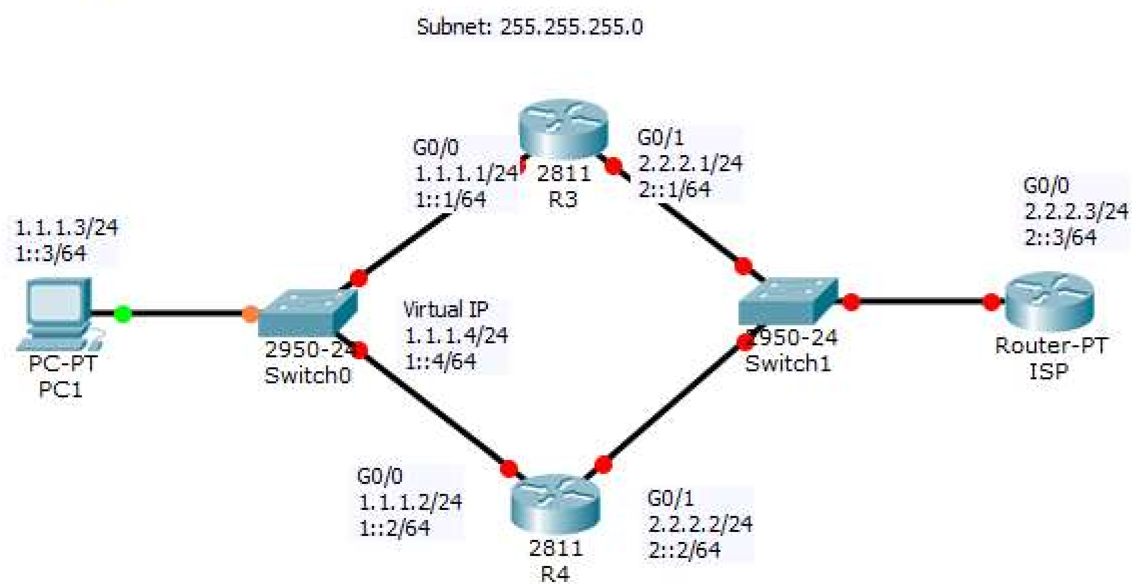
In this lab, we set up 2 routers that are connected a switch on one side. A PC is connected on the other end of the switch. The other side of the 2 routers represented the Internet. We set up HSRP with a virtual IP address on the network with the host using the standby command. We used group 1 for IPv4 and group 2 for IPv6. Then we did the same thing for GLBP, but instead of using the standby command, we used the glbp command with 2 groups. Finally, we set up VRRP. On this one instead of using 2 routers, we used one router and a Cisco Catalyst 6500 switch. We used the vrrp command to create a group for IPv4 and create a virtual IP address for the local network. In HSRP and GLBP we also configured OSPF to create connectivity between the two routers and the ISP.

Lab Commands

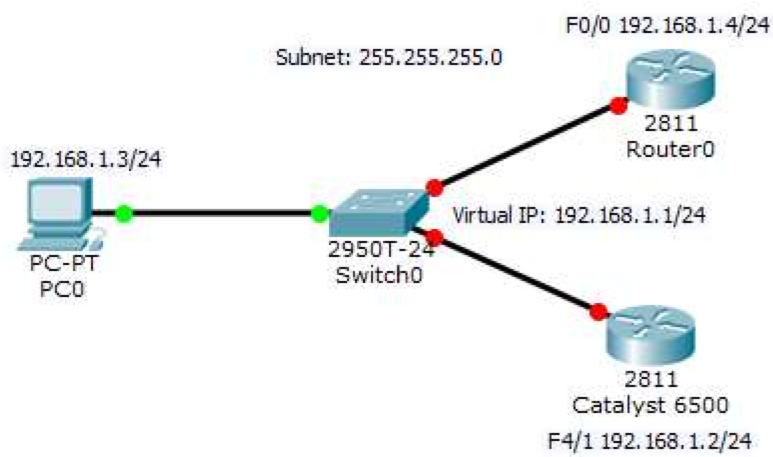
`standby version` *`2`*	This command enables the router to run HSRPv2 instead of HSRPv1. On HSRPv1 timer values are not advertised but in HSRPv2 they are.
`standby` *`1`* **`ip`** *`1.1.1.4`*	This command creates a virtual IP address (1.1.1.4) for group 1 which is also the default gateway for the local PC. It is used only to configure HSRP.
`standby` *`1`* **`timers`** *`1 2`*	This command is used to configure the time between hello packets and the time before other routers declare the active router to be down.
`standby` *`1`* **`preempt`**	This command is used so that if a router fails and comes back up, the preemption occurs and restores load-balancing.
`glbp` *`1`* **`ip`** *`1.1.1.4`*	This command creates a virtual IP address (1.1.1.4) for group 1 which is also the default gateway for the local PC. It is used only to configure GLBP.
`glbp` *`1`* **`timers`** *`1 2`*	Configures the interval between successive hello packets sent by the active virtual gateway in a GLBP group.
`glbp` *`1`* **`preempt`**	This command is used so that if a router fails and comes back up, the preemption occurs and restores load-balancing.
`vrrp` *`10`* **`ip`** *`192.168.1.1`*	This command creates a virtual IP address (192.168.1.1) for group 10 which is also the default gateway for the local PC. It is used only to configure VRRP.

Network Diagrams

HSRP, GLBP



VRRP



Configurations

HSRP
R3
Show run

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R3
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180M5
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 1.1.1.1 255.255.255.0
 standby version 2
 standby 1 ip 1.1.1.4
 standby 1 timers 1 2
 standby 2 timers 1 2
 duplex auto
 speed auto
 ipv6 address 1::1/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/1
 ip address 2.2.2.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2::1/64
 ipv6 ospf 1 area 0
interface Serial0/0/0
 no ip address
 shutdown
interface Serial0/0/1
 no ip address
```

```
 shutdown
 clock rate 2000000
router ospf 1
 network 0.0.0.0 255.255.255.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, GigabitEthernet0/0
L        1.1.1.1/32 is directly connected, GigabitEthernet0/0
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, GigabitEthernet0/1
L        2.2.2.1/32 is directly connected, GigabitEthernet0/1
```

Show ipv6 route

```
C   1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   1::1/128 [0/0]
     via GigabitEthernet0/0, receive
C   2::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2::1/128 [0/0]
     via GigabitEthernet0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

R4

Show run

```
version 15.2
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
no service password-encryption
hostname R4
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180M8
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 1.1.1.2 255.255.255.0
 standby version 2
 standby 1 ip 1.1.1.4
 standby 1 timers 1 2
 standby 1 preempt
 standby 2 timers 1 2
 standby 2 preempt
 duplex auto
 speed auto
 ipv6 address 1::2/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/1
 ip address 2.2.2.2 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2::2/64
 ipv6 ospf 1 area 0
interface Serial0/0/0
 no ip address
 shutdown
 ipv6 address 3::2/64
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router ospf 1
 network 1.1.1.0 0.0.0.255 area 0
```

```
 network 2.2.2.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
End
```

Show ip route

```
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, GigabitEthernet0/0
L        1.1.1.2/32 is directly connected, GigabitEthernet0/0
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, GigabitEthernet0/1
L        2.2.2.2/32 is directly connected, GigabitEthernet0/1
```

Show ipv6 route

```
C   1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   1::2/128 [0/0]
     via GigabitEthernet0/0, receive
C   2::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2::2/128 [0/0]
     via GigabitEthernet0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

ISP

Show run

```
Current configuration : 1378 bytes
Last configuration change at 20:58:27 UTC Fri Oct 2 2015
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
 hostname ISP
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
 ipv6 unicast-routing
ipv6 cef
ip source-route
ip cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX15208074
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
redundancy
interface GigabitEthernet0/0
 ip address 2.2.2.3 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2::3/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
router ospf 1
 log-adjacency-changes
 network 2.2.2.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
 log-adjacency-changes
control-plane
gatekeeper
 shutdown
line con 0
line aux 0
line vty 0 4
 login
```

```
scheduler allocate 20000 1000
end
```

Show ip route

```
   1.0.0.0/24 is subnetted, 1 subnets
O        1.1.1.0 [110/2] via 2.2.2.2, 00:14:52, GigabitEthernet0/0
                 [110/2] via 2.2.2.1, 00:15:29, GigabitEthernet0/0
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, GigabitEthernet0/0
L        2.2.2.3/32 is directly connected, GigabitEthernet0/0
```

Show ipv6 route

```
O   1::/64 [110/2]
     via FE80::26E9:B3FF:FE3C:1949, GigabitEthernet0/0
     via FE80::7ADA:6EFF:FE99:AA01, GigabitEthernet0/0
C   2::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2::3/128 [0/0]
     via GigabitEthernet0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

GLBP
R3
Show run

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R3
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180M5
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
```

```
 ip address 1.1.1.1 255.255.255.0
 glbp 1 ip 1.1.1.4
 glbp 1 timers 1 2
 glbp 2 timers 1 2
 duplex auto
 speed auto
 ipv6 address 1::1/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/1
 ip address 2.2.2.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2::1/64
 ipv6 ospf 1 area 0
interface Serial0/0/0
 no ip address
 shutdown
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router ospf 1
 network 0.0.0.0 255.255.255.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
   1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, GigabitEthernet0/0
L        1.1.1.1/32 is directly connected, GigabitEthernet0/0
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
```

```
C        2.2.2.0/24 is directly connected, GigabitEthernet0/1
L        2.2.2.1/32 is directly connected, GigabitEthernet0/1
```

Show ipv6 route

```
C   1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   1::1/128 [0/0]
     via GigabitEthernet0/0, receive
C   2::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2::1/128 [0/0]
     via GigabitEthernet0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

R4

Show run

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R4
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ip domain lookup
 ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX180180M8
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 1.1.1.2 255.255.255.0
 glbp 1 ip 1.1.1.4
 glbp 1 timers 1 2
 glbp 1 preempt
 glbp 2 timers 1 2
 glbp 2 preempt
 duplex auto
 speed auto
```

```
 ipv6 address 1::2/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/1
 ip address 2.2.2.2 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2::2/64
 ipv6 ospf 1 area 0
interface Serial0/0/0
 no ip address
 shutdown
 ipv6 address 3::2/64
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router ospf 1
 network 1.1.1.0 0.0.0.255 area 0
 network 2.2.2.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
End
```

Show ip route

```
1.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        1.1.1.0/24 is directly connected, GigabitEthernet0/0
L        1.1.1.2/32 is directly connected, GigabitEthernet0/0
L        1.1.1.4/32 is directly connected, GigabitEthernet0/0
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, GigabitEthernet0/1
L        2.2.2.2/32 is directly connected, GigabitEthernet0/1
```

Show ipv6 route

```
C   1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   1::2/128 [0/0]
     via GigabitEthernet0/0, receive
C   2::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2::2/128 [0/0]
     via GigabitEthernet0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

ISP

Show run

```
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
 hostname ISP
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
 ipv6 unicast-routing
ipv6 cef
ip source-route
ip cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX15208074
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
redundancy
interface GigabitEthernet0/0
 ip address 2.2.2.3 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2::3/64
 ipv6 ospf 1 area 0
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
```

```
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
router ospf 1
 log-adjacency-changes
 network 2.2.2.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ipv6 router ospf 1
 log-adjacency-changes
control-plane
gatekeeper
 shutdown
line con 0
line aux 0
line vty 0 4
 login
scheduler allocate 20000 1000
end
```

Show ip route

```
   1.0.0.0/24 is subnetted, 1 subnets
O        1.1.1.0 [110/2] via 2.2.2.2, 00:03:43, GigabitEthernet0/0
                 [110/2] via 2.2.2.1, 00:04:29, GigabitEthernet0/0
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, GigabitEthernet0/0
L        2.2.2.3/32 is directly connected, GigabitEthernet0/0
```

Show ipv6 route

```
O   1::/64 [110/2]
     via FE80::7ADA:6EFF:FE99:AA01, GigabitEthernet0/0
     via FE80::26E9:B3FF:FE3C:1949, GigabitEthernet0/0
C   2::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2::3/128 [0/0]
     via GigabitEthernet0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

VRRP

R8

Show run

```
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R8
boot-start-marker
boot system flash:c2800nm-adventerprisek9-mz.151-4.M8.bin
```

```
boot-end-marker
no aaa new-model
memory-size iomem 10
dot11 syslog
ip source-route
ip cef
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
crypto pki token default removal timeout 0
license udi pid CISCO2811 sn FTX1024A4AS
archive
 log config
  hidekeys
vtp domain cisco
vtp mode transparent
redundancy
interface FastEthernet0/0
 ip address 192.168.1.4 255.255.255.0
 duplex auto
 speed auto
 vrrp 10 ip 192.168.1.1
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/1/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
interface FastEthernet0/3/0
 no ip address
interface FastEthernet0/3/1
 no ip address
interface FastEthernet0/3/2
 no ip address
interface FastEthernet0/3/3
 no ip address
```

```
interface Vlan1
 no ip address
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
mgcp profile default
line con 0
line aux 0
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route

```
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, FastEthernet0/0
L        192.168.1.4/32 is directly connected, FastEthernet0/0
```

Catalyst 6500

Show run

```
upgrade fpd auto
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service counters max age 5
hostname Catalyst_6500
boot-start-marker
boot system sup-bootdisk:s3223-advipservicesk9_wan-mz.122-33.SXH4.bin
boot-end-marker
no aaa new-model
call-home
  alert-group configuration
  alert-group diagnostic
  alert-group environment
  alert-group inventory
  alert-group syslog
 profile "CiscoTAC-1"
   no active
   no destination transport-method http
   destination transport-method email
   destination address email callhome@cisco.com
   destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
   subscribe-to-alert-group diagnostic severity minor
   subscribe-to-alert-group environment severity minor
   subscribe-to-alert-group syslog severity major pattern ".*"
   subscribe-to-alert-group configuration periodic monthly 25 13:19
```

```
   subscribe-to-alert-group inventory periodic monthly 25 13:04
ip subnet-zero
no ip domain-lookup
mls ip slb purge global
mls netflow interface
no mls flow ip
no mls flow ipv6
mls cef error action reset
redundancy
 keepalive-enable
 mode sso
 main-cpu
  auto-sync running-config
spanning-tree mode pvst
spanning-tree extend system-id
system flowcontrol bus auto
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
interface FastEthernet4/1
 ip address 192.168.1.2 255.255.255.0
 vrrp 10 ip 192.168.1.1
interface Vlan1
 no ip address
 shutdown
ip classless
no ip http server
no ip http secure-server
control-plane
dial-peer cor custom
line con 0
 logging synchronous
line vty 0 4
 login
line vty 5 15
 login
end
```

Show ip route

```
C    192.168.1.0/24 is directly connected, FastEthernet4/1
```

Proof of FHRP

HSRP

IPv4

```
C:\Users\Admin>ping -t 2.2.2.3

Pinging 2.2.2.3 with 32 bytes of data:
Reply from 2.2.2.3: bytes=32 time=1ms TTL=254
Reply from 2.2.2.3: bytes=32 time=1ms TTL=254
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 2.2.2.3: bytes=32 time=1ms TTL=254
Reply from 2.2.2.3: bytes=32 time<1ms TTL=254
Reply from 2.2.2.3: bytes=32 time=1ms TTL=254
Reply from 2.2.2.3: bytes=32 time=1ms TTL=254

Ping statistics for 2.2.2.3:
    Packets: Sent = 14, Received = 6, Lost = 8 (57% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Pinging from one active route

First route fails, HSRP detects the problem.

HSRP recovers and switches to the other route

IPv6:

```
C:\Users\Admin>ping -t 2::3

Pinging 2::3 with 32 bytes of data:
Reply from 2::3: time=1ms
Reply from 2::3: time=1ms
Reply from 2::3: time=1ms
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 2::3: time=1ms
Reply from 2::3: time=1ms
Reply from 2::3: time=1ms
Reply from 2::3: time<1ms
Reply from 2::3: time<1ms
```

Pinging from one active route

First route fails, HSRP detects the problem.

HSRP recovers and switches to the other route

GLBP

IPv4:

```
Reply from 2.2.2.3: bytes=32 time=1ms TTL=254
Reply from 2.2.2.3: bytes=32 time=1ms TTL=254
Reply from 2.2.2.3: bytes=32 time=1ms TTL=254
Reply from 2.2.2.3: bytes=32 time=1ms TTL=254
Reply from 2.2.2.3: bytes=32 time<1ms TTL=254
Reply from 2.2.2.3: bytes=32 time=1ms TTL=254
```

Pinging from one active route

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

First route fails, GLBP detects the problem.

```
Reply from 2.2.2.3: bytes=32 time=1ms TTL=254
Reply from 2.2.2.3: bytes=32 time=1ms TTL=254
Reply from 2.2.2.3: bytes=32 time=1ms TTL=254
Reply from 2.2.2.3: bytes=32 time<1ms TTL=254
Reply from 2.2.2.3: bytes=32 time=1ms TTL=254
Reply from 2.2.2.3: bytes=32 time=1ms TTL=254
Reply from 2.2.2.3: bytes=32 time=1ms TTL=254
Reply from 2.2.2.3: bytes=32 time=1ms TTL=254
```

GLBP recovers and switches to the other route

IPv6

```
Reply from 2::3: time<1ms
Reply from 2::3: time=1ms
Reply from 2::3: time<1ms
Reply from 2::3: time=1ms
Reply from 2::3: time<1ms
```

Pinging from one active route

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

First route fails, GLBP detects the problem.

```
Reply from 2::3: time=1ms
Reply from 2::3: time=1ms
Reply from 2::3: time=1ms
Reply from 2::3: time<1ms
Reply from 2::3: time<1ms
```

GLBP recovers and switches to the other route

VRRP

IPv4:

```
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
```

Pinging from one active route

```
Request timed out.
```

First route fails, VRRP detects the problem.

```
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
```

VRRP recovers and switches to the other route

Problems

We didn't have any problems with setting GLBP and VRRP after doing HSRP. We only had problems while setting up the HSRP.

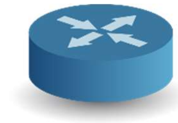
We didn't treat one side of the network as Internet. We tried to have connection from the local PC to the host in the internet and from the host in the internet to the local host, however we forgot that the host in the internet didn't have to be able to connect to the local PC, it was just the local PC that had to have connection to the host in internet. We first configured HSRP so that both sides had a different standby number. But we only needed a standby number on the network of the local host.

We fixed the standby problem by just using one standby number in the local network but now there was a default gateway problem with the host that represented the internet. When we set the default gateway as the interface of one of the routers, pings were trying to get back from that same router whether it was down or not. We decided to replace that host with a router to get rid of the default gateway problem, then we configured OSPF on all 3 routers so they had connectivity between each other.

After we fixed the standby number, default gateway and OSPF problems HSRP was up and running.

Conclusion

In this lab, we used 3 First-Hop Redundancy Protocols to create redundant networks that connected to the internet from 2 routes. We used HSRP, GLBP and VRRP to reach to ISP from two different routes. We configured OSPF on the HSRP and GLBP networks to create connectivity between routers and the ISP. We had problems while configuring HSRP but once we understood how it worked we were able to implement that experience and knowledge on GLBP and VRRP without any problems. They are really similar to each other while configuring with only some subtle differences. The hardest part of this lab was creating the topology. We had a hard time on figuring out how to make a network redundant and how to implement HSRP to a redundant network. But once figured that out, the rest was easy. This lab helped me understand the concept of redundancy and the different protocols that are used to implement redundancy in a network.



Layer 2 Attacks

DHCP Starvation Attack and Mitigation

Purpose

The purpose of the DHCP starvation attack is to stop a DHCP server from lending IP address to its clients and eventually prevent those clients from entering the network with using DHCP.

Background Information

Every building has to have an address in order to receive mail or in order for other people to easily find the building. However, people don't generally come up with their home or office addresses, their address are generally assigned by the city they belong to. The same idea works for the internet. Every computer has to have an IP address in order to be connected to the internet and access billions of websites. But computers generally don't come up with their own IP addresses either. In this case Dynamic Host Configuration Protocol (DHCP) servers in the internet do city's job of giving addresses. DHCP clients, which are computers, laptops, smart phones, smart TVs, tablets, smart watches and pretty much everything people use that is connected to the internet, ask for IP addresses from DHCP servers, which can be your home router or a giant server in the internet. DHCP servers lend addresses to the clients. The time the address will be lend to a client can be controlled along with how often the server is going to relend a new address to the client. Lending IP addresses to hosts is pretty much what DHCP is all about.

DHCP starvation attack is when an attacker sends ton of DHCP discovery packets to the router. When the router gets all of these messages at the same time, it will have really hard time processing them, its CPU will increase dramatically just in matter of seconds, it will become really slow and it won't be able to send out address after one point. The DHCP server will stop working. This can be viewed like a busy intersection that is not designed to the huge demand and can't handle the busy traffic. There will be huge lines of cars at the end of every light and since the traffic is moving really slowly, one way at a time, the cars will keep piling, the line will get longer and the traffic will eventually stop and no one would be able to go through the intersection. In this case router is the intersection, and the cars are the DHCP discover packets. There are so many of that router can't process them anymore and eventually fail.

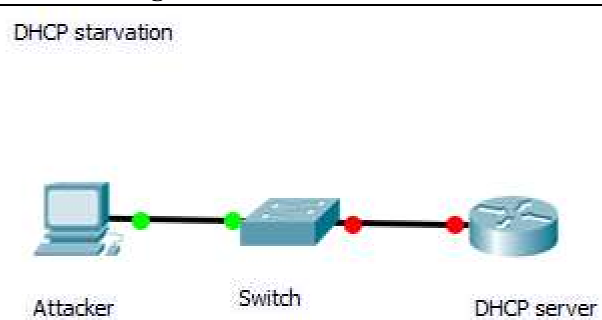
Lab Summary

In this lab, we first created the topology, connected a PC and a router to a switch. We did not configure an IP address on the PC, instead we configured it as a DHCP client and configured the router as a DHCP server to give out an IP address to the PC. After we had connectivity between the PC and the router, we were ready to move on to the DHCP starvation attack. We ran Kali Linux as a virtual machine in the host. In the Kali Linux command line, we entered the "yersinia –G" command that opened the Yersinia program. In the program, we first clicked on the "Launch Attack" button and in the window, that popped up, we clicked on the DHCP tab. Under the DHCP tab we selected the "sending DISCOVER packet" option and clicked OK. The attacked has started after we clicked OK. We were monitoring the attack from the router at the same time and the CPU percentage on the router went from 0% to 97% in seconds. The router got really slow. We also tried to get an IP address from the Router's DHCP server on a host and it said that the DHCP server failed and could not give out addresses. Our attack was successful. To mitigate this attack, we had to go to the switch and configure port security. We configured the used interfaces so that they only allowed 2 MAC addresses maximum, and if there were more than 2 address the ports would shut down automatically. We then shut down all the unused ports. We then cleared router's mac address table and stopped the attack so that the CPU was back to normal and the DHCP server was working again. After the PC got an IP address, we launched the same attack using Kali Linux but with port security on the switch this time. Nothing happened to the router. The CPU was normal and the DHCP server working just fine. Our mitigation of the attack was successful.

Lab Commands

yersinia -G	This command is used in Kali Linux terminal and it launches the Yersinia application.
ip dhcp excluded-address *192.168.1.1*	This command defines the IP addresses a DHCP server should not give out to its clients.
ip dhcp pool *Starvation*	This command creates the DHCP on a Cisco Router and gives a name for the DHCP server.
network *192.168.1.0 255.255.255.0*	This command defines which network the router is going give out IP addresses from.
domain-name *Starvation*	This command gives a domain name to the DHCP pool.
dns-server *192.168.1.1*	This command defines the IP address of the DNS server.
default-router *192.168.1.1*	This command defines the IP address of the default router for the DHCP server and pool.
switchport mode access	This command is entered under an interface on the switch and it only allows one VLAN on that switch.
switchport port-security	This command creates port securtiy on an interface on the switch.
switchport port-security maximum *2*	This command only allows 2 MAC address maximum on an interface on the switch and if there are more than 2 MAC address it autamatically shuts down the interface.
switchport port-security mac-address sticky	With this command, the switch saves the MAC address that it already learned in the past and those address stay on the switch until the command is disabled.
spanning-tree portfast	This command enables PortFast on the interface and puts the interface into a forwarding state.

Network Diagram



Configurations

Router

```
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname DHCP_SERVER
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
no ipv6 cef
ip source-route
ip cef
ip dhcp excluded-address 192.168.1.1
ip dhcp pool Starvation
 network 192.168.1.0 255.255.255.0
 domain-name Starvation
 dns-server 192.168.1.1
 default-router 192.168.1.1
no ip domain lookup
multilink bundle-name authenticated
crypto pki token default removal timeout 0
voice-card 0
license udi pid CISCO2901/K9 sn FTX1704Y03B
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
license boot module c2900 technology-package datak9
vtp domain cisco
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
no shutdownyersi
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
```

```
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
 logging synchronous
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Switch (with mitigation)

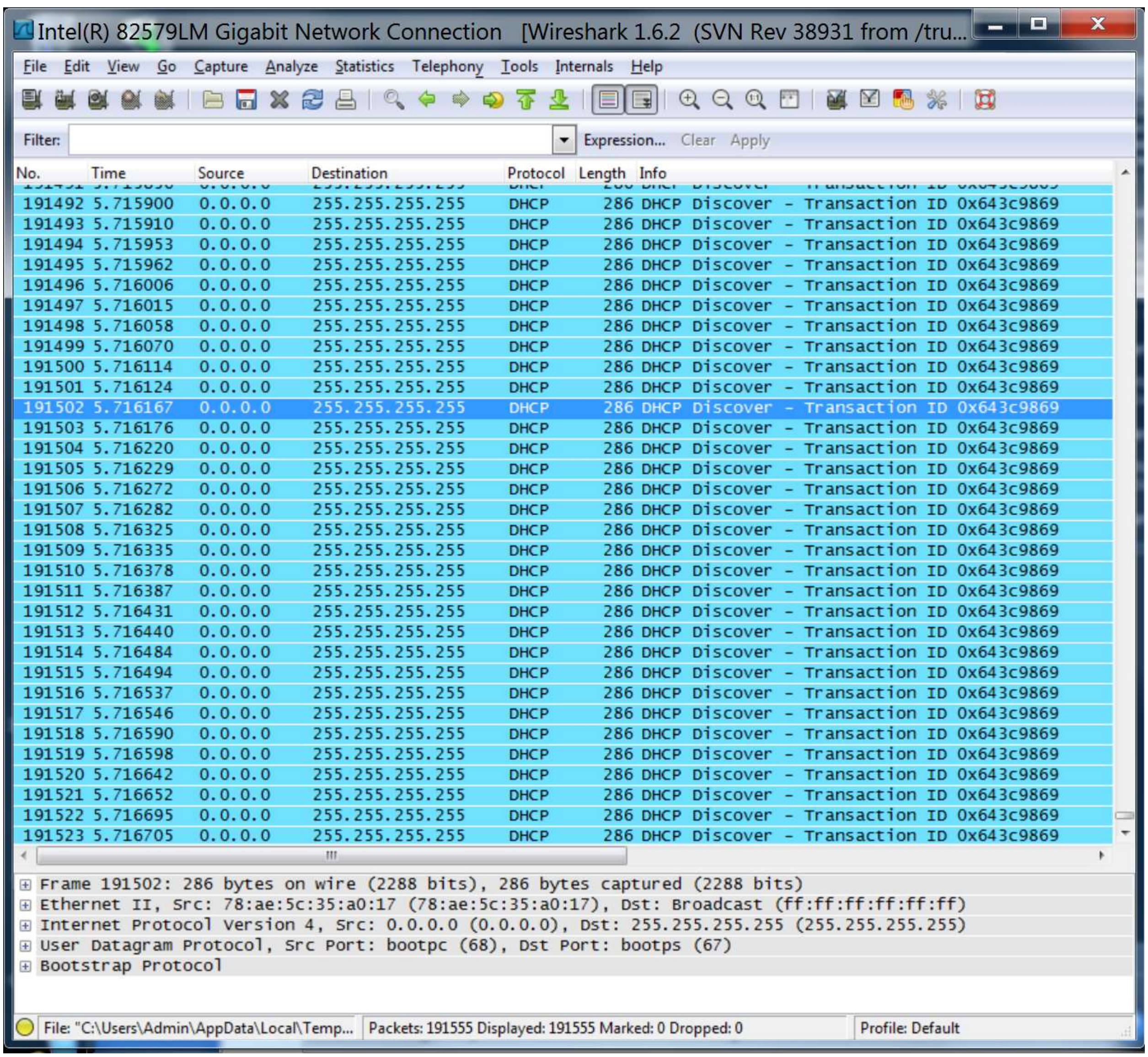
```
Current configuration : 4080 bytes
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname Switch
ip subnet-zero
no ip domain-lookup
vtp mode transparent
spanning-tree mode pvst
spanning-tree extend system-id
vlan 2-3,5
vlan 10
 name Google
vlan 20
vlan 100
 name Microsoft
vlan 192
 name Guest
interface FastEthernet0/1
 switchport mode access
 switchport port-security
```

```
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 1803.73c4.602f
 spanning-tree portfast
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 4055.39b7.61e8
 spanning-tree portfast
interface FastEthernet0/3
 switchport mode dynamic desirable
 spanning-tree portfast
interface FastEthernet0/4
 switchport mode dynamic desirable
 spanning-tree portfast
interface FastEthernet0/5
 switchport mode dynamic desirable
interface FastEthernet0/6
 switchport mode dynamic desirable
interface FastEthernet0/7
 switchport mode dynamic desirable
interface FastEthernet0/8
 switchport mode dynamic desirable
interface FastEthernet0/9
 switchport mode dynamic desirable
interface FastEthernet0/10
 switchport mode dynamic desirable
interface FastEthernet0/11
 switchport mode dynamic desirable
interface FastEthernet0/12
 switchport mode dynamic desirable
interface FastEthernet0/13
 switchport mode dynamic desirable
interface FastEthernet0/14
 switchport mode dynamic desirable
interface FastEthernet0/15
 switchport mode dynamic desirable
interface FastEthernet0/16
 switchport mode dynamic desirable
interface FastEthernet0/17
 switchport mode dynamic desirable
interface FastEthernet0/18
 switchport mode dynamic desirable
interface FastEthernet0/19
 switchport mode dynamic desirable
interface FastEthernet0/20
 switchport mode dynamic desirable
interface FastEthernet0/21
 switchport mode dynamic desirable
interface FastEthernet0/22
```

```
 switchport mode dynamic desirable
interface FastEthernet0/23
 switchport mode dynamic desirable
interface FastEthernet0/24
 switchport mode dynamic desirable
interface FastEthernet0/25
 switchport mode dynamic desirable
interface FastEthernet0/26
 switchport mode dynamic desirable
interface FastEthernet0/27
 switchport mode dynamic desirable
interface FastEthernet0/28
 switchport mode dynamic desirable
interface FastEthernet0/29
 switchport mode dynamic desirable
interface FastEthernet0/30
 switchport mode dynamic desirable
interface FastEthernet0/31
 switchport mode dynamic desirable
interface FastEthernet0/32
 switchport mode dynamic desirable
interface FastEthernet0/33
 switchport mode dynamic desirable
interface FastEthernet0/34
 switchport mode dynamic desirable
interface FastEthernet0/35
 switchport mode dynamic desirable
interface FastEthernet0/36
 switchport mode dynamic desirable
interface FastEthernet0/37
 switchport mode dynamic desirable
interface FastEthernet0/38
 switchport mode dynamic desirable
interface FastEthernet0/39
 switchport mode dynamic desirable
interface FastEthernet0/40
 switchport mode dynamic desirable
interface FastEthernet0/41
 switchport mode dynamic desirable
interface FastEthernet0/42
 switchport mode dynamic desirable
interface FastEthernet0/43
 switchport mode dynamic desirable
interface FastEthernet0/44
 switchport mode dynamic desirable
interface FastEthernet0/45
 switchport mode dynamic desirable
interface FastEthernet0/46
 switchport mode dynamic desirable
interface FastEthernet0/47
 switchport mode dynamic desirable
interface FastEthernet0/48
```

```
 switchport mode dynamic desirable
interface GigabitEthernet0/1
 switchport mode dynamic desirable
interface GigabitEthernet0/2
 switchport mode dynamic desirable
interface Vlan1
 no ip address
 shutdown
ip classless
ip http server
line con 0
line vty 5 15
end
```

Wireshark capture of the DHCP discovery packets that are sent to the router:



Cam Table Flow Attack

Purpose

The purpose of this lab is to overload a switch with so many MAC address that it can't do any other task and eventually crash.

Background Information

Cam table flow attack is when an attacker sends thousands and thousands of random MAC address to a switch. Normally switches keep all the MAC address that they have learned in their MAC address table and this is really critical for switches because this is how they distribute traffic. When this attack is made and all these random addresses are being sent to the switch, the switch tries to save them all to its MAC address table. But since there are so many addresses coming in at a really short period of time, the switch cannot handle it after one point and eventually crash.

A great way to explain this is if we think of Mr. Mason as a switch that has multiple tasks to do. He has to teach 15 periods a day, he has to grade tons of labs, he has to manage the CTE department, he has to clean up the Cisco room, he has to go to Fluke Networks every so often and the list goes on. When everything goes normal Mr. Mason can manage all of these tasks. Now we can think of the Cam table flow attack as the increased number of labs that Mr. Mason has to grade. If he gets ton of them at the same time, he won't be able to do any other task other than grading labs like a robot and after one point he will be exhausted and he won't even be able to grade labs anymore. This is the same thing that happens to the switch when it gets a ton of MAC addresses at the same time due to a Cam table flow attack.

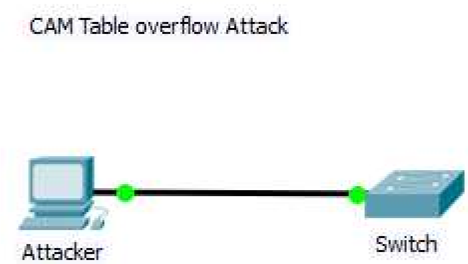
Lab Summary

In this lab we just connected a PC to a switch. The Pc was attacker and on the PC we ran Kali Linux as a virtual machine. We typed the "yersinia –G" command on the Kali Linux terminal which launched the Yersinina application. In the application, we clicked on "Launch Attack", under the CDP tab we selected flooding CDP table and clicked OK. Once we have done that, ton of MAC addresses flooded to the switch and switch's MAC address table went from only 2 MAC address to thousands of MAC address. The switching got so overloaded that it stopped doing any task at one point. Then we stopped the attack, cleared the MAC table and got the switch back to normal. To prevent this attack to happening again, we configured port security on the port that was connected to the PC and shut down all the unused ports. We then launched the attack again and nothing happened to the switch, it still only had 2 MAC addresses on its MAC address table and was functioning perfectly fine. Our mitigation was successful.

Lab Commands

yersinia -G	This command is used in Kali Linux terminal and it launches the Yersinia application.
switchport mode access	This command is entered under an interface on the switch and it only allows one VLAN on that switch.
switchport port-security	This command creates port securtiy on an interface on the switch.
switchport port-security maximum *2*	This command only allows 2 MAC address maximum on an interface on the switch and if there are more than 2 MAC address it autamatically shuts down the interface.
switchport port-security mac-address sticky	With this command, the switch saves the MAC address that it already learned in the past and those address stay on the switch until the command is disabled.
spanning-tree portfast	This command enables PortFast on the interface and puts the interface into a forwarding state.

Network Diagram



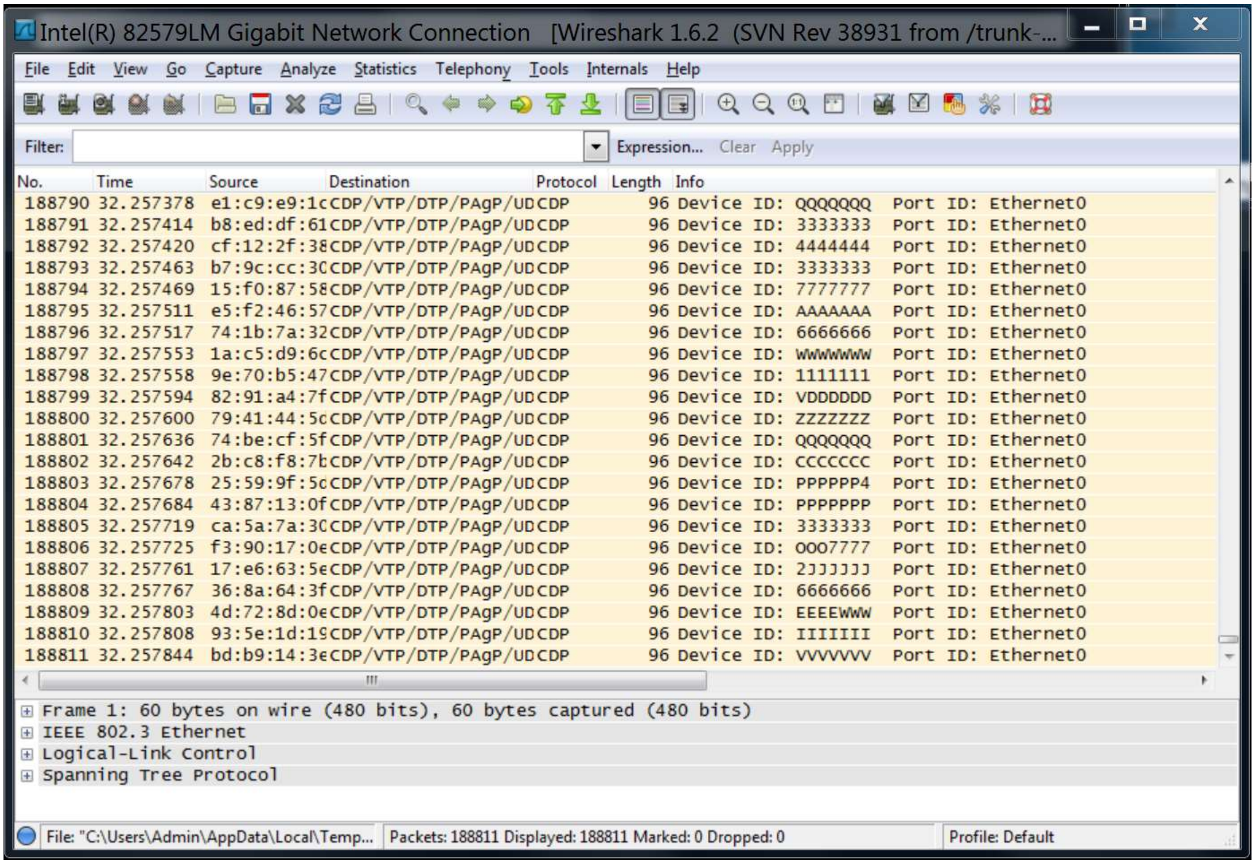
Configurations

Switch (with mitigation)

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname Switch
ip subnet-zero
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 1803.73c4.602f
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
ip http server
line con 0
line vty 0 4
```

```
 login
line vty 5 15
 login
End
```

Wireshark capture that shows the MAC addresses flowing to the switch



VLAN Hopping/Double-Tagging Attack

Purpose

The purpose of this lab is to move between 2 different VLANs in a network and mitigate it.

Background Information

VLAN hopping is an attack specifically targeted on VLANs. With VLAN hopping, the attacker is able to go between different VLANs. Normally, every VLAN is a different network and the users on one VLAN cannot have any connection to the users in another VLAN without the aid of a router. VLAN hopping enables the attacker to connect to different VLANs without using a router. In this lab we used a specific type of VLAN hopping which is called a double-tagging attack. In double-tagging the packets that are sent by the attacker have 2 different VLAN tags on them. For example if the attacker is trying to go from VLAN 1 to VLAN 20, the packets have both VLAN 1 and VLAN 20 tags on them so that they can get into both VLANs.

We can think of double-tagged packet as a secret agent. Let's say our secret agent works for the MI6 and his mission was to get information from KGB. He applies for a job at KGB and gets in. Now he has access to all the information KGB has and he can report those back to the MI6. In this case MI6 is on one VLAN and is the attacker and KGB is on another VLAN and is the target.

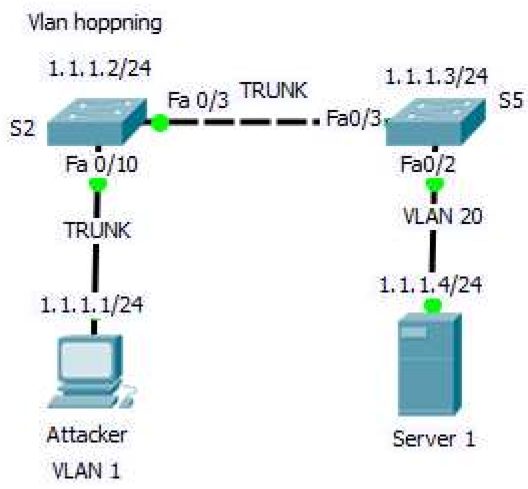
Lab Summary

In this lab we first created the topology. We first assigned IP address to every host and the two switches. We then assigned the switches, the host and server to two different VLANs. Host and the switches to VLAN 1 and the server to VLAN 20. We configured the link between two switches and between S2 and the host as trunk so that they allow all the VLANs to use that link. The link between S5 and the server is an accesses port that only allows 1 VLAN which is the VLAN 20. To hops between the two switches and S2 and the PC allow all VLANs. We then launched Kali Linux as a virtual router on the host. We opened yersinisa -G using the Kali Linux terminal. In "802.1Q" tab we edited the VLANs so that the attack went from VLAN 1 to VLAN 20. Then we clicked on "Launch Attack". Under the "802.1Q" tab, we chose the "sending 802.1Q double enc. packet" option then clicked "OK". We had Wireshark open in two different places in the network. One on S2 and one on S5. When we launched the attack both Wiresharks got a packet that had an ICMP packet with both VLANs tagged on it. The attack was successful. Then we mitigated the attack by changing the native VLAN on the switches to 99. We performed the same attack again but this time only the Wireshark that was connected to S2 got the ICMP packet with 2 VLAN tags. The other Wireshark, which was connected to S5, did not get any packets which means the attack did not reach the other VLAN and the mitigation was successful.

Lab Commands

`switchport mode access`	This command turns the port on the switch into an access port that only allows one VLAN.
`switchport trunk native vlan` *`99`*	This command changes the native VLAN on the switch to VLAN 99
`switchport trunk allowed vlan` *`1,20`*	This command defines which VLANs can use the trunked link.
`switchport trunk encapsulation dot1q`	This command allows to port to use encapsulation while allowing more than one VLAN through that port.

Network Diagram



Configurations

S5 (without mititgation)

```
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname S5
boot-start-marker
boot-end-marker
no aaa new-model
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
vlan internal allocation policy ascending
interface FastEthernet0/1
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
interface FastEthernet0/2
 switchport mode access
 shutdown
 spanning-tree portfast
interface FastEthernet0/3
 switchport trunk allowed vlan 1,20
 spanning-tree portfast
interface FastEthernet0/4
 spanning-tree portfast
interface FastEthernet0/5
```

```
 spanning-tree portfast
interface FastEthernet0/6
 spanning-tree portfast
interface FastEthernet0/7
 spanning-tree portfast
interface FastEthernet0/8
 spanning-tree portfast
interface FastEthernet0/9
 spanning-tree portfast
interface FastEthernet0/10
 spanning-tree portfast
interface FastEthernet0/11
 spanning-tree portfast
interface FastEthernet0/12
 spanning-tree portfast
interface FastEthernet0/13
 spanning-tree portfast
interface FastEthernet0/14
 spanning-tree portfast
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface FastEthernet0/25
interface FastEthernet0/26
interface FastEthernet0/27
interface FastEthernet0/28
interface FastEthernet0/29
interface FastEthernet0/30
interface FastEthernet0/31
interface FastEthernet0/32
interface FastEthernet0/33
interface FastEthernet0/34
interface FastEthernet0/35
interface FastEthernet0/36
interface FastEthernet0/37
interface FastEthernet0/38
interface FastEthernet0/39
interface FastEthernet0/40
interface FastEthernet0/41
interface FastEthernet0/42
interface FastEthernet0/43
interface FastEthernet0/44
interface FastEthernet0/45
interface FastEthernet0/46
interface FastEthernet0/47
```

```
interface FastEthernet0/48
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface GigabitEthernet0/3
interface GigabitEthernet0/4
interface Vlan1
 ip address 1.1.1.3 255.255.255.0
interface Vlan10
 no ip address
interface Vlan20
 no ip address
ip classless
ip http server
ip http secure-server
ip sla enable reaction-alerts
line con 0
line vty 5 15
End
```

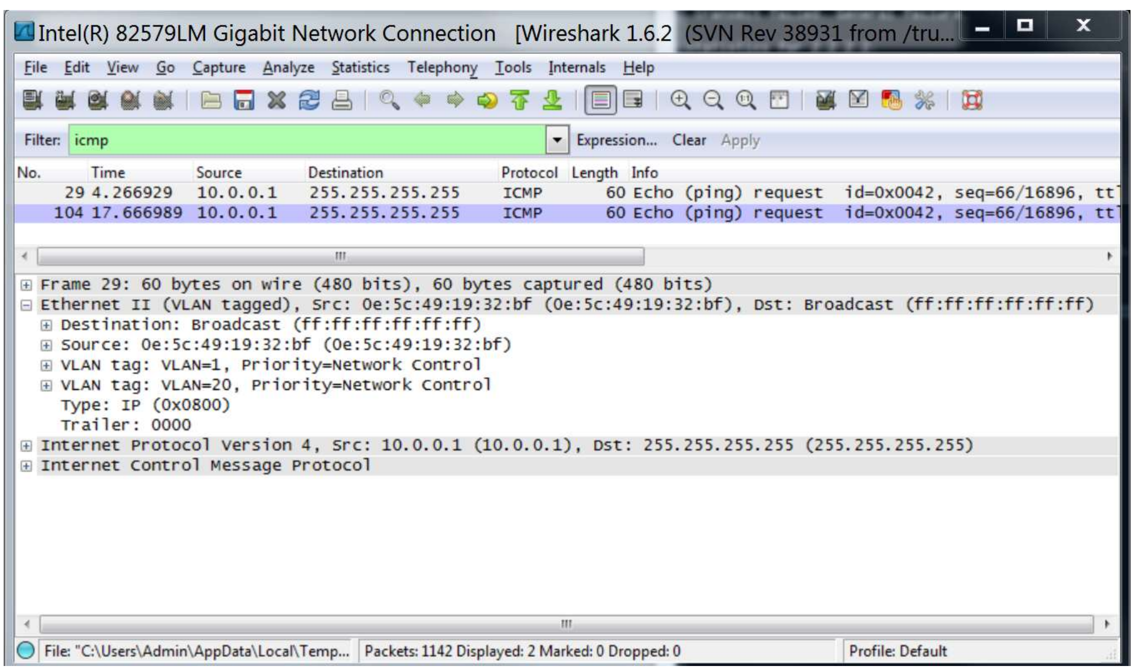
S2(without mitigation)

```
Current configuration : 3049 bytes
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname S2
boot-start-marker
boot-end-marker
no aaa new-model
system mtu routing 1500
vtp domain HackAttacks
vtp mode transparent
authentication mac-move permit
ip subnet-zero
spanning-tree mode pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
vlan internal allocation policy ascending
vlan 2-5,7,10,12,20,99
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
 spanning-tree portfast
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface FastEthernet0/25
interface FastEthernet0/26
interface FastEthernet0/27
interface FastEthernet0/28
interface FastEthernet0/29
interface FastEthernet0/30
interface FastEthernet0/31
interface FastEthernet0/32
interface FastEthernet0/33
```

```
interface FastEthernet0/34
interface FastEthernet0/35
interface FastEthernet0/36
interface FastEthernet0/37
interface FastEthernet0/38
interface FastEthernet0/39
interface FastEthernet0/40
interface FastEthernet0/41
interface FastEthernet0/42
interface FastEthernet0/43
interface FastEthernet0/44
interface FastEthernet0/45
interface FastEthernet0/46
interface FastEthernet0/47
interface FastEthernet0/48
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface GigabitEthernet0/3
interface GigabitEthernet0/4
interface Vlan1
 ip address 1.1.1.2 255.255.255.0
ip classless
ip http server
ip http secure-server
ip sla enable reaction-alerts
line con 0
line vty 5 15
end
```

Wireshark capture that shows the double tagging on the packet



HTTP Man-In-The-Middle Attack

Purpose

The purpose of this lab is to intercept a PC that is trying to access a webpage and see the webpage URL along with images from the page.

Background Information

Man-in-the-middle attacks are almost like tell something to someone in public where there are a lot people around. Since there are people between the two, they listen to their conversation and can get information from it. In HTTP man-in-the-middle attacks, the host and the web server or the router are the two people telling something to each other in public, the attacker is the person who listens to the conversation and the conversation is the HTTP packets. HTTP packets store all the sate about which website the host is trying to access and the attacker in between can easily capture information from those packets. To prevent this from happening, the host should use HTTPS instead of HTTP. Because in HTTPS the people or the hackers in between the host and the server cannot hear anything or see any information inside the packets since they are encrypted.

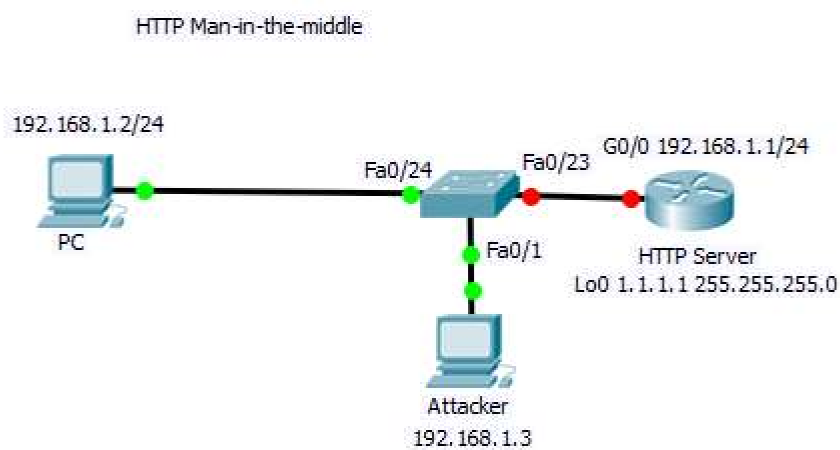
Lab Summary

In this lab we first created our topology. The target/host is connected to a switch and the switch is connected to a router. The thing that target doesn't know is that another host is connected to the switch and is about to watch all the HTTP traffic that will be going on between the target and the router. We first assigned IP addresses to all hosts and established connectivity between all hosts and the router. We then configured a loopback and also configured the router as a HTTP server. After we were able to view the webpage from the target, we launched Kali Linux on the attacker. On Kali Linux terminal we first typed "`sudo arpspoof -i eth0 -t 192.168.1.1 192.168.1.2`" and "`sudo arpspoof -i eth0 -t 192.168.1.2 192.168.1.1`". This way, even though the attacker was in-between the target and the router, neither the target nor the router realized that there was someone else in between. Then we entered the "`sudo driftnet -i eth0`" which allowed us to see the images on the website the target was accessing. Then we entered the "`sudo urlsnarf -i eth0`" and this command gave us the URL of the website the target was accessing. The attack was successful, we were seeing the HTTP traffic between the target and the router. To mitigate this, we decided to use HTTPS instead of HTTP. To do this we first disabled the HTTP server on the router and then enabled HTTPS server. After doing this, we followed the same steps as we did for HTTP but we could not get any image nor URL while the target was still accessing the webpage. So our mitigation was also successful.

Lab Commands

`ip http server`	This command allows the router to be a HTTP server.
`ip http secure-server`	This command allows the router to be a HTTPS server.
`ip http authentication local`	This command allows access to the web server by using a username and password.
`username` *`admin`* **`privilege 15 password 0`** *`admin`*	This command sets a username and password for the webpage.
`sudo urlsnarf -i eth0`	This command captures the URL of the target on the Kali Linux terminal.
`sudo driftnet -i eth0`	This command launches driftnet on Kali Linux which captures images that the target is accessing at a webpage.
`sudo arpspoof -i eth0 -t` *`192.168.1.1 192.168.1.2`*	This command tells the host 192.168.1.1 that the IP address of the Kali Linux is 192.168.1.2.

Network Diagram



Configurations

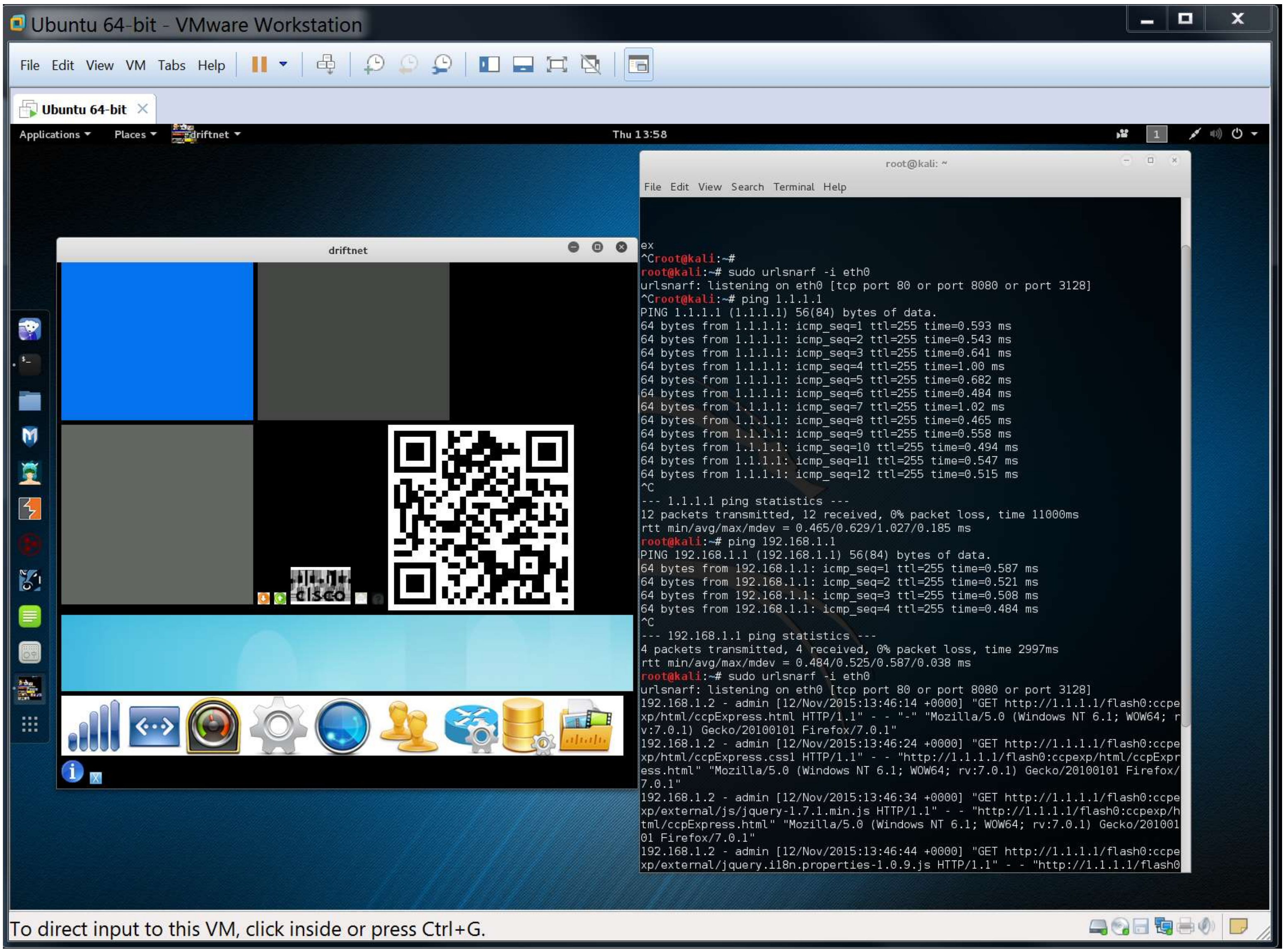
Router (with mitigation):

```
Current configuration : 3413 bytes
 Last configuration change at 22:10:36 UTC Thu Nov 12 2015
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname MIMattackR9router
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
no ipv6 cef
ip source-route
ip cef
ip domain name calvin.com
multilink bundle-name authenticated
crypto pki token default removal timeout 0
crypto pki trustpoint TP-self-signed-2309102217
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2309102217
 revocation-check none
 rsakeypair TP-self-signed-2309102217
crypto pki certificate chain TP-self-signed-2309102217
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101
05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D
43657274
  69666963 6174652D 32333039 31303232 3137301E 170D3135 31313132
32323034
  32335A17 0D323030 31303130 30303030 305A3031 312F302D 06035504
03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32
33303931
  30323231 3730819F 300D0609 2A864886 F70D0101 01050003 818D0030
81890281
  81008B87 B0E4976D 7FF10A33 1DD7D6B0 A65B29A8 9BE760F4 E9695BEA
AE77DF9E
  E79D8FDB 989317F6 8FC19382 A7576FB1 AF607A62 D06A580C 4F0F9A67
902D20DF
  241554C5 69BF1CE5 628056B2 1EAE1DFB 546AF081 73812DB0 C5969402
12CDE9FA
  F4758EDF 43ABECD1 5E9715BF 01B9AE3E 921A8B10 F0D7F5E5 D2CF89D8
5E3AD240
  47C30203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
301F0603
  551D2304 18301680 1428D16F 0B7BF750 467EC2D3 E112760A B7085802
C4301D06
```

```
  03551D0E 04160414 28D16F0B 7BF75046 7EC2D3E1 12760AB7 085802C4
300D0609
  2A864886 F70D0101 05050003 81810033 DCAB434F 082DD00A D66B5809
486DD19F
  42AA0BC0 77F94E90 3C6B3764 0E7F96D3 7ABBBDE6 7E4FC76C D2B10F5D
95906253
  E95F97A9 D2991C28 9505887F 1F02EB2C DD9C6E01 0DF32746 C4186630
F1182A50
  D64928F7 EC8F5203 884F10D3 2BAADAF5 E7667FC7 7D3E27AC 43722A1F
06F30A58
  26E629DD 4BB49F15 507AC3C4 4C17A0
        quit
voice-card 0
license udi pid CISCO2901/K9 sn FTX1704Y03B
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
license boot module c2900 technology-package datak9
vtp domain cisco
vtp mode transparent
username admin privilege 15 password 0 admin
redundancy
interface Loopback0
 no ip address
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 1.1.1.1 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
no ip http server
ip http authentication local
ip http secure-server
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
control-plane
mgcp profile default
gatekeeper
 shutdown
```

```
line con 0
line aux 0
line 2 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

The image and URL capture from target on Kali Linux



Overall

Problems

In DHCP starvation and CAM table attacks we did not have any problems in either the attacks or the mitigations.

On VLAN hopping, we first successfully did the attack and hopped between 2 VLANs, but our ping attempts to the other VLAN was failing. That made us think that our VLAN hopping attack failed. So we made more research to figure out why the double tagging was not working. We tried many times and we ended up with the same result. There was a ping request with double tagging that was going into the VLAN we wanted to hop, but there was no ping reply coming back. We thought that was a problem and we were supposed to get a reply. After days of research and collaboration with other groups, we figured out that VLAN hopping only sends double tagged ICMP requests but we were not supposed to get a reply. We were able to see that message in the other VLAN and our attack was complete. We just spent a long time trying to figure out what we were doing wrong even though everything was right.

In the HTTP man-in-the-middle attack, we had some HTTP server problems. We were able to connect to the server but it was not accepting the username and the password we were entering. We made sure we did not have any typos. We changed the username and password couple of times but it was still not working. We finally figured out there we were missing the “ip http authentication local” command which allowed user to access the http server using a browser with usernames and passwords. Everything worked fine after that and we captured all the HTTP traffic of the target.

Conclusion

In this lab, we learned how to do 4 different layers 2 attacks and mitigate them. We did HTTP man-in-the-middle, CAM table flow, VLAN hopping and DHCP starvation attacks. In terms of time management, unlike the previous labs, we spent most of our time researching rather than troubleshooting. Creating the attacks were pretty easy because we used tools from the Kali Linux operating system which did all the work for us. We thought we had problems on the HTTP man-in-the-middle attack and we also spent a significant amount of time trying to figure out the problem in the VLAN hopping attack even though we were successfully attacking form the beginning. So, we basically did troubleshooting for nothing until we realized that our attack was actually working. In terms of applying these skills in the field, this was a great way to learn how to deal with some basic threats to any network out there. However, it was also a little bit scary to see how many tools and different attacks can be done from a simple operating system and not much knowledge is required to do these attacks. The good news is the only attacks that don’t have

AAA Server

Purpose

The purpose of this lab is to set up an AAA server that will provide username and passwords for a router. Then use a username and password to enter the router command line.

Background Information

AAA (authentication, authorization, and accounting) is a service that provides routers and switches with usernames and passwords for others to access them. With AAA, the passwords are not stored in the server. The AAA feature allows you to verify the identity of, grant access to, and track the actions of users managing a Cisco router or switch.

We can think of a router that is using AAA as an office building that requires everyone who works in the building to carry badges and use those badges to open doors and gates. In the office building all the employees have to use their badges to open a door and every badge is different, they carry different information about the owner of the badge. The computers in the building recognize every badge and when the person scans it and it opens the door. The computers that store every badge and the information on them is like the AAA server. Every different badge is like every user on the AAA server and the different information that is on the badges is like how every user has their own username and password on a router that is using a AAA server. In order to gain access to the router, users have to have their own username and password, just like how employees need their own personal badges.

One benefit of having a remote server is that the passwords are not stored inside the router. They are all stored in the server. So in case something happens to the router, if someone tries to steal it or access it, they won't be able to gain access to any of the passwords.

Lab Summary

In this lab, I first created the Windows 2016 Server as a virtual machine on my desktop computer. I first set an IP address on the virtual machine which was bridged to the NIC driver of the computer and I established connectivity between the router and the server. Before I created the AAA server, I first had to install Active Directory Domain Services (AD DS), DNS Server, and Network Policy and Access Services. Then I set the domain name of the server using AD DS. I also set the domain at the router so the router and the server can be on the same domain. While setting the domain name, I also set a password that the router will use when it is getting information form the server.

After the domain name was set, I set a user group called "Router users" I opened the Network Policy Server from NPAS. In the policy server I created a RADIUS client called Router. Then I created a network policy and a connection request policy. In the connection request policy I set the Router as a client friendly same so the clients could access it. And in the network policy I set it so that only the members of the "Router users" would be able to access the router.

Then I moved on to creating the users. From the AD DS, I went to the Active Directory Users and Computers. In there I got to the users folder and created users with specific username and password for each user. I also assigned those users under the "Router users" group.

After the AAA server was set, I configured the router so it used the server for username and password while a user is logging into the router.

Lab Commands

ip domain name *doruk.com*	This command sets the domain name on the router so that the router can use the server with that domain name.
aaa new-model	This command enables AAA on the router or switch.
aaa authentication login default group radius	This command is used to authenticate users who want access into the router or switch.
radius-server host *192.168.1.2* **key** *cisco*	This command is used to tell the switch or router the IP address of the AAA server and the password so that the device can gain access to use the server.

Network Diagram

Configurations

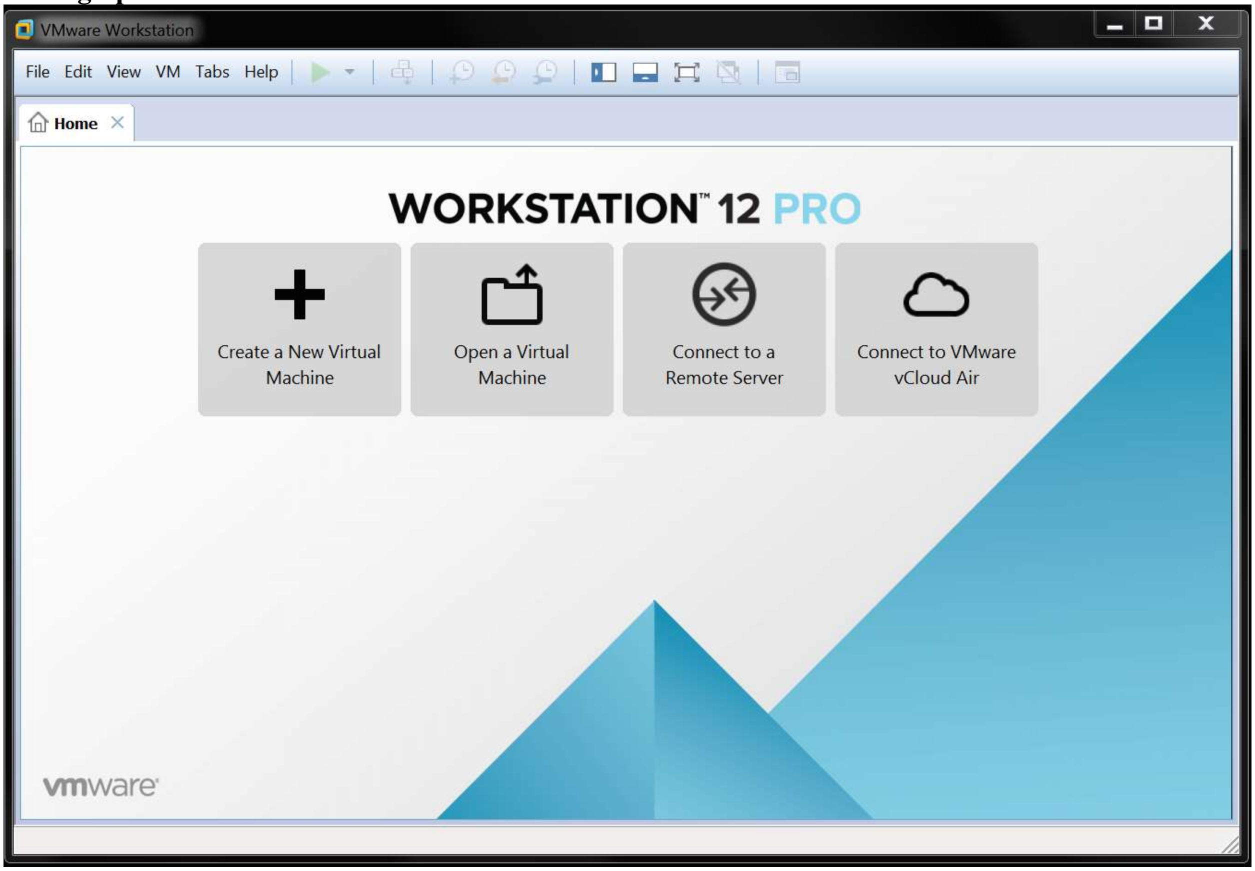
Router

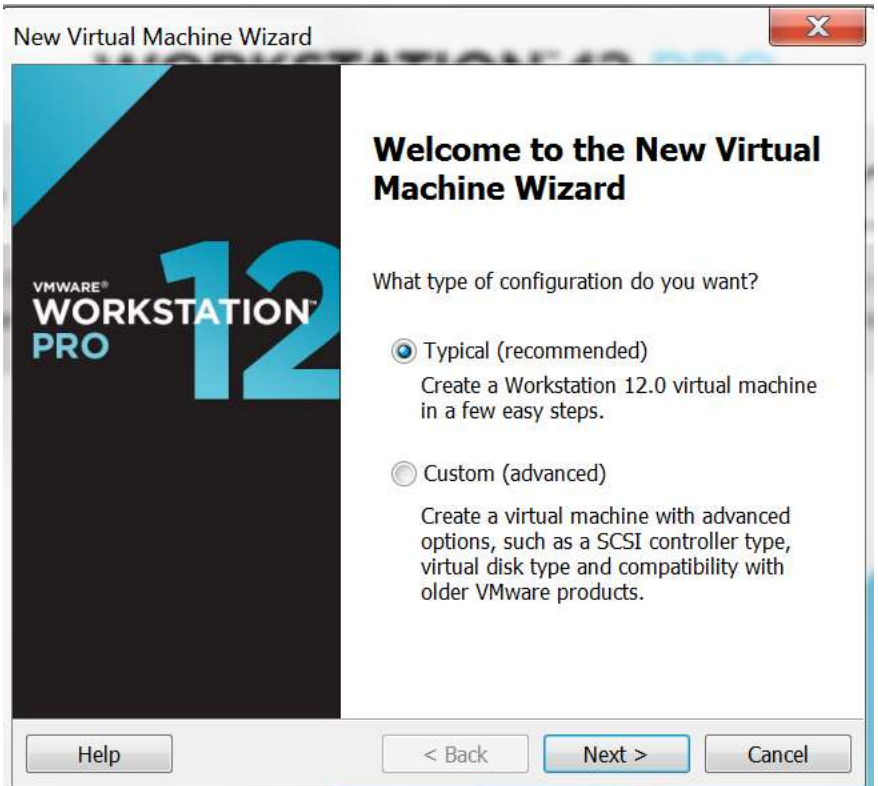
```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
aaa new-model
aaa authentication login default group radius
aaa session-id common
memory-size iomem 10
ip cef
ip domain name doruk.com
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
icense udi pid CISCO2901/K9 sn FTX1520806Y
license accept end user agreement
license boot module c2900 technology-package uck9
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
```

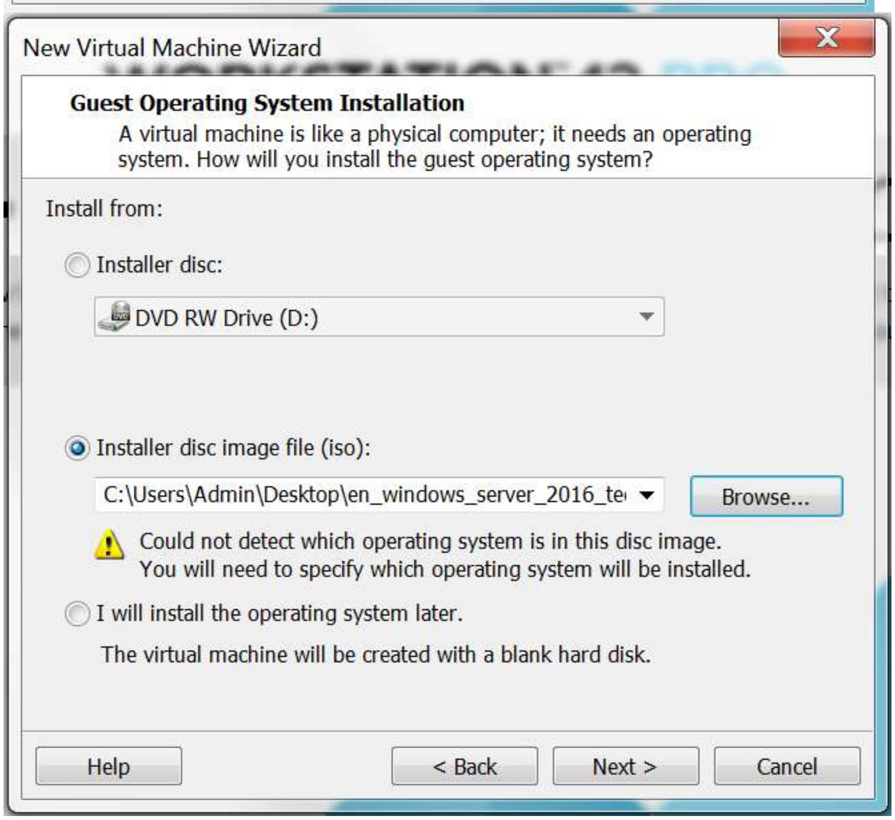
```
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 duplex auto
 speed auto
ip forward-protocol nd
no ip http server
no ip http secure-server
radius-server host 192.168.1.2 key cisco
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 transport input all
scheduler allocate 20000 1000
end
```

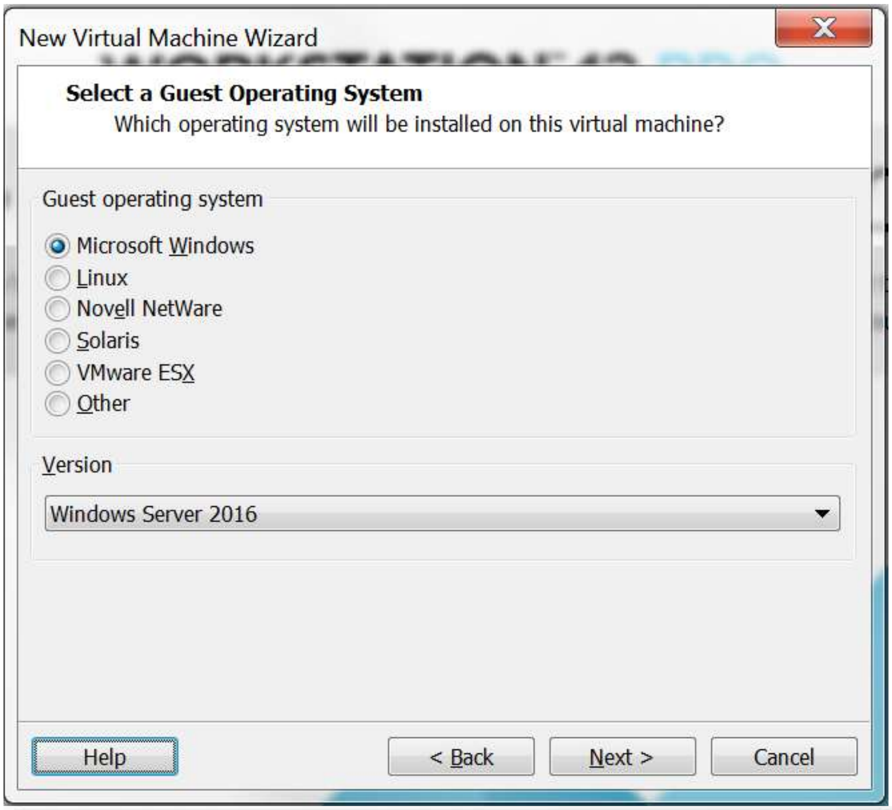
Screenshots

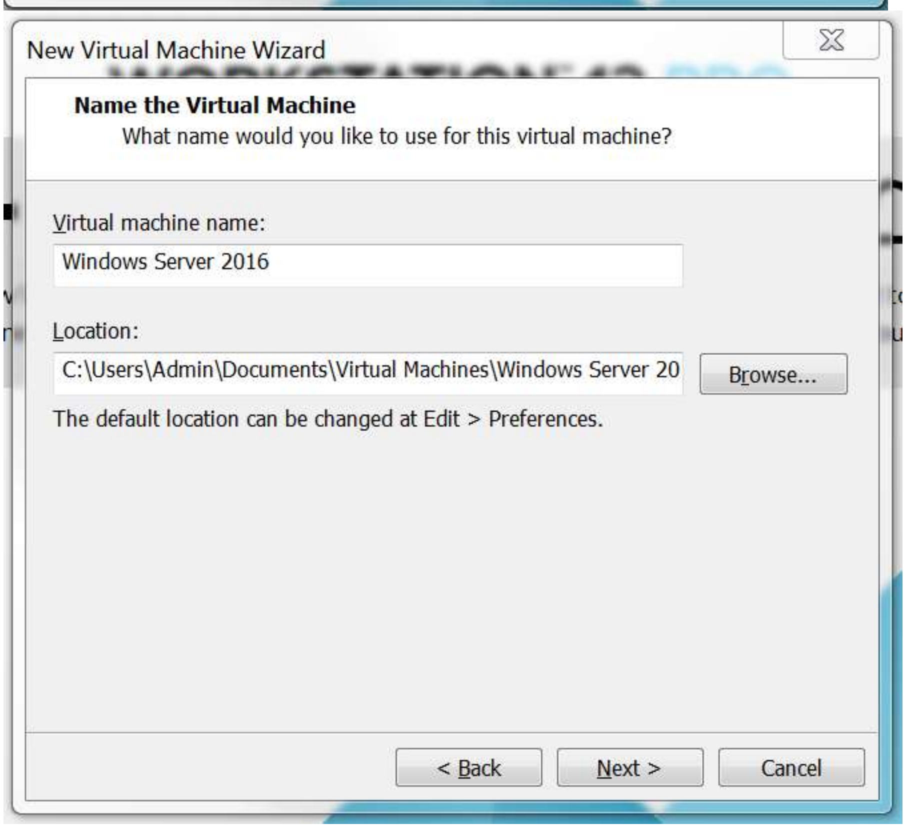
Setting up the virtual machine:

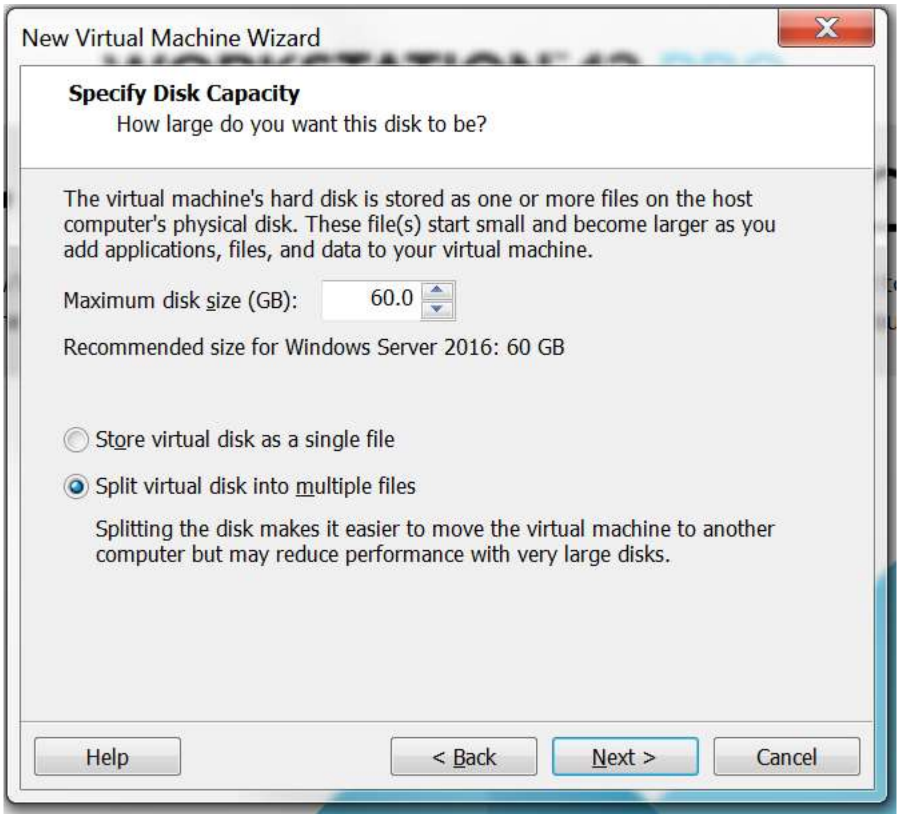


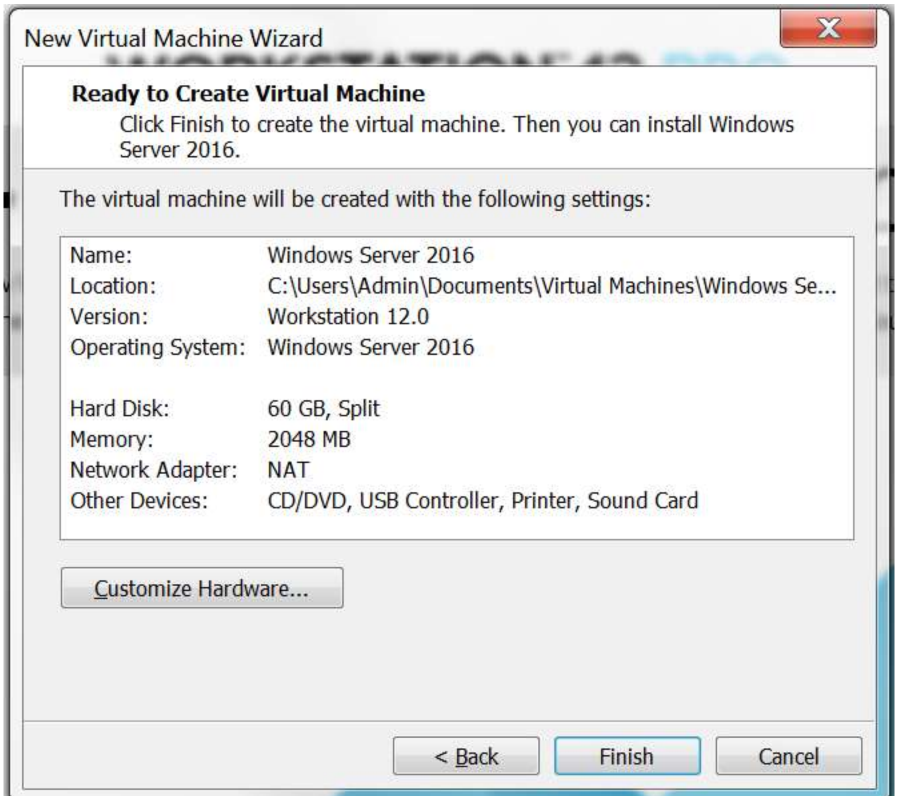

New Virtual Machine Wizard
VMWARE®
WORKSTATION
PRO
12
Welcome to the New Virtual Machine Wizard
What type of configuration do you want?
Typical (recommended)
Create a Workstation 12.0 virtual machine in a few easy steps.
Custom (advanced)
Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.
Help
< Back
Next >
Cancel

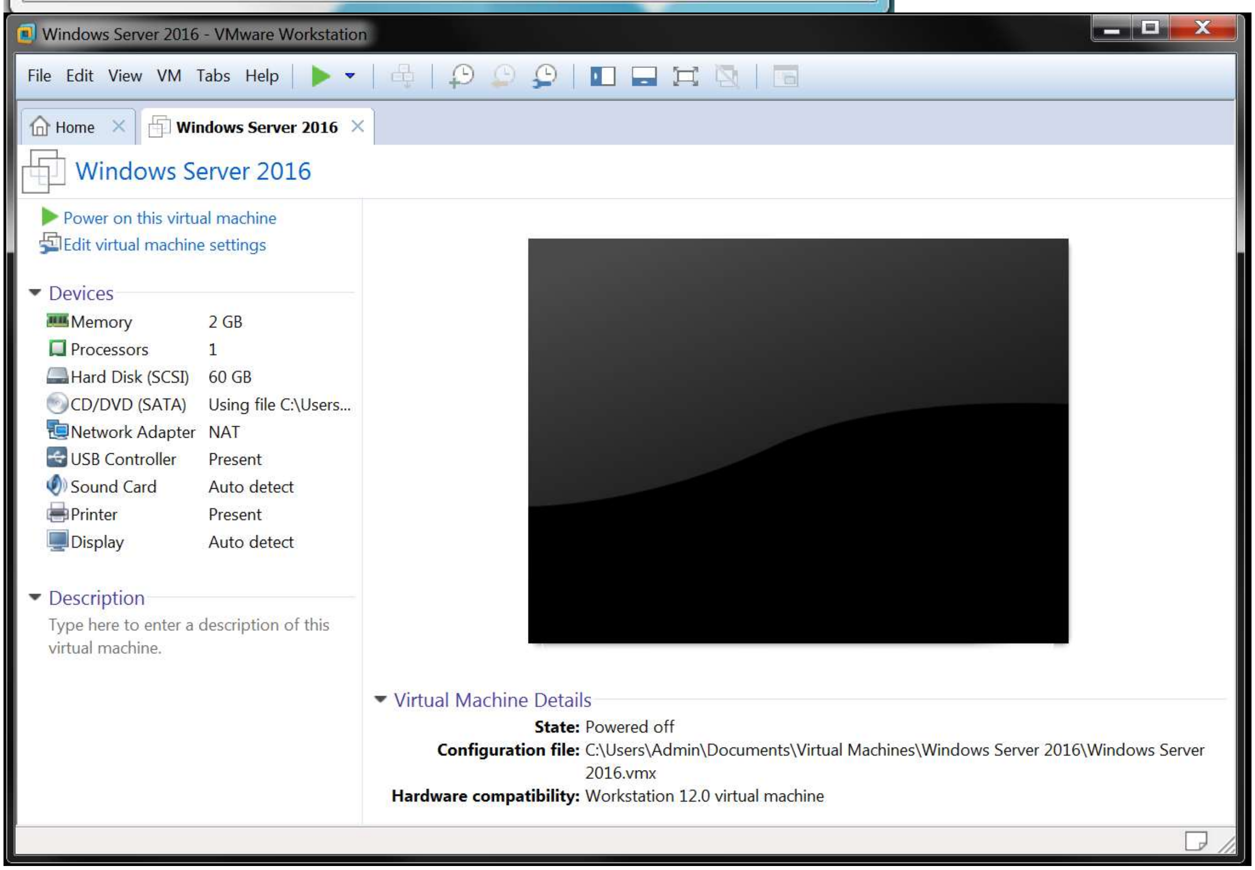

New Virtual Machine Wizard
Guest Operating System Installation
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?
Install from:
Installer disc:
DVD RW Drive (D:)
Installer disc image file (iso):
C:\Users\Admin\Desktop\en_windows_server_2016_te
Browse...
Could not detect which operating system is in this disc image.
You will need to specify which operating system will be installed.
I will install the operating system later.
The virtual machine will be created with a blank hard disk.
Help
< Back
Next >
Cancel


New Virtual Machine Wizard
Select a Guest Operating System
Which operating system will be installed on this virtual machine?
Guest operating system
Microsoft Windows
Linux
Novell NetWare
Solaris
VMware ESX
Other
Version
Windows Server 2016
Help
< Back
Next >
Cancel

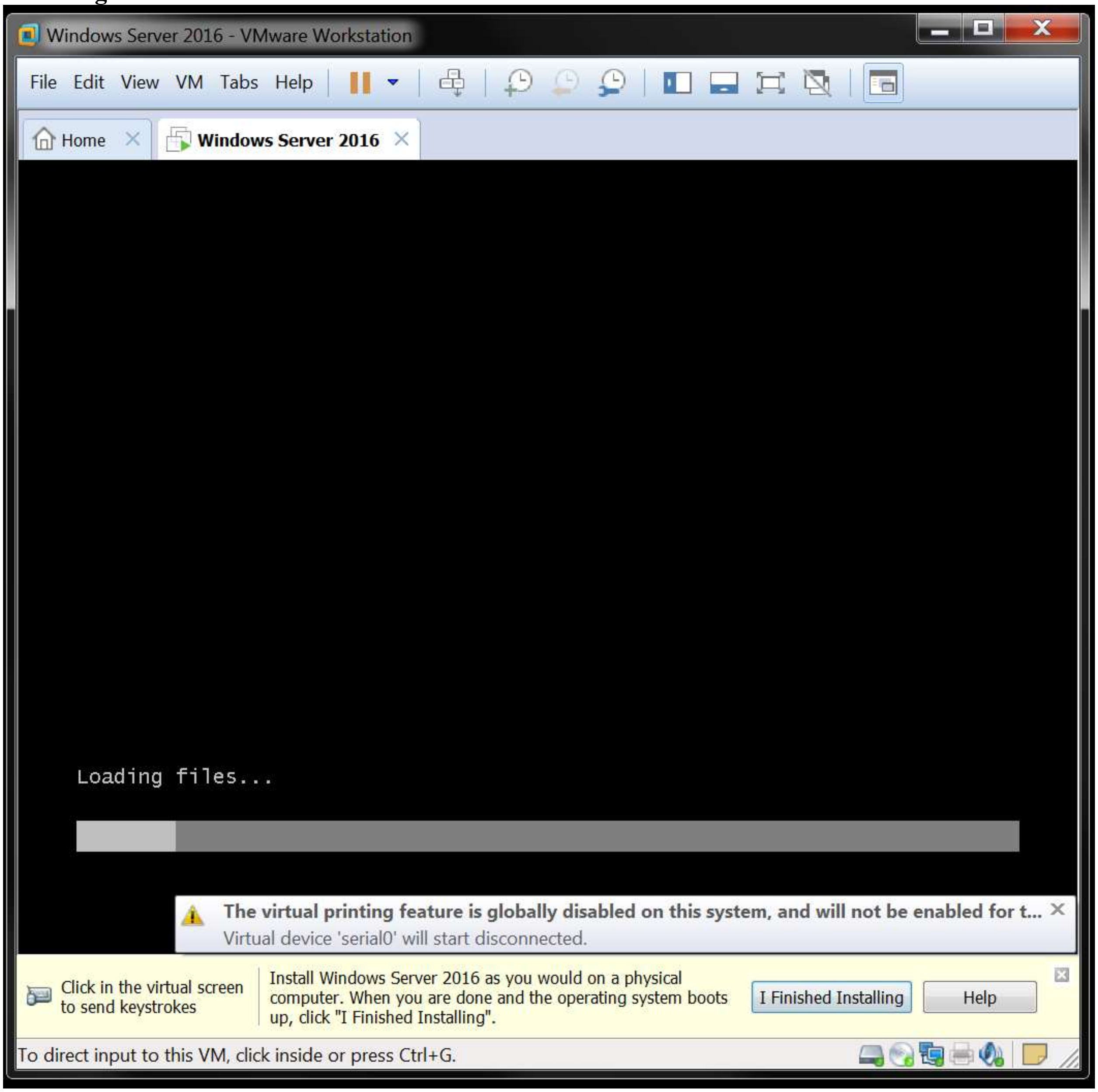

New Virtual Machine Wizard
Name the Virtual Machine
What name would you like to use for this virtual machine?
Virtual machine name:
Windows Server 2016
Location:
C:\Users\Admin\Documents\Virtual Machines\Windows Server 20
Browse...
The default location can be changed at Edit > Preferences.
< Back
Next >
Cancel

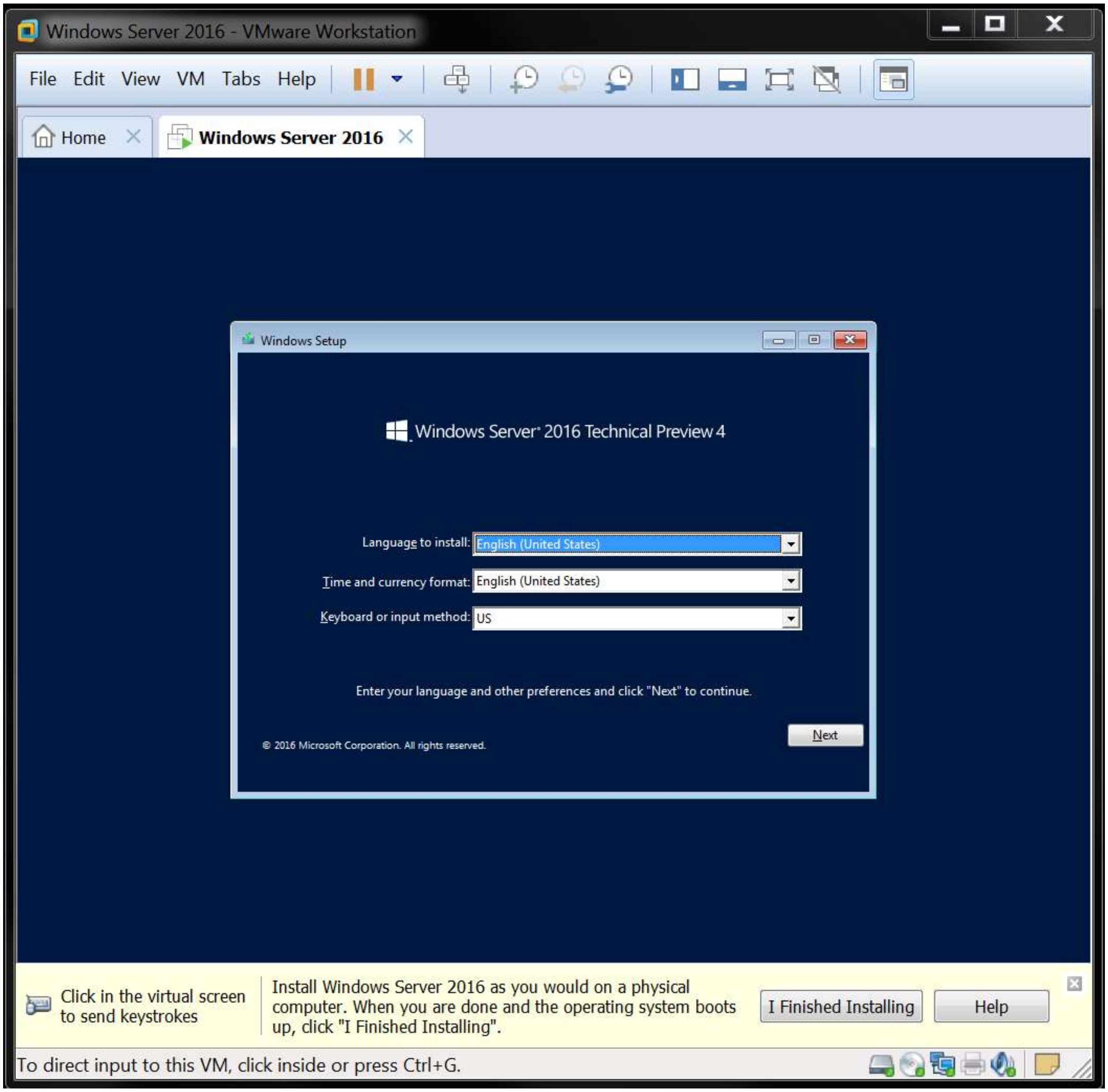

New Virtual Machine Wizard
Specify Disk Capacity
How large do you want this disk to be?
The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.
Maximum disk size (GB):
60.0
Recommended size for Windows Server 2016: 60 GB
Store virtual disk as a single file
Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Help
< Back
Next >
Cancel


New Virtual Machine Wizard
Ready to Create Virtual Machine
Click Finish to create the virtual machine. Then you can install Windows Server 2016.
The virtual machine will be created with the following settings:
Name: Windows Server 2016
Location: C:\Users\Admin\Documents\Virtual Machines\Windows Se...
Version: Workstation 12.0
Operating System: Windows Server 2016
Hard Disk: 60 GB, Split
Memory: 2048 MB
Network Adapter: NAT
Other Devices: CD/DVD, USB Controller, Printer, Sound Card
Customize Hardware...
< Back
Finish
Cancel

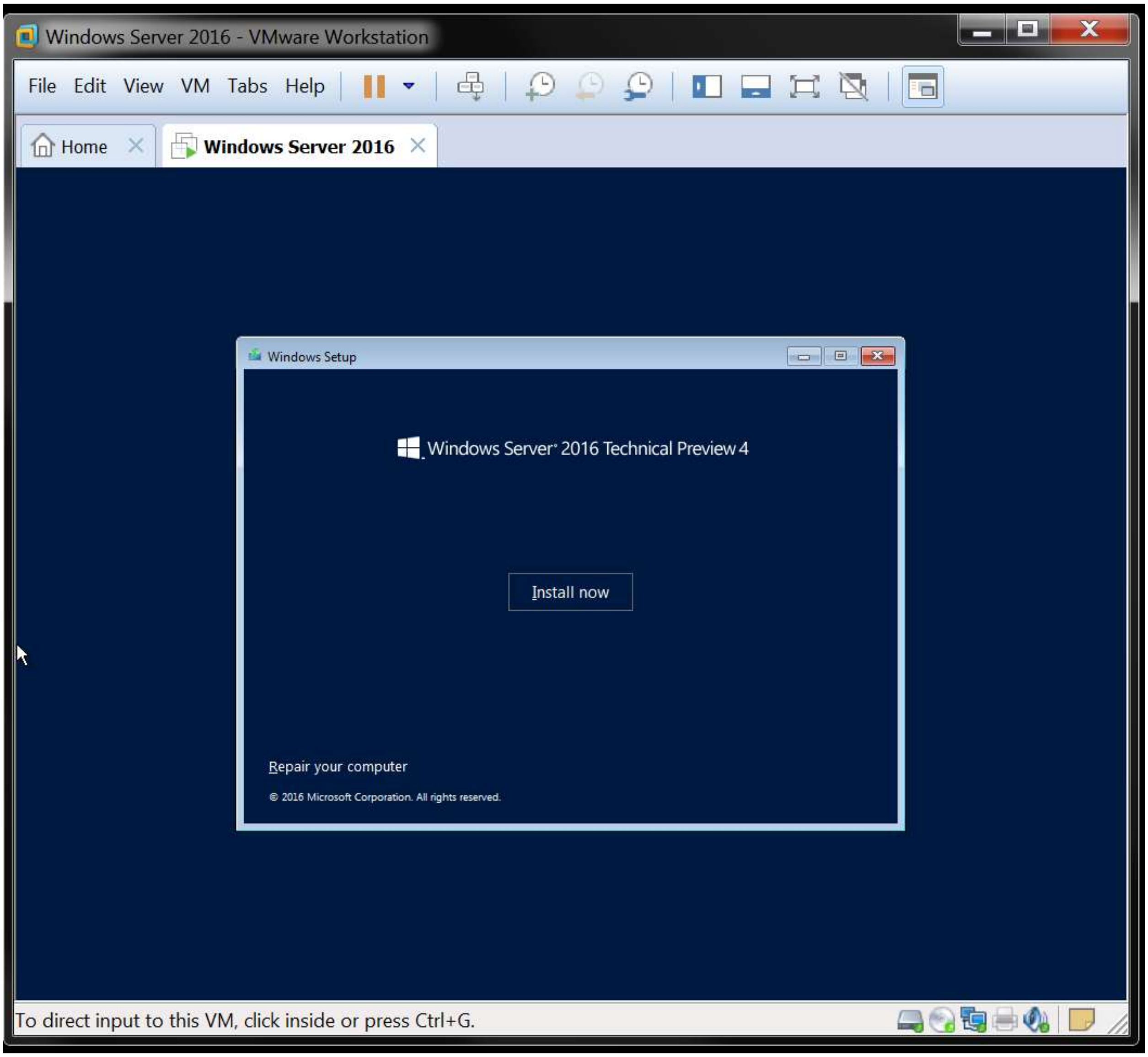

Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Server 2016
Power on this virtual machine
Edit virtual machine settings
Devices
Memory 2 GB
Processors 1
Hard Disk (SCSI) 60 GB
CD/DVD (SATA) Using file C:\Users...
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Printer Present
Display Auto detect
Description
Type here to enter a description of this virtual machine.
Virtual Machine Details
State: Powered off
Configuration file: C:\Users\Admin\Documents\Virtual Machines\Windows Server 2016\Windows Server 2016.vmx
Hardware compatibility: Workstation 12.0 virtual machine

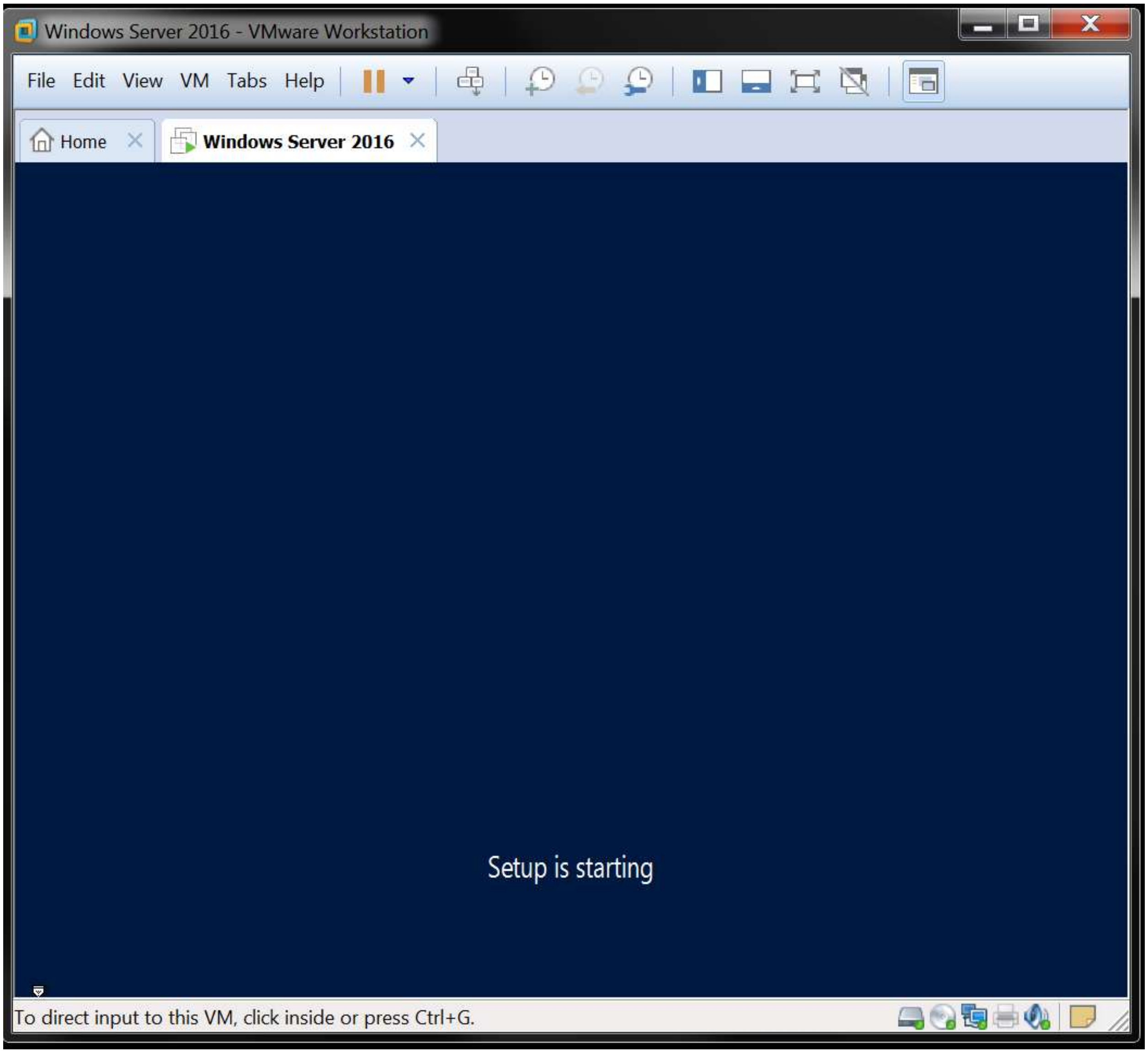
Installing Windows Server 2016:

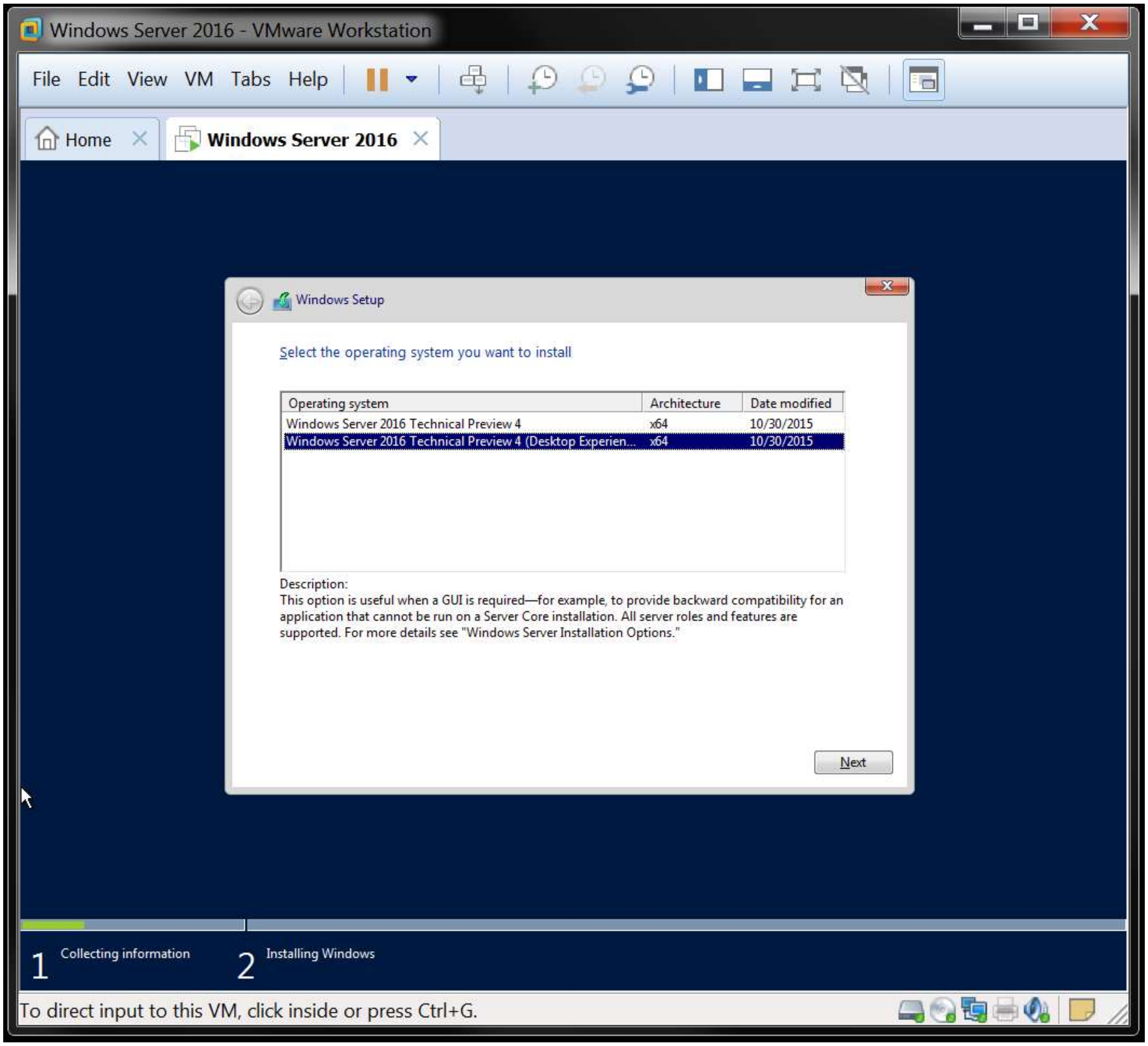


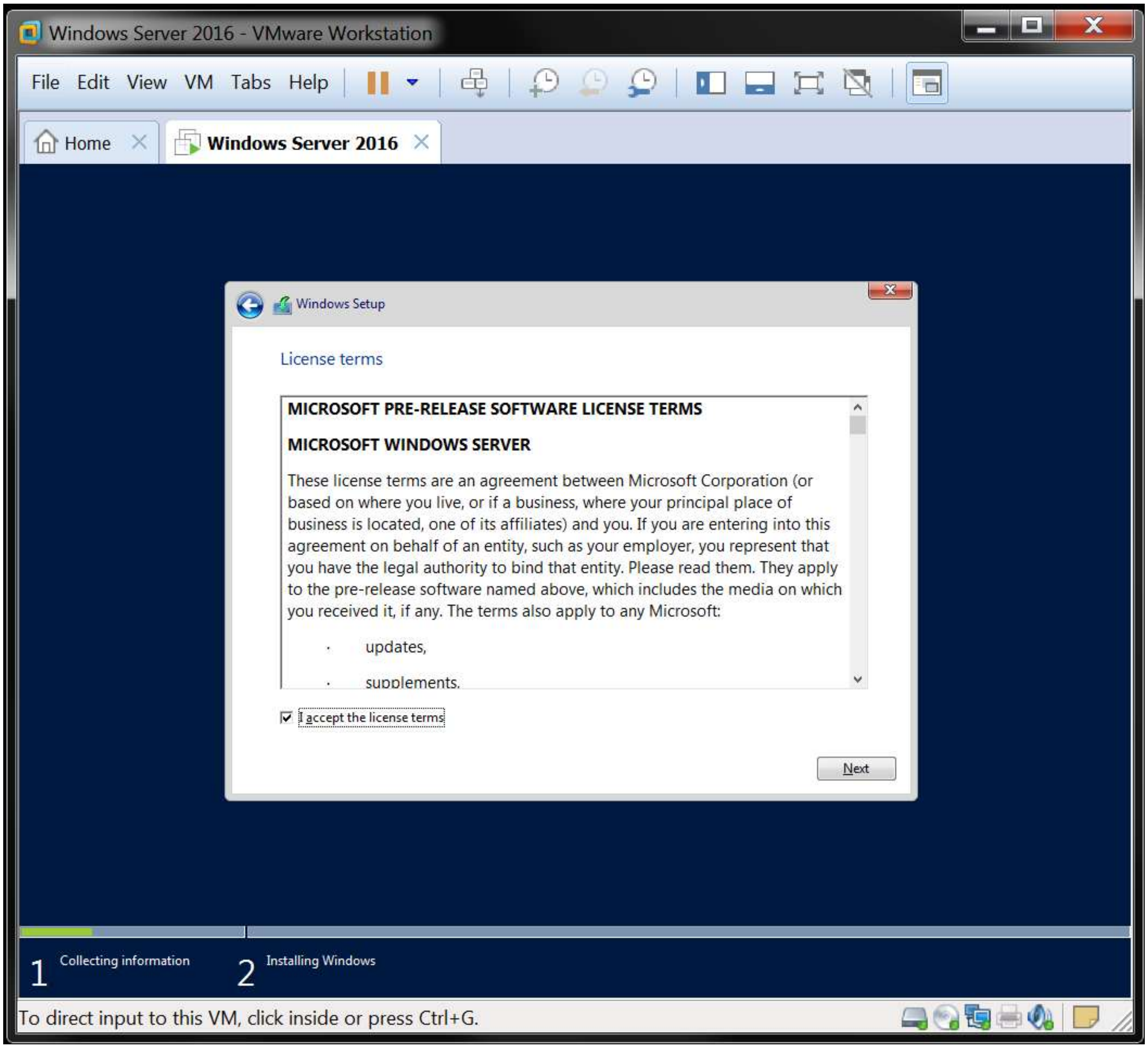


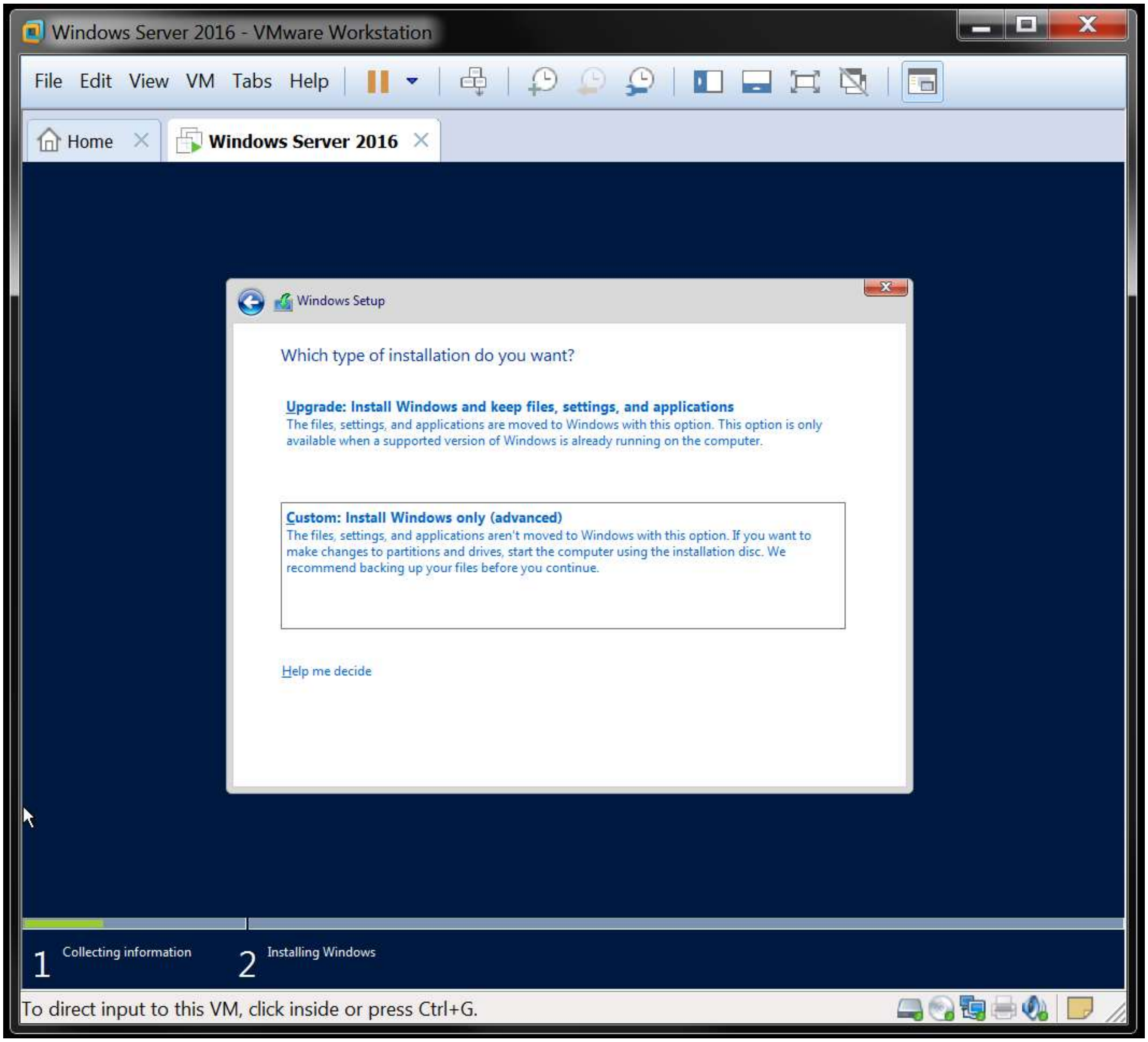
Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Setup
Windows Server 2016 Technical Preview 4
Language to install: English (United States)
Time and currency format: English (United States)
Keyboard or input method: US
Enter your language and other preferences and click "Next" to continue.
© 2016 Microsoft Corporation. All rights reserved.
Next
Click in the virtual screen to send keystrokes
Install Windows Server 2016 as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
Help
To direct input to this VM, click inside or press Ctrl+G.

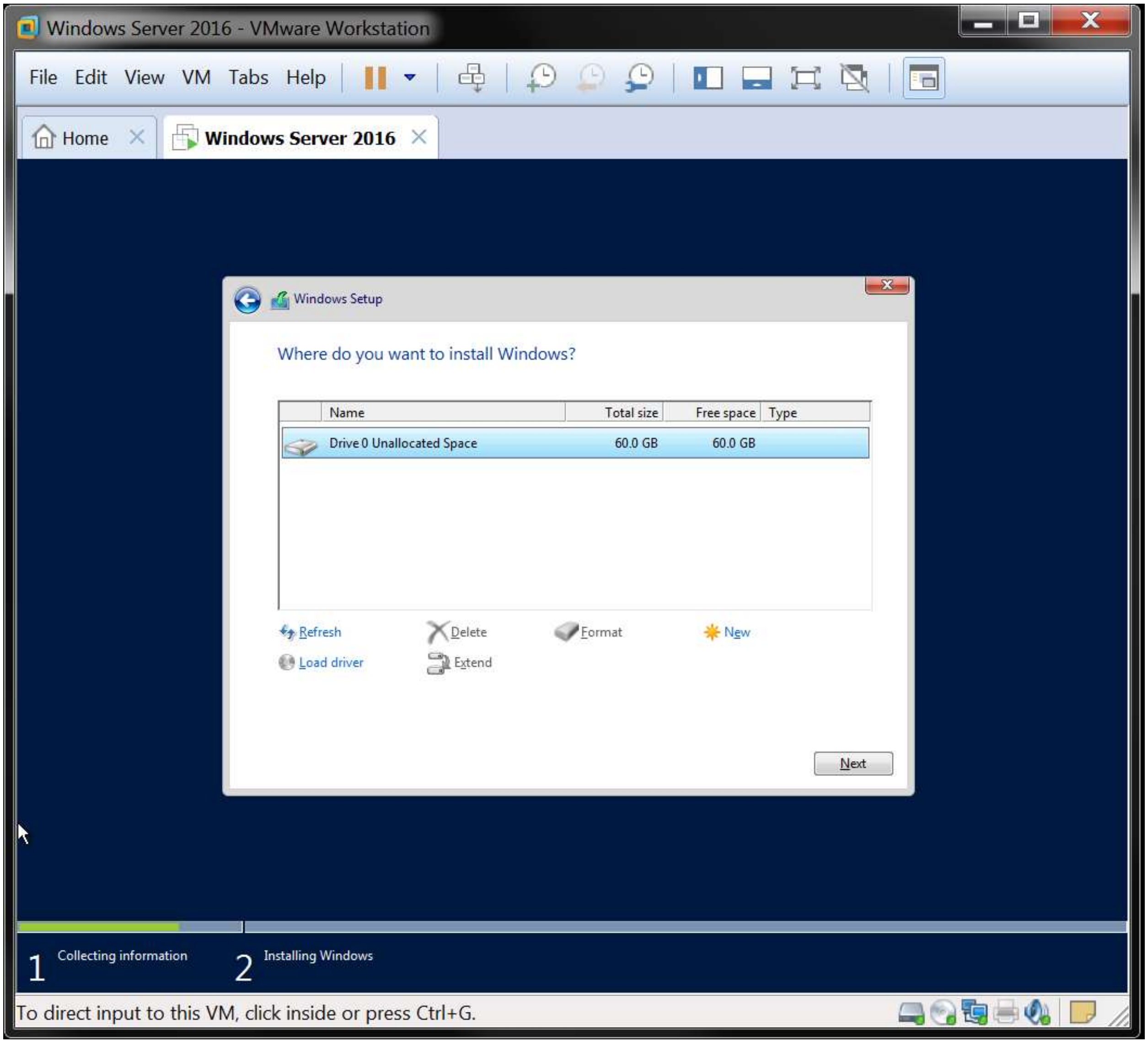

Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Setup
Windows Server 2016 Technical Preview 4
Install now
Repair your computer
© 2016 Microsoft Corporation. All rights reserved.
To direct input to this VM, click inside or press Ctrl+G.

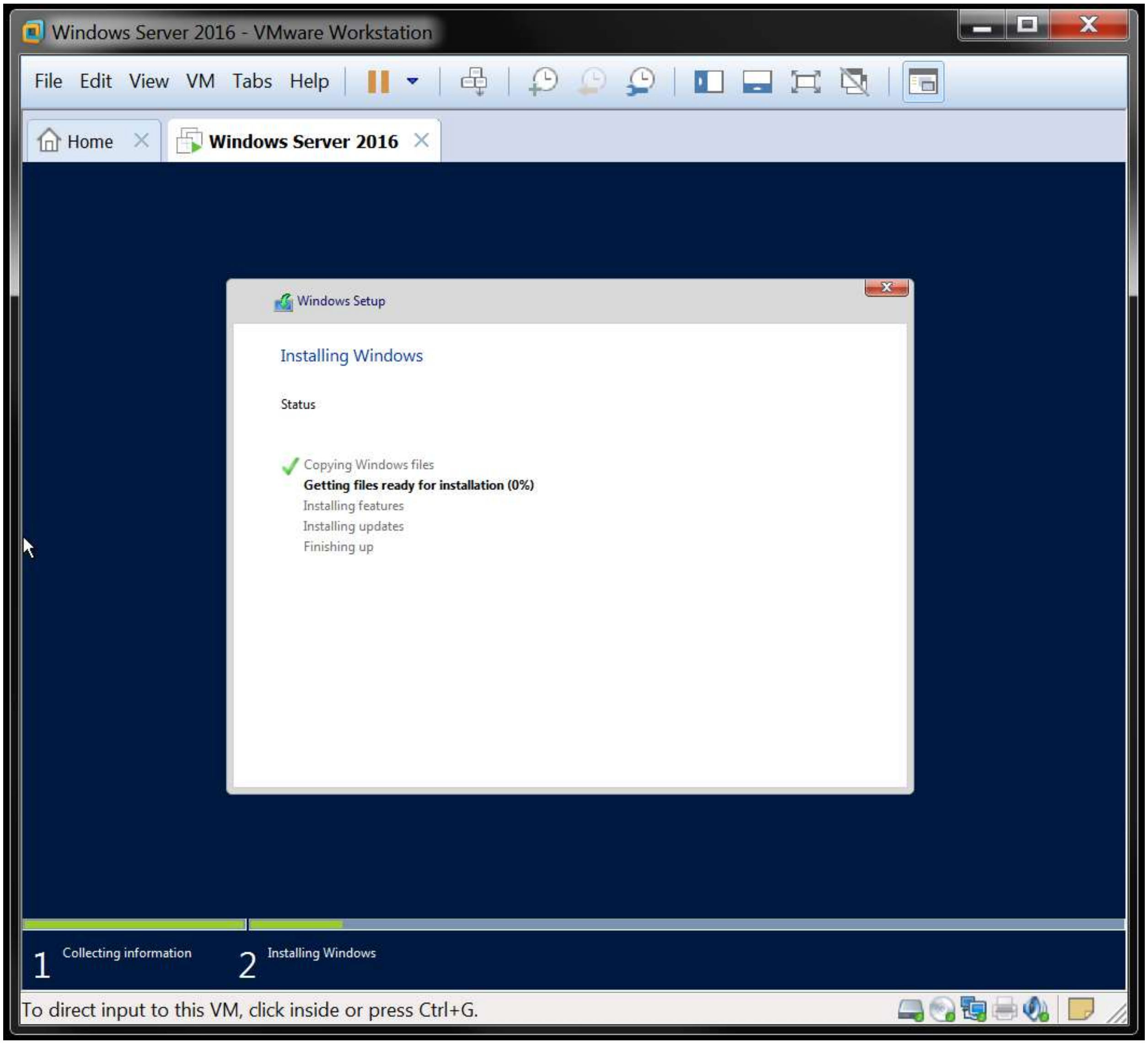

Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Setup is starting
To direct input to this VM, click inside or press Ctrl+G.

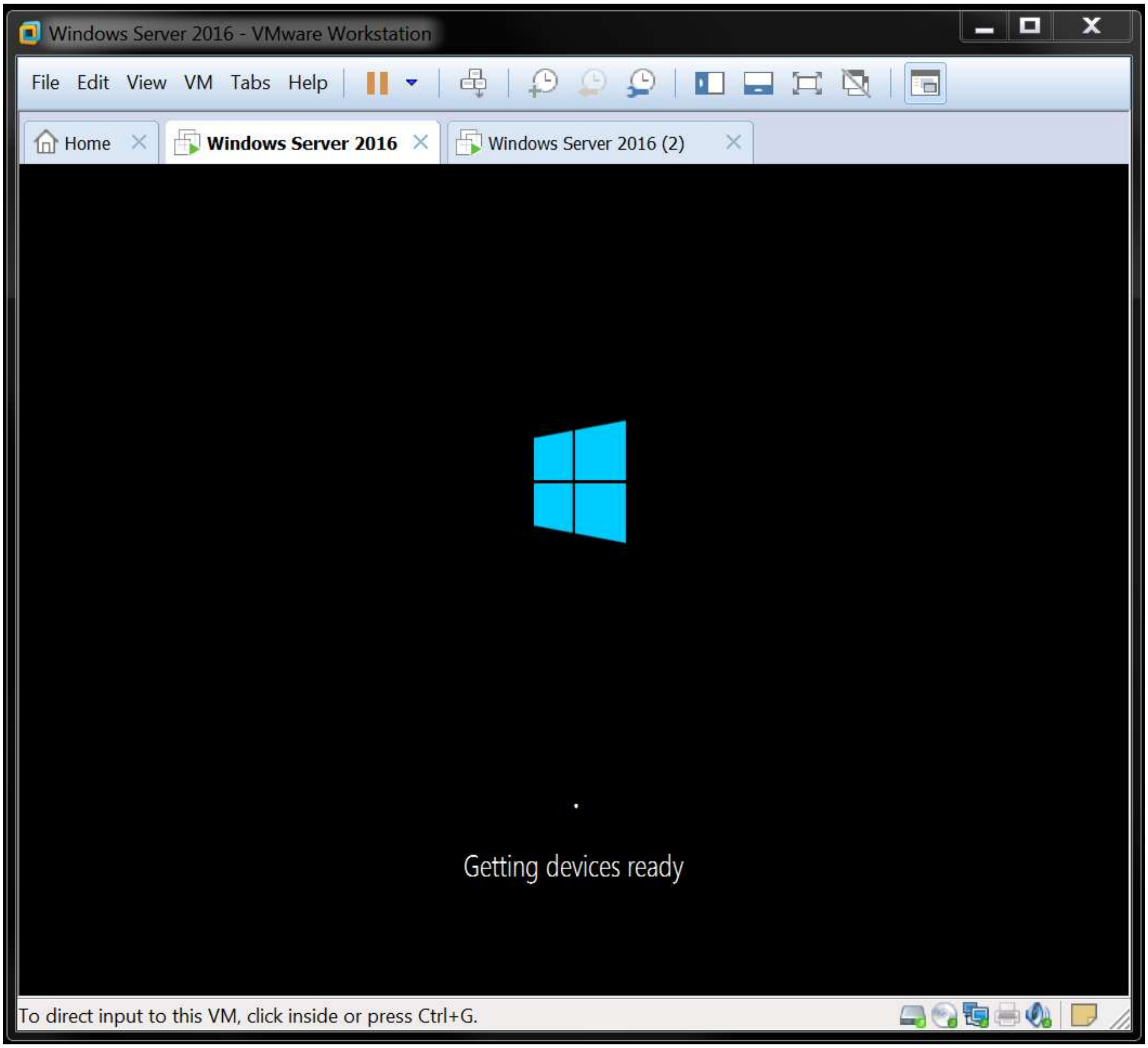

Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Setup
Select the operating system you want to install
Operating system | Architecture | Date modified
Windows Server 2016 Technical Preview 4 | x64 | 10/30/2015
Windows Server 2016 Technical Preview 4 (Desktop Experien... | x64 | 10/30/2015
Description:
This option is useful when a GUI is required—for example, to provide backward compatibility for an application that cannot be run on a Server Core installation. All server roles and features are supported. For more details see "Windows Server Installation Options."
Next
1 Collecting information
2 Installing Windows
To direct input to this VM, click inside or press Ctrl+G.

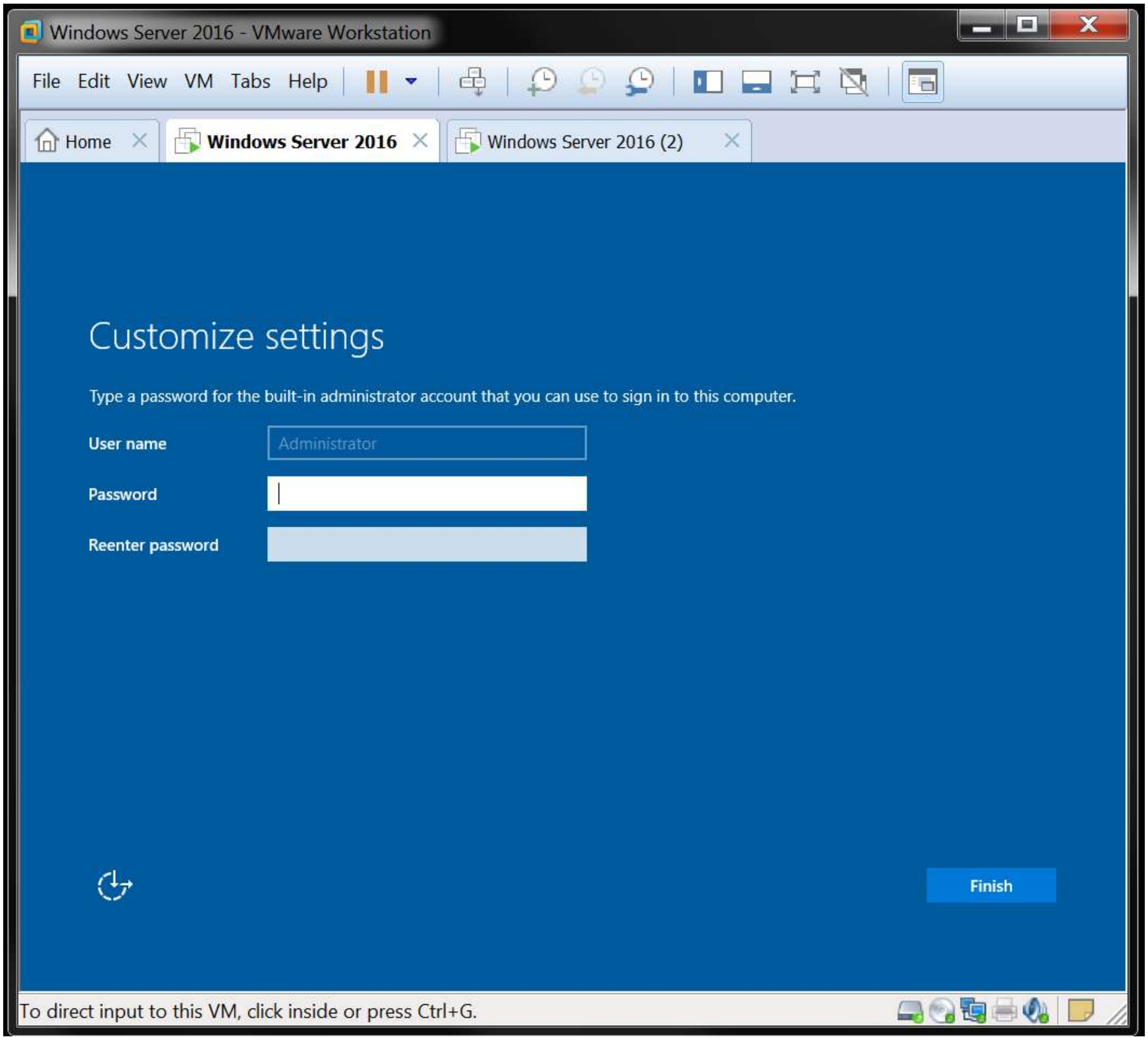

Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Setup
License terms
MICROSOFT PRE-RELEASE SOFTWARE LICENSE TERMS
MICROSOFT WINDOWS SERVER
These license terms are an agreement between Microsoft Corporation (or based on where you live, or if a business, where your principal place of business is located, one of its affiliates) and you. If you are entering into this agreement on behalf of an entity, such as your employer, you represent that you have the legal authority to bind that entity. Please read them. They apply to the pre-release software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft:
updates,
supplements,
I accept the license terms
Next
1 Collecting information
2 Installing Windows
To direct input to this VM, click inside or press Ctrl+G.

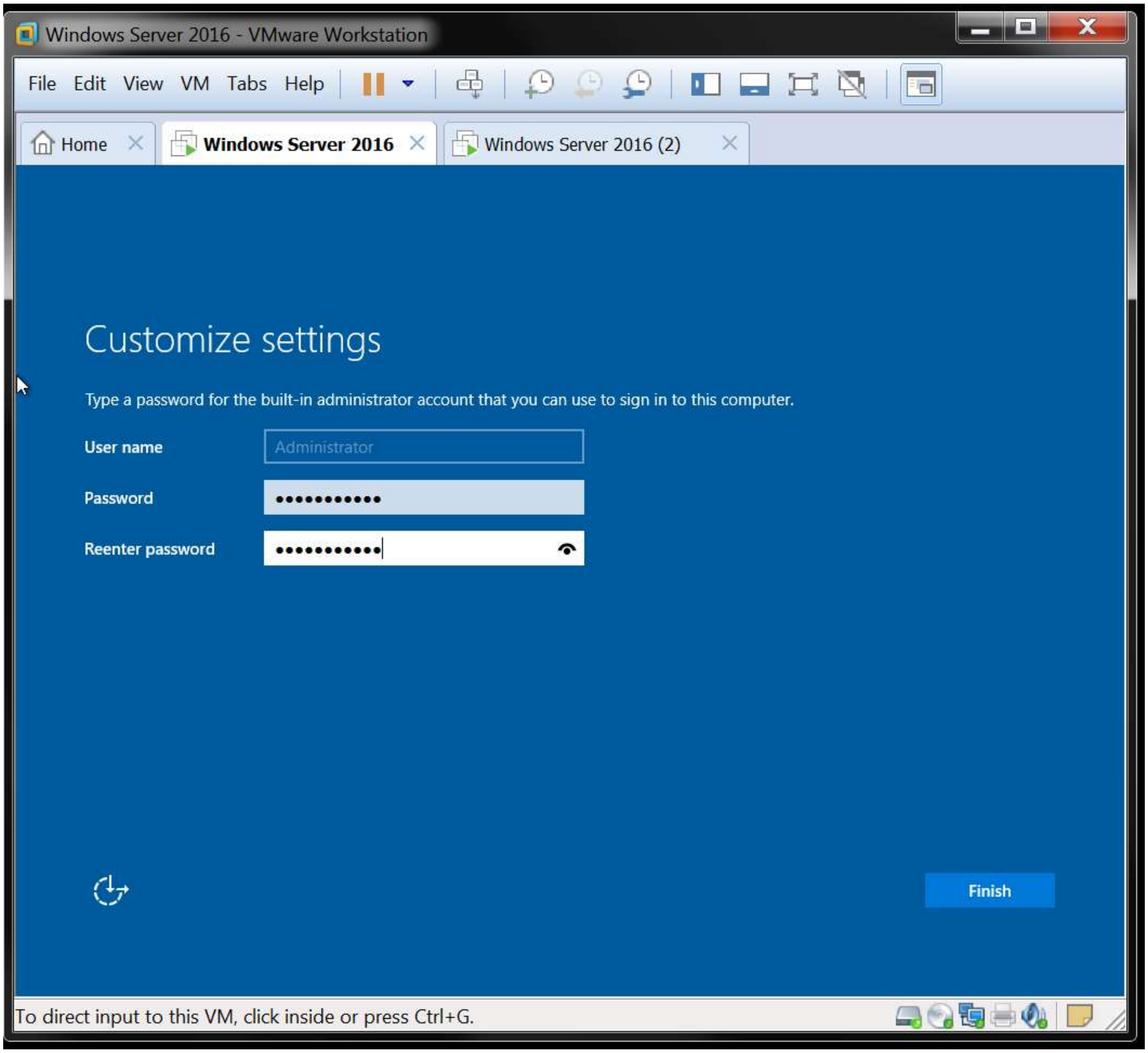

Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Setup
Which type of installation do you want?
Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.
Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.
Help me decide
1 Collecting information
2 Installing Windows
To direct input to this VM, click inside or press Ctrl+G.

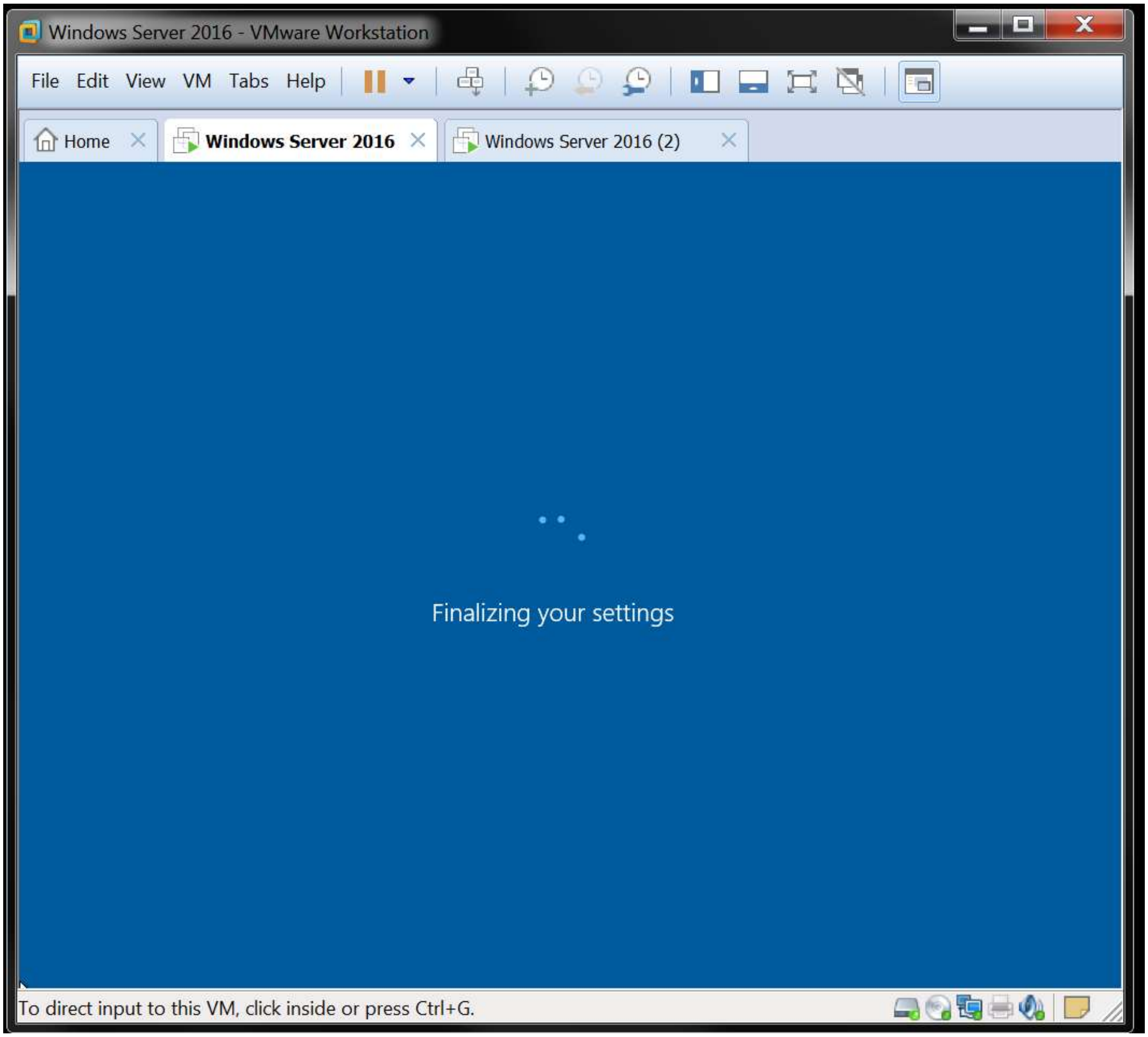

Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Setup
Where do you want to install Windows?
Name
Total size
Free space
Type
Drive 0 Unallocated Space
60.0 GB
60.0 GB
Refresh
Delete
Format
New
Load driver
Extend
Next
1 Collecting information
2 Installing Windows
To direct input to this VM, click inside or press Ctrl+G.


Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Setup
Installing Windows
Status
Copying Windows files
Getting files ready for installation (0%)
Installing features
Installing updates
Finishing up
1 Collecting information
2 Installing Windows
To direct input to this VM, click inside or press Ctrl+G.

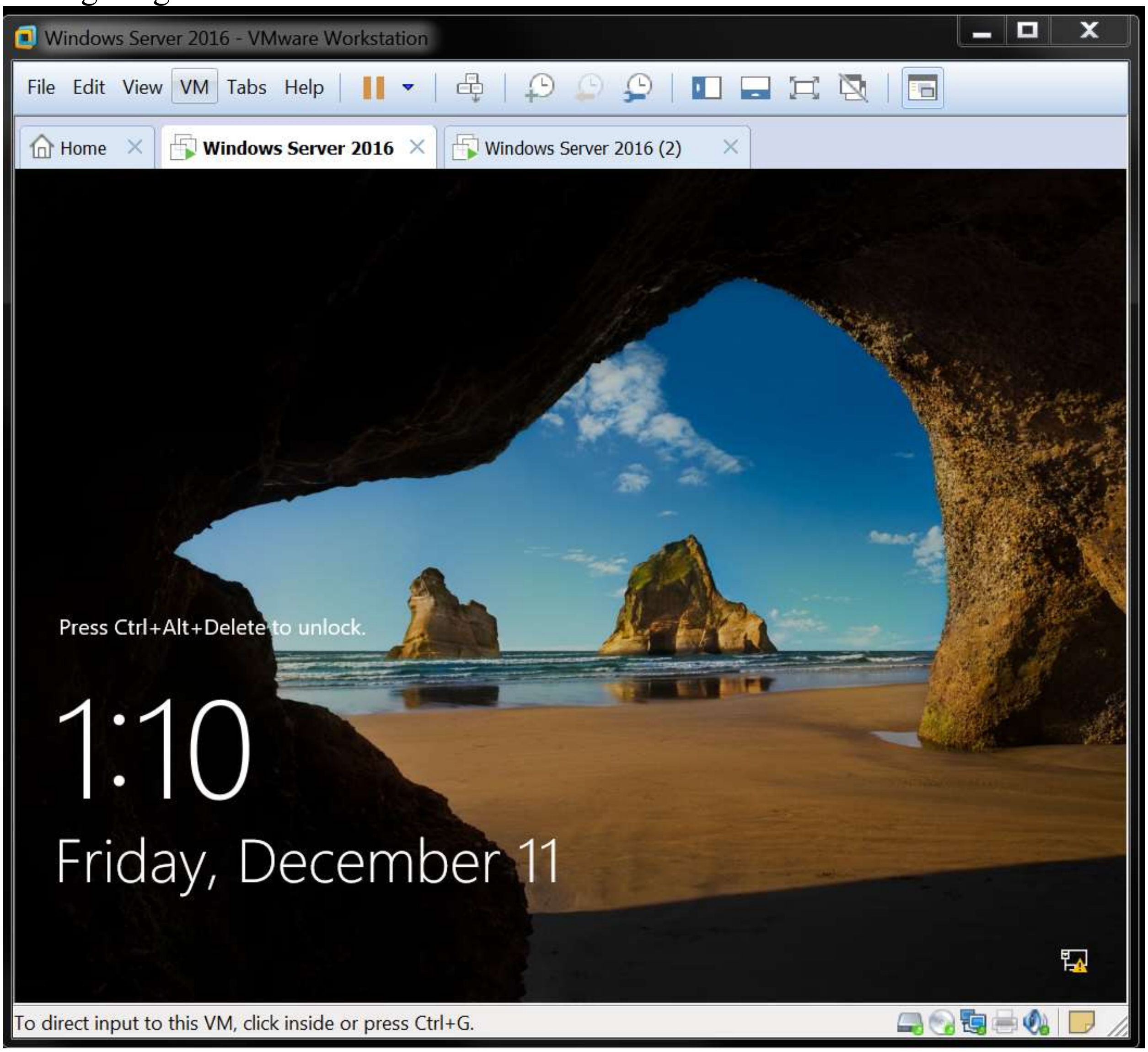

Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Server 2016 (2)
Getting devices ready
To direct input to this VM, click inside or press Ctrl+G.

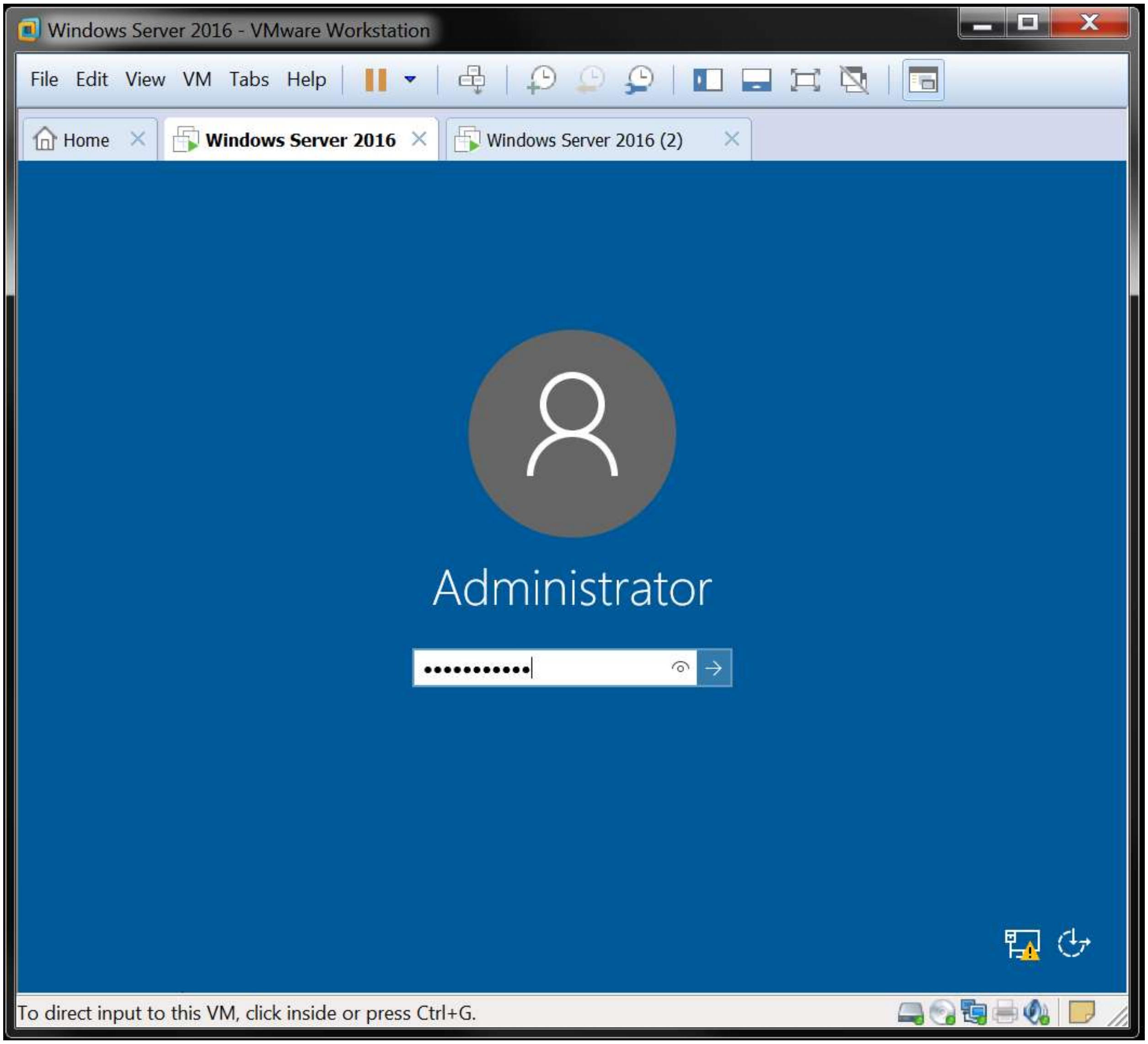

Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Server 2016 (2)
Customize settings
Type a password for the built-in administrator account that you can use to sign in to this computer.
User name
Administrator
Password
Reenter password
Finish
To direct input to this VM, click inside or press Ctrl+G.

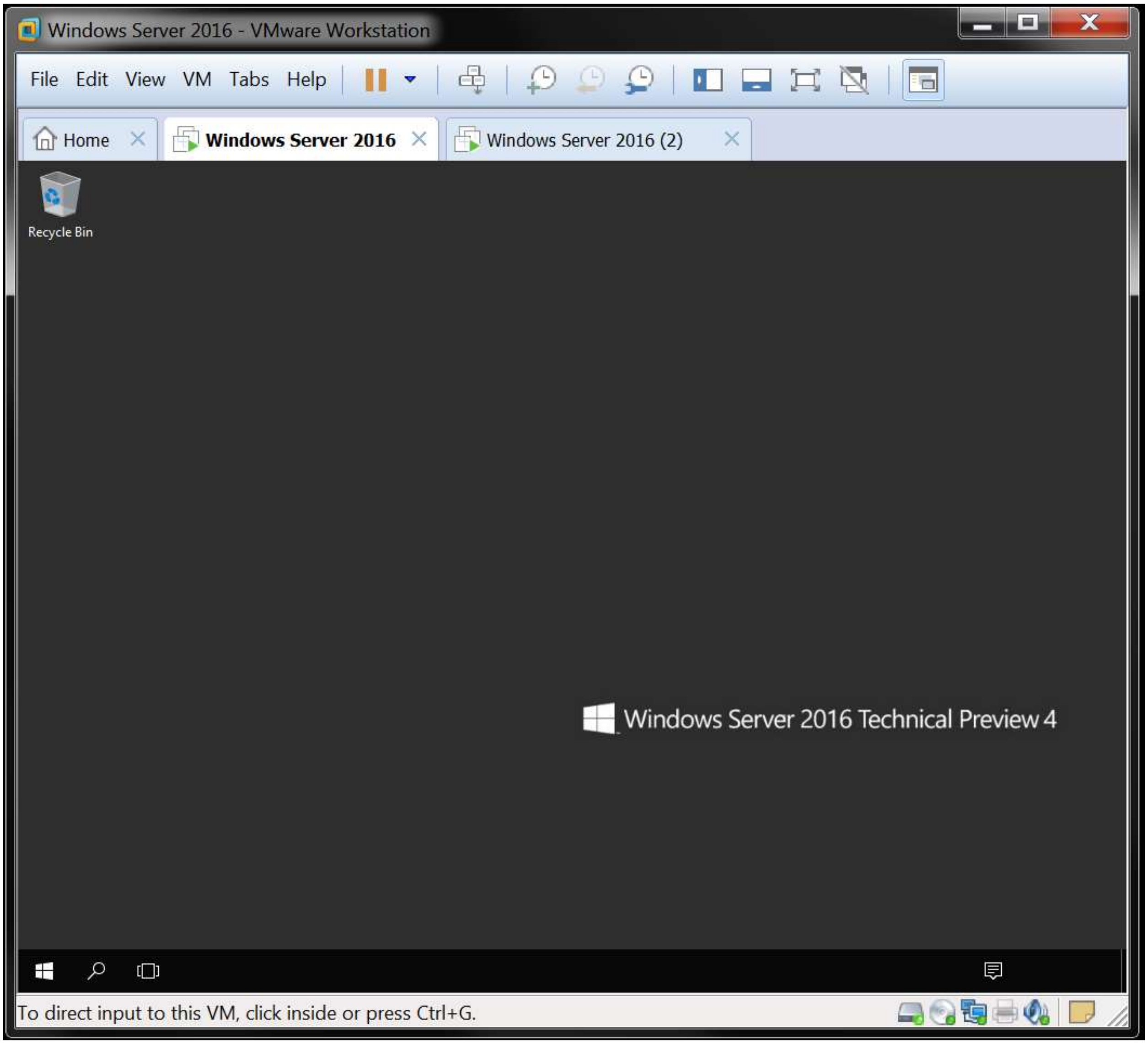

Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Server 2016 (2)
Customize settings
Type a password for the built-in administrator account that you can use to sign in to this computer.
User name
Administrator
Password
Reenter password
Finish
To direct input to this VM, click inside or press Ctrl+G.

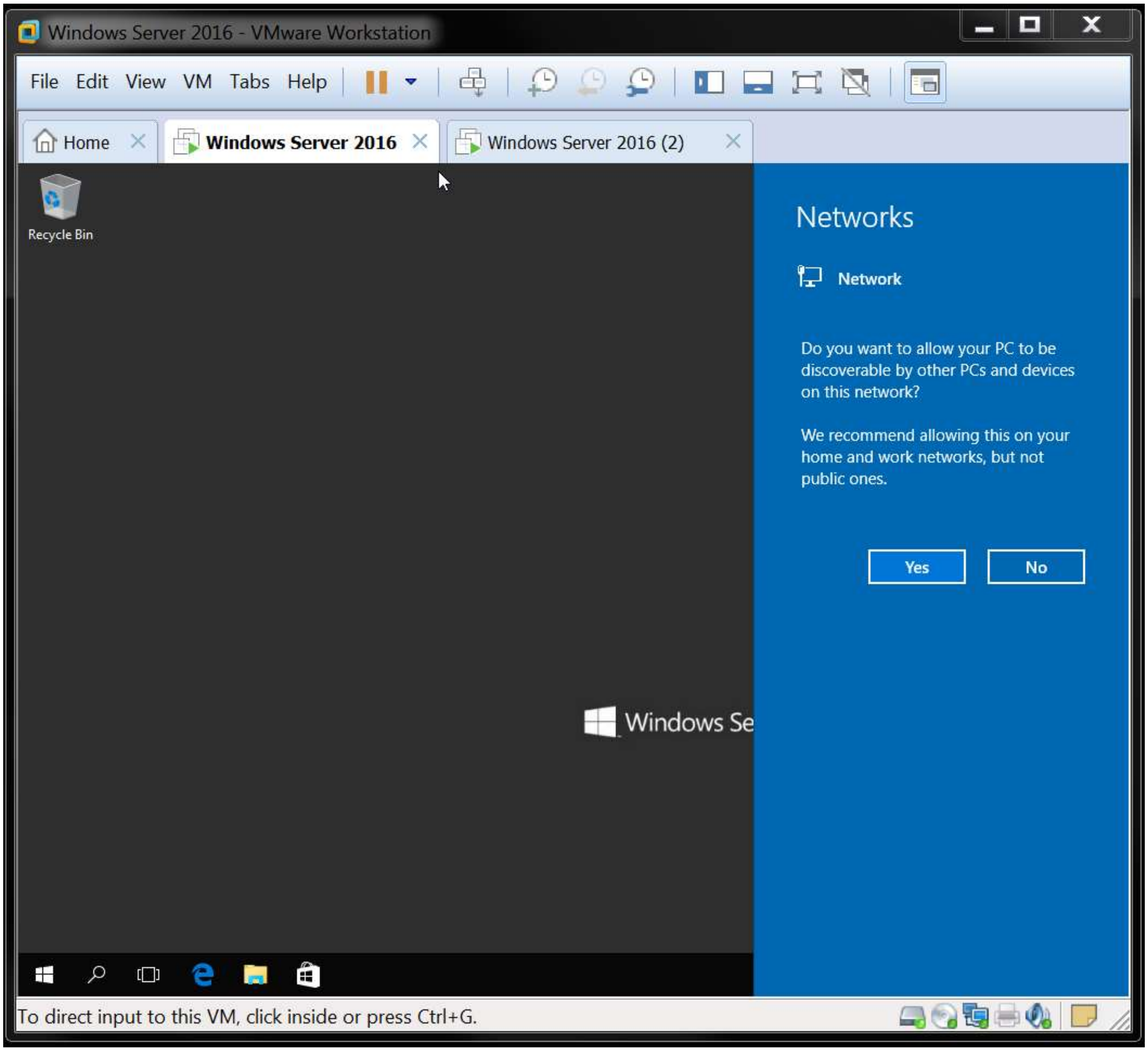

Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Server 2016 (2)
Finalizing your settings
To direct input to this VM, click inside or press Ctrl+G.

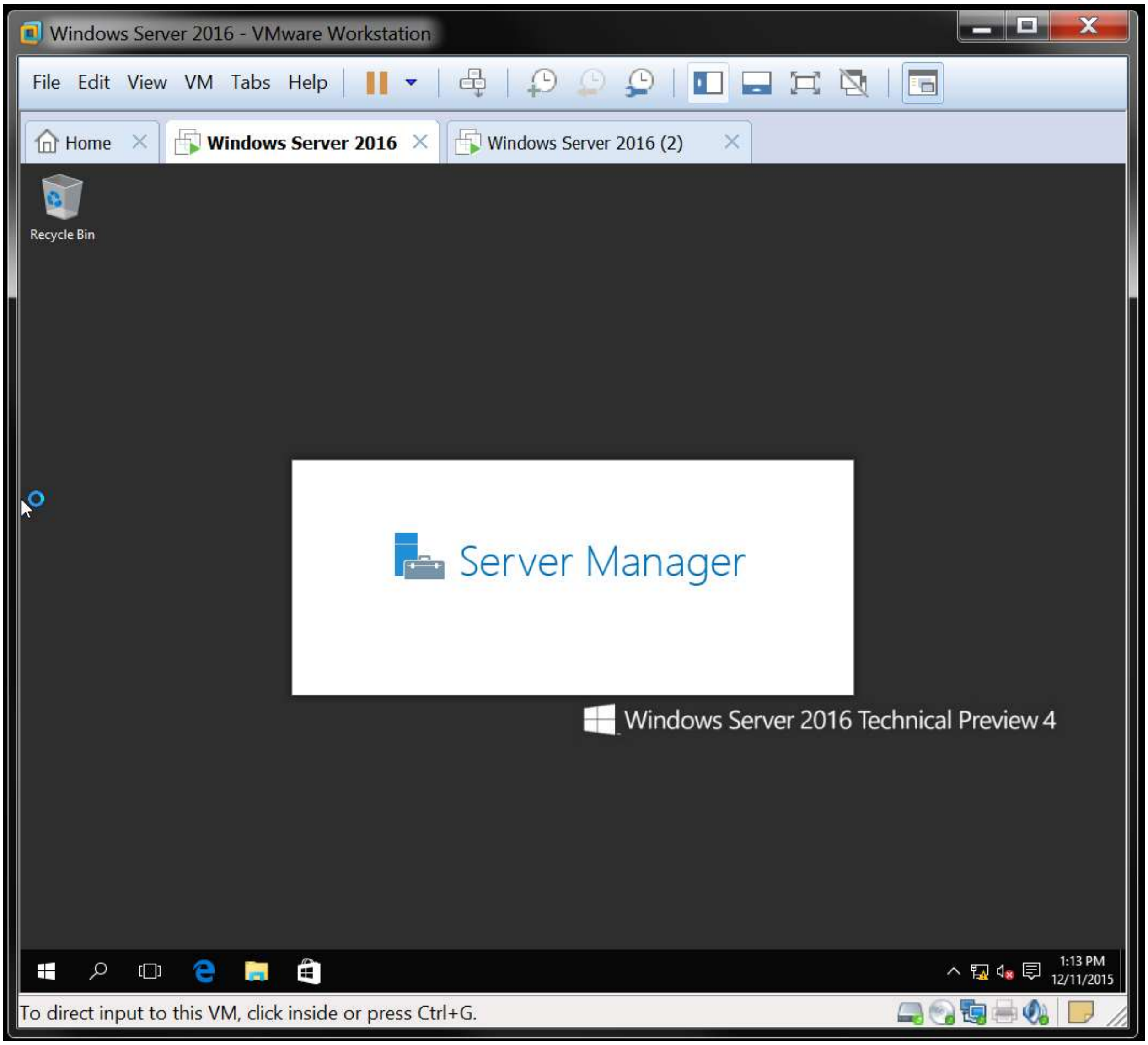
Configuring the AAA server

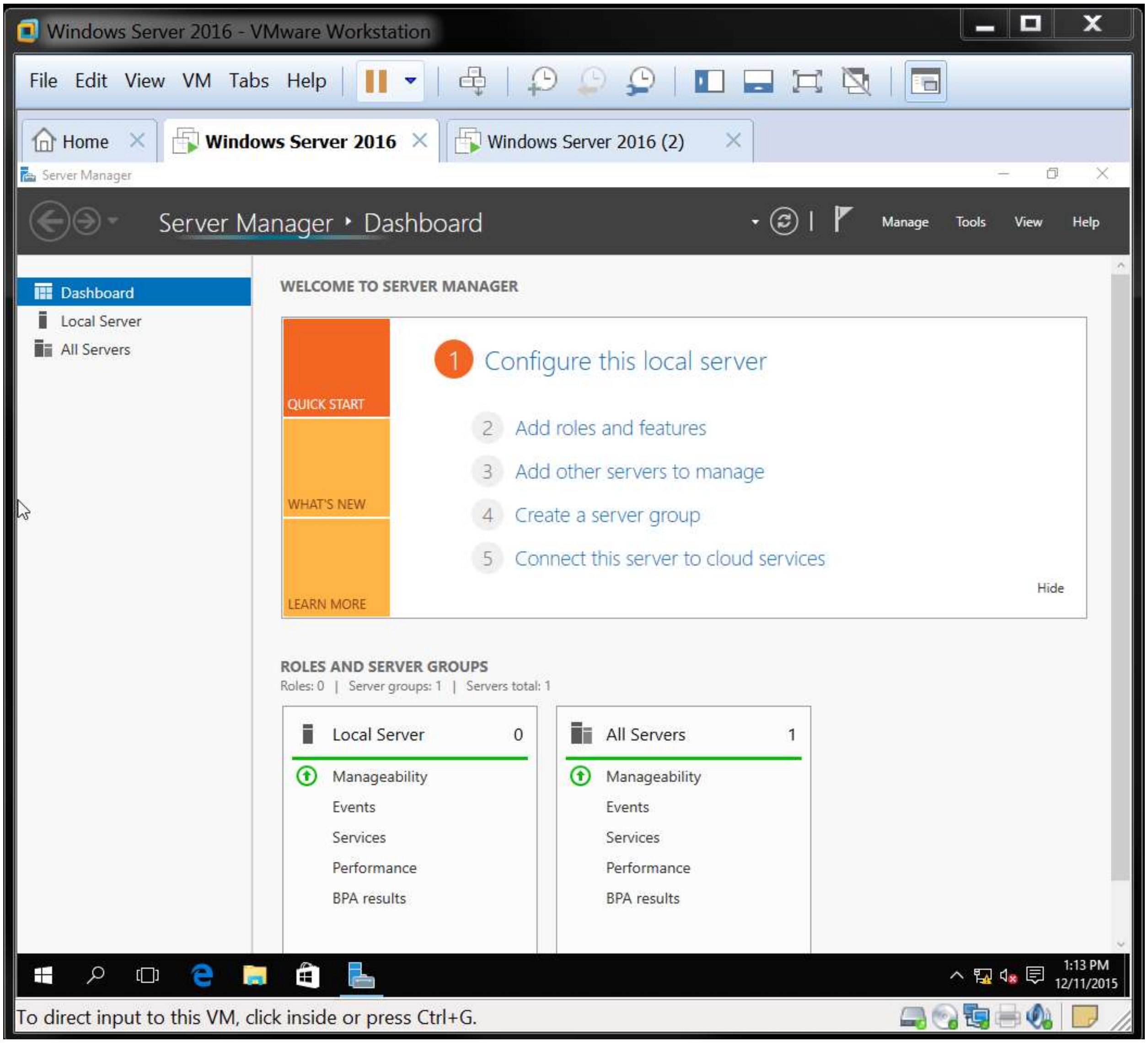



Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Server 2016 (2)
Administrator
To direct input to this VM, click inside or press Ctrl+G.


Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Server 2016 (2)
Recycle Bin
Windows Server 2016 Technical Preview 4
To direct input to this VM, click inside or press Ctrl+G.

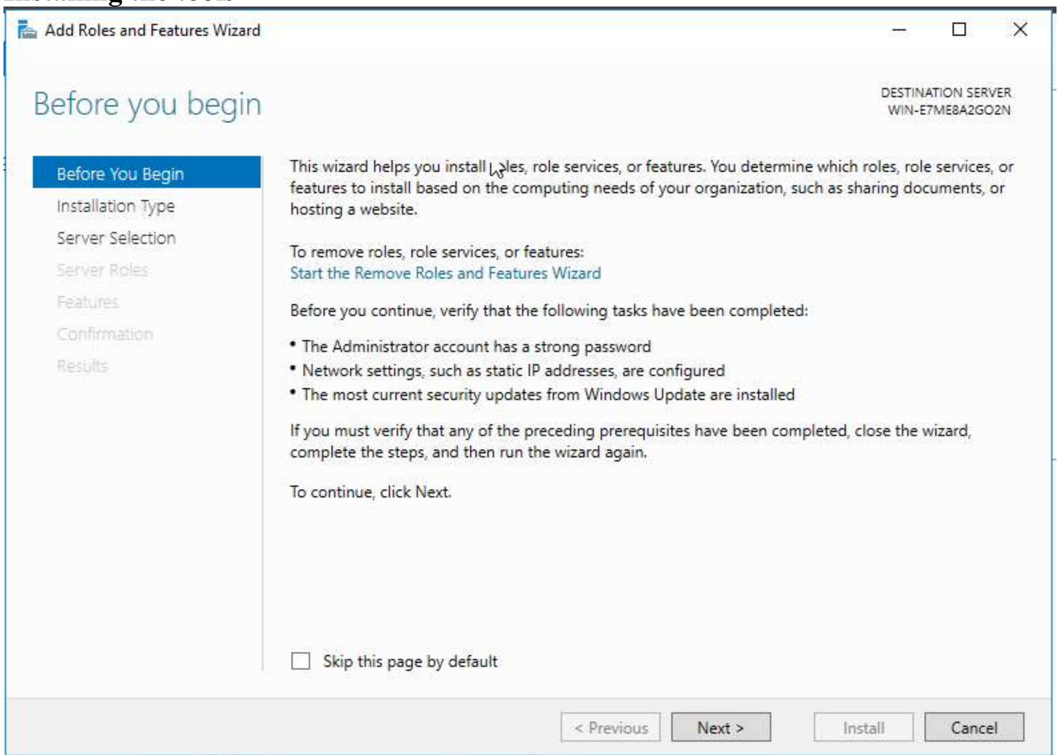

Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Server 2016 (2)
Recycle Bin
Networks
Network
Do you want to allow your PC to be discoverable by other PCs and devices on this network?
We recommend allowing this on your home and work networks, but not public ones.
Yes
No
Windows Se
To direct input to this VM, click inside or press Ctrl+G.

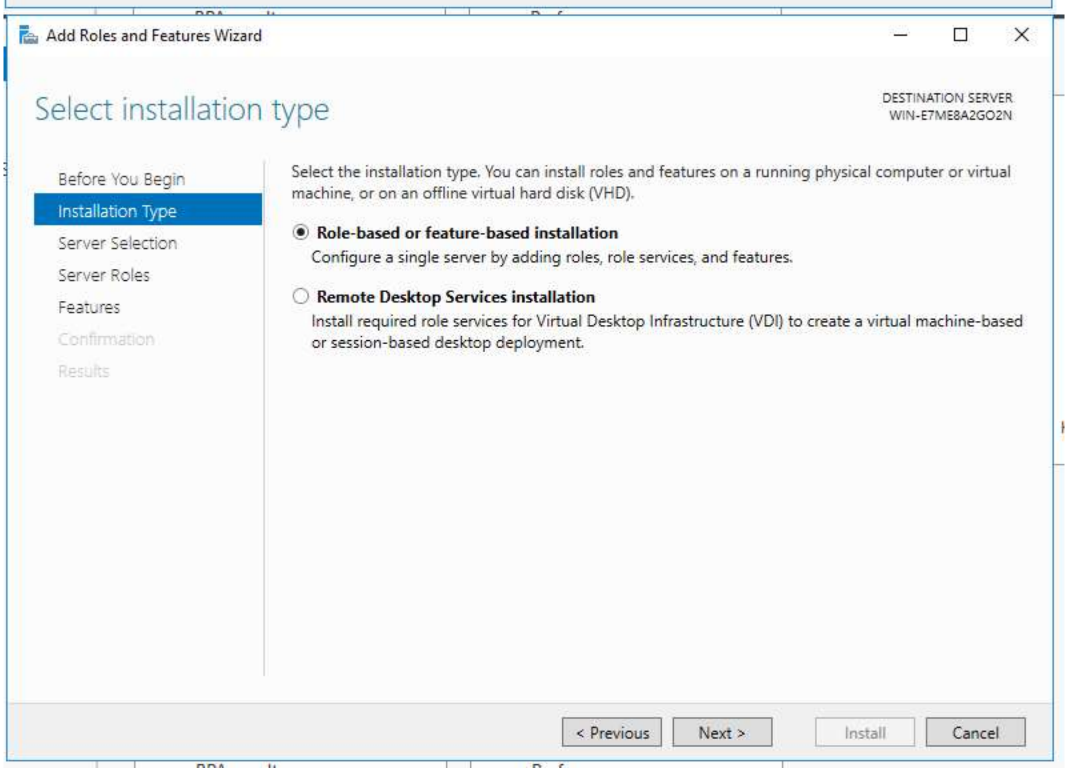

Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Server 2016 (2)
Recycle Bin
Server Manager
Windows Server 2016 Technical Preview 4
1:13 PM
12/11/2015
To direct input to this VM, click inside or press Ctrl+G.

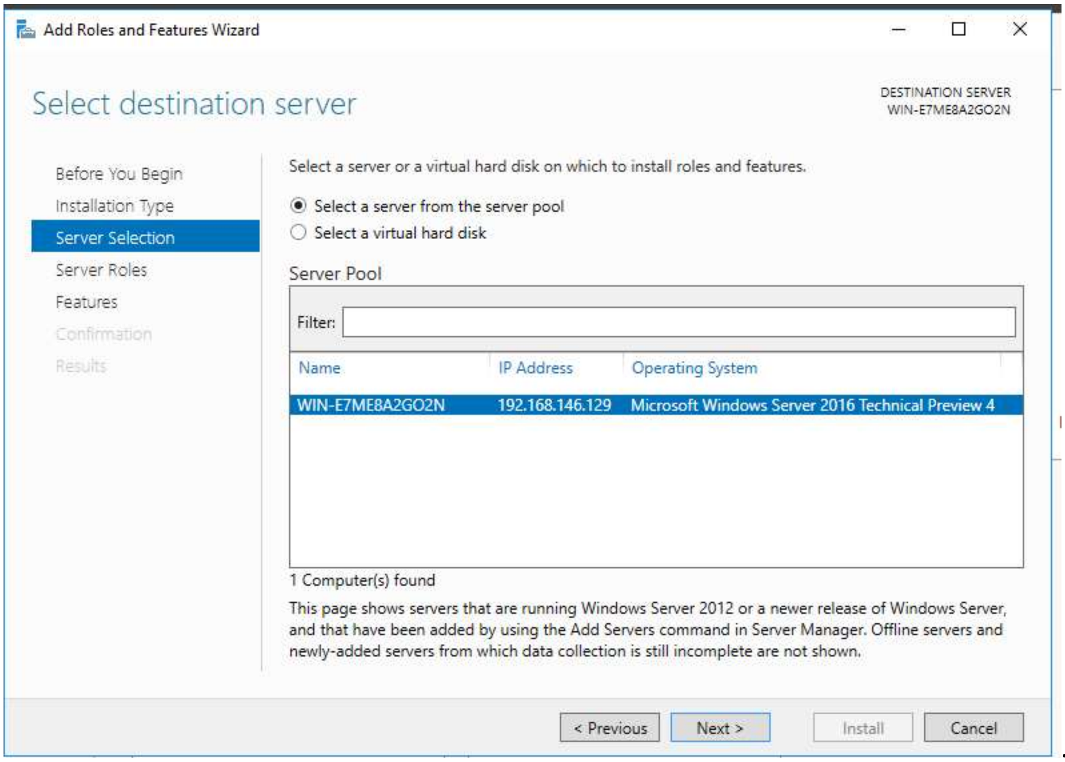


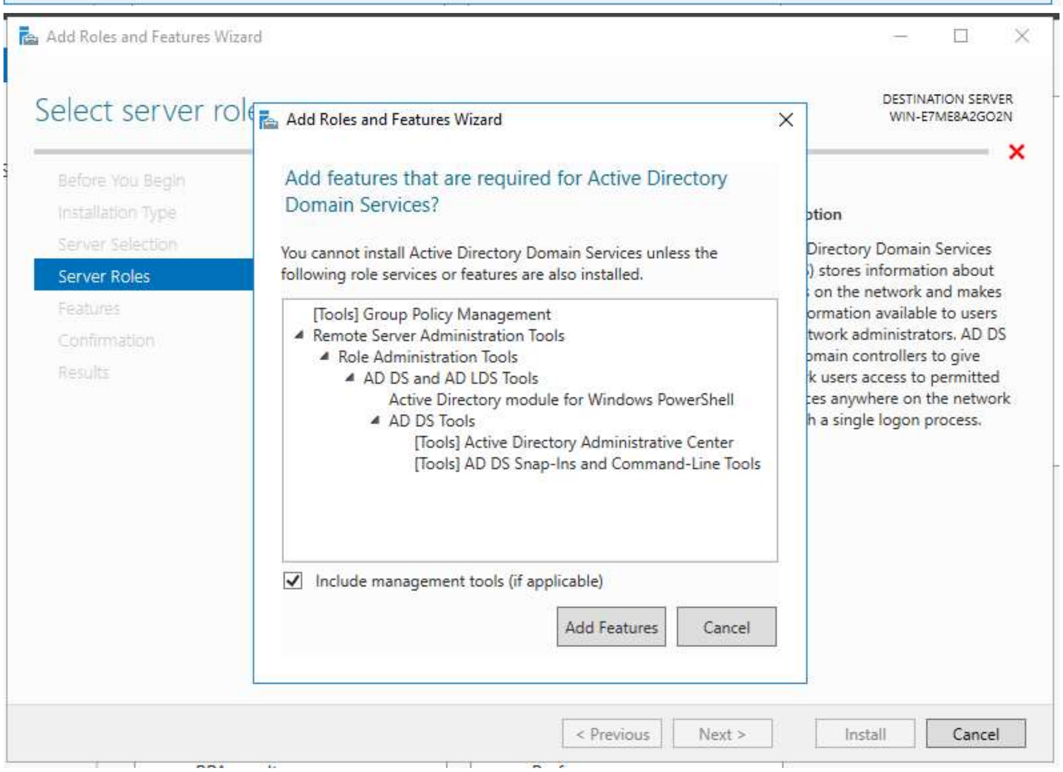
Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Server 2016 (2)
Server Manager
Server Manager ‣ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 0 | Server groups: 1 | Servers total: 1
Local Server 0
Manageability
Events
Services
Performance
BPA results
All Servers 1
Manageability
Events
Services
Performance
BPA results
1:13 PM
12/11/2015
To direct input to this VM, click inside or press Ctrl+G.

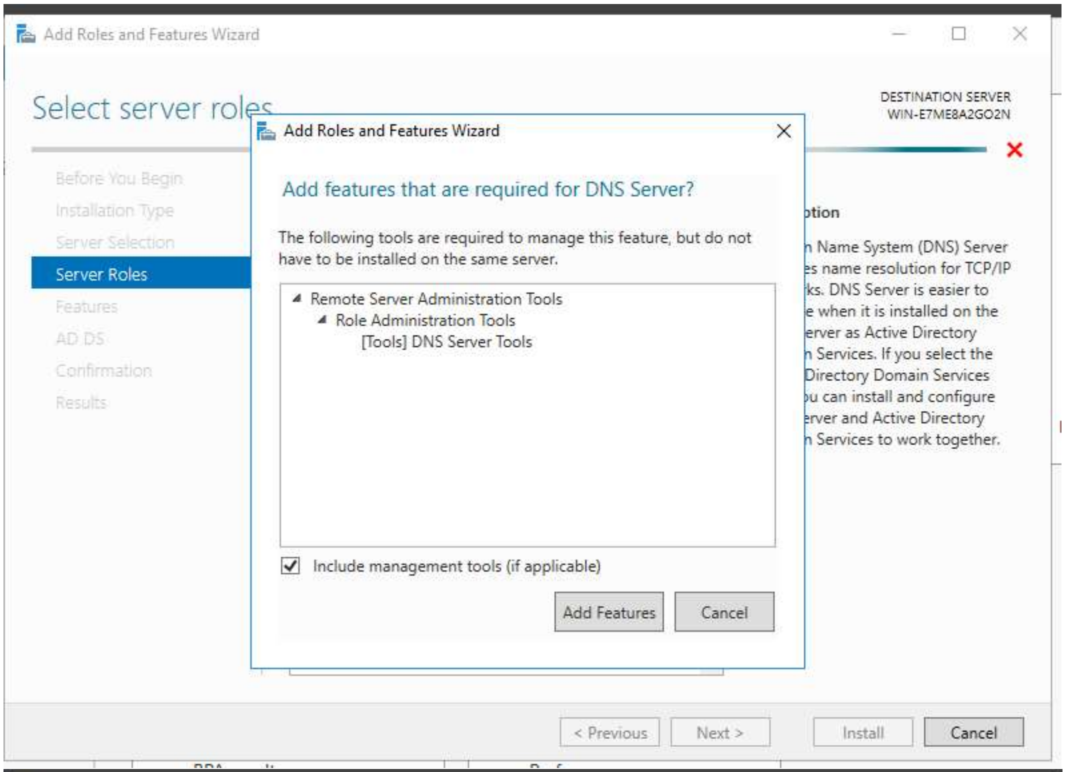
Installing the tools

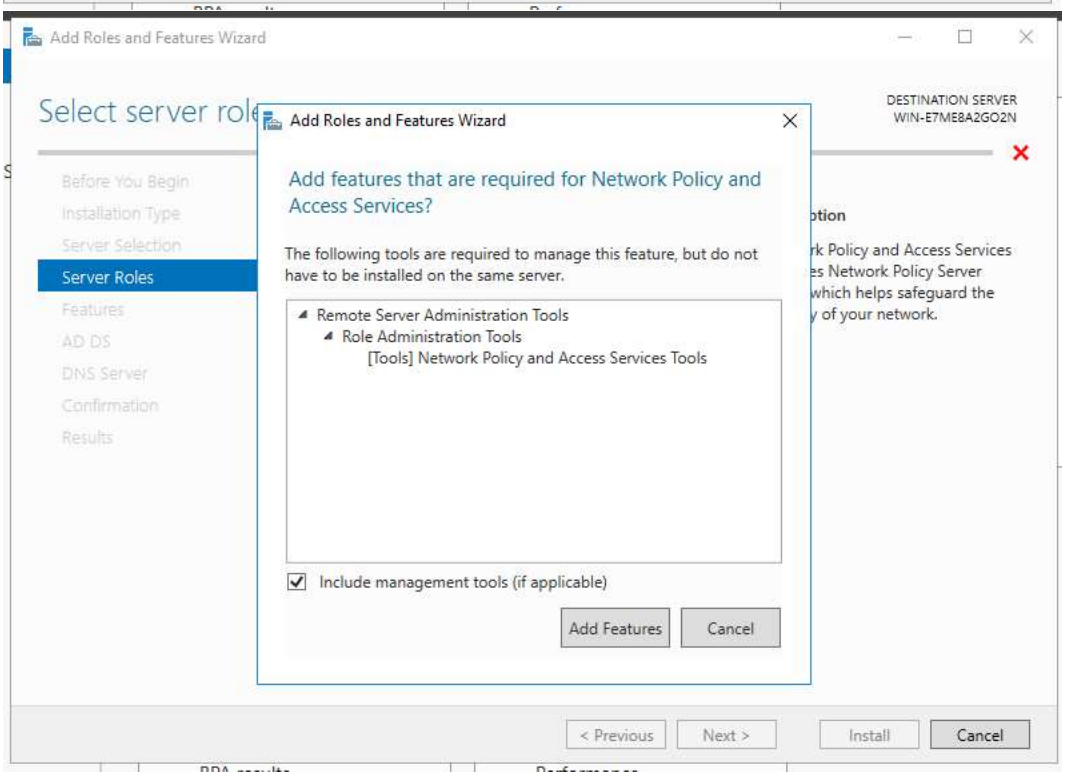


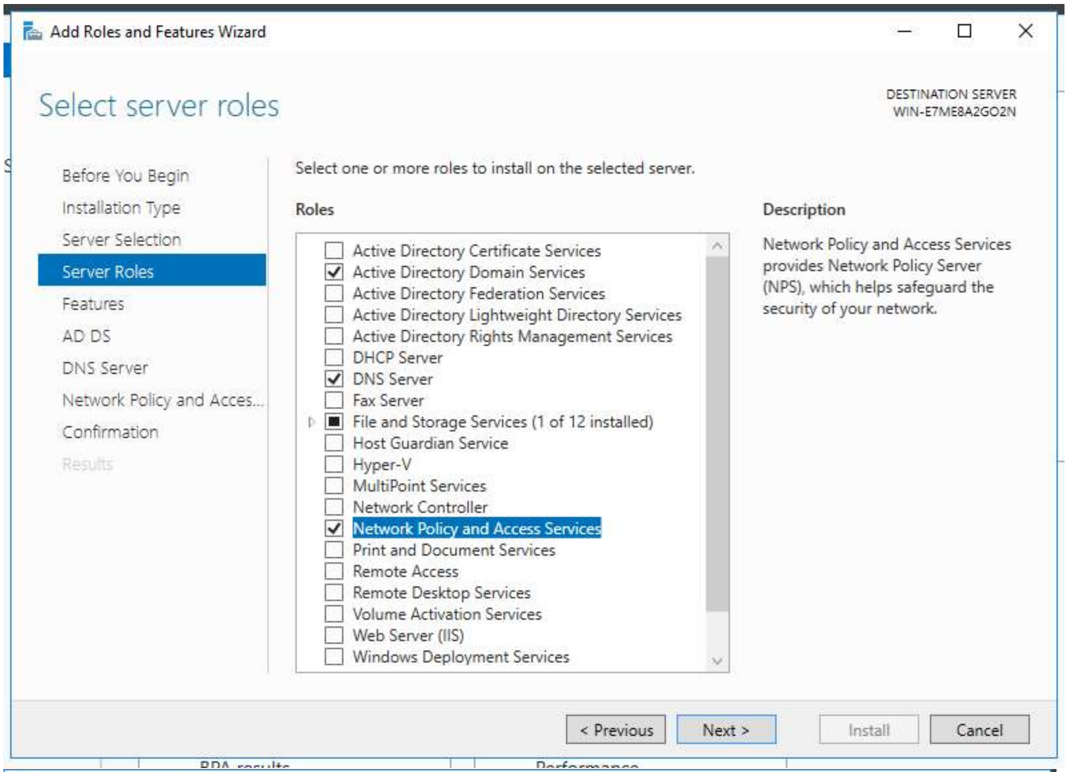


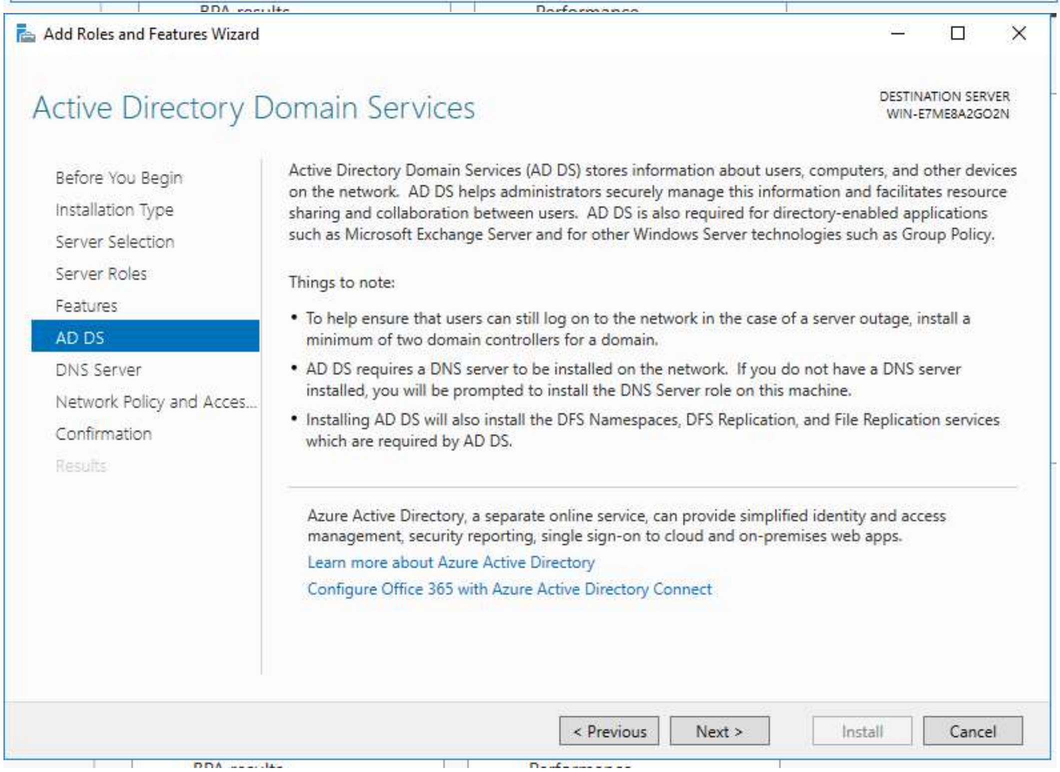

Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
WIN-E7ME8A2GO2N
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
WIN-E7ME8A2GO2N
192.168.146.129
Microsoft Windows Server 2016 Technical Preview 4
1 Computer(s) found
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel

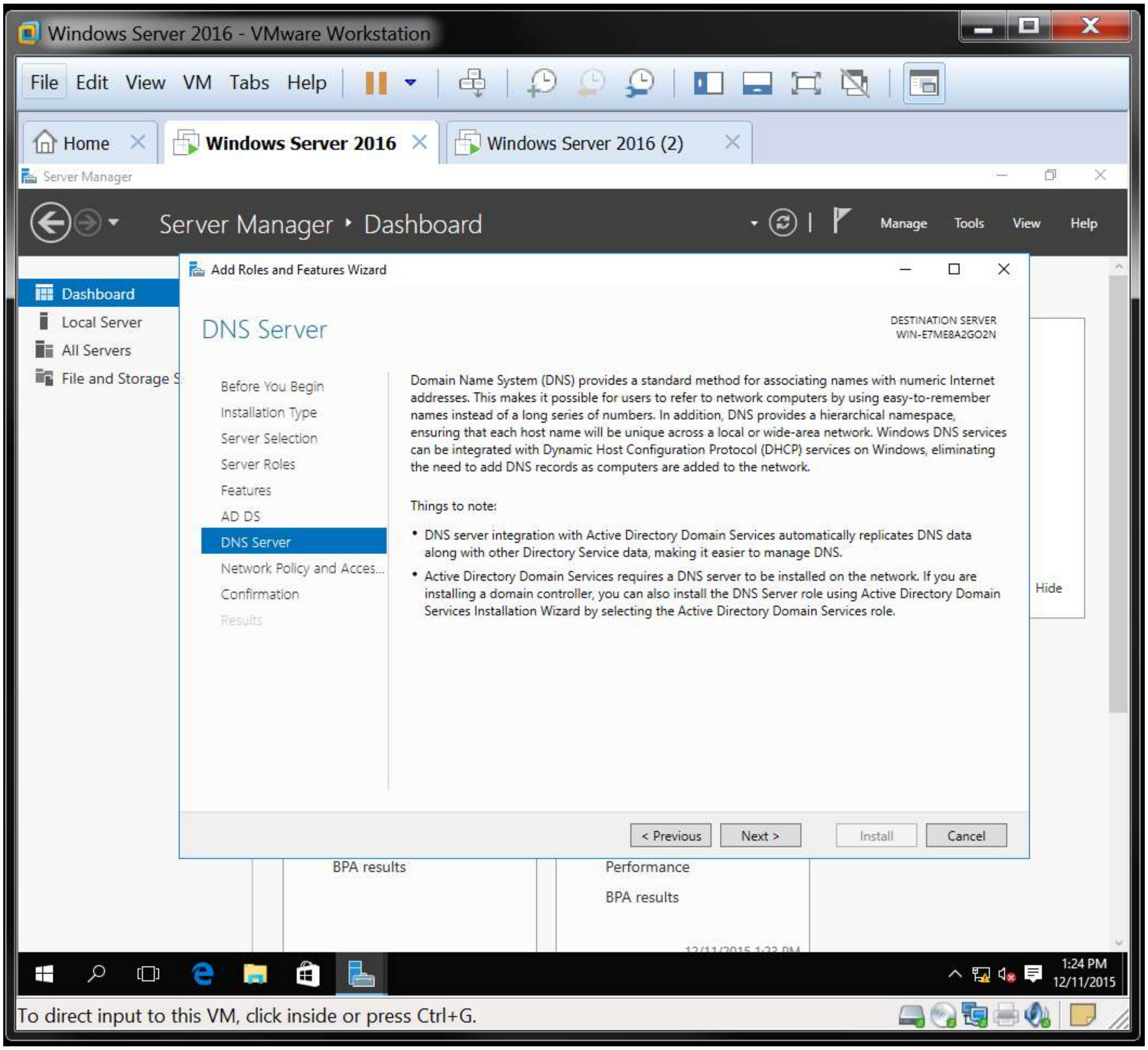

Add Roles and Features Wizard
Select server role
DESTINATION SERVER
WIN-E7ME8A2GO2N
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Add features that are required for Active Directory Domain Services?
You cannot install Active Directory Domain Services unless the following role services or features are also installed.
[Tools] Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
[Tools] Active Directory Administrative Center
[Tools] AD DS Snap-Ins and Command-Line Tools
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel

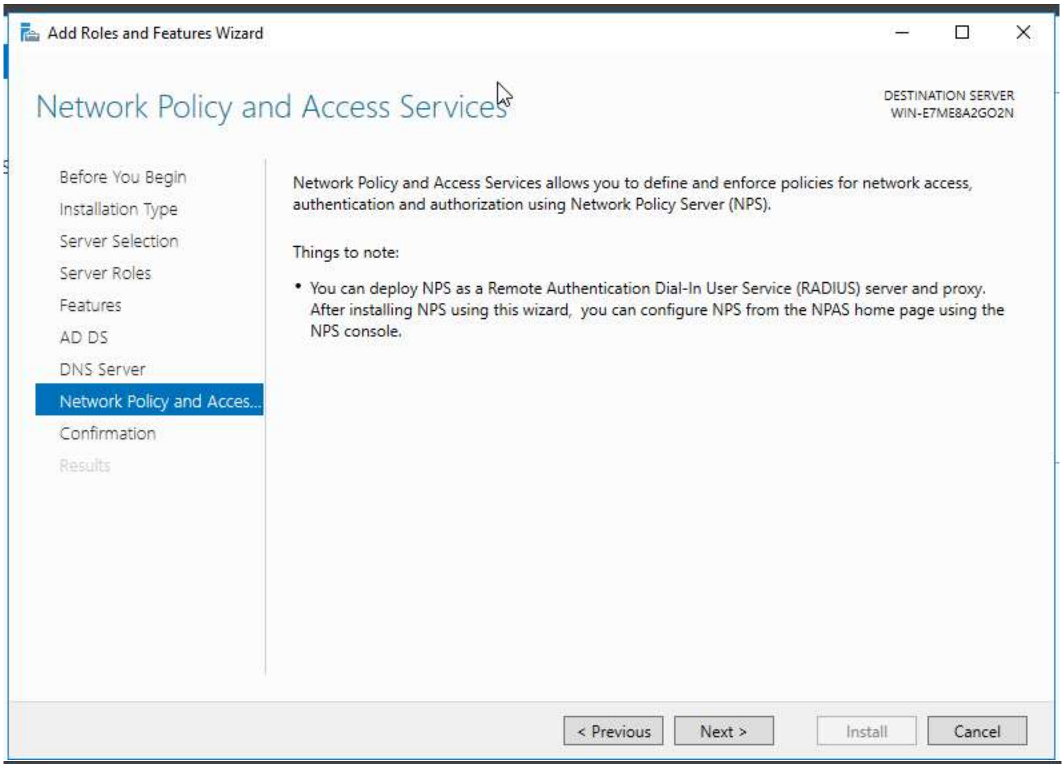

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-E7ME8A2GO2N
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
Add features that are required for DNS Server?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
[Tools] DNS Server Tools
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel

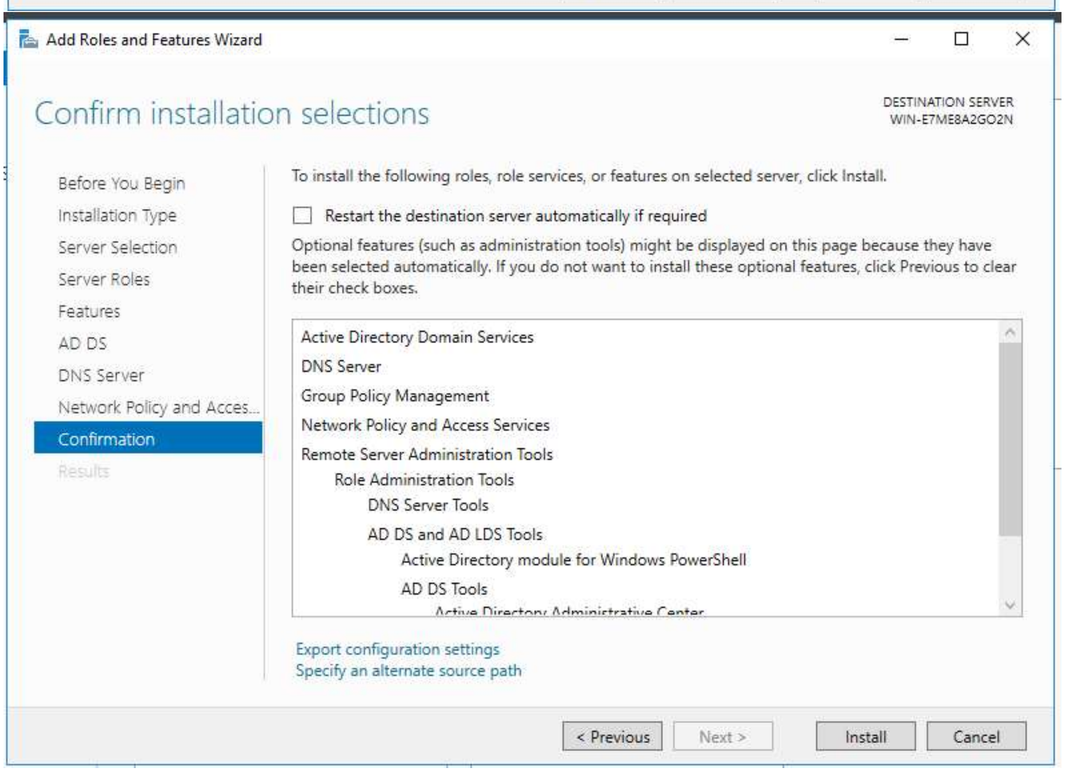

Add Roles and Features Wizard
Select server rol
DESTINATION SERVER
WIN-E7ME8A2GO2N
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Confirmation
Results
Add features that are required for Network Policy and Access Services?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
[Tools] Network Policy and Access Services Tools
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel

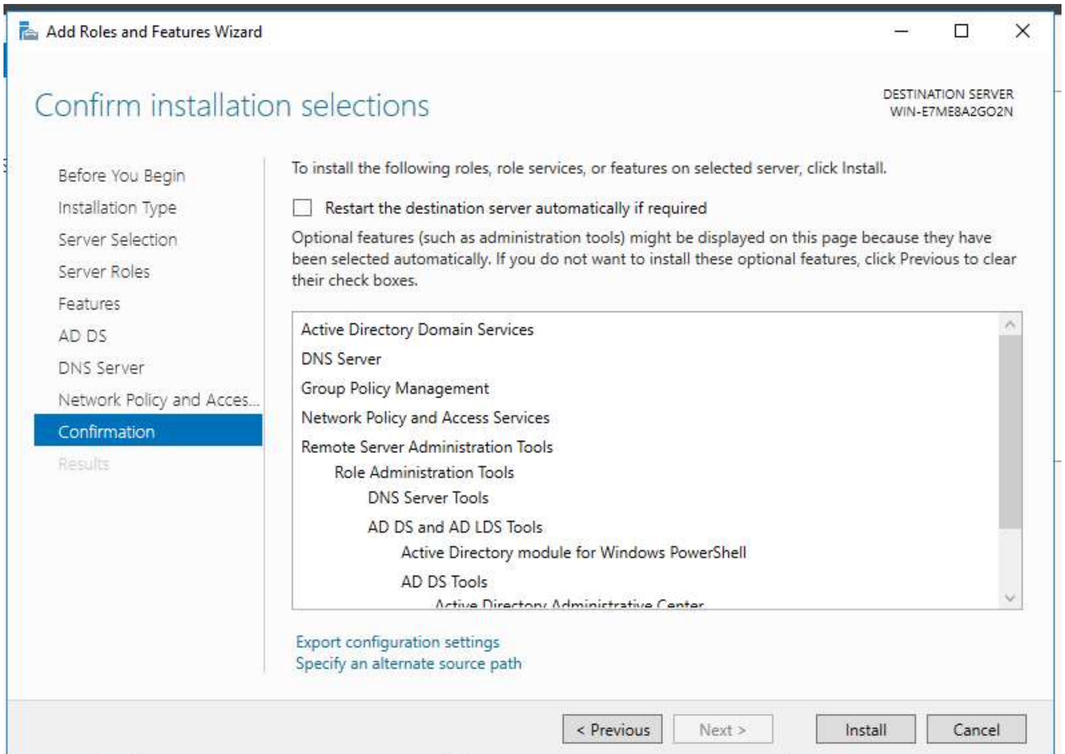

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-E7ME8A2GO2N
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Network Policy and Acces...
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
MultiPoint Services
Network Controller
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Description
Network Policy and Access Services provides Network Policy Server (NPS), which helps safeguard the security of your network.
< Previous
Next >
Install
Cancel

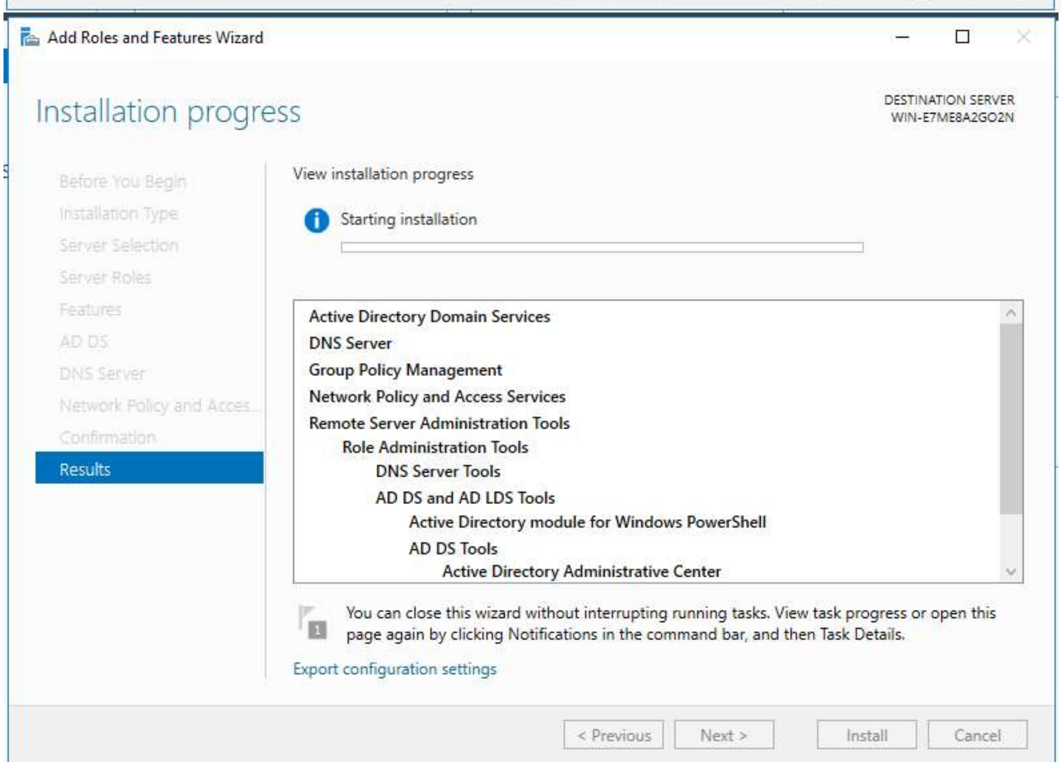

Add Roles and Features Wizard
Active Directory Domain Services
DESTINATION SERVER
WIN-E7ME8A2GO2N
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Network Policy and Acces...
Confirmation
Results
Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users. AD DS is also required for directory-enabled applications such as Microsoft Exchange Server and for other Windows Server technologies such as Group Policy.
Things to note:
• To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
• AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.
• Installing AD DS will also install the DFS Namespaces, DFS Replication, and File Replication services which are required by AD DS.
Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.
Learn more about Azure Active Directory
Configure Office 365 with Azure Active Directory Connect
< Previous
Next >
Install
Cancel

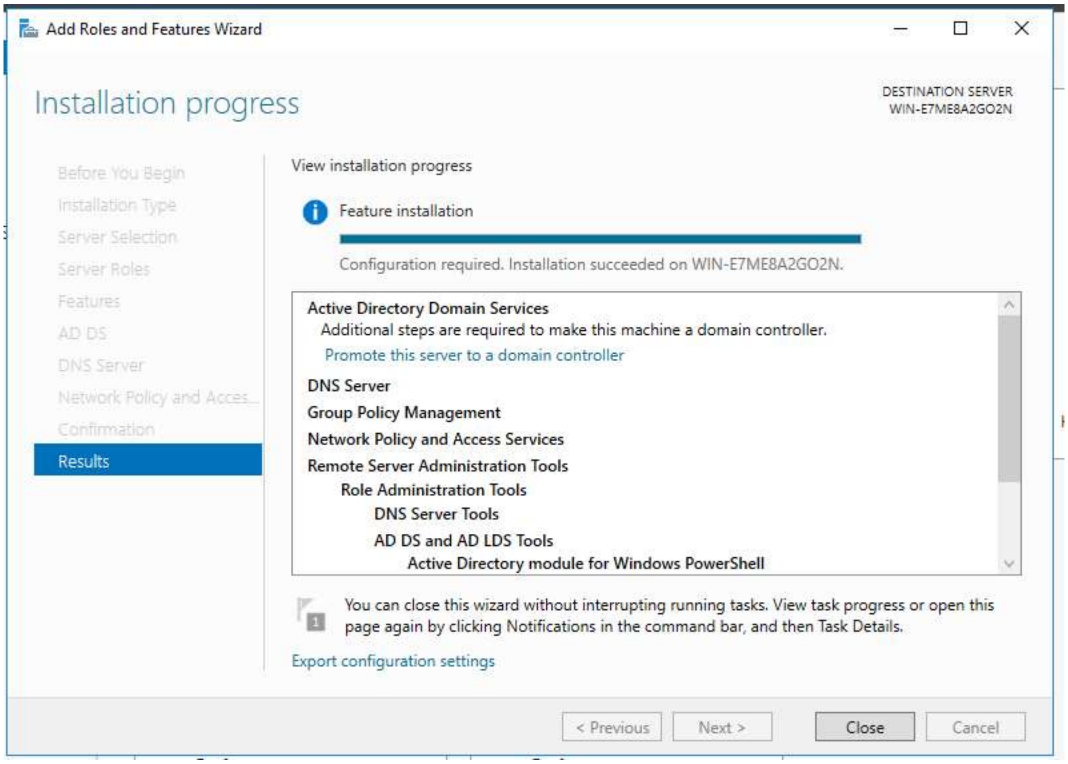

Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Server 2016 (2)
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
File and Storage S
Add Roles and Features Wizard
DNS Server
DESTINATION SERVER
WIN-E7ME8A2GO2N
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Network Policy and Acces...
Confirmation
Results
Domain Name System (DNS) provides a standard method for associating names with numeric Internet addresses. This makes it possible for users to refer to network computers by using easy-to-remember names instead of a long series of numbers. In addition, DNS provides a hierarchical namespace, ensuring that each host name will be unique across a local or wide-area network. Windows DNS services can be integrated with Dynamic Host Configuration Protocol (DHCP) services on Windows, eliminating the need to add DNS records as computers are added to the network.
Things to note:
• DNS server integration with Active Directory Domain Services automatically replicates DNS data along with other Directory Service data, making it easier to manage DNS.
• Active Directory Domain Services requires a DNS server to be installed on the network. If you are installing a domain controller, you can also install the DNS Server role using Active Directory Domain Services Installation Wizard by selecting the Active Directory Domain Services role.
Hide
< Previous
Next >
Install
Cancel
BPA results
Performance
BPA results
1:24 PM
12/11/2015
To direct input to this VM, click inside or press Ctrl+G.


Add Roles and Features Wizard
Network Policy and Access Services
DESTINATION SERVER
WIN-E7ME8A2GO2N
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Network Policy and Acces...
Confirmation
Results
Network Policy and Access Services allows you to define and enforce policies for network access, authentication and authorization using Network Policy Server (NPS).
Things to note:
• You can deploy NPS as a Remote Authentication Dial-In User Service (RADIUS) server and proxy. After installing NPS using this wizard, you can configure NPS from the NPAS home page using the NPS console.
< Previous
Next >
Install
Cancel

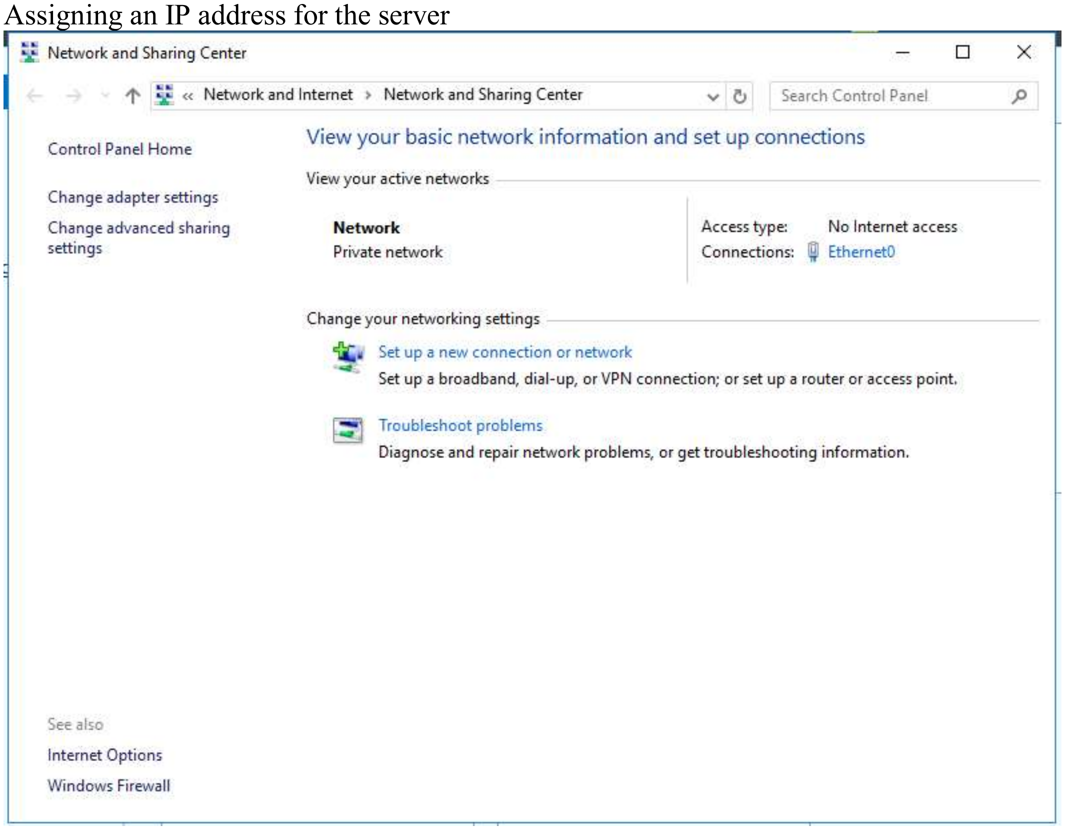

Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
WIN-E7ME8A2GO2N
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Network Policy and Acces...
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Active Directory Domain Services
DNS Server
Group Policy Management
Network Policy and Access Services
Remote Server Administration Tools
Role Administration Tools
DNS Server Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

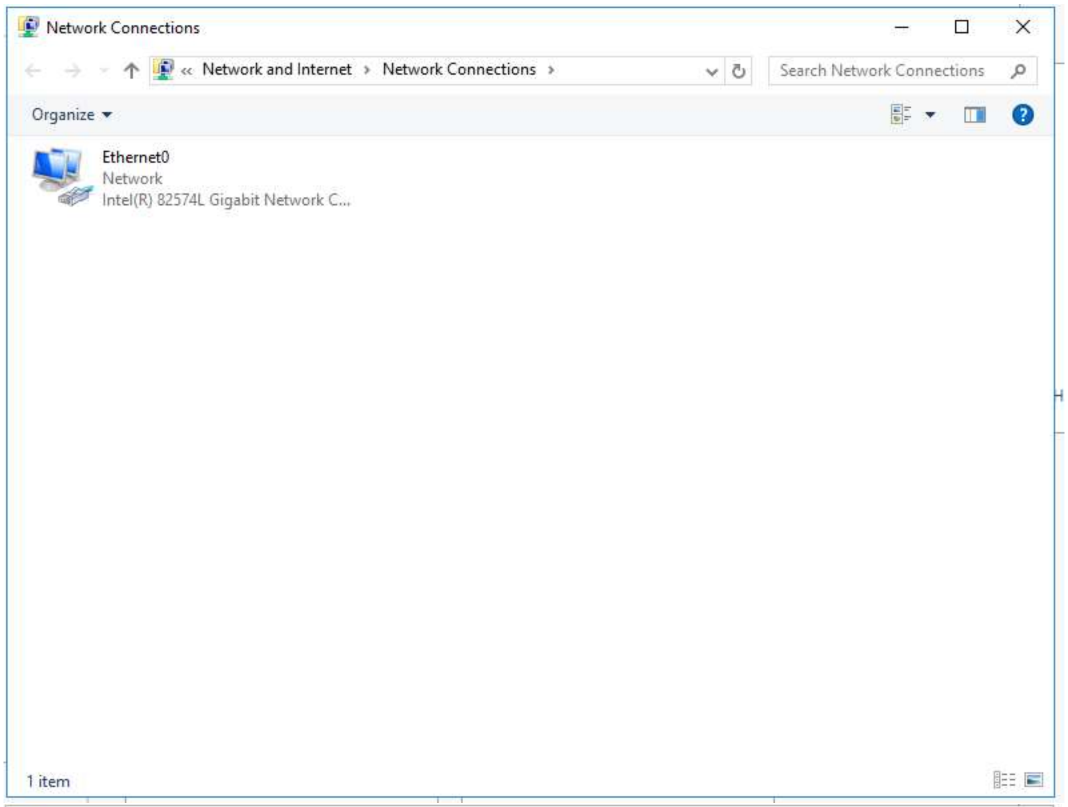

Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
WIN-E7ME8A2GO2N
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Network Policy and Acces...
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Active Directory Domain Services
DNS Server
Group Policy Management
Network Policy and Access Services
Remote Server Administration Tools
Role Administration Tools
DNS Server Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
WIN-E7ME8A2GO2N
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Network Policy and Acces...
Confirmation
Results
View installation progress
Starting installation
Active Directory Domain Services
DNS Server
Group Policy Management
Network Policy and Access Services
Remote Server Administration Tools
Role Administration Tools
DNS Server Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Install
Cancel

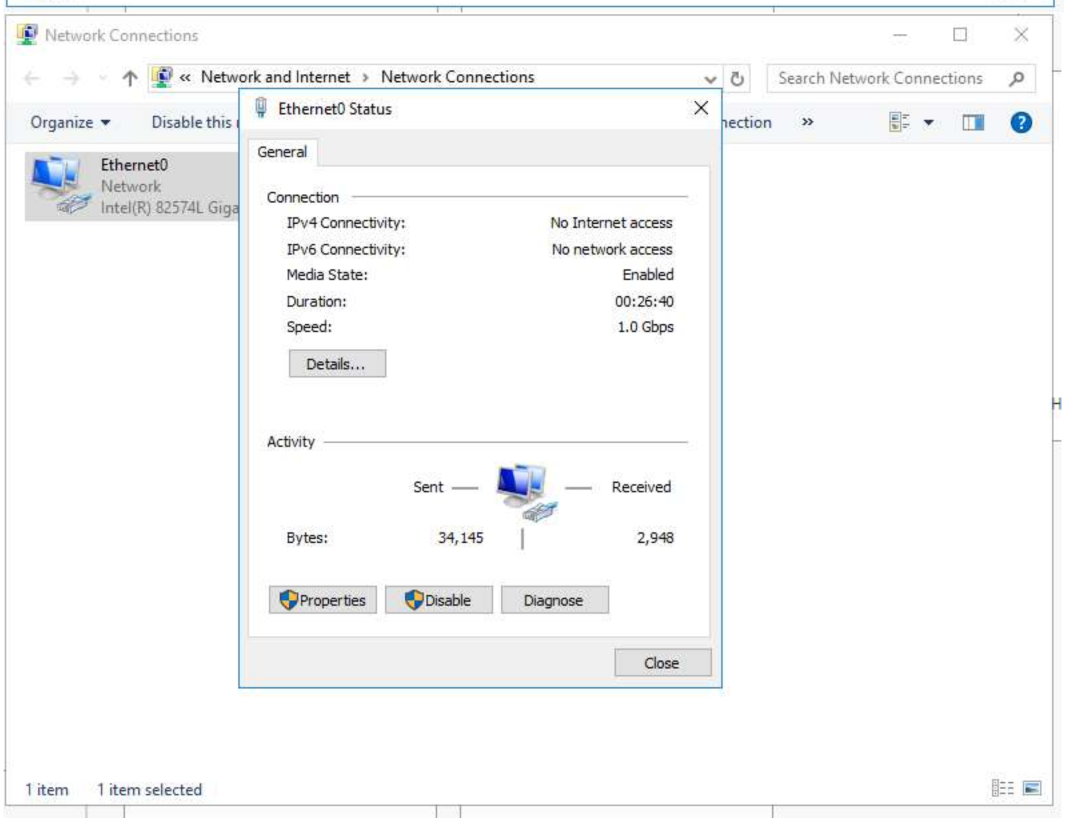


Assigning an IP address for the server

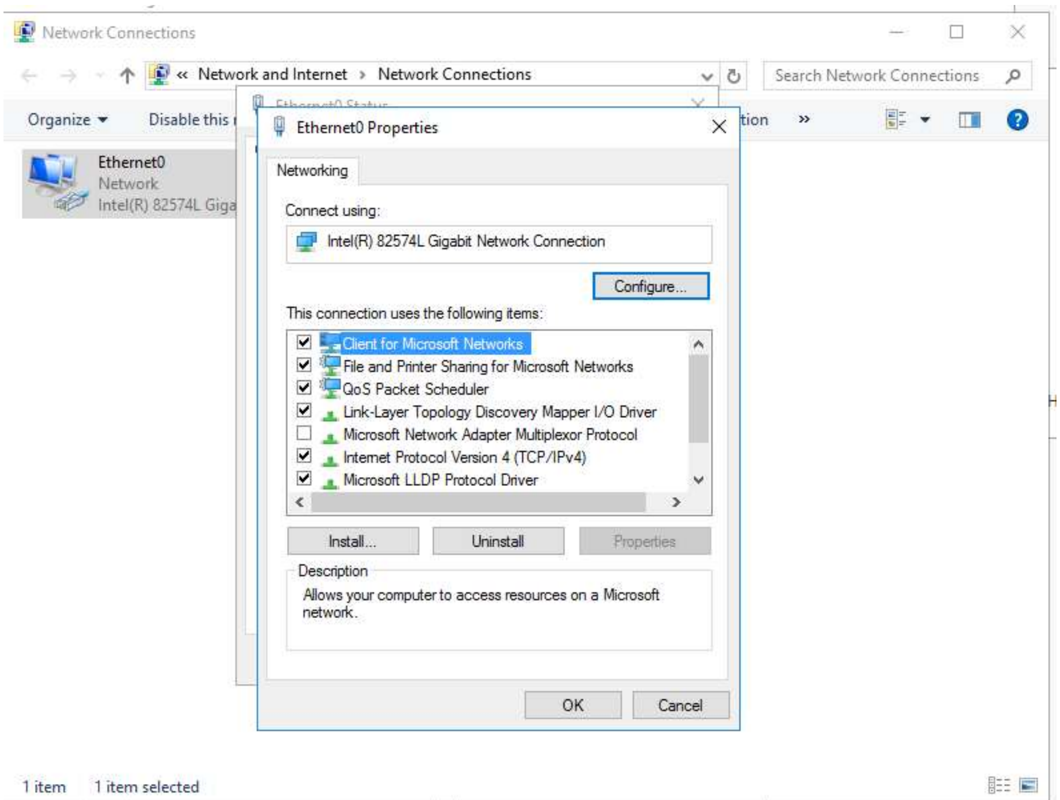


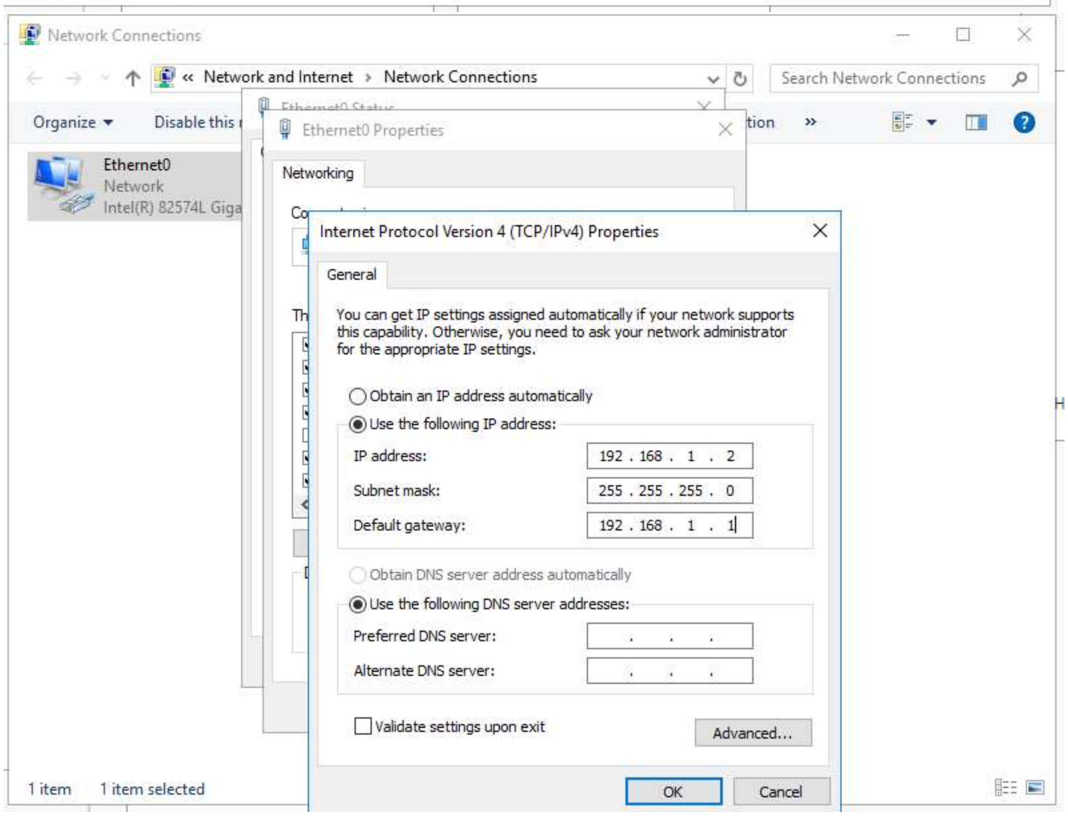


Network Connections
Network and Internet
Network Connections
Search Network Connections
Organize
Ethernet0
Network
Intel(R) 82574L Gigabit Network C...
1 item

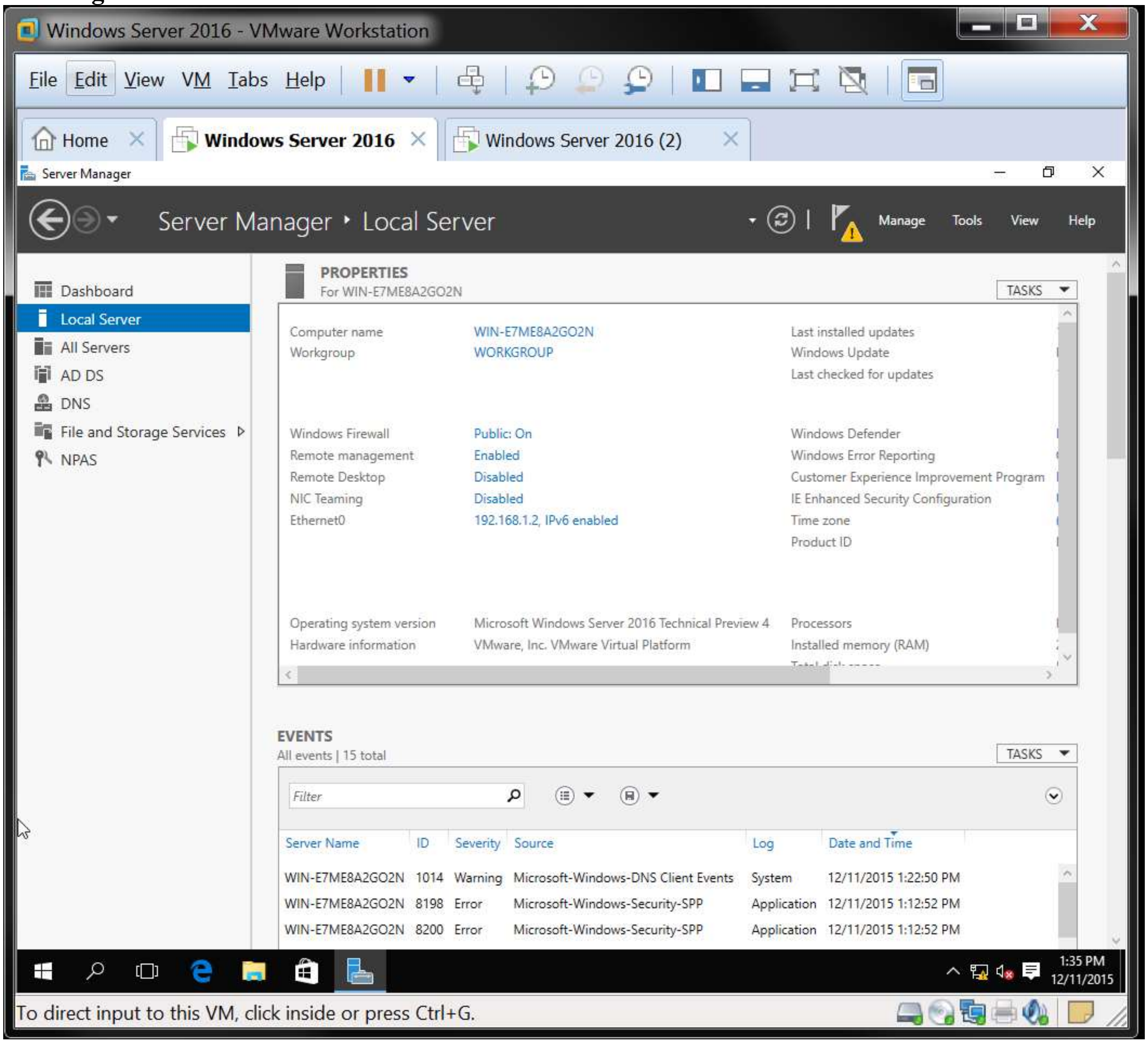


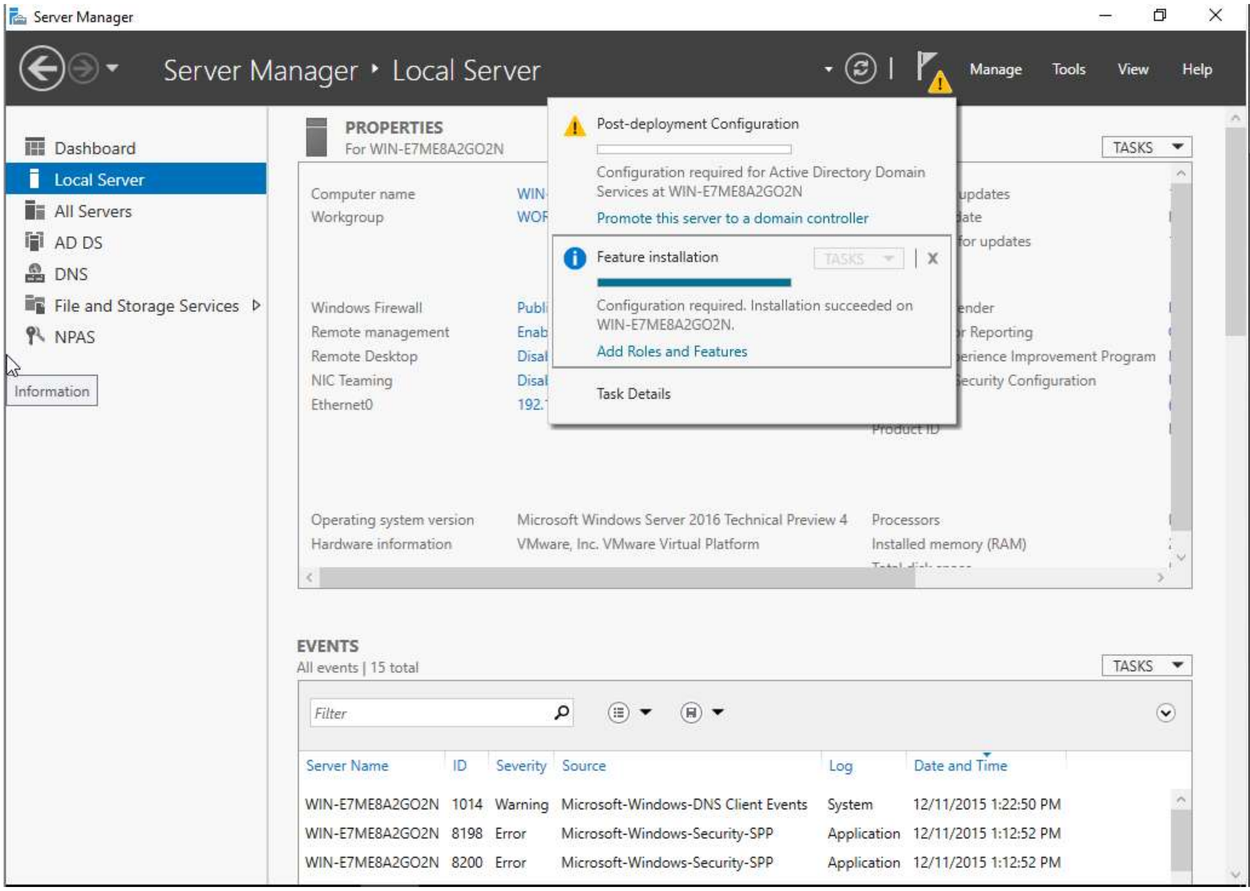
Network Connections
Network and Internet
Network Connections
Search Network Connections
Organize
Disable this
Ethernet0
Network
Ethernet0 Status
General
Connection
IPv4 Connectivity:
No Internet access
IPv6 Connectivity:
No network access
Media State:
Enabled
Duration:
00:26:40
Speed:
1.0 Gbps
Details...
Activity
Sent
Received
Bytes:
34,145
2,948
Properties
Disable
Diagnose
Close
1 item
1 item selected


Network Connections
Network and Internet > Network Connections
Search Network Connections
Organize
Ethernet0
Network
Intel(R) 82574L Giga
Ethernet0 Properties
Networking
Connect using:
Intel(R) 82574L Gigabit Network Connection
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Link-Layer Topology Discovery Mapper I/O Driver
Microsoft Network Adapter Multiplexor Protocol
Internet Protocol Version 4 (TCP/IPv4)
Microsoft LLDP Protocol Driver
Install...
Uninstall
Properties
Description
Allows your computer to access resources on a Microsoft network.
OK
Cancel
1 item
1 item selected

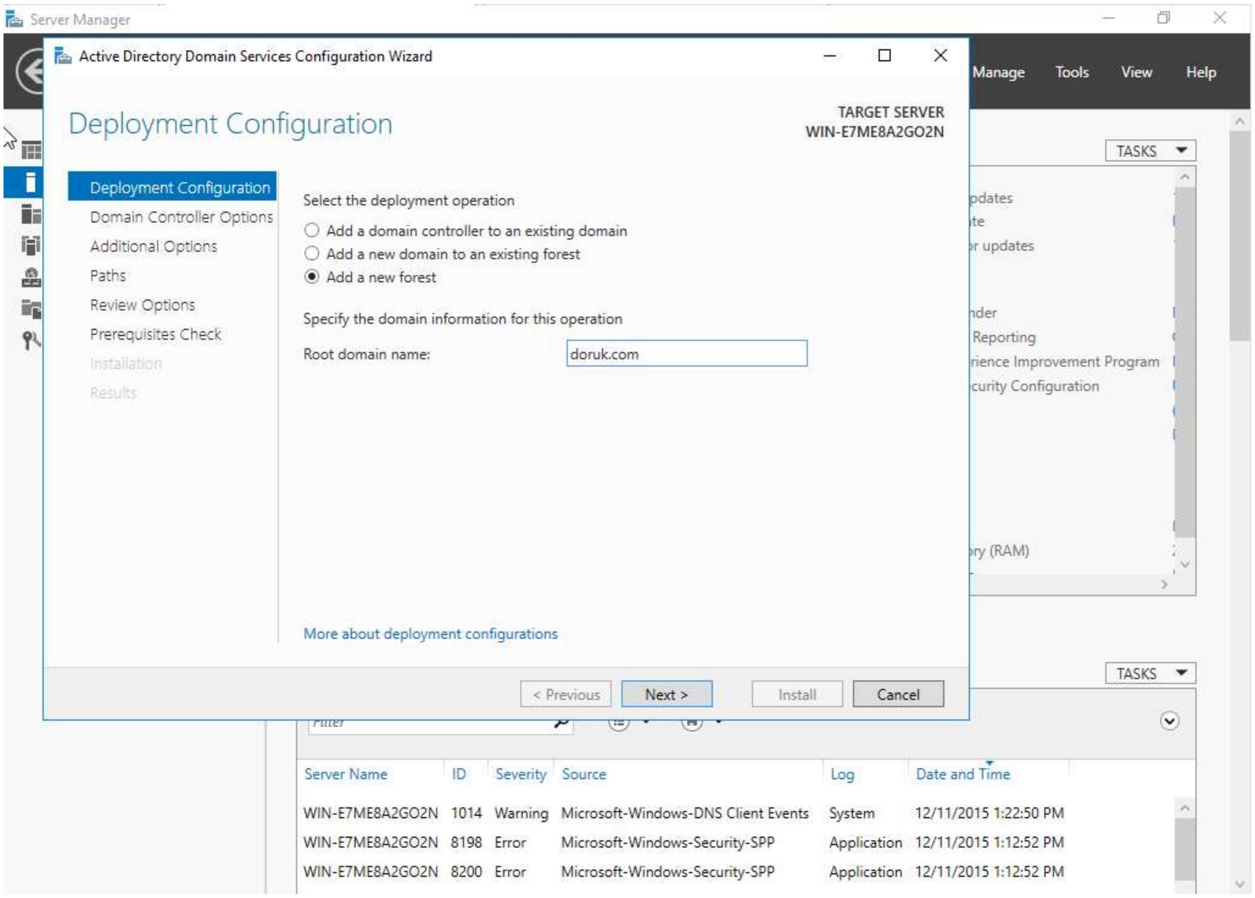

Network Connections
Network and Internet > Network Connections
Search Network Connections
Organize
Ethernet0
Network
Intel(R) 82574L Giga
Ethernet0 Properties
Networking
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
1 item
1 item selected

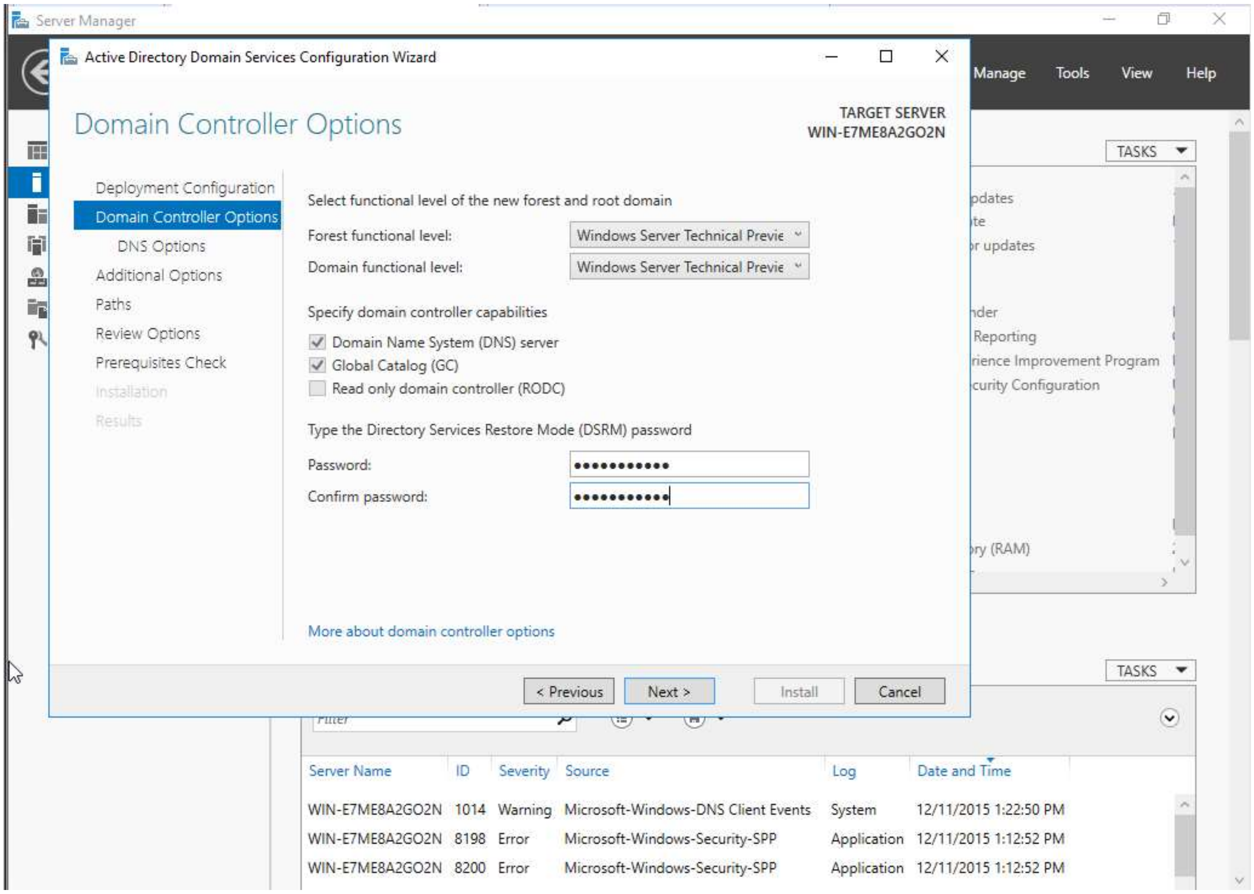
Creating the domain



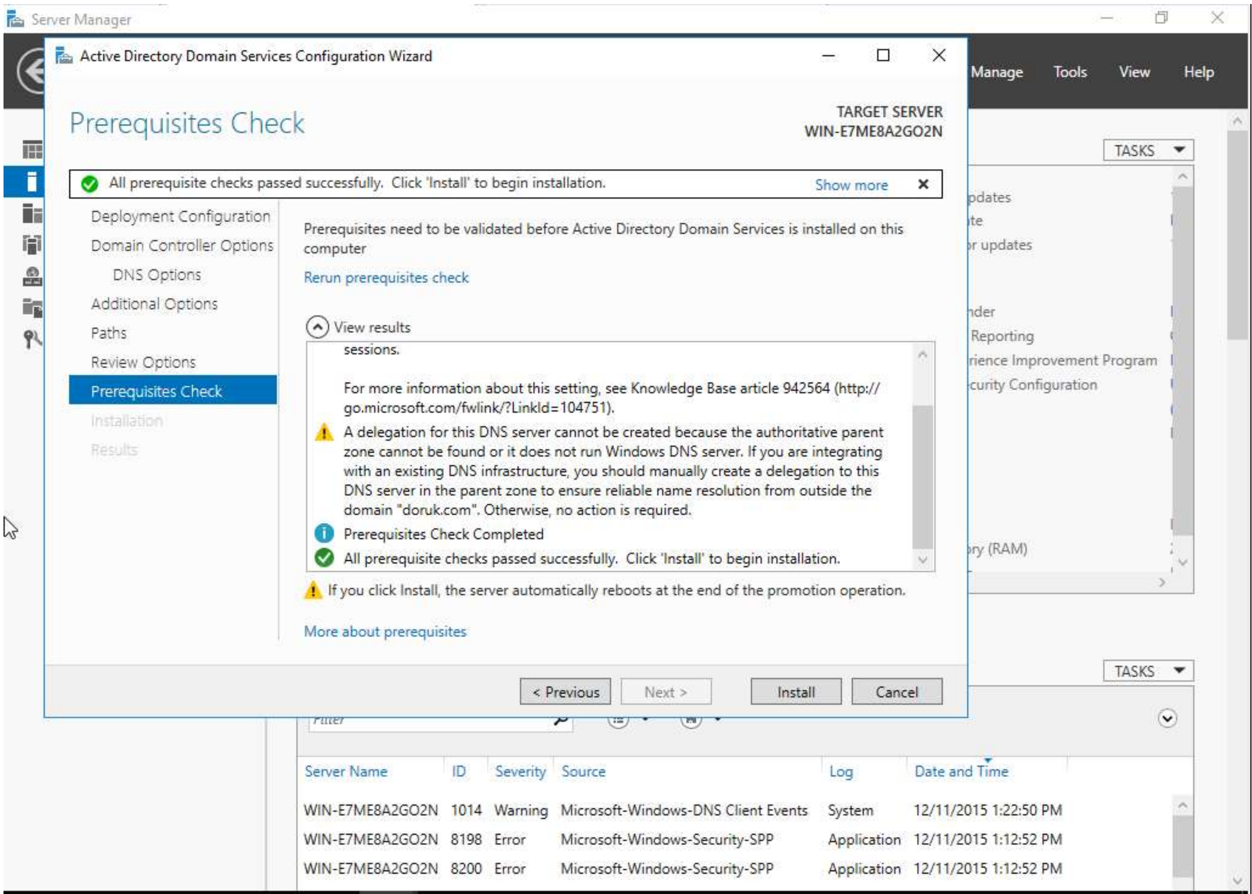


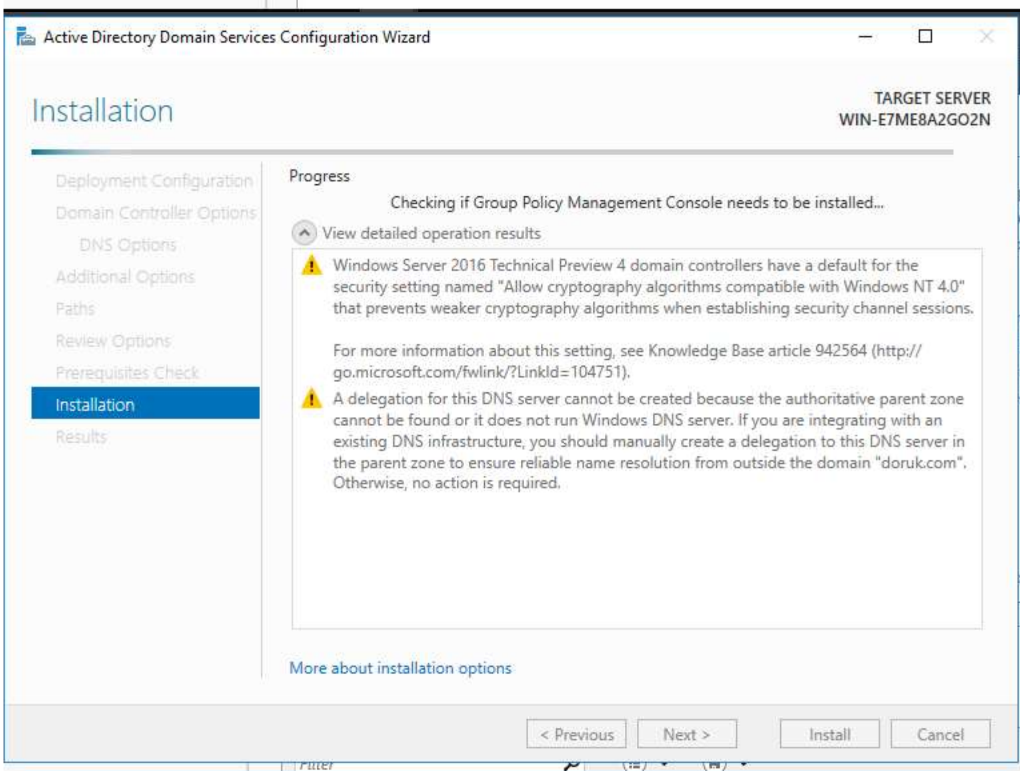
Server Manager
Server Manager ‣ Local Server
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
NPAS
Information
PROPERTIES
For WIN-E7ME8A2GO2N
TASKS
Post-deployment Configuration
Configuration required for Active Directory Domain Services at WIN-E7ME8A2GO2N
Promote this server to a domain controller
Feature installation
Configuration required. Installation succeeded on WIN-E7ME8A2GO2N.
Add Roles and Features
Task Details
Computer name
Workgroup
Windows Firewall
Remote management
Remote Desktop
NIC Teaming
Ethernet0
Operating system version
Microsoft Windows Server 2016 Technical Preview 4
Hardware information
VMware, Inc. VMware Virtual Platform
Processors
Installed memory (RAM)
EVENTS
All events | 15 total
Filter
Server Name
ID
Severity
Source
Log
Date and Time
WIN-E7ME8A2GO2N 1014 Warning Microsoft-Windows-DNS Client Events System 12/11/2015 1:22:50 PM
WIN-E7ME8A2GO2N 8198 Error Microsoft-Windows-Security-SPP Application 12/11/2015 1:12:52 PM
WIN-E7ME8A2GO2N 8200 Error Microsoft-Windows-Security-SPP Application 12/11/2015 1:12:52 PM

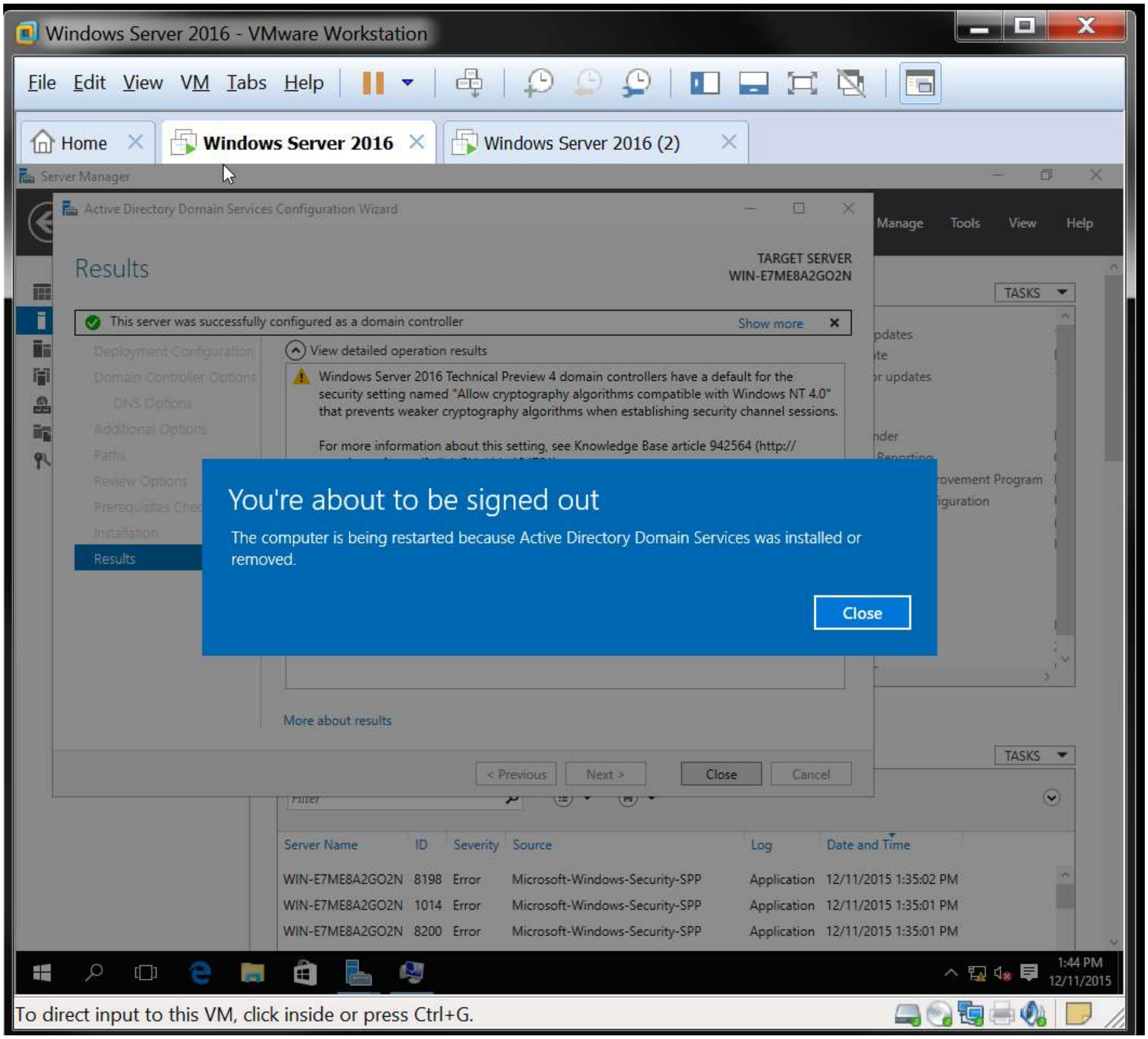

Server Manager
Active Directory Domain Services Configuration Wizard
Manage
Tools
View
Help
Deployment Configuration
TARGET SERVER
WIN-E7ME8A2GO2N
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
Specify the domain information for this operation
Root domain name:
doruk.com
More about deployment configurations
< Previous
Next >
Install
Cancel
TASKS
Server Name
ID
Severity
Source
Log
Date and Time
WIN-E7ME8A2GO2N 1014 Warning Microsoft-Windows-DNS Client Events System 12/11/2015 1:22:50 PM
WIN-E7ME8A2GO2N 8198 Error Microsoft-Windows-Security-SPP Application 12/11/2015 1:12:52 PM
WIN-E7ME8A2GO2N 8200 Error Microsoft-Windows-Security-SPP Application 12/11/2015 1:12:52 PM

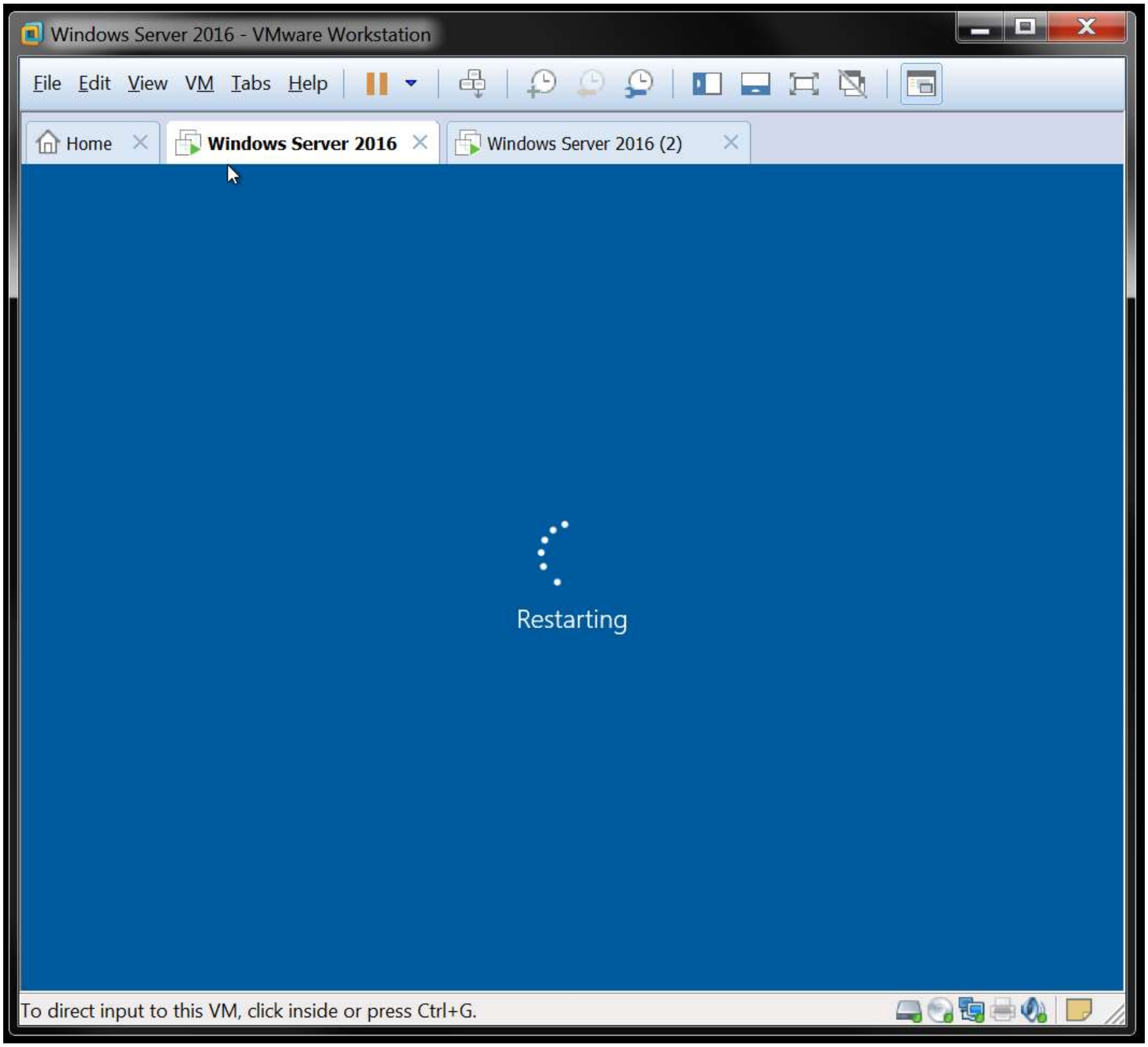


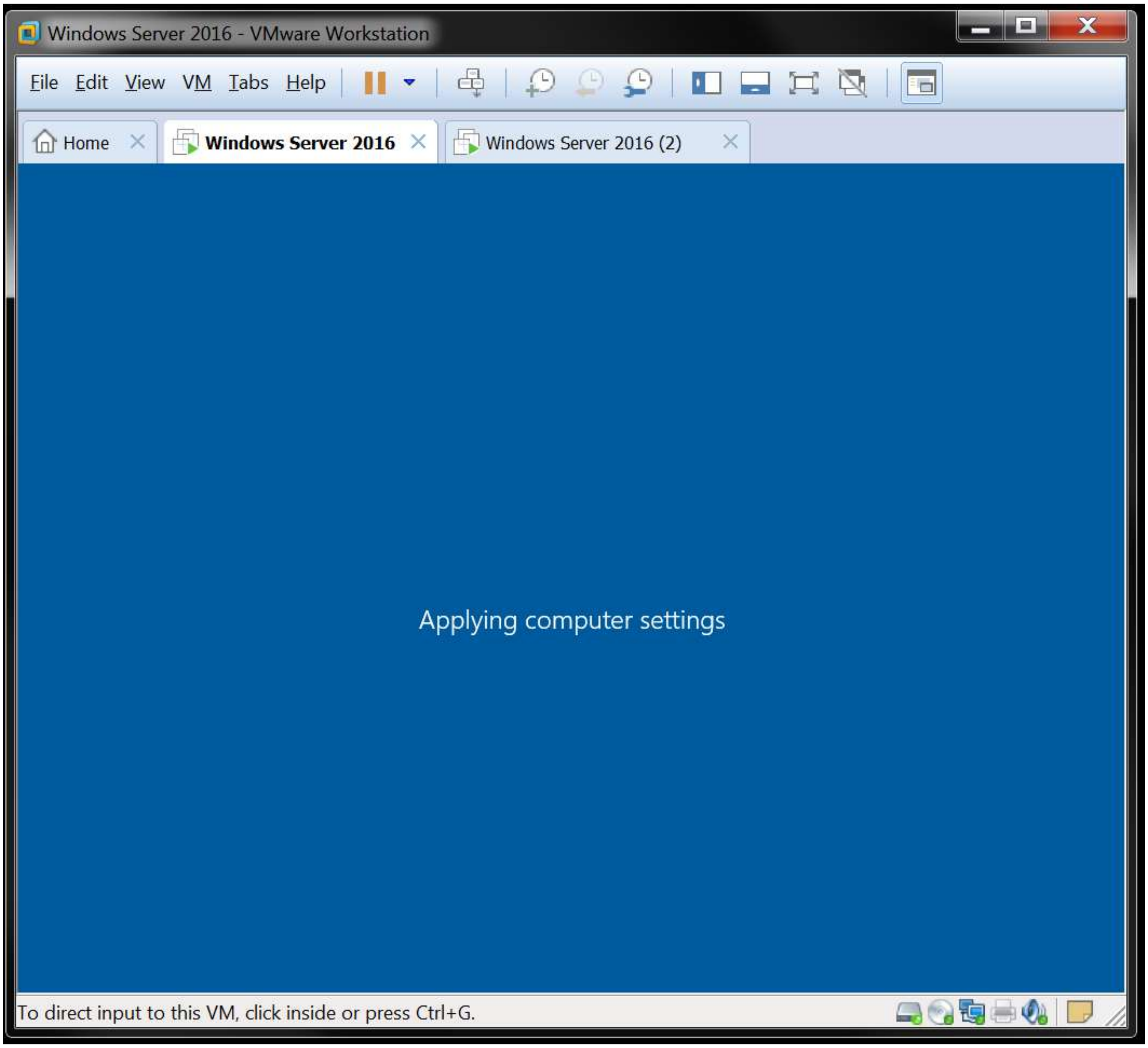
Server Manager
Active Directory Domain Services Configuration Wizard
Manage
Tools
View
Help
Domain Controller Options
TARGET SERVER
WIN-E7ME8A2GO2N
TASKS
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select functional level of the new forest and root domain
Forest functional level:
Windows Server Technical Previe
Domain functional level:
Windows Server Technical Previe
Specify domain controller capabilities
Domain Name System (DNS) server
Global Catalog (GC)
Read only domain controller (RODC)
Type the Directory Services Restore Mode (DSRM) password
Password:
Confirm password:
More about domain controller options
< Previous
Next >
Install
Cancel
TASKS
Server Name
ID
Severity
Source
Log
Date and Time
WIN-E7ME8A2GO2N 1014 Warning Microsoft-Windows-DNS Client Events System 12/11/2015 1:22:50 PM
WIN-E7ME8A2GO2N 8198 Error Microsoft-Windows-Security-SPP Application 12/11/2015 1:12:52 PM
WIN-E7ME8A2GO2N 8200 Error Microsoft-Windows-Security-SPP Application 12/11/2015 1:12:52 PM

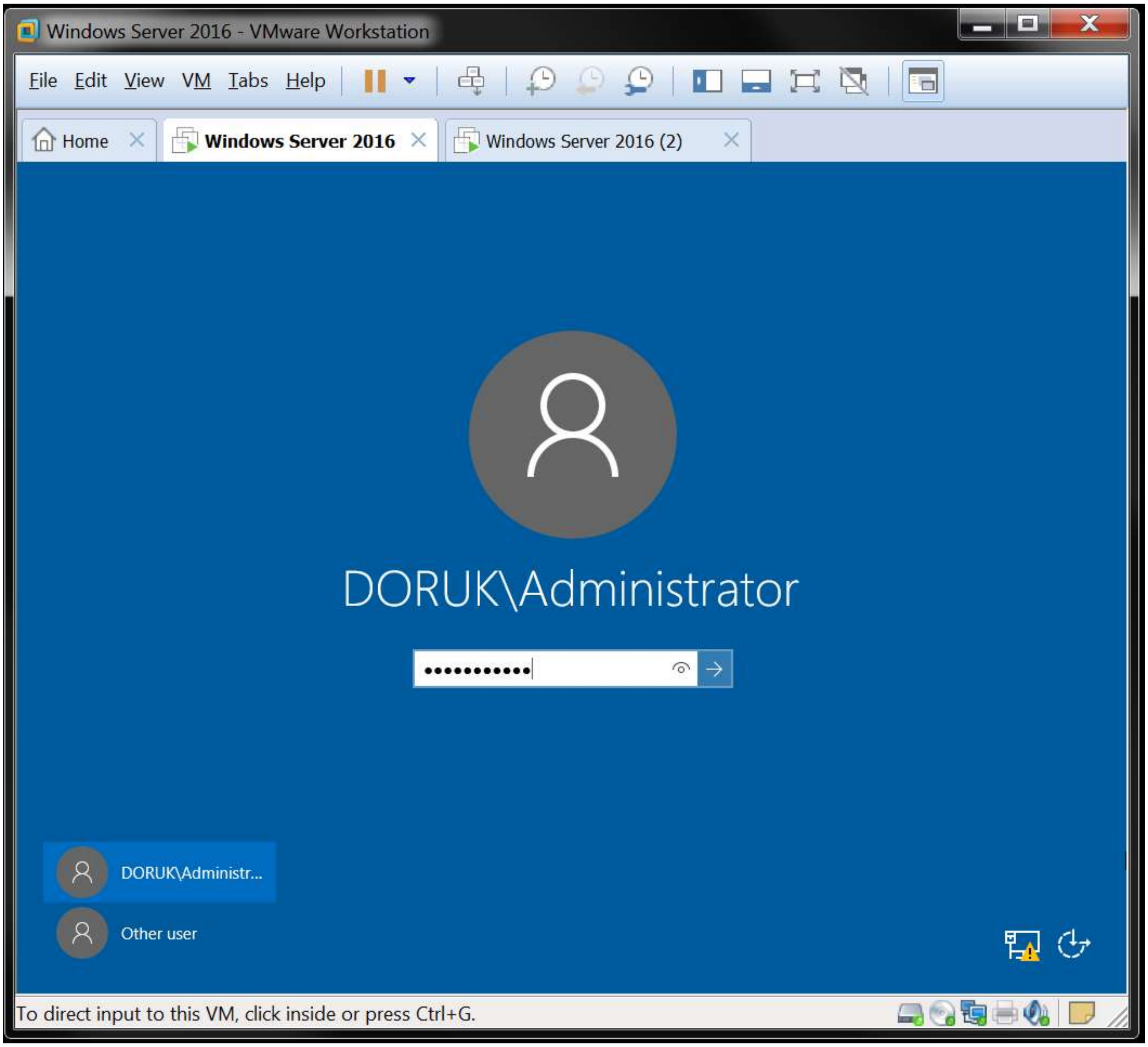

Server Manager
Active Directory Domain Services Configuration Wizard
Manage
Tools
View
Help
Prerequisites Check
TARGET SERVER
WIN-E7ME8A2GO2N
All prerequisite checks passed successfully. Click 'Install' to begin installation.
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Prerequisites need to be validated before Active Directory Domain Services is installed on this computer
Rerun prerequisites check
View results
sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "doruk.com". Otherwise, no action is required.
Prerequisites Check Completed
All prerequisite checks passed successfully. Click 'Install' to begin installation.
If you click Install, the server automatically reboots at the end of the promotion operation.
More about prerequisites
< Previous
Next >
Install
Cancel
TASKS
Reporting
Security Configuration
Server Name | ID | Severity | Source | Log | Date and Time
WIN-E7ME8A2GO2N 1014 Warning Microsoft-Windows-DNS Client Events System 12/11/2015 1:22:50 PM
WIN-E7ME8A2GO2N 8198 Error Microsoft-Windows-Security-SPP Application 12/11/2015 1:12:52 PM
WIN-E7ME8A2GO2N 8200 Error Microsoft-Windows-Security-SPP Application 12/11/2015 1:12:52 PM

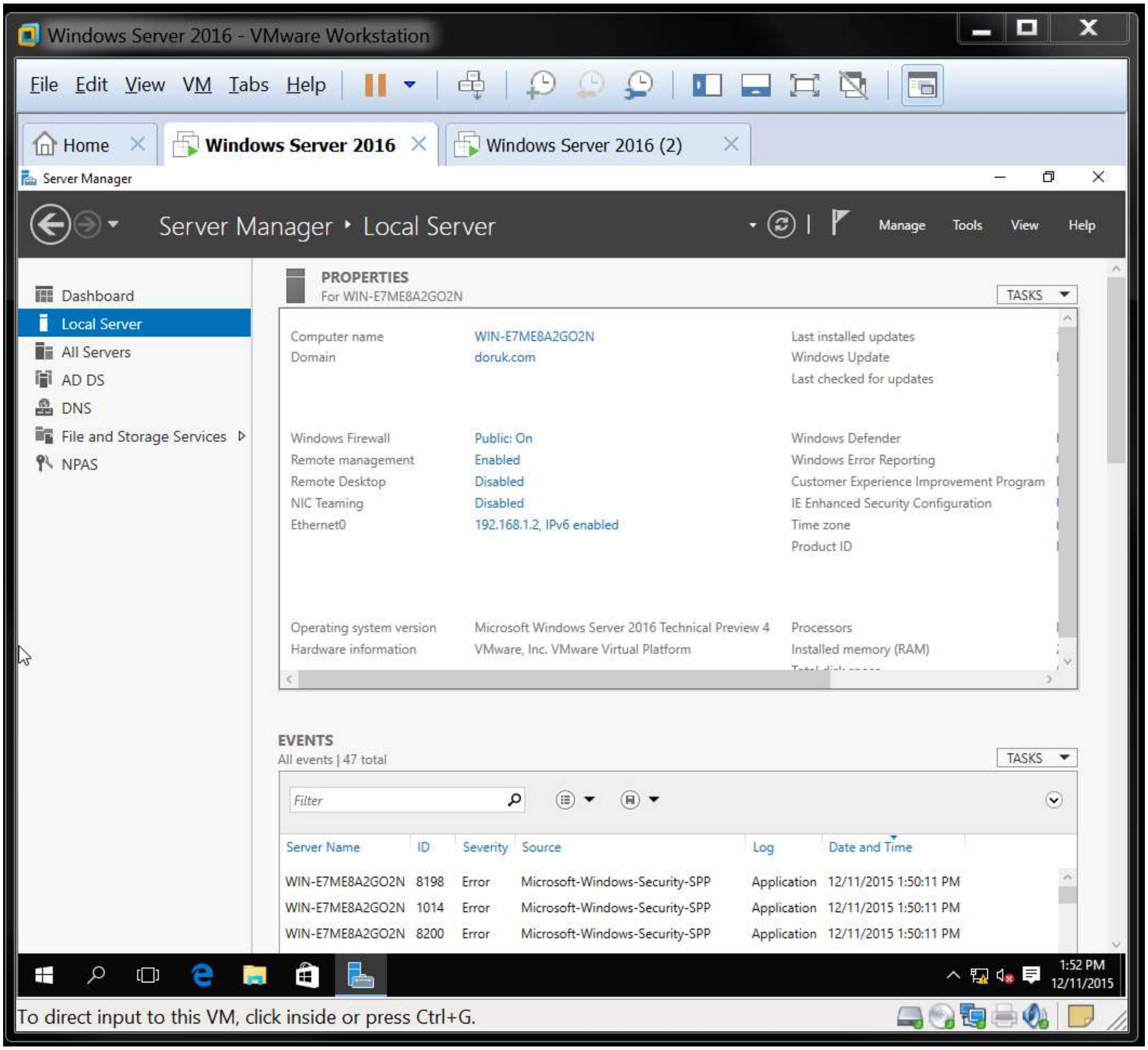

Active Directory Domain Services Configuration Wizard
Installation
TARGET SERVER
WIN-E7ME8A2GO2N
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Progress
Checking if Group Policy Management Console needs to be installed...
View detailed operation results
Windows Server 2016 Technical Preview 4 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "doruk.com". Otherwise, no action is required.
More about installation options
< Previous
Next >
Install
Cancel


Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Server 2016 (2)
Server Manager
Active Directory Domain Services Configuration Wizard
Manage Tools View Help
Results
TARGET SERVER
WIN-E7ME8A2GO2N
This server was successfully configured as a domain controller
Show more
View detailed operation results
Windows Server 2016 Technical Preview 4 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://
Results
You're about to be signed out
The computer is being restarted because Active Directory Domain Services was installed or removed.
Close
More about results
< Previous
Next >
Close
Cancel
TASKS
Server Name
ID
Severity
Source
Log
Date and Time
WIN-E7ME8A2GO2N 8198 Error Microsoft-Windows-Security-SPP Application 12/11/2015 1:35:02 PM
WIN-E7ME8A2GO2N 1014 Error Microsoft-Windows-Security-SPP Application 12/11/2015 1:35:01 PM
WIN-E7ME8A2GO2N 8200 Error Microsoft-Windows-Security-SPP Application 12/11/2015 1:35:01 PM
1:44 PM
12/11/2015
To direct input to this VM, click inside or press Ctrl+G.

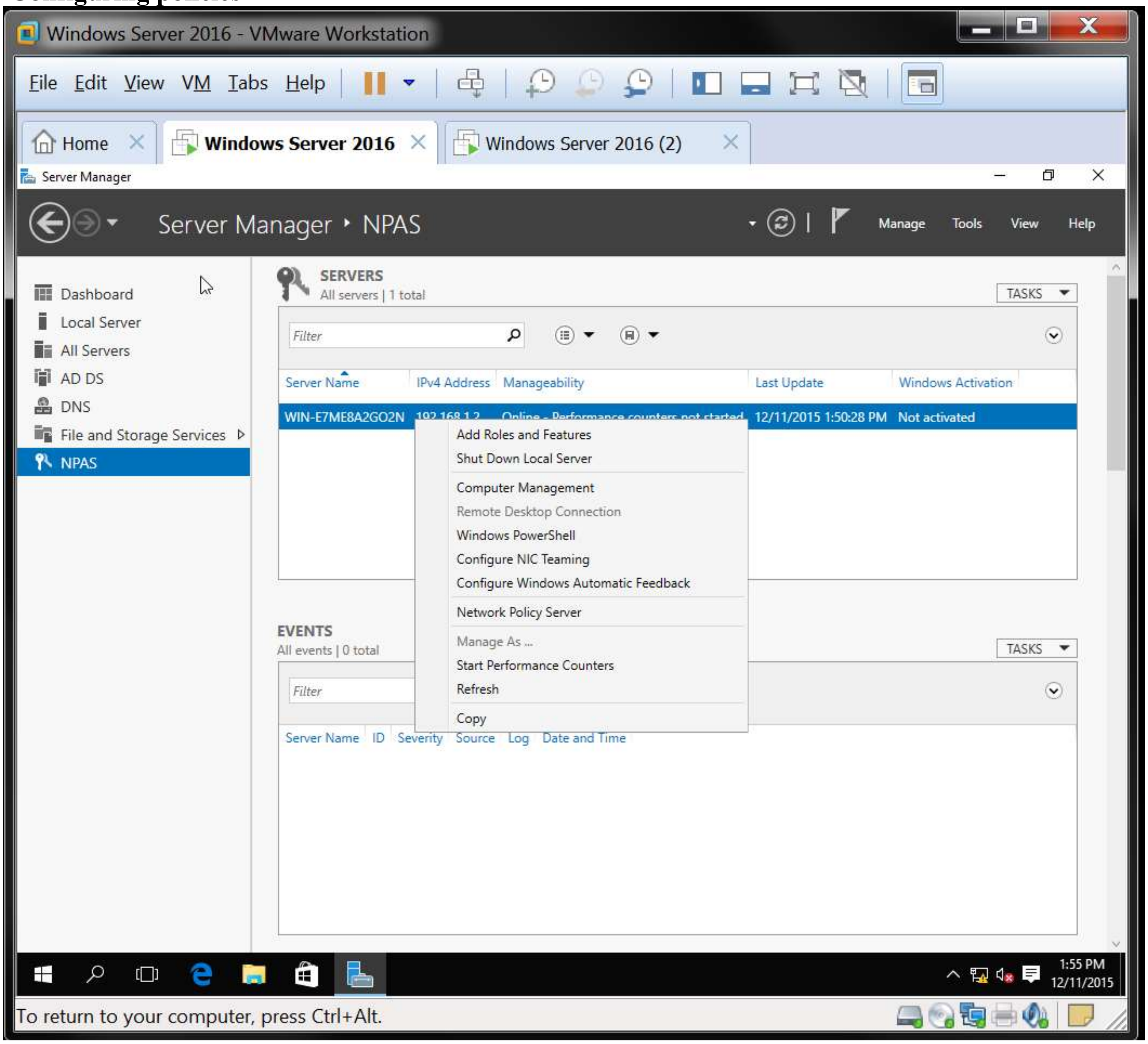

Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Server 2016 (2)
Restarting
To direct input to this VM, click inside or press Ctrl+G.

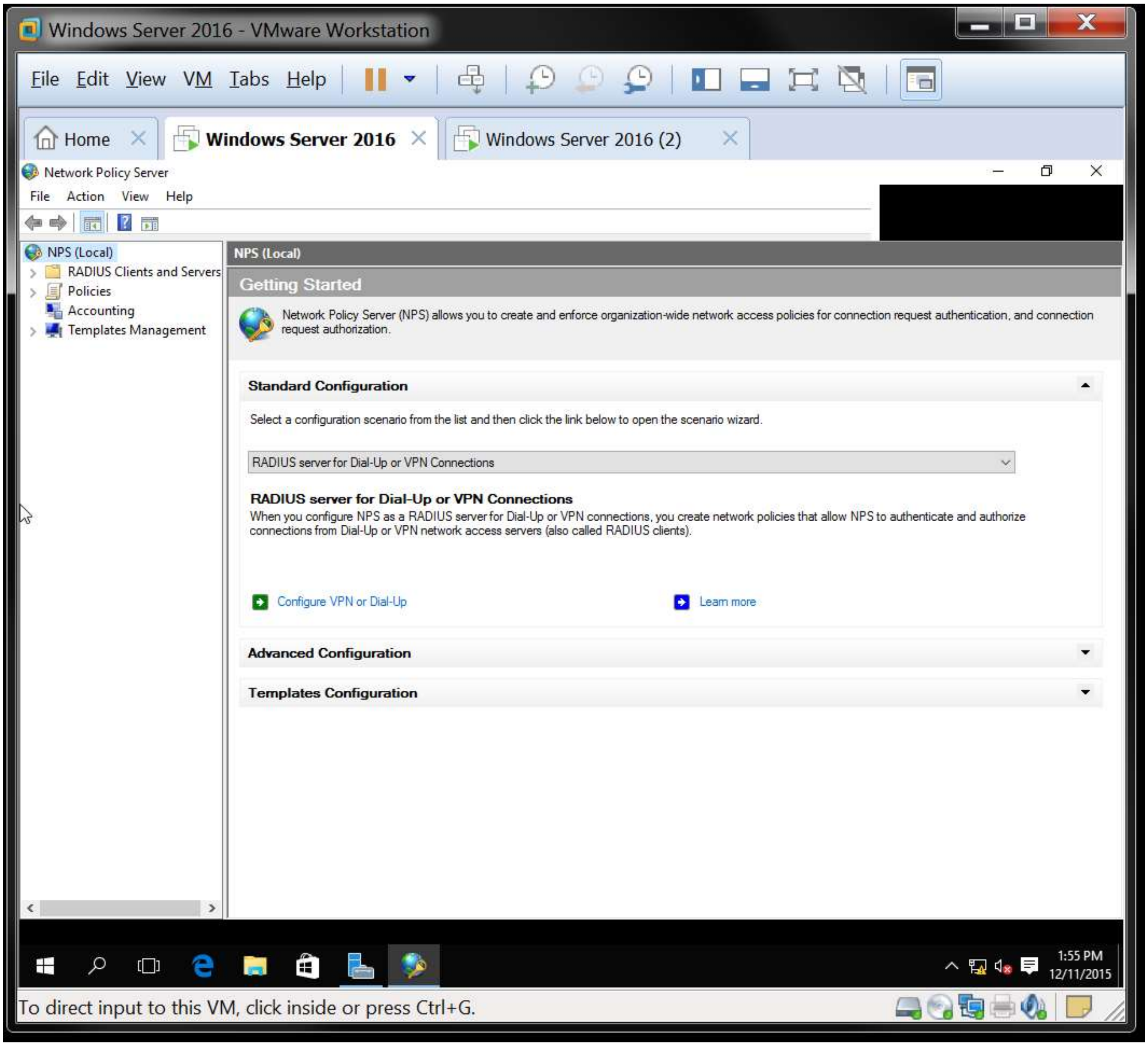

Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Server 2016 (2)
Applying computer settings
To direct input to this VM, click inside or press Ctrl+G.

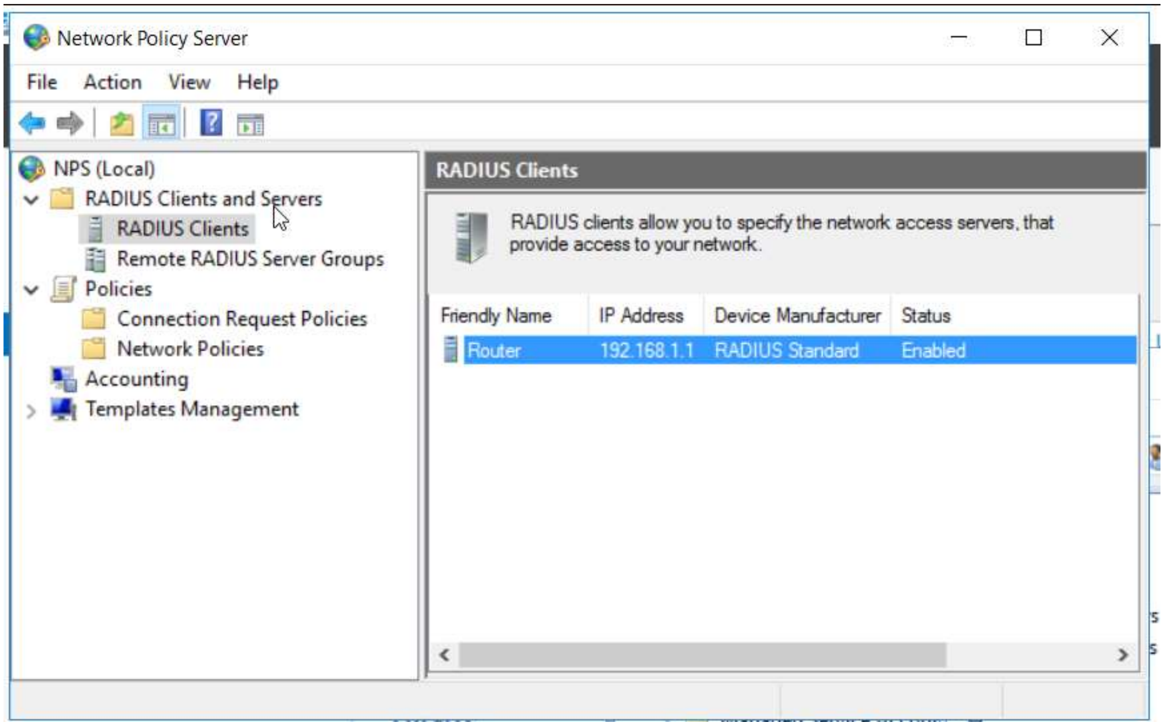

Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Server 2016 (2)
DORUK\Administrator
DORUK\Administr...
Other user
To direct input to this VM, click inside or press Ctrl+G.

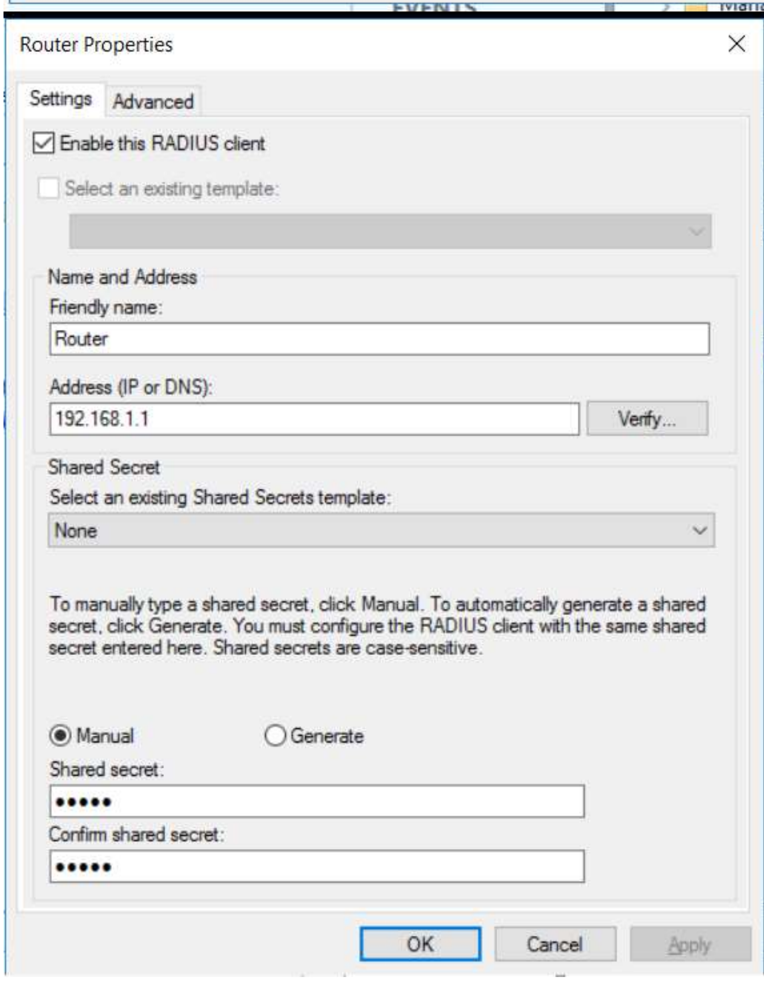

Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Server 2016 (2)
Server Manager
Server Manager • Local Server
Manage Tools View Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
NPAS
PROPERTIES
For WIN-E7ME8A2GO2N
TASKS
Computer name WIN-E7ME8A2GO2N
Domain doruk.com
Last installed updates
Windows Update
Last checked for updates
Windows Firewall Public: On
Remote management Enabled
Remote Desktop Disabled
NIC Teaming Disabled
Ethernet0 192.168.1.2, IPv6 enabled
Windows Defender
Windows Error Reporting
Customer Experience Improvement Program
IE Enhanced Security Configuration
Time zone
Product ID
Operating system version Microsoft Windows Server 2016 Technical Preview 4
Hardware information VMware, Inc. VMware Virtual Platform
Processors
Installed memory (RAM)
EVENTS
All events | 47 total
TASKS
Filter
Server Name ID Severity Source Log Date and Time
WIN-E7ME8A2GO2N 8198 Error Microsoft-Windows-Security-SPP Application 12/11/2015 1:50:11 PM
WIN-E7ME8A2GO2N 1014 Error Microsoft-Windows-Security-SPP Application 12/11/2015 1:50:11 PM
WIN-E7ME8A2GO2N 8200 Error Microsoft-Windows-Security-SPP Application 12/11/2015 1:50:11 PM
1:52 PM
12/11/2015
To direct input to this VM, click inside or press Ctrl+G.

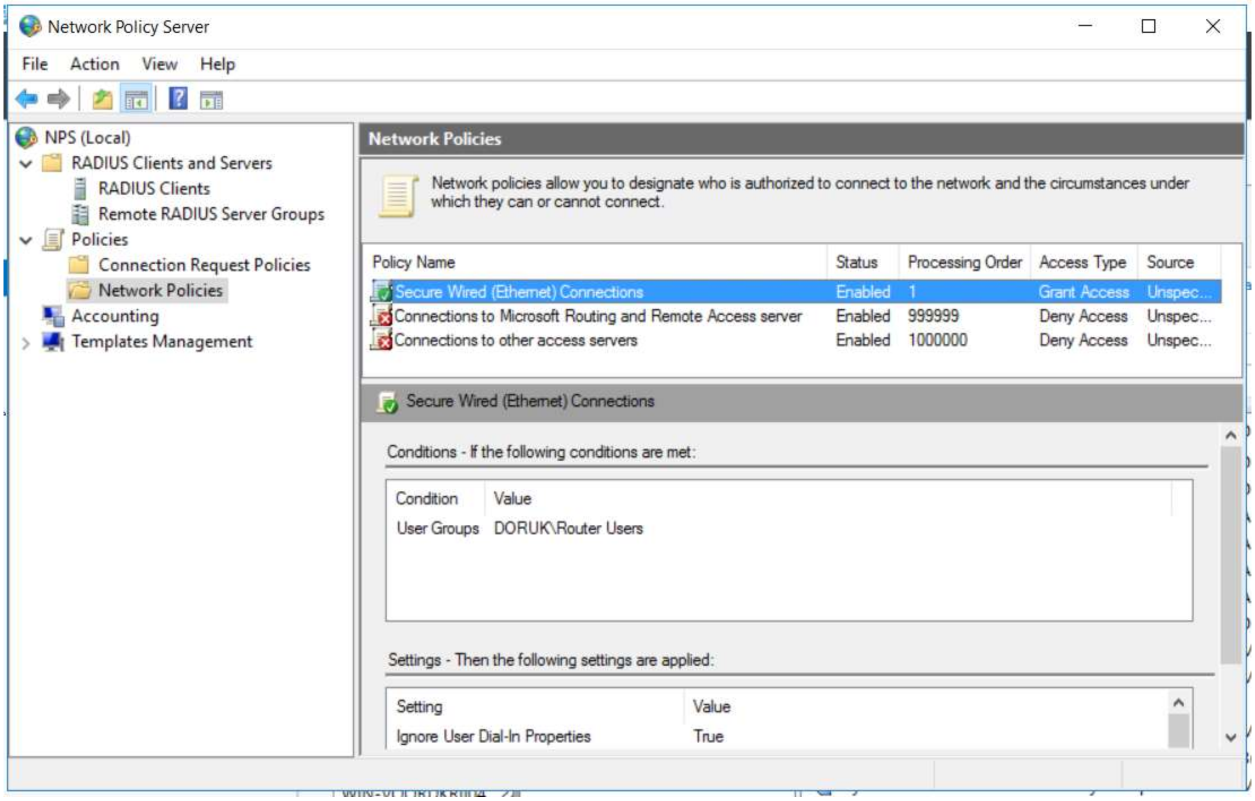
Configuring policies

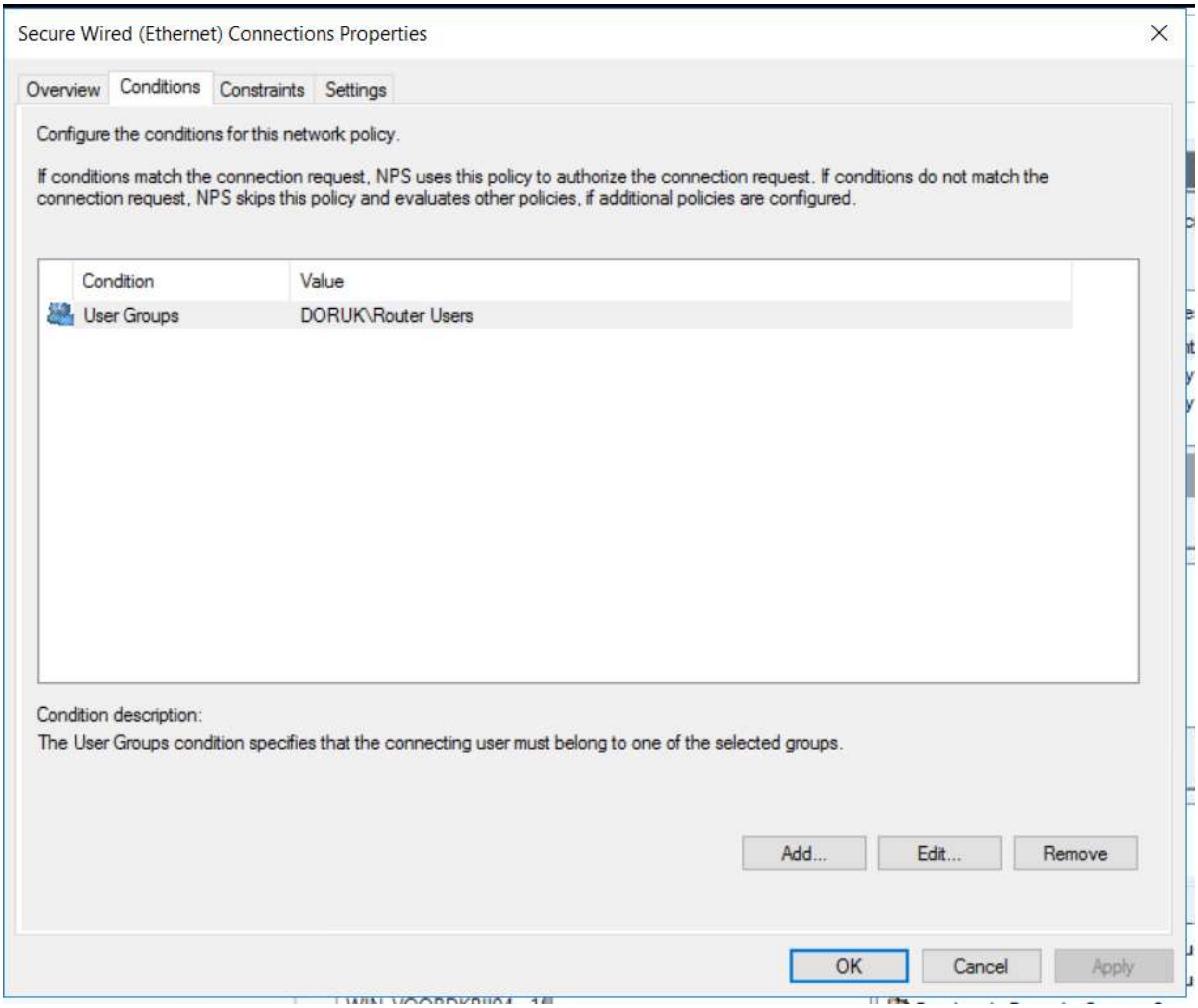


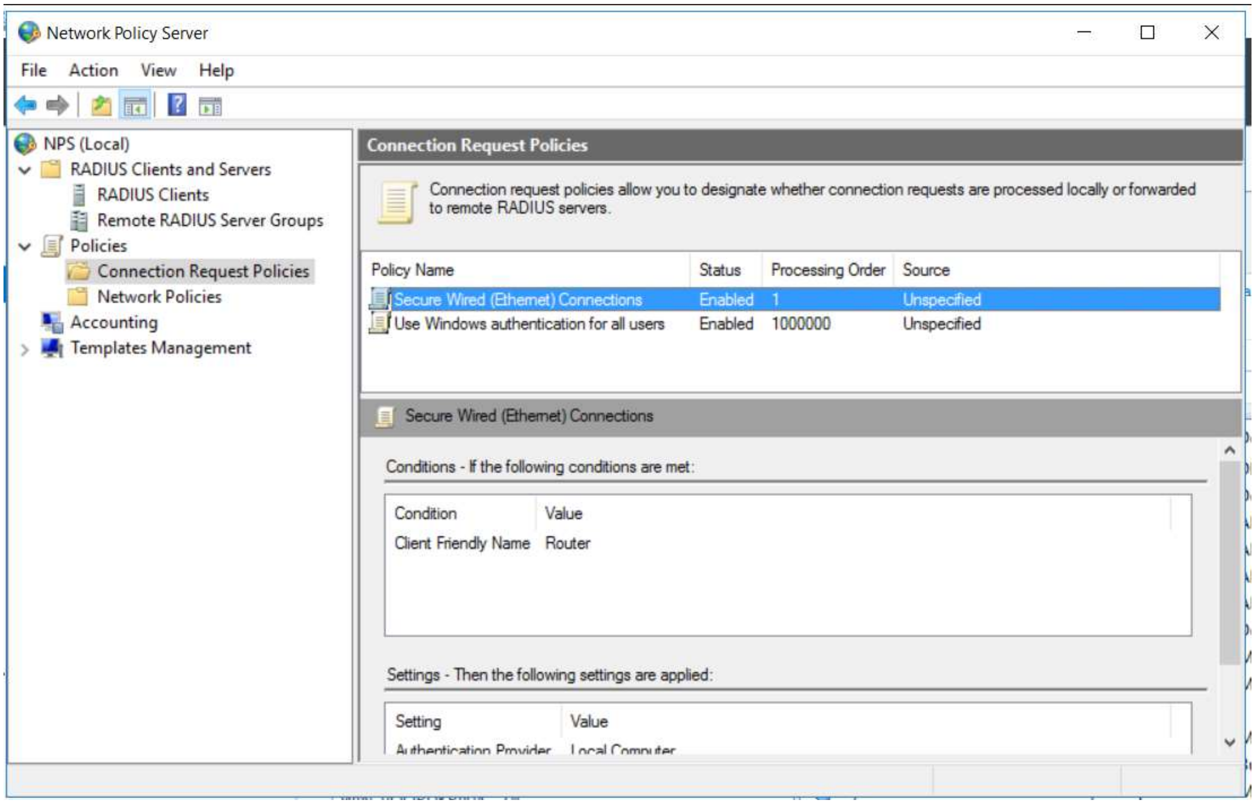

Windows Server 2016 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows Server 2016
Windows Server 2016 (2)
Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
Policies
Accounting
Templates Management
NPS (Local)
Getting Started
Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for connection request authentication, and connection request authorization.
Standard Configuration
Select a configuration scenario from the list and then click the link below to open the scenario wizard.
RADIUS server for Dial-Up or VPN Connections
RADIUS server for Dial-Up or VPN Connections
When you configure NPS as a RADIUS server for Dial-Up or VPN connections, you create network policies that allow NPS to authenticate and authorize connections from Dial-Up or VPN network access servers (also called RADIUS clients).
Configure VPN or Dial-Up
Learn more
Advanced Configuration
Templates Configuration
1:55 PM
12/11/2015
To direct input to this VM, click inside or press Ctrl+G.

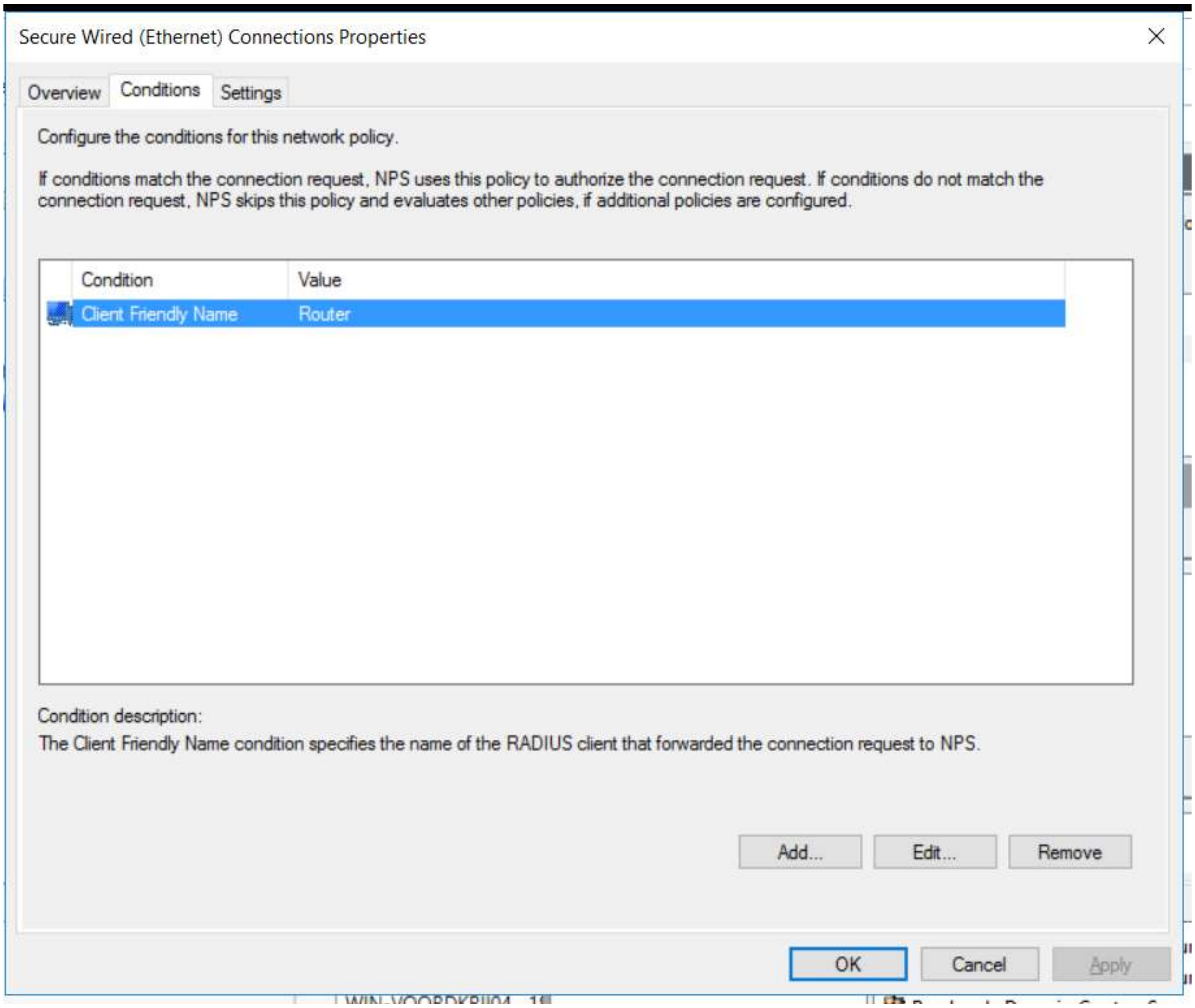

Network Policy Server
File
Action
View
Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Accounting
Templates Management
RADIUS Clients
RADIUS clients allow you to specify the network access servers, that provide access to your network.
Friendly Name
IP Address
Device Manufacturer
Status
Router
192.168.1.1
RADIUS Standard
Enabled


Router Properties
Settings
Advanced
Enable this RADIUS client
Select an existing template:
Name and Address
Friendly name:
Router
Address (IP or DNS):
192.168.1.1
Verify...
Shared Secret
Select an existing Shared Secrets template:
None
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.
Manual
Generate
Shared secret:
•••••
Confirm shared secret:
•••••
OK
Cancel
Apply

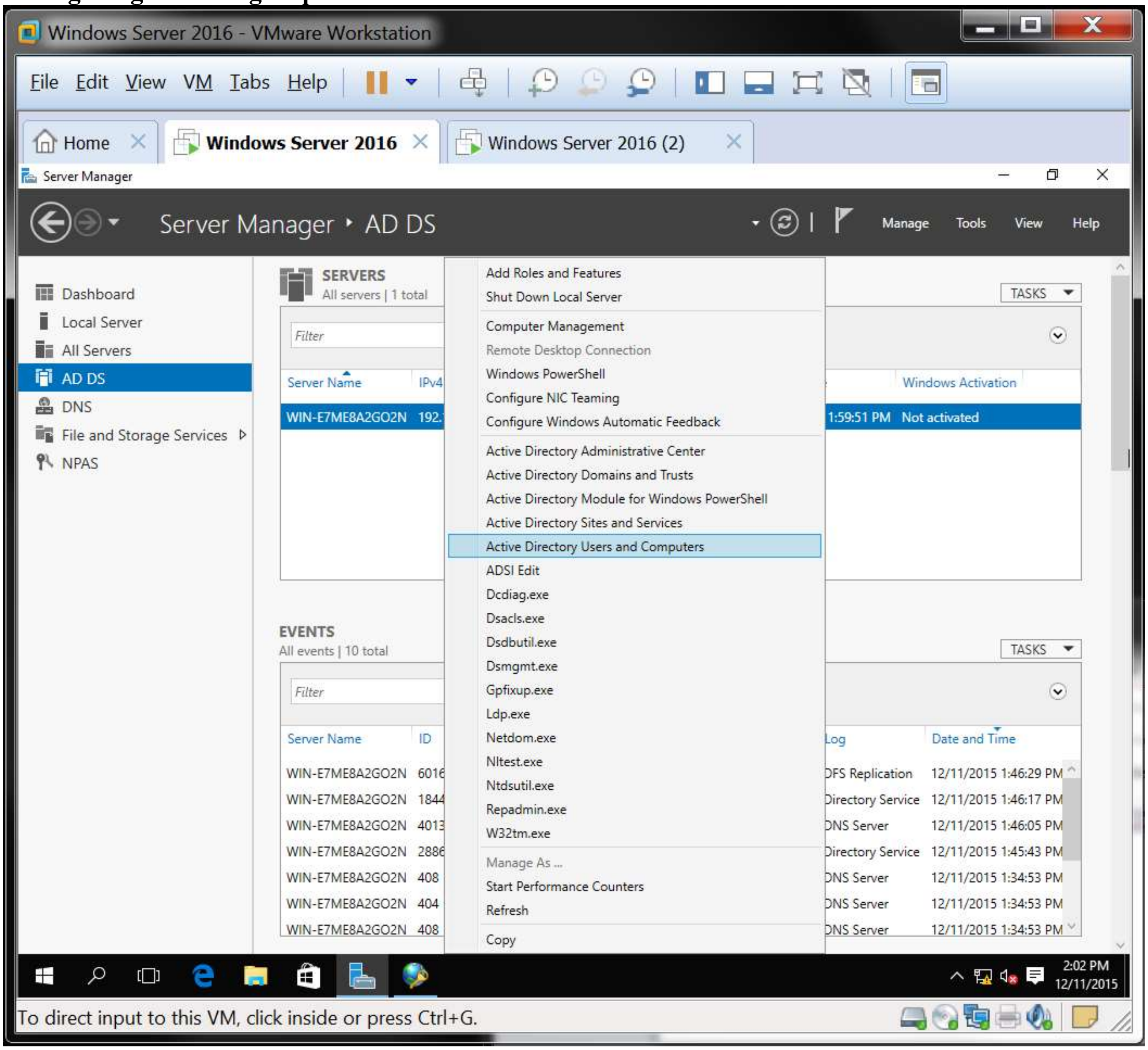

Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Accounting
Templates Management
Network Policies
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.
Policy Name | Status | Processing Order | Access Type | Source
Secure Wired (Ethernet) Connections | Enabled | 1 | Grant Access | Unspec...
Connections to Microsoft Routing and Remote Access server | Enabled | 999999 | Deny Access | Unspec...
Connections to other access servers | Enabled | 1000000 | Deny Access | Unspec...
Secure Wired (Ethernet) Connections
Conditions - If the following conditions are met:
Condition | Value
User Groups | DORUK\Router Users
Settings - Then the following settings are applied:
Setting | Value
Ignore User Dial-In Properties | True

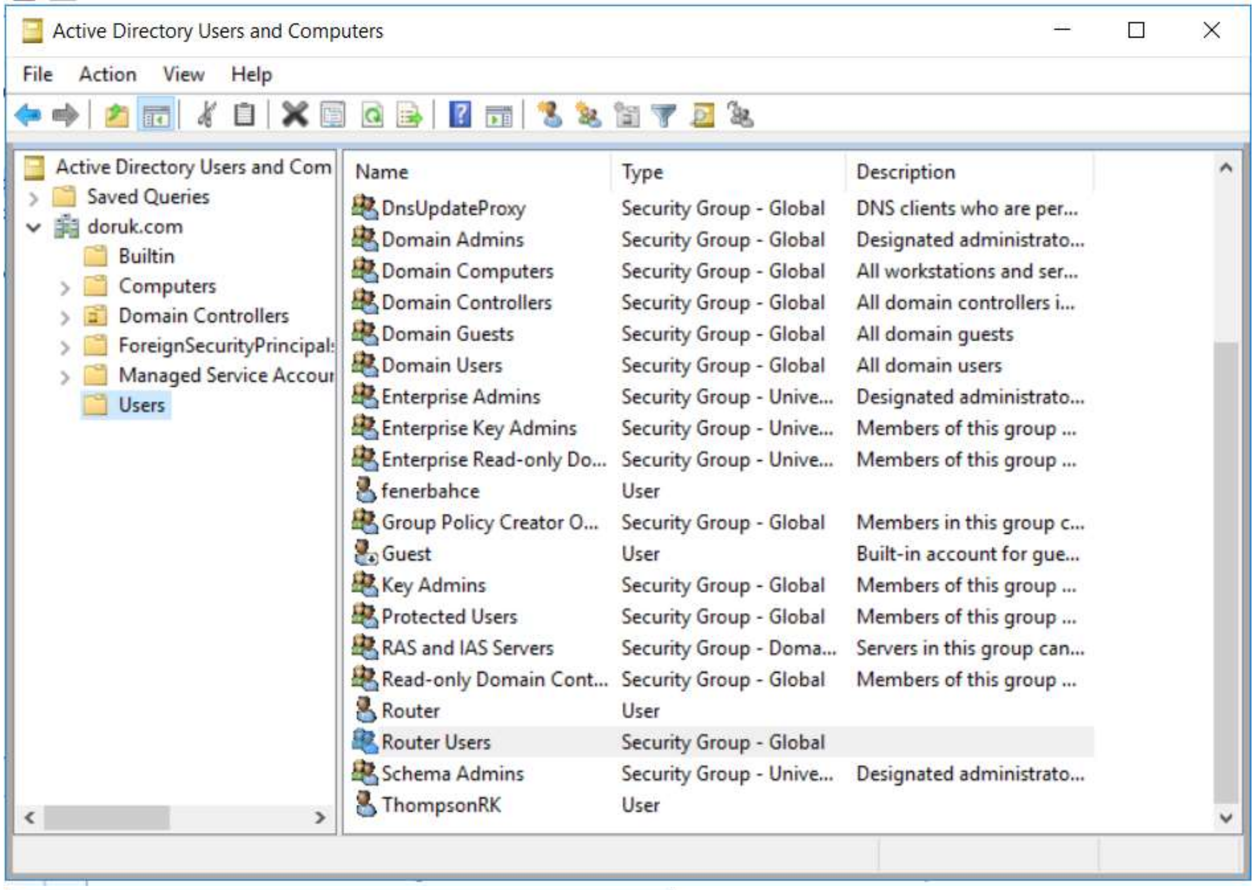

Secure Wired (Ethernet) Connections Properties
Overview
Conditions
Constraints
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.
Condition
Value
User Groups
DORUK\Router Users
Condition description:
The User Groups condition specifies that the connecting user must belong to one of the selected groups.
Add...
Edit...
Remove
OK
Cancel
Apply

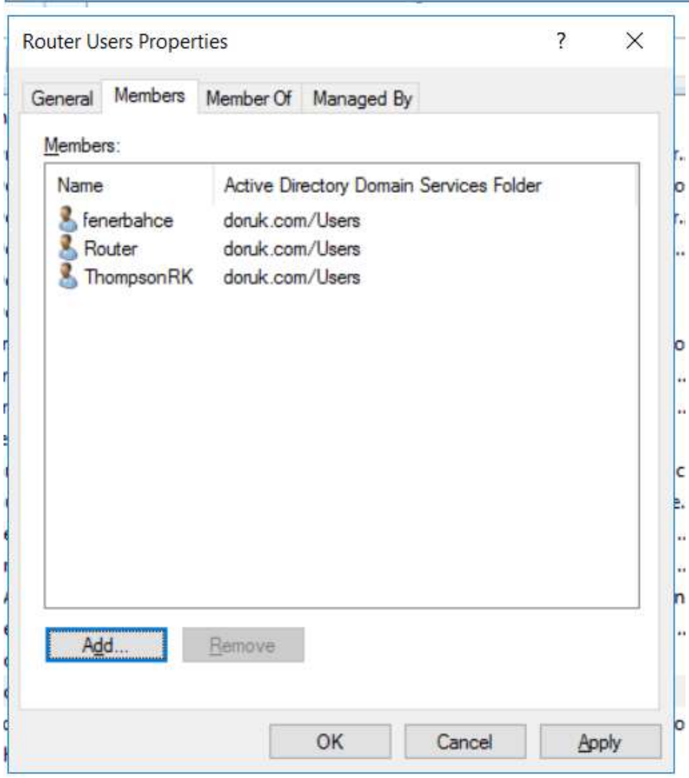

Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Accounting
Templates Management
Connection Request Policies
Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers.
Policy Name
Status
Processing Order
Source
Secure Wired (Ethernet) Connections
Enabled
1
Unspecified
Use Windows authentication for all users
Enabled
1000000
Unspecified
Secure Wired (Ethernet) Connections
Conditions - If the following conditions are met:
Condition
Value
Client Friendly Name
Router
Settings - Then the following settings are applied:
Setting
Value


Secure Wired (Ethernet) Connections Properties
Overview
Conditions
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.
Condition
Value
Client Friendly Name
Router
Condition description:
The Client Friendly Name condition specifies the name of the RADIUS client that forwarded the connection request to NPS.
Add...
Edit...
Remove
OK
Cancel
Apply

Configuring the user group and users




Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
doruk.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
Name
Type
Description
DnsUpdateProxy
Security Group - Global
DNS clients who are per...
Domain Admins
Security Group - Global
Designated administrato...
Domain Computers
Security Group - Global
All workstations and ser...
Domain Controllers
Security Group - Global
All domain controllers i...
Domain Guests
Security Group - Global
All domain guests
Domain Users
Security Group - Global
All domain users
Enterprise Admins
Security Group - Unive...
Designated administrato...
Enterprise Key Admins
Security Group - Unive...
Members of this group ...
Enterprise Read-only Do...
Security Group - Unive...
Members of this group ...
fenerbahce
User
Group Policy Creator O...
Security Group - Global
Members in this group c...
Guest
User
Built-in account for gue...
Key Admins
Security Group - Global
Members of this group ...
Protected Users
Security Group - Global
Members of this group ...
RAS and IAS Servers
Security Group - Doma...
Servers in this group can...
Read-only Domain Cont...
Security Group - Global
Members of this group ...
Router
User
Router Users
Security Group - Global
Schema Admins
Security Group - Unive...
Designated administrato...
ThompsonRK
User


Router Users Properties
General
Members
Member Of
Managed By
Members:
Name
Active Directory Domain Services Folder
fenerbahce
doruk.com/Users
Router
doruk.com/Users
ThompsonRK
doruk.com/Users
Add...
Remove
OK
Cancel
Apply

Problems

I did not have any major problems in this lab because I made good research and found good resources that explained everything step by step. The only small problem I had was establishing connectivity between the server and the router. I wasn’t able to ping between the two devices but immediately realized that the firewall on the server was turned on and turned it off to solve the problem.

Conclusion

In this lab, I configured an AAA server for the first time however it wasn’t as challenging as I thought it would be. I installed the needed tools on the server, created a domain, entered the router’s information, configured policies, a user group and users that are assigned into that group. Then I enabled AAA on the router and I was able to access the router using the usernames and passwords of the users that were set on the server. Installing the server as a virtual machine takes a while but after the server is set, the other steps are fairly simple and straight forward. Before this lab I did not know how AAA worked and how critical it is, but now I can configure it for any router or switch and make it the network more secure by storing the passwords in a remote server.

VoIP part 1

Purpose

The purpose of this lab was to make two IP phones to call and talk to each other, using the Cisco Unified Communications server.

Background Information

A Network Time Protocol (NTP) server is a server in a network that is responsible for telling and keeping track of the time to the other devices in the network. NTP is one of the oldest protocol that is used to synchronize clocks throughout a network which is essential for a network. A network cannot operate if the clocks of different devices is not synchronized. Small fractions of time differences through a network can cause many problems. Many security mechanisms depend on coordinated time across the network. So not having a NTP server or having a faulty NTP server can open a network to any outside threat. This is one of many problems the absence or lack of NTP can cause in a network.

One can think of NTP like a head chef in a big kitchen. He is responsible on when food should come out of every station and the chefs in every station like fish, chicken, meat, soup, dessert and salad stations. Those chefs rely on the head chef and his timing. The head chef is like the NTP server that is letting the other chefs who are working in the stations of the time. Those other chefs represent the other devices in the network. An industrial kitchen cannot work without a head chef and a network cannot function well without a NTP server.

Voice over IP (VoIP) is a combination of a group of technologies that are used to for the delivery of voice communications over a network that is using an Internet Protocol (IP) such as the internet. From the user interface, the way one uses a VoIP phone is the same as using a traditional phone. The only difference user sees it the cable that is going into the phone. Phones that are in a VoIP network use Ethernet cables which are slightly bigger than traditional phone cables. Special IP phones are used in order for people to be able to talk over the internet. These phones have the ability to convert voice into a digital signal that travels over the internet which is also a service of VoIP. Traditional phones use analog which sends a signal directly from the wire to transfer voice but IP phones transfer the analog signal into digital signal and put IP address on the digital voice packets so that they can travel across IP enabled networks like the internet.

Some advantages of using VoIP is that additional useful services can be bought for VoIP like calling phones that are outside of the network the IP Phone is connected to. Some services enable users to do that no matter what type of phone the destination is using, IP or traditional. A user also doesn't have to pay for both a broadband connection and a traditional phone line when they are using VoIP which makes it cheaper. However, there can be some disadvantages to VoIP. Some VoIP services don't work during power outages and not all VoIP services connect directly to emergency services through 9-1-1.

One can think of VoIP and tradition phones like shipping products. Traditional phones can be like a ground delivery system that goes from roads and VoIP can be a shipping company that uses subways to deliver packets to their customers. It still does the same job in a different way. Subways are meant to be used by people not for shipping just like how the first intent of internet is not to call people.

Lab Summary

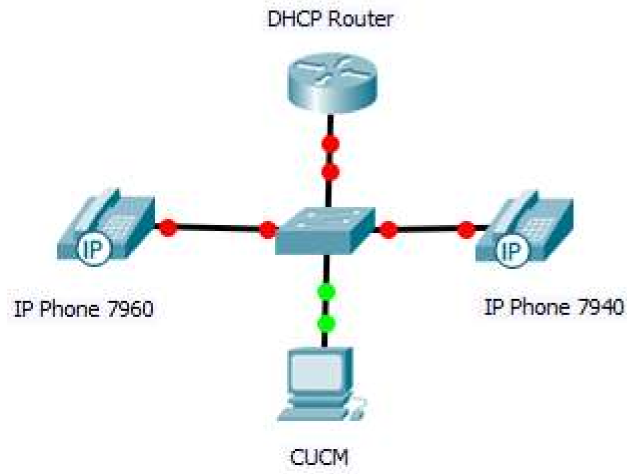
In this lab, we first had to install the Cisco Unified Communications Manager (CUCM). We first created a new virtual machine and used a template to install the server. We also configured the router as a DHCP and NTP server for the virtual machine to use. We set the username, password, IP address, default gateway, NTP server address, entered email address and information about our organization and enabled Smart Call Home on System Start. After the installation was complete, we ran the virtual machine, entered our username and password and the server was set. Then we opened Microsoft Edge, a web browser, and entered https://192.168.1.2/ccmadmin to access the server. We entered the username and password to gain access to the server and configure the phones.

We cabled the phones to a switch that had Power over Ethernet (PoE) enabled. They got their IP addresses from the router which was also connected to the switch. On the server, we first went to the Cisco Unified OS (Operating System) Administrator and enabled all the services, then we went to the Cisco Unified CM (Communications Manager) Administrator mode. We did the rest of the configurations in this mode. In this mode, we first created 2 users, one for each phone. In every user we entered a name, last name and a pin. Every user had their own unique pin. After the users were created, we then created the phones in the server. We entered what type of IP phone our phones were. One was 7940 and the other one was 7960. We entered the mac address of the phones, assigned a user to each phone and finally assigned a line number which is the same as the pin of their users. This is really critical the pin of the user has to be same as the number on the line. After we have done all the configurations for the phones, we were able to see that the phones were registered on the server and we were also able to see that the phones were ready to call one another from their screens. To call a phone from the other one, we dialed the number we set for the other phone's line and the other phone started to ring once we did that. Then we picked up the phone that was ringing and we were able to talk to each other. So, our VoIP setup worked successfully.

Lab Commands

option *150* **ip** *192.168.1.10*	This command is used to define the IP address of the TFTP server, which is the CUCM server, to download the phone configuration files.
ip dhcp excluded-address *192.168.1.1*	When this command is entered, the DHCP server does not send out the address 192.168.0.1 to clients
ip dhcp pool *nam*	This command gives the pool of addresses that are going to be send out to the hosts by the DHCP server a name.
network *192.168.1.0 255.255.255.0*	This command defines the network that the DHCP server can send addresses from.
domain-name *calvin.com*	This command gives a domain name to the DHCP pool.
dns-server *192.168.1.1*	This command specifies the IP address of a DNS server that is available to a DHCP client.
default-router *192.168.1.1*	This command specifies the IP address of the default router for a DHCP client.
ntp master	This command is used to make the router act as an Network Time Protocol (NTP) server with its own hardware clock.
ntp server *192.168.1.1*	This command defines which device on the IP address is going to be the NTP server. It is device that is associated with 192.168.1.1 IP address in this case.

Network Diagram



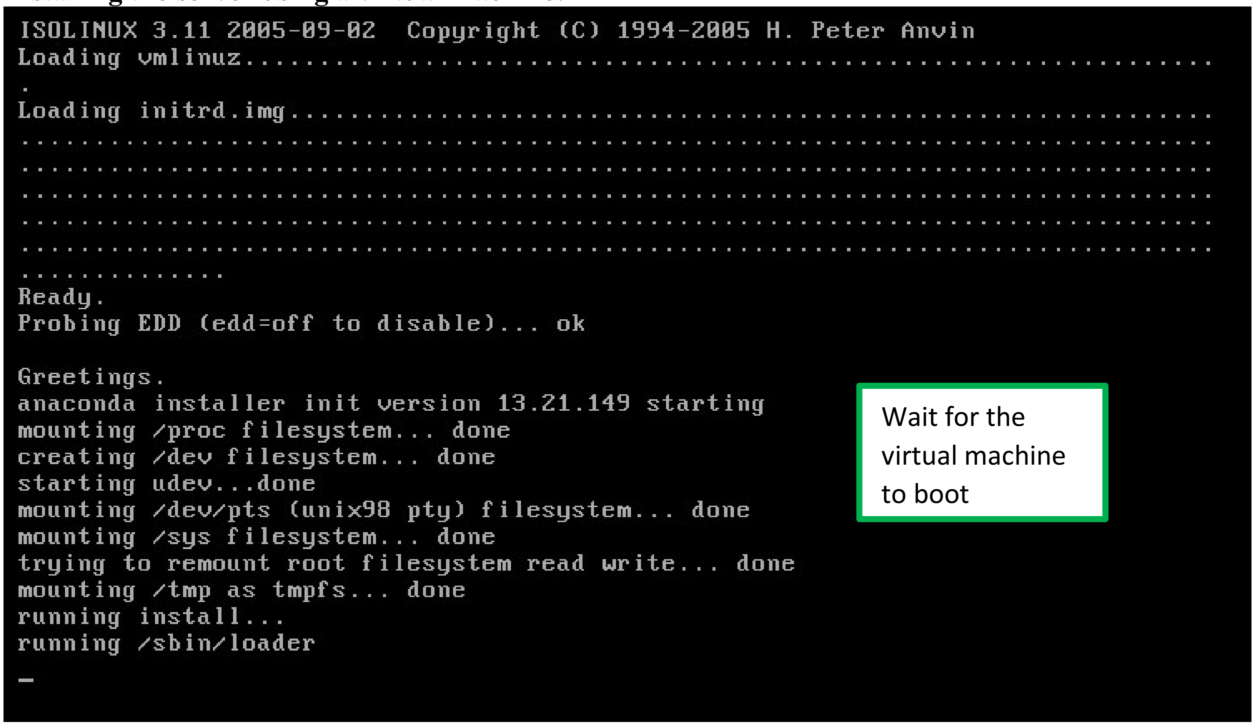
Configurations

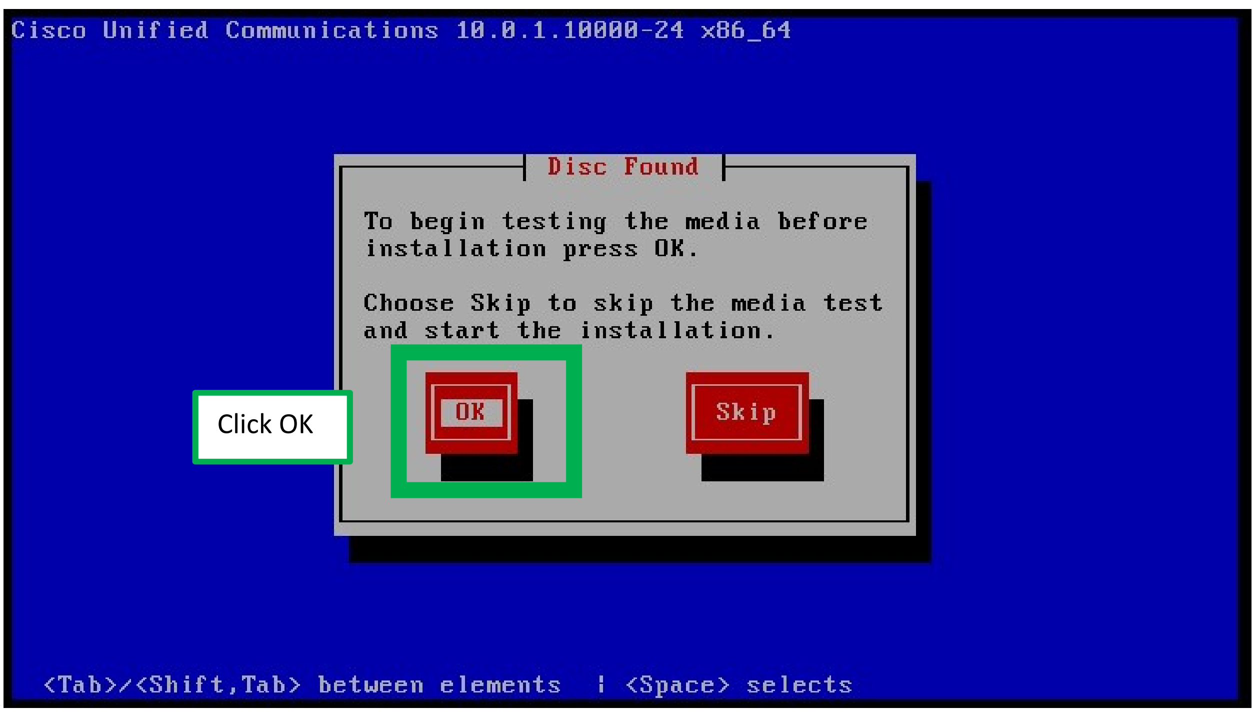
Router:

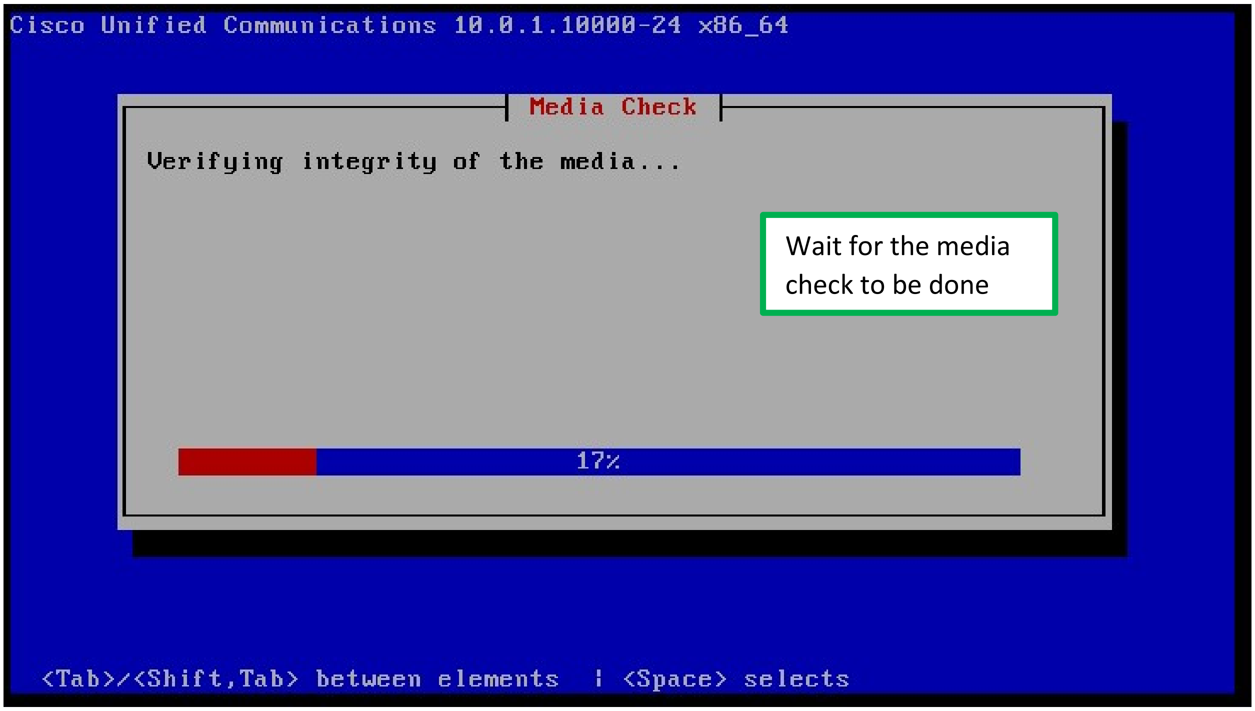
```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname DHCPserver
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
ip dhcp excluded-address 192.168.1.7 192.168.1.11
ip dhcp pool nam
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 192.168.1.1
 domain-name calvin.com
 option 150 ip 192.168.1.10
ip domain name calvin.com
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX1520806Z
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
```

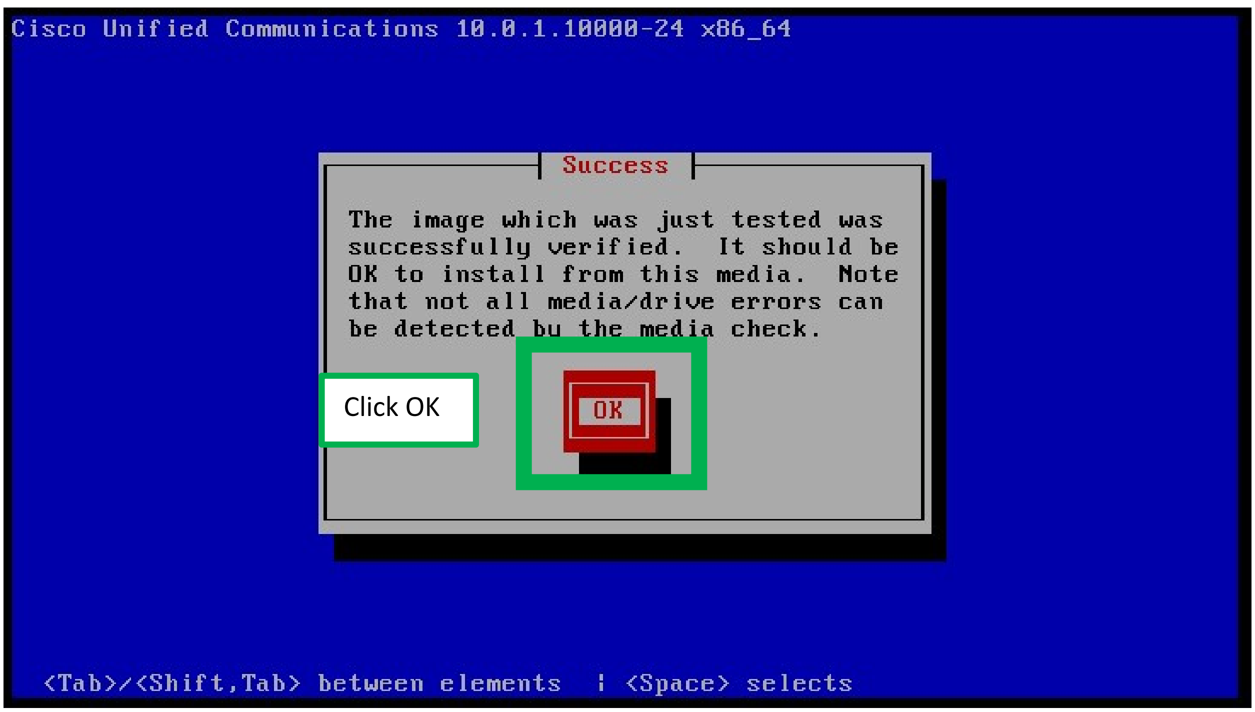
```
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 duplex auto
 speed auto
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
ntp master
ntp server 192.168.1.1
End
```

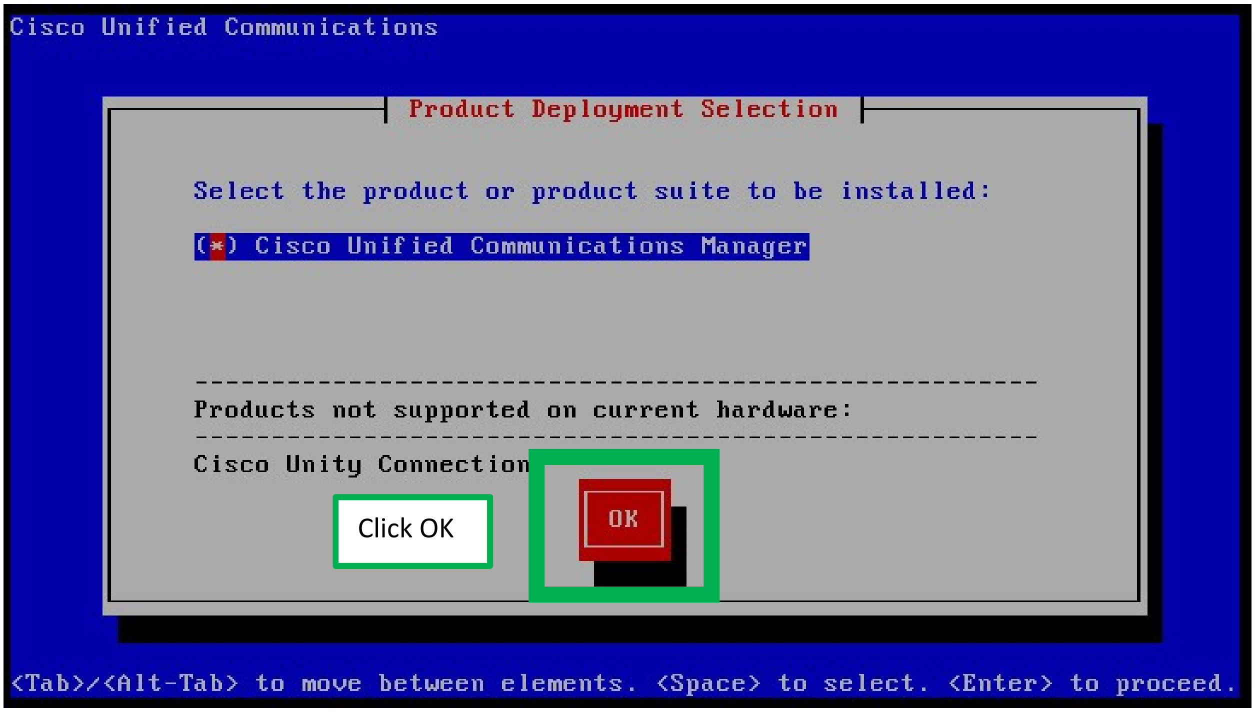
Installing the server using a virtual machine:

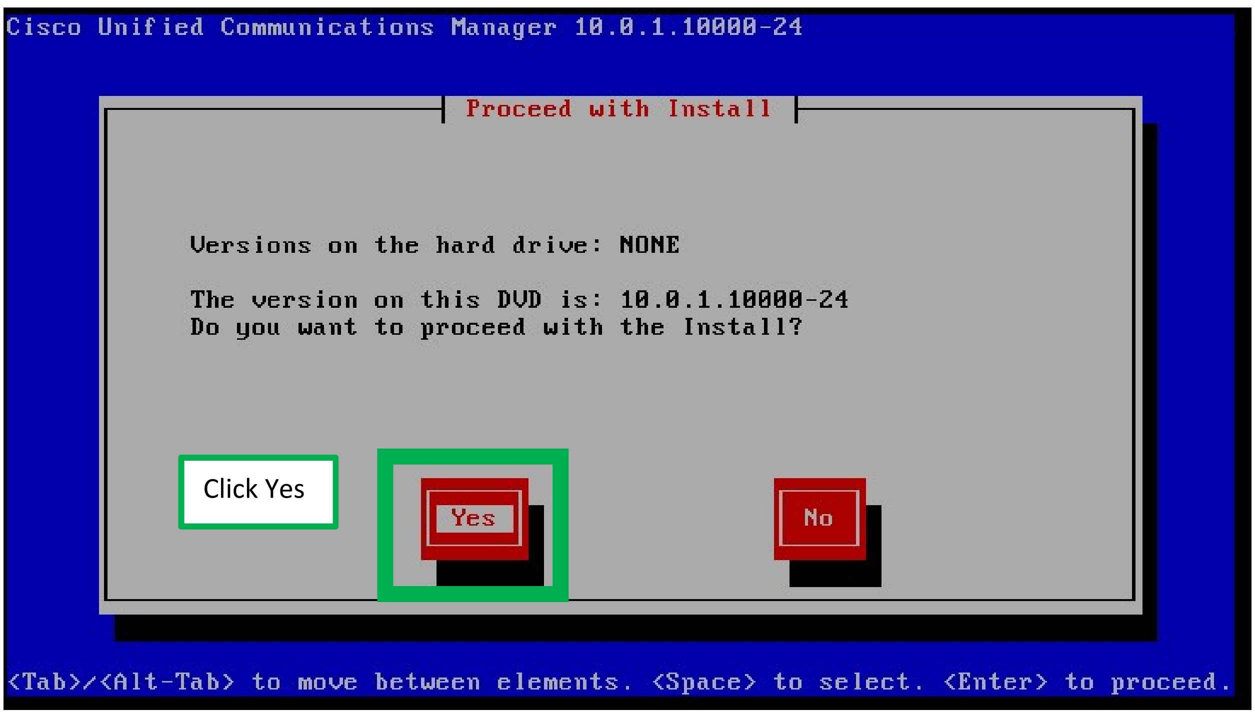


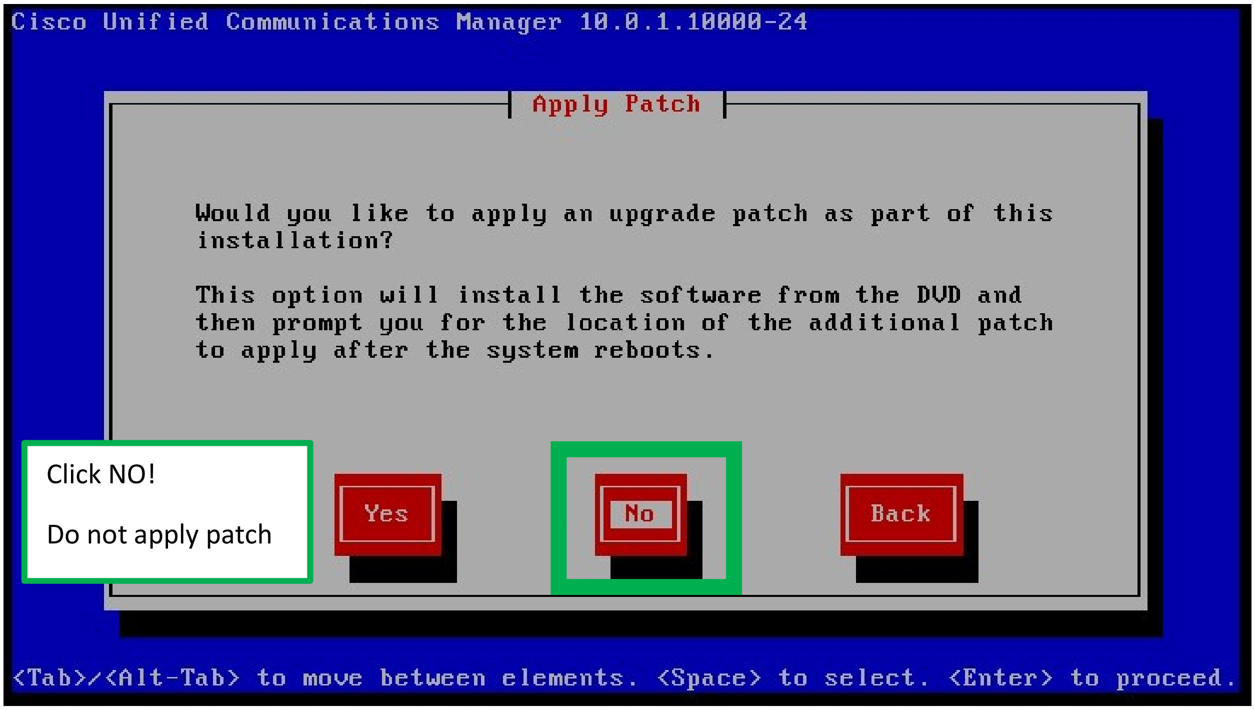


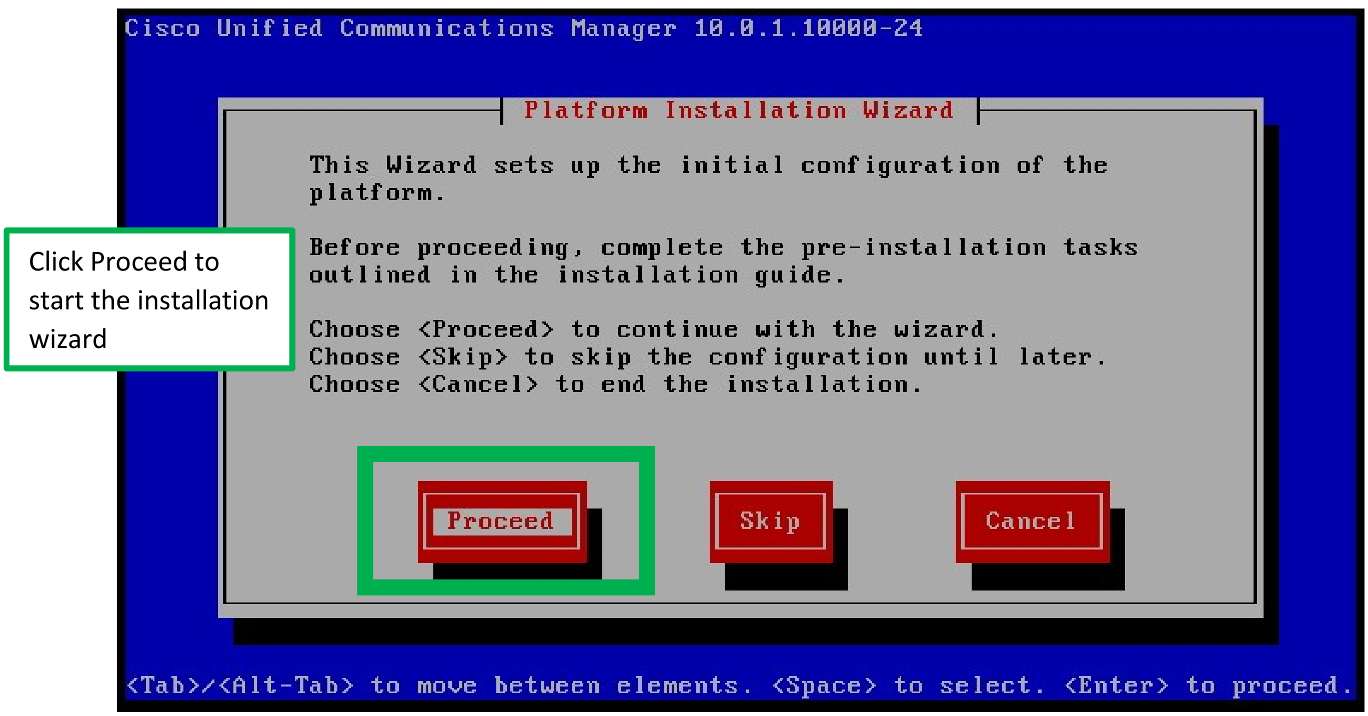

Cisco Unified Communications 10.0.1.10000-24 x86_64
Media Check
Verifying integrity of the media...
Wait for the media check to be done
17%
<Tab>/<Shift,Tab> between elements | <Space> selects

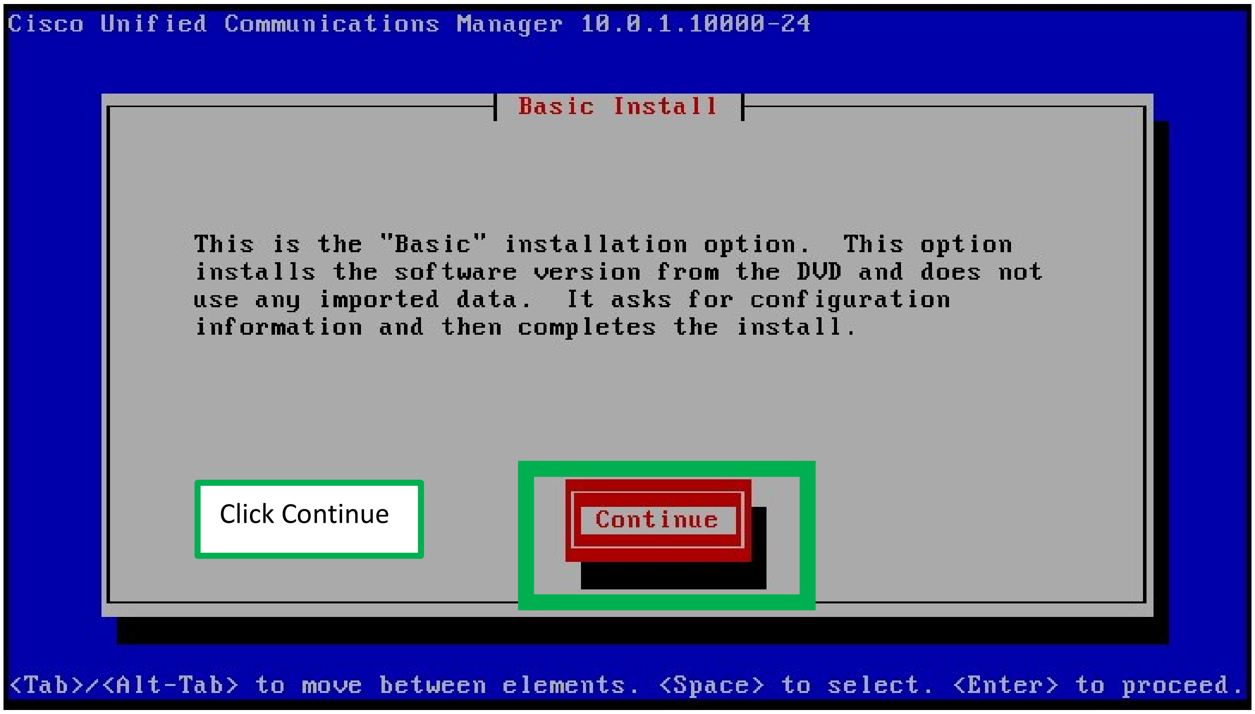

Cisco Unified Communications 10.0.1.10000-24 x86_64
Success
The image which was just tested was successfully verified. It should be OK to install from this media. Note that not all media/drive errors can be detected by the media check.
Click OK
OK
<Tab>/<Shift,Tab> between elements | <Space> selects

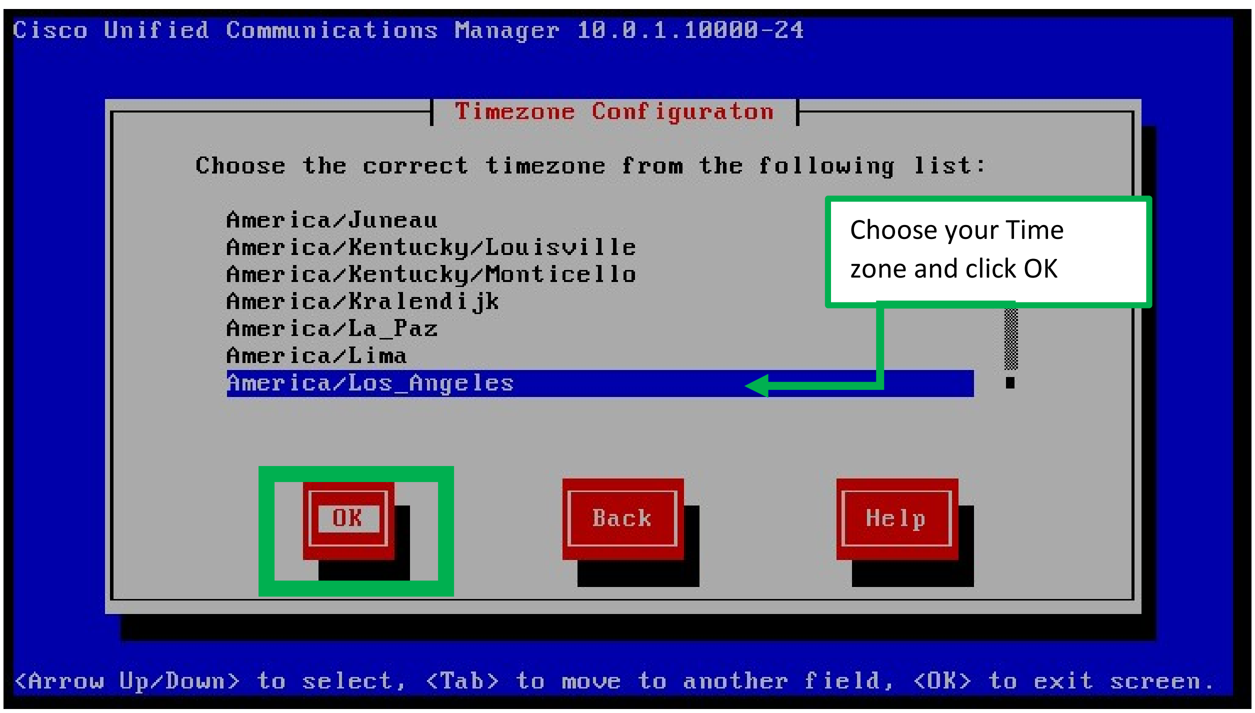

Cisco Unified Communications
Product Deployment Selection
Select the product or product suite to be installed:
(*) Cisco Unified Communications Manager
Products not supported on current hardware:
Cisco Unity Connection
Click OK
OK
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

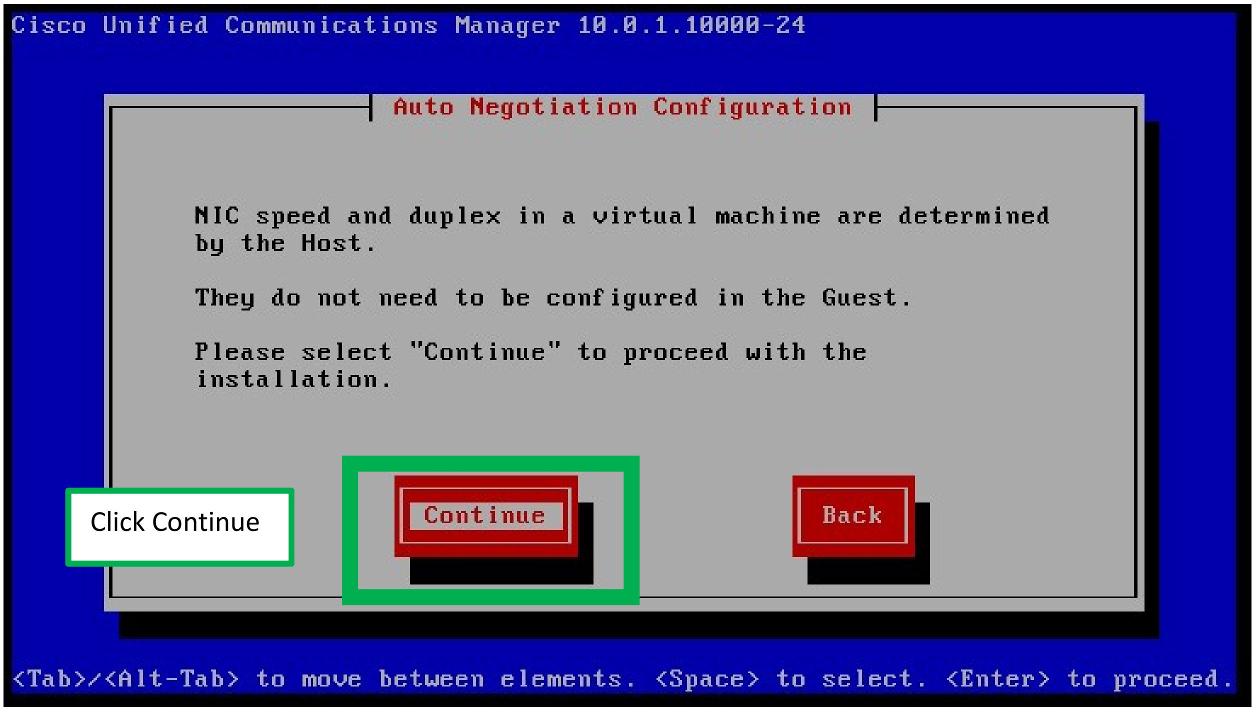

Cisco Unified Communications Manager 10.0.1.10000-24
Proceed with Install
Versions on the hard drive: NONE
The version on this DVD is: 10.0.1.10000-24
Do you want to proceed with the Install?
Click Yes
Yes
No
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

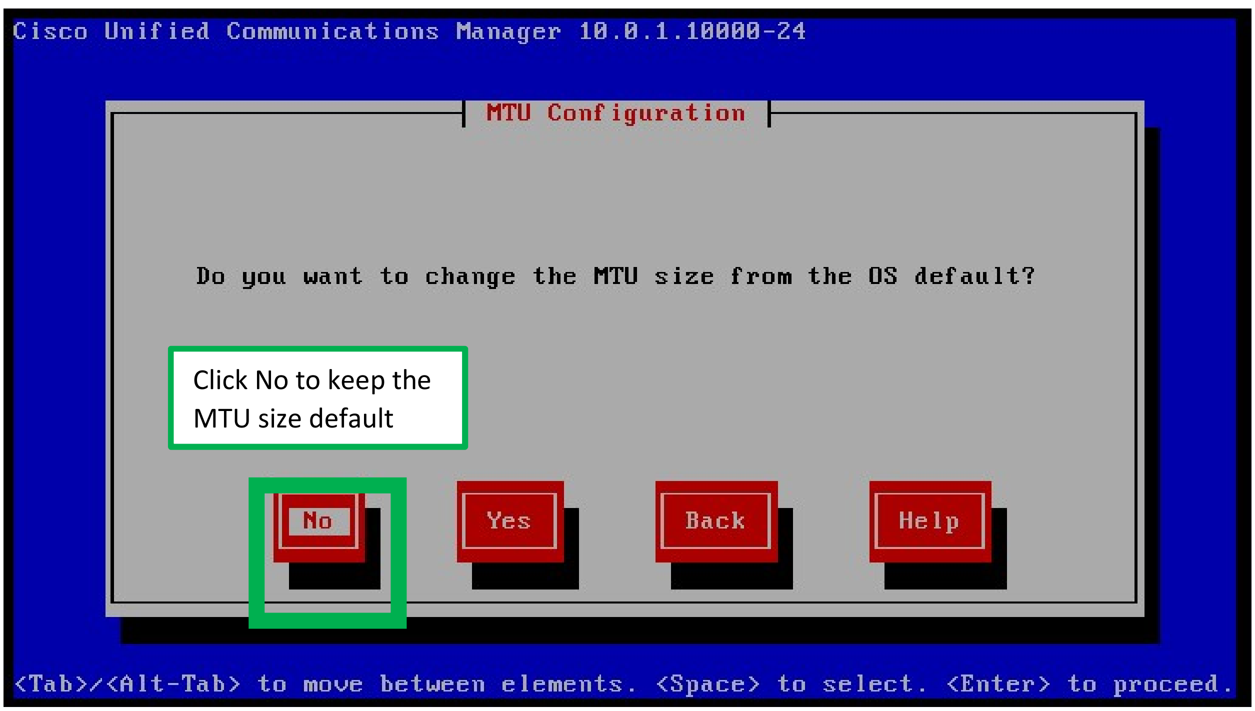

Cisco Unified Communications Manager 10.0.1.10000-24
Apply Patch
Would you like to apply an upgrade patch as part of this installation?
This option will install the software from the DVD and then prompt you for the location of the additional patch to apply after the system reboots.
Click NO!
Do not apply patch
Yes
No
Back
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

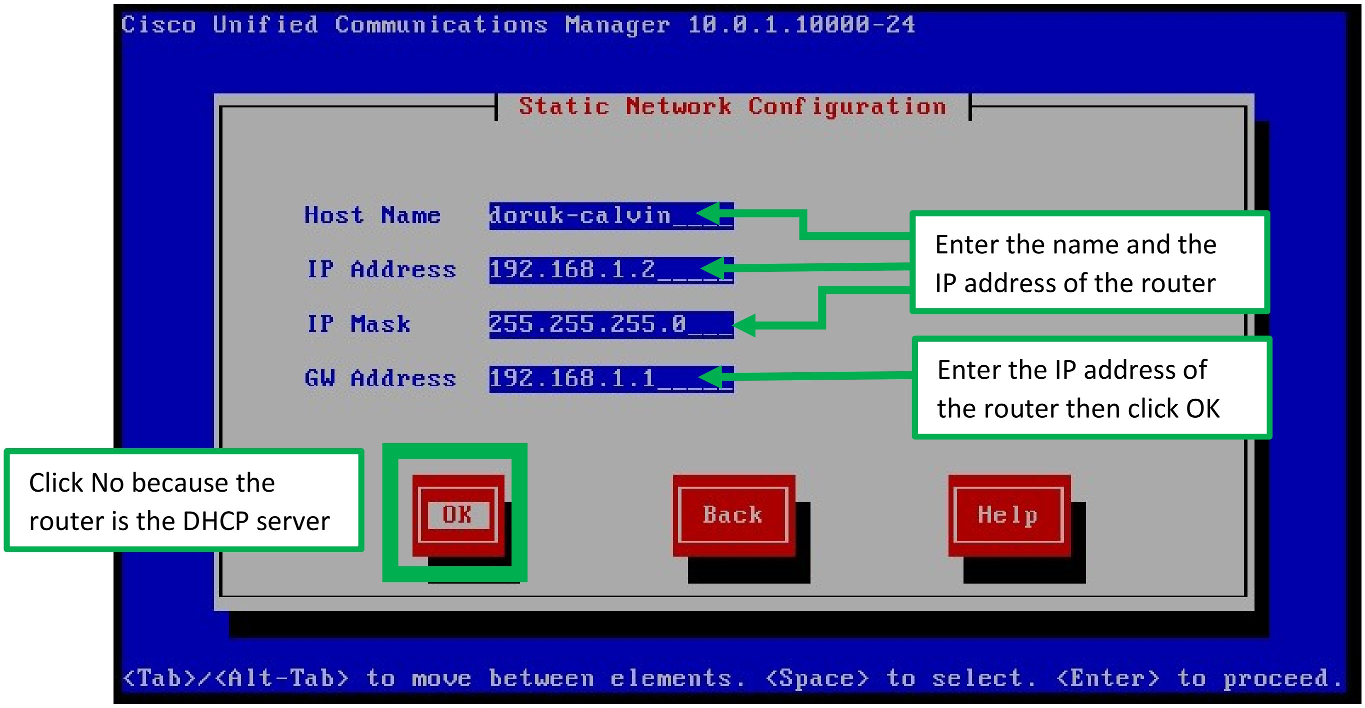

Cisco Unified Communications Manager 10.0.1.10000-24
Platform Installation Wizard
This Wizard sets up the initial configuration of the platform.
Before proceeding, complete the pre-installation tasks outlined in the installation guide.
Choose <Proceed> to continue with the wizard.
Choose <Skip> to skip the configuration until later.
Choose <Cancel> to end the installation.
Click Proceed to start the installation wizard
Proceed
Skip
Cancel
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

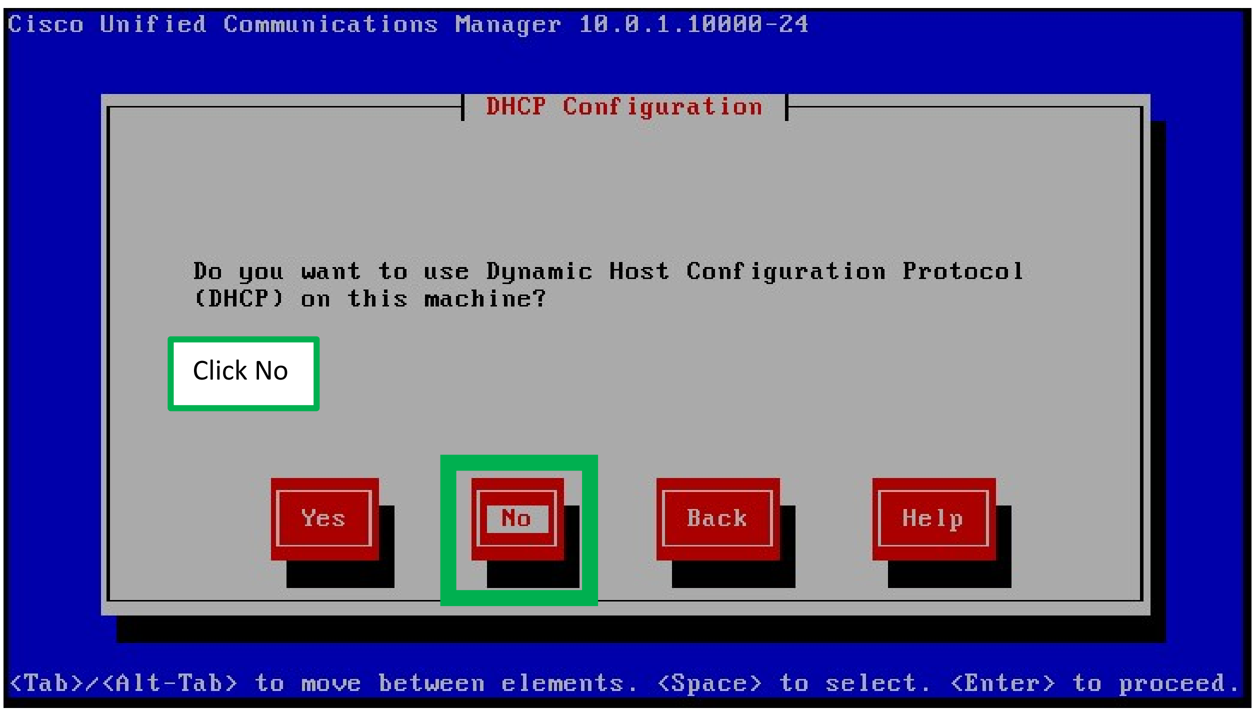

Cisco Unified Communications Manager 10.0.1.10000-24
Basic Install
This is the "Basic" installation option. This option installs the software version from the DVD and does not use any imported data. It asks for configuration information and then completes the install.
Click Continue
Continue
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

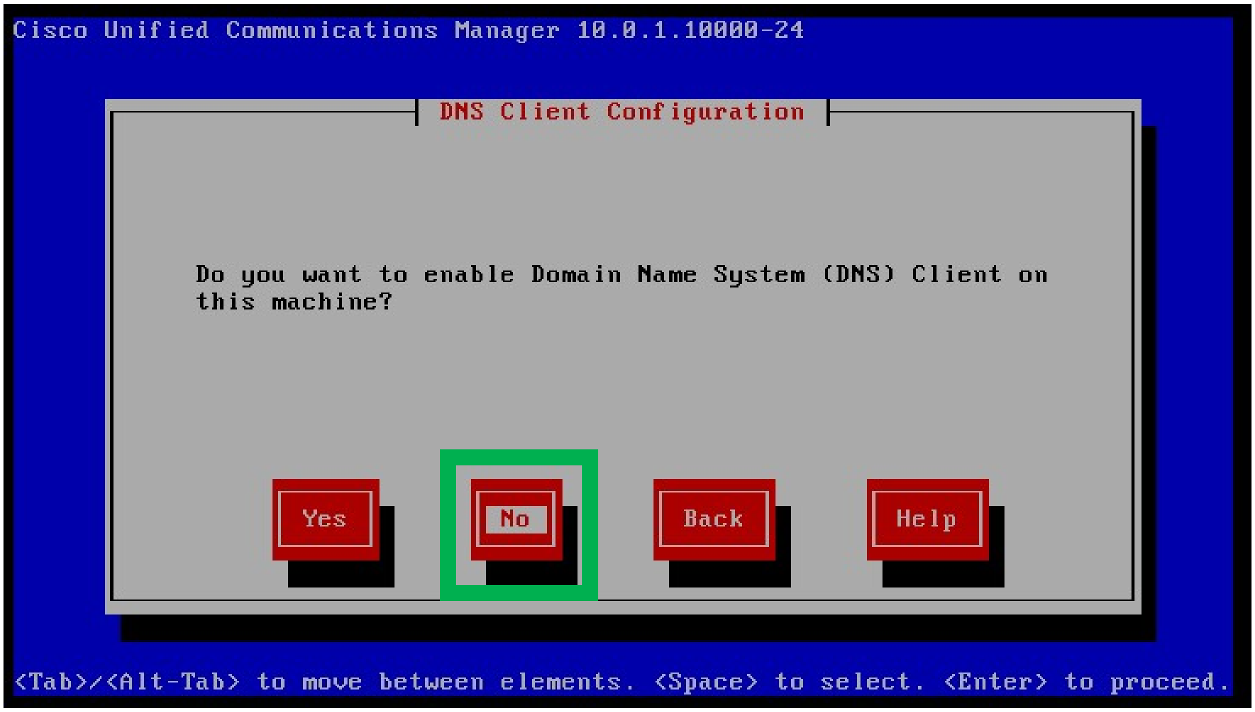

Cisco Unified Communications Manager 10.0.1.10000-24
Timezone Configuraton
Choose the correct timezone from the following list:
America/Juneau
America/Kentucky/Louisville
America/Kentucky/Monticello
America/Kralendijk
America/La_Paz
America/Lima
America/Los_Angeles
Choose your Time zone and click OK
OK
Back
Help
<Arrow Up/Down> to select, <Tab> to move to another field, <OK> to exit screen.

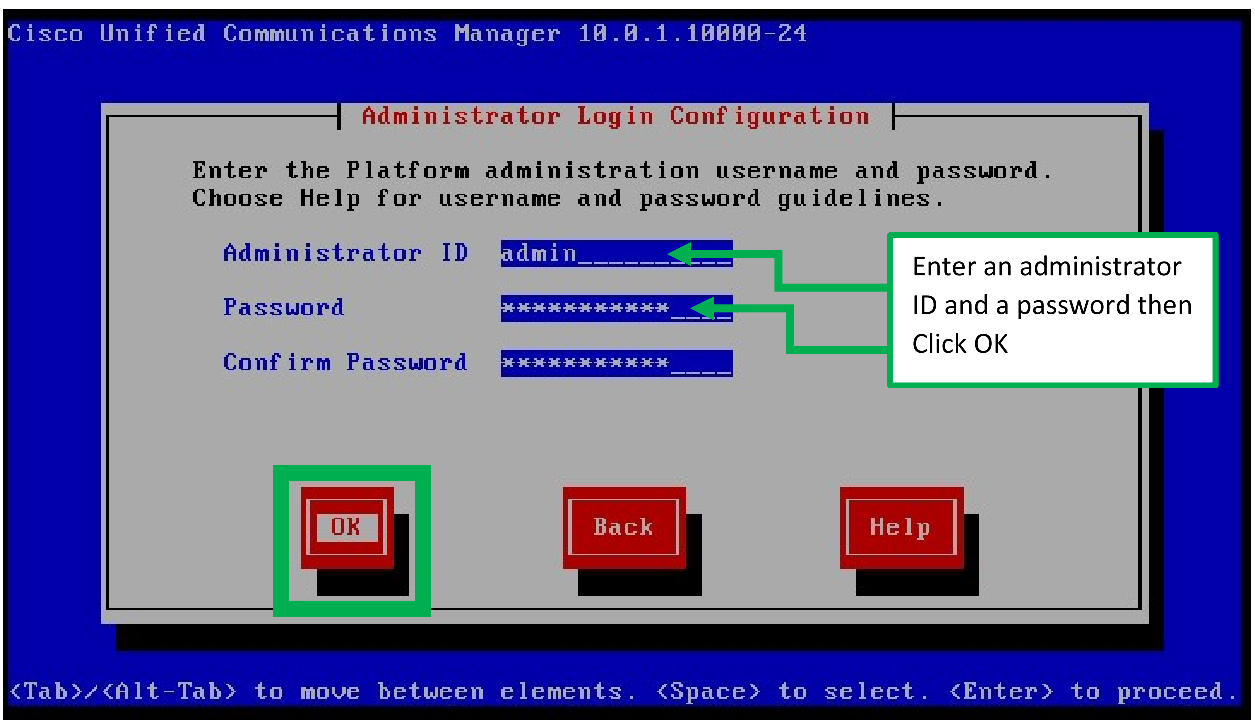

Cisco Unified Communications Manager 10.0.1.10000-24
Auto Negotiation Configuration
NIC speed and duplex in a virtual machine are determined by the Host.
They do not need to be configured in the Guest.
Please select "Continue" to proceed with the installation.
Click Continue
Continue
Back
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

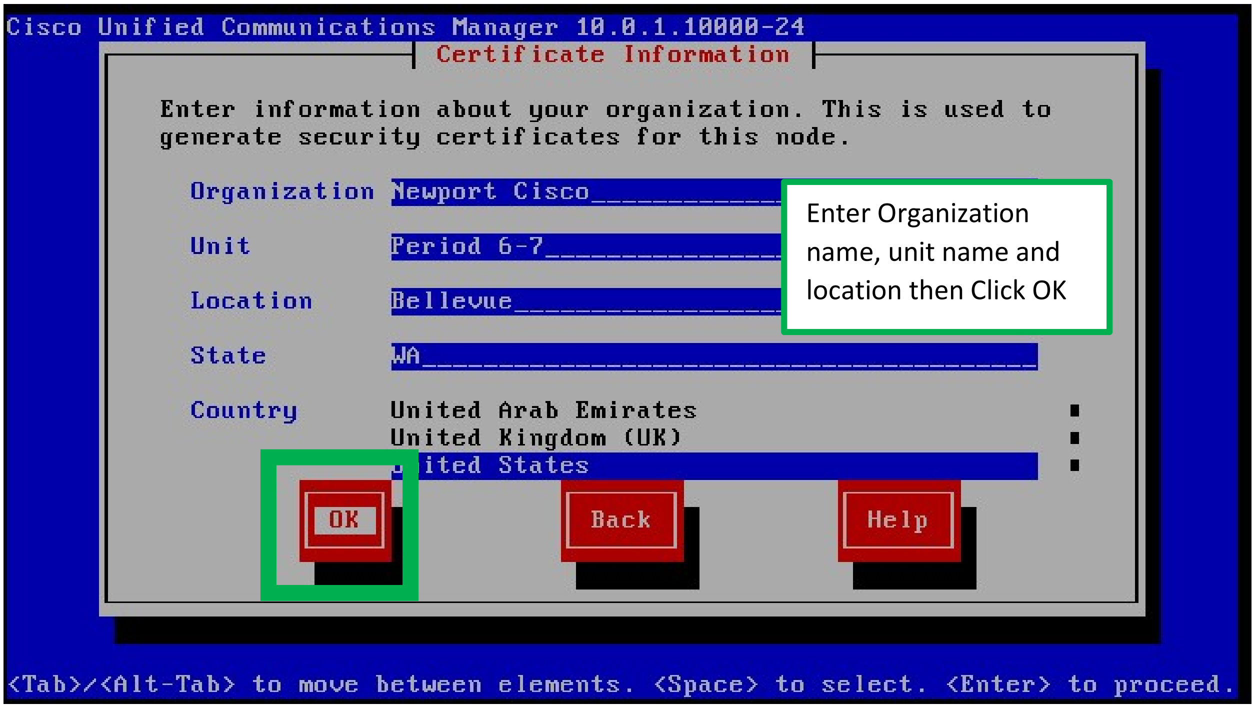

Cisco Unified Communications Manager 10.0.1.10000-24
MTU Configuration
Do you want to change the MTU size from the OS default?
Click No to keep the MTU size default
No
Yes
Back
Help
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

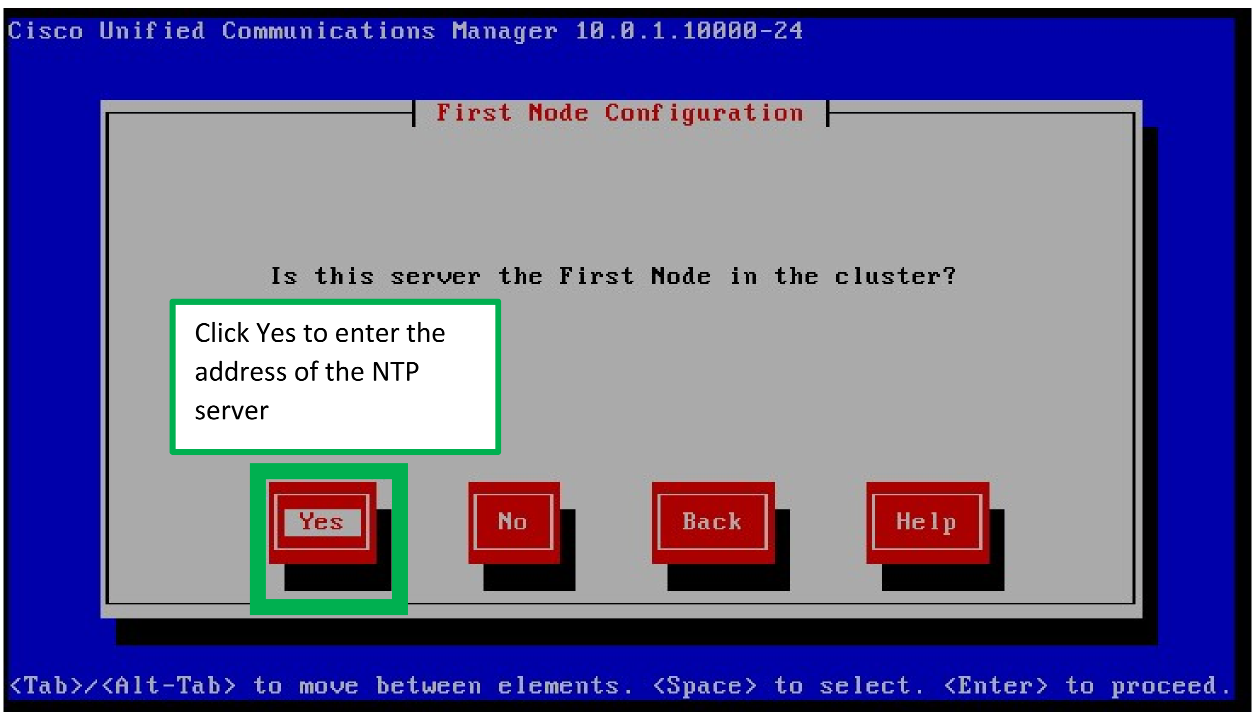

Cisco Unified Communications Manager 10.0.1.10000-24
Static Network Configuration
Host Name
doruk-calvin___
IP Address
192.168.1.2____
IP Mask
255.255.255.0__
GW Address
192.168.1.1____
Enter the name and the IP address of the router
Enter the IP address of the router then click OK
Click No because the router is the DHCP server
OK
Back
Help
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

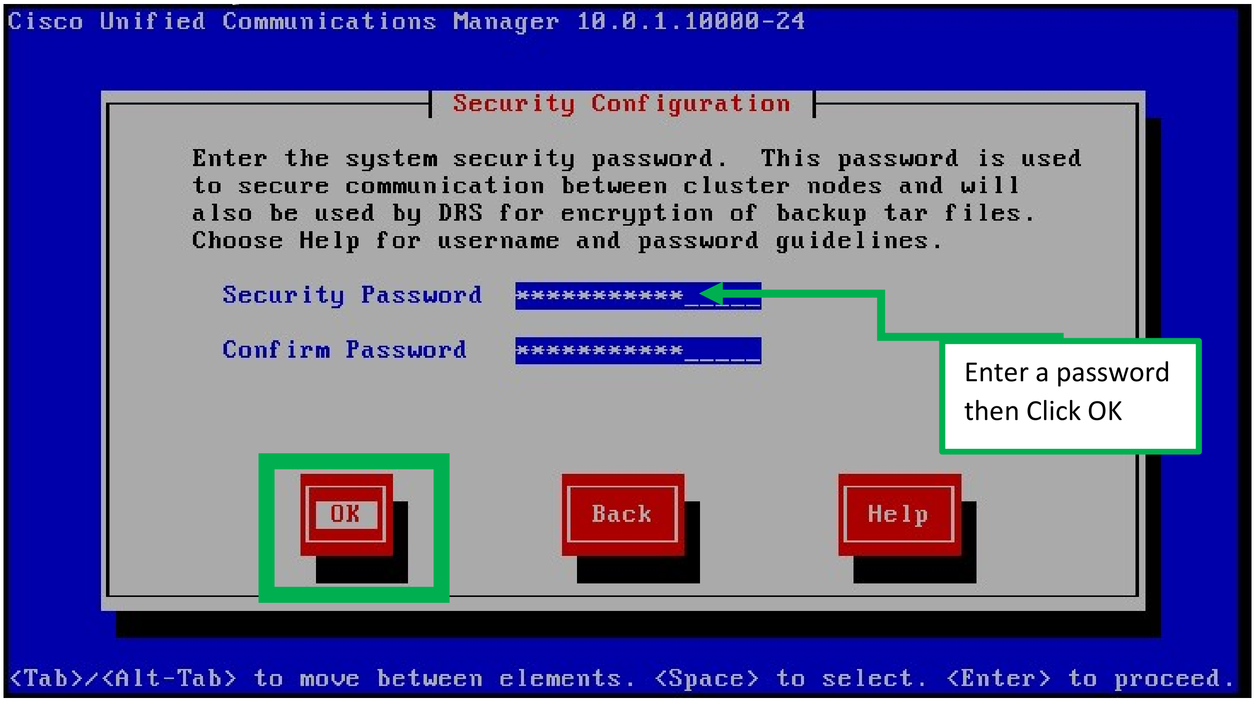

Cisco Unified Communications Manager 10.0.1.10000-24
DHCP Configuration
Do you want to use Dynamic Host Configuration Protocol (DHCP) on this machine?
Click No
Yes
No
Back
Help
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

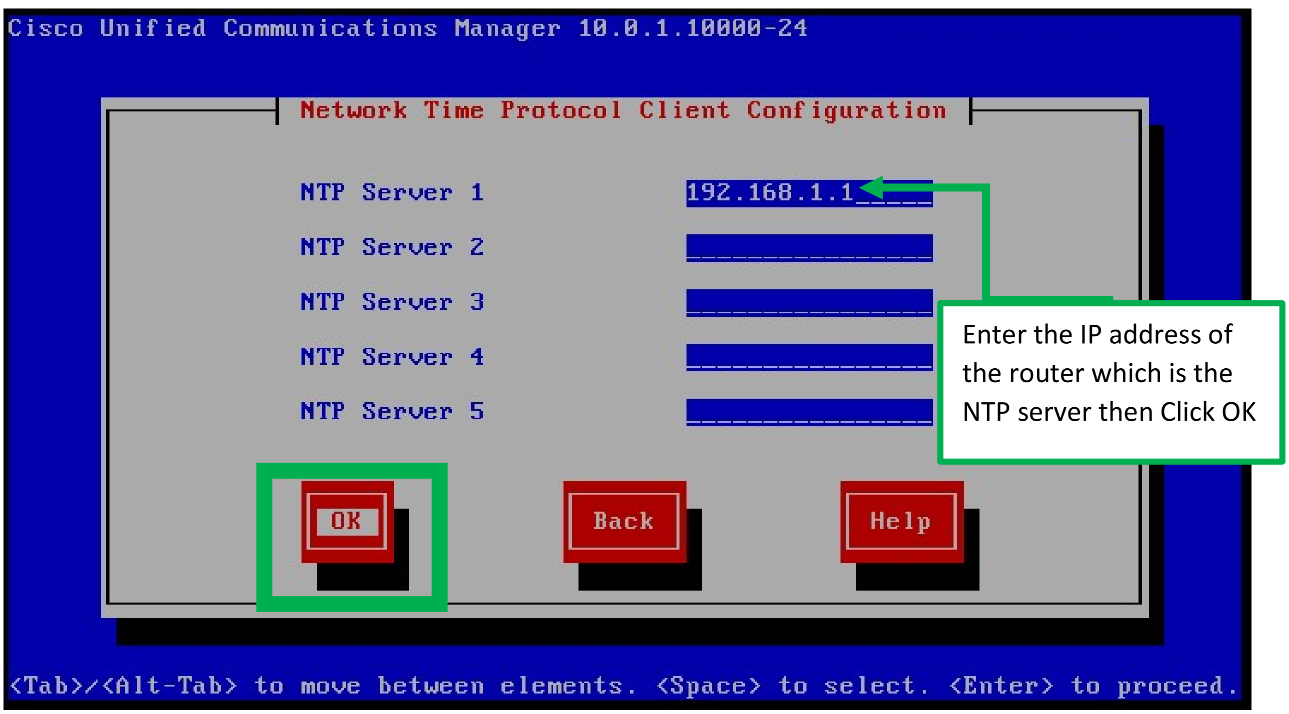

Cisco Unified Communications Manager 10.0.1.10000-24
DNS Client Configuration
Do you want to enable Domain Name System (DNS) Client on this machine?
Yes
No
Back
Help
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

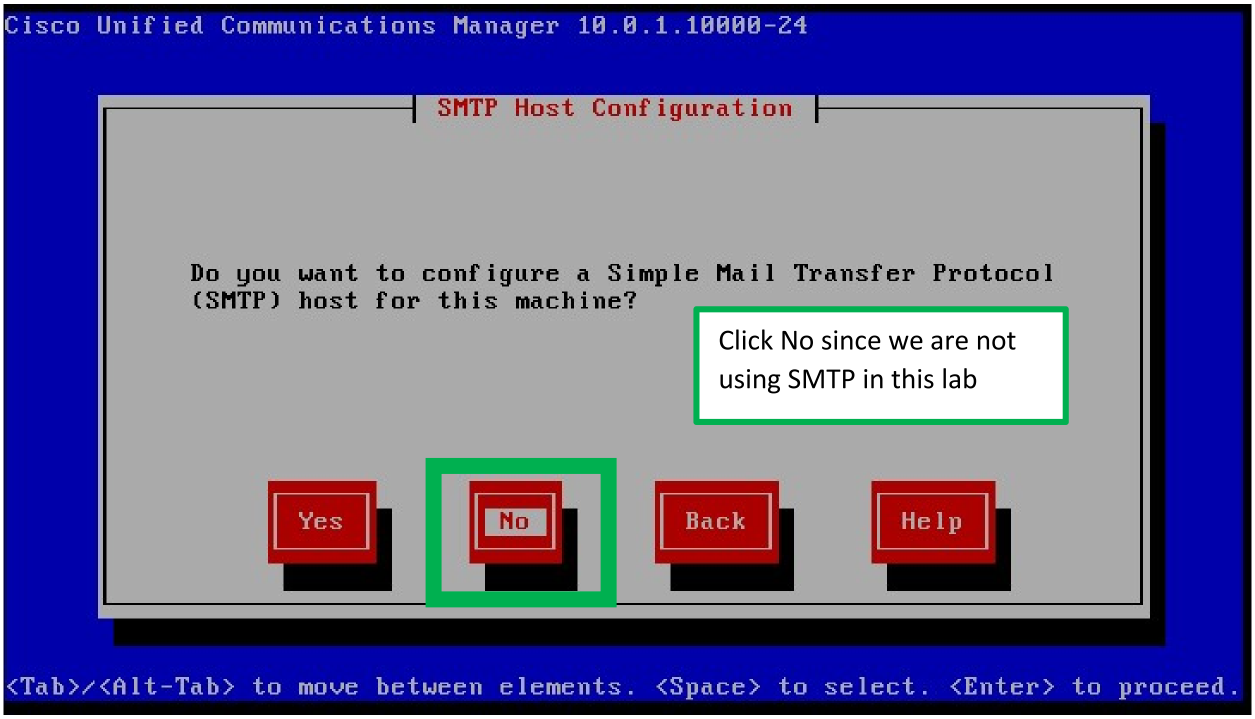

Cisco Unified Communications Manager 10.0.1.10000-24
Administrator Login Configuration
Enter the Platform administration username and password.
Choose Help for username and password guidelines.
Administrator ID
admin
Password
Confirm Password
Enter an administrator ID and a password then Click OK
OK
Back
Help
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

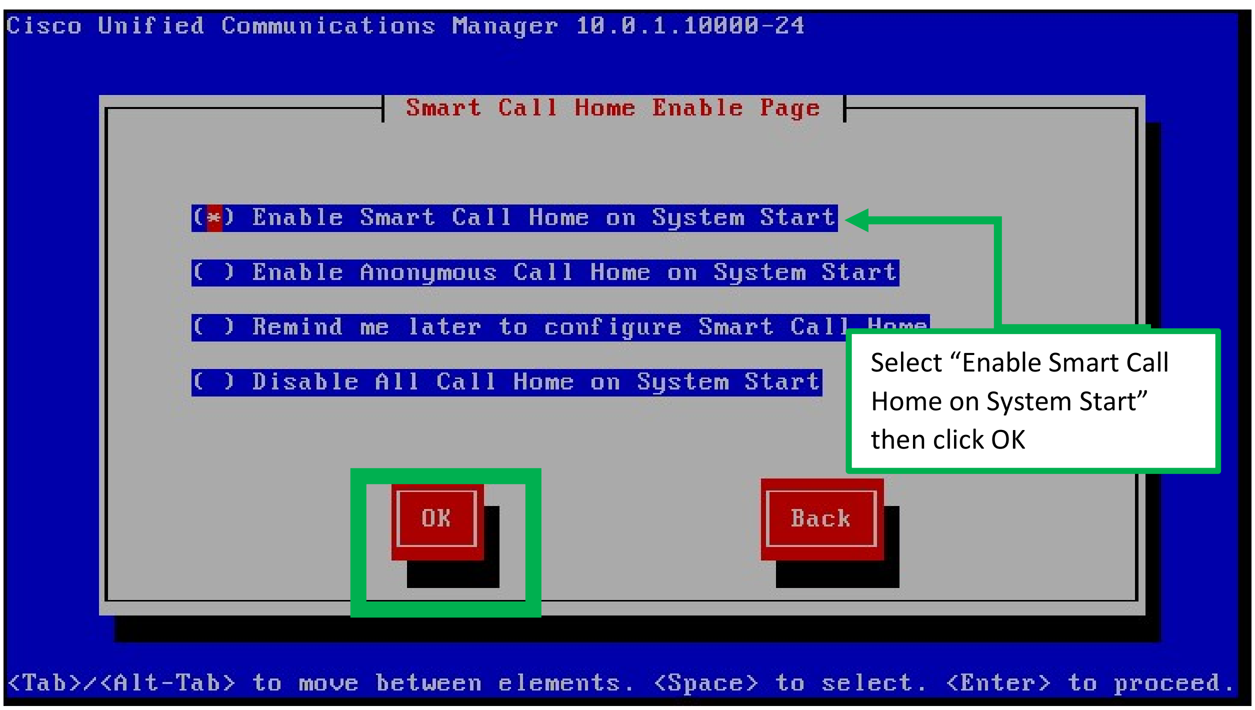

Cisco Unified Communications Manager 10.0.1.10000-24
Certificate Information
Enter information about your organization. This is used to generate security certificates for this node.
Organization Newport Cisco_
Unit Period 6-7_
Location Bellevue_
State WA_
Country United Arab Emirates
United Kingdom (UK)
ited States
OK
Back
Help
Enter Organization name, unit name and location then Click OK
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

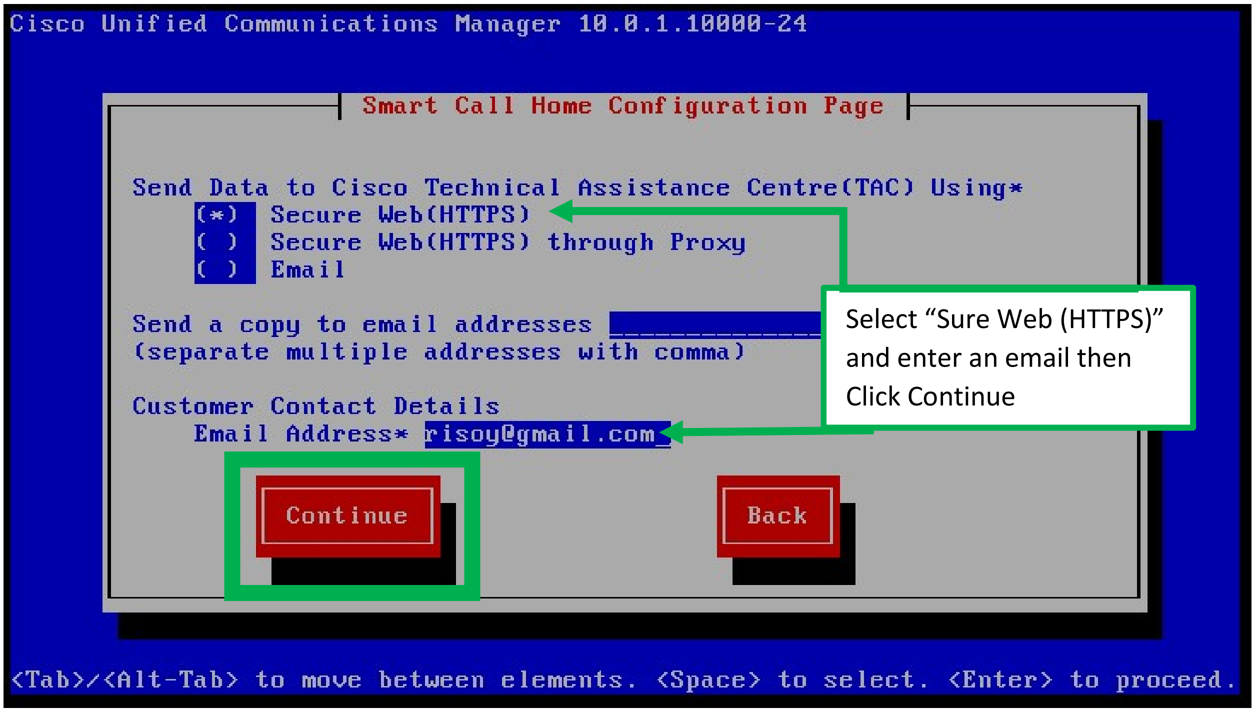

Cisco Unified Communications Manager 10.0.1.10000-24
First Node Configuration
Is this server the First Node in the cluster?
Click Yes to enter the address of the NTP server
Yes
No
Back
Help
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

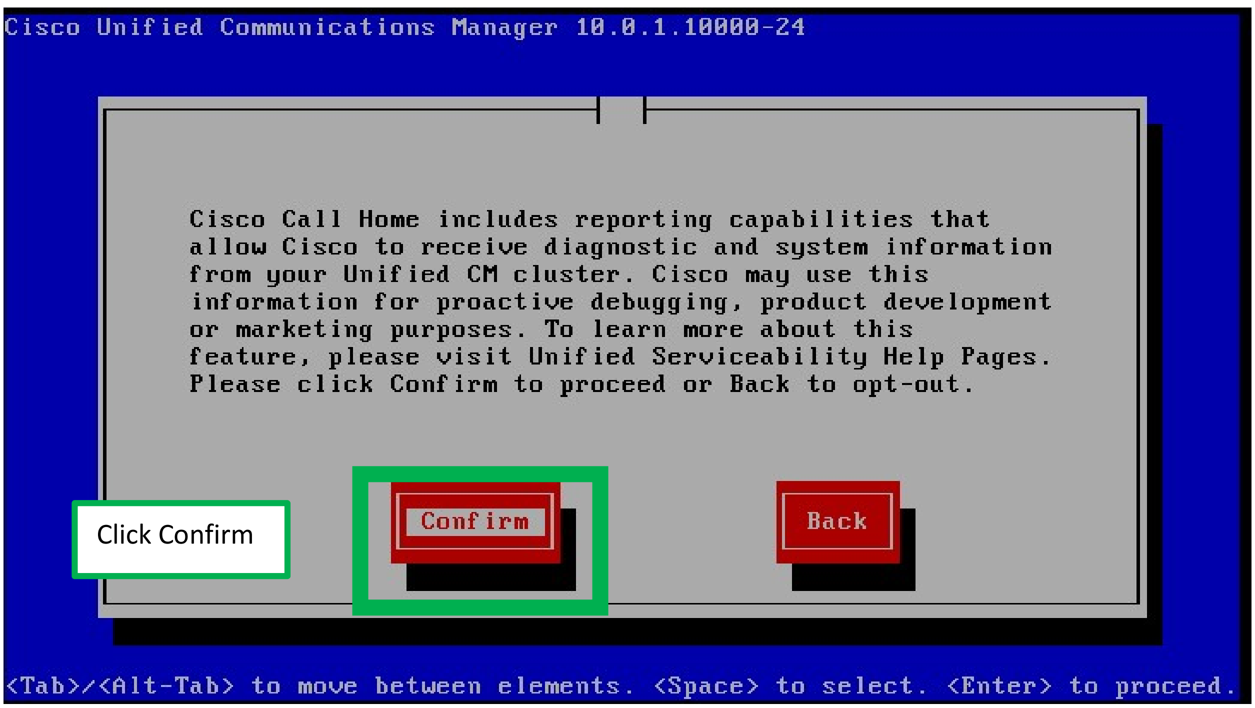

Cisco Unified Communications Manager 10.0.1.10000-24
Security Configuration
Enter the system security password. This password is used to secure communication between cluster nodes and will also be used by DRS for encryption of backup tar files. Choose Help for username and password guidelines.
Security Password
Confirm Password
Enter a password then Click OK
OK
Back
Help
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

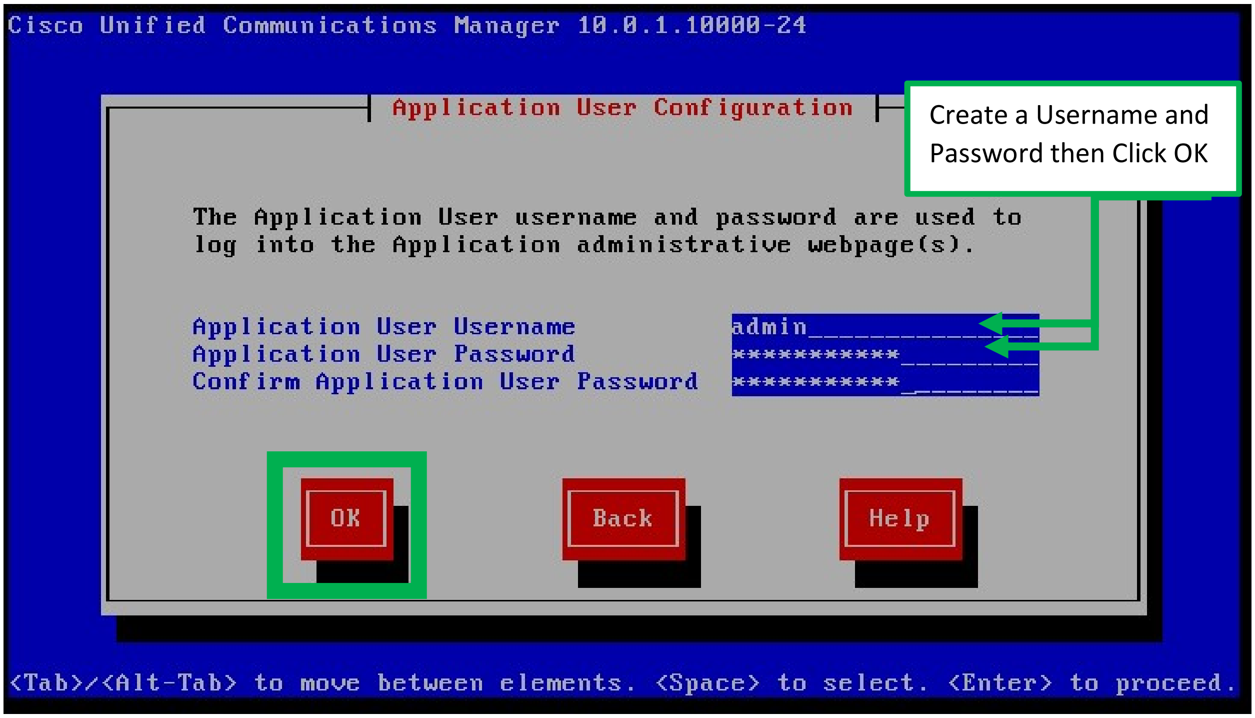

Cisco Unified Communications Manager 10.0.1.10000-24
Network Time Protocol Client Configuration
NTP Server 1
192.168.1.1
NTP Server 2
NTP Server 3
NTP Server 4
NTP Server 5
Enter the IP address of the router which is the NTP server then Click OK
OK
Back
Help
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

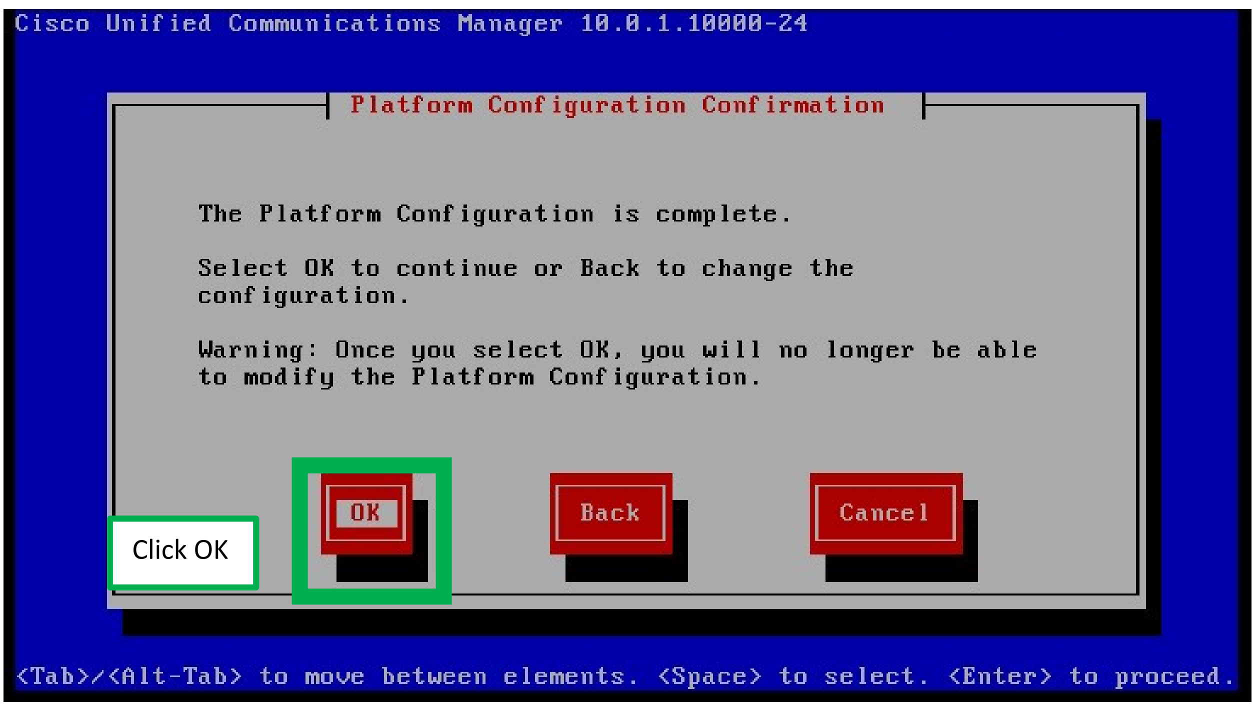

Cisco Unified Communications Manager 10.0.1.10000-24
SMTP Host Configuration
Do you want to configure a Simple Mail Transfer Protocol
(SMTP) host for this machine?
Click No since we are not using SMTP in this lab
Yes
No
Back
Help
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

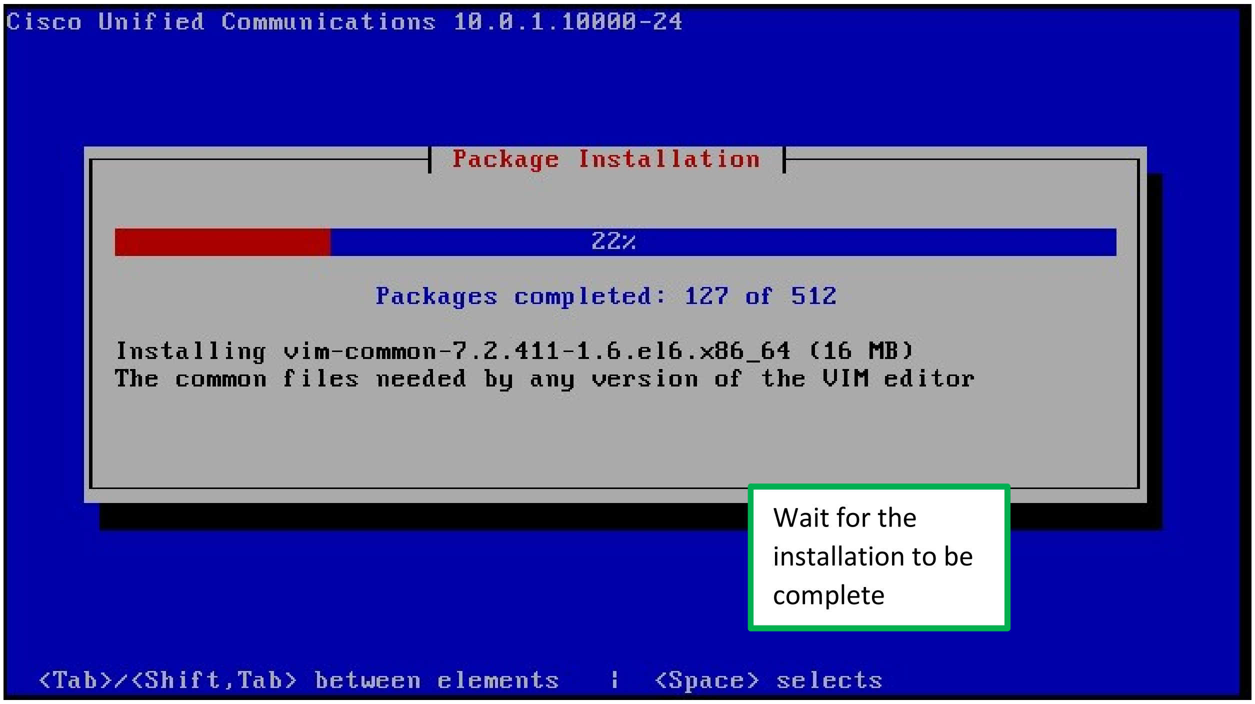

Cisco Unified Communications Manager 10.0.1.10000-24
Smart Call Home Enable Page
(*) Enable Smart Call Home on System Start
( ) Enable Anonymous Call Home on System Start
( ) Remind me later to configure Smart Call Home
( ) Disable All Call Home on System Start
Select "Enable Smart Call Home on System Start" then click OK
OK
Back
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

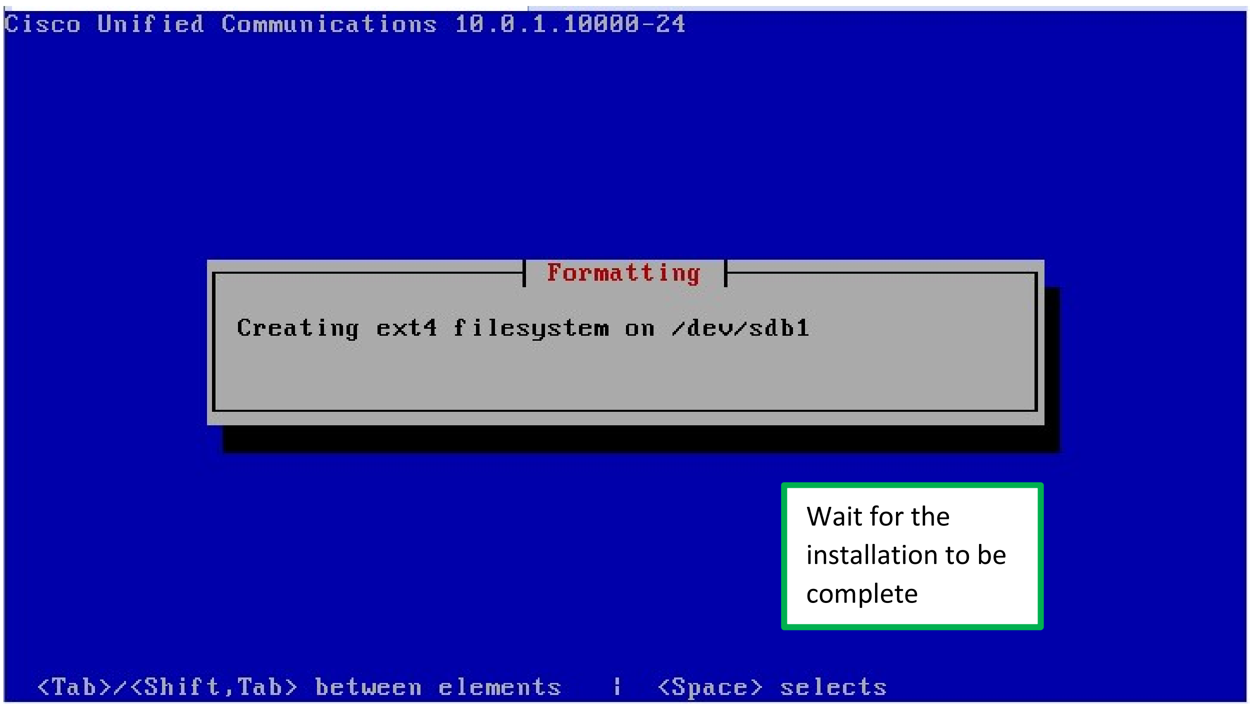

Cisco Unified Communications Manager 10.0.1.10000-24
Smart Call Home Configuration Page
Send Data to Cisco Technical Assistance Centre(TAC) Using*
(*) Secure Web(HTTPS)
( ) Secure Web(HTTPS) through Proxy
( ) Email
Send a copy to email addresses
(separate multiple addresses with comma)
Customer Contact Details
Email Address* risoy@gmail.com_
Continue
Back
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.
Select “Sure Web (HTTPS)” and enter an email then Click Continue

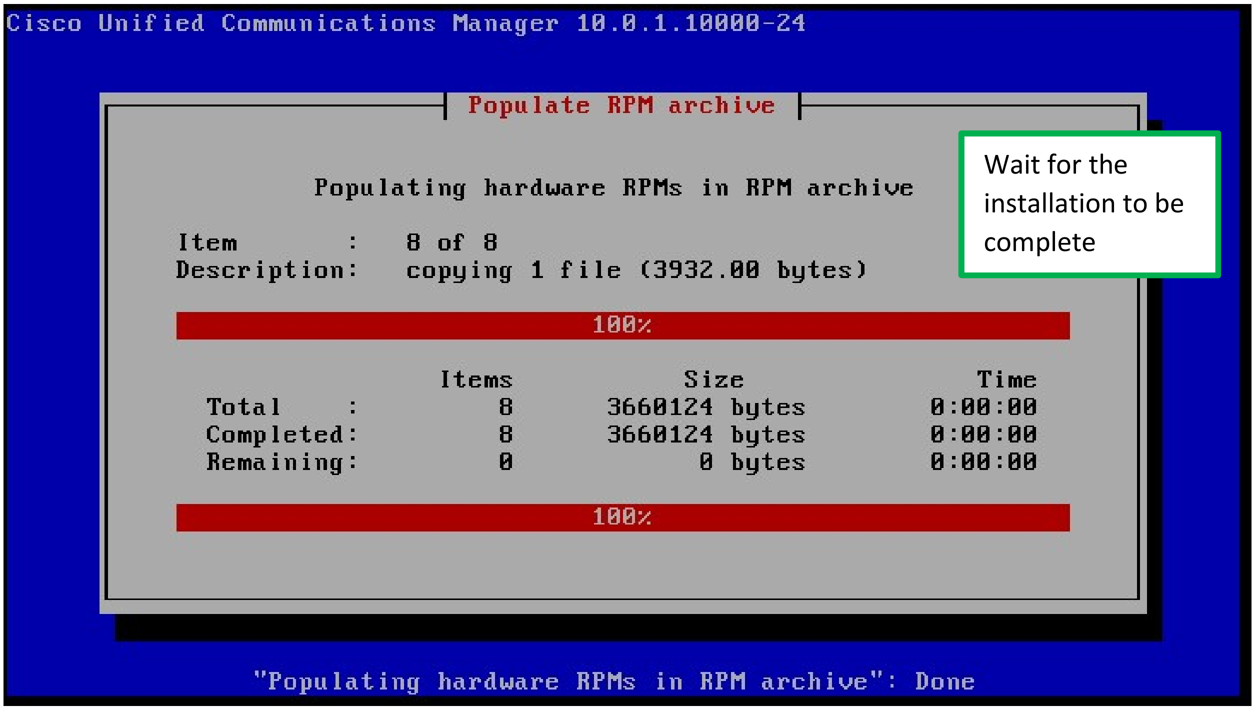

Cisco Unified Communications Manager 10.0.1.10000-24
Cisco Call Home includes reporting capabilities that allow Cisco to receive diagnostic and system information from your Unified CM cluster. Cisco may use this information for proactive debugging, product development or marketing purposes. To learn more about this feature, please visit Unified Serviceability Help Pages. Please click Confirm to proceed or Back to opt-out.
Confirm
Back
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.
Click Confirm

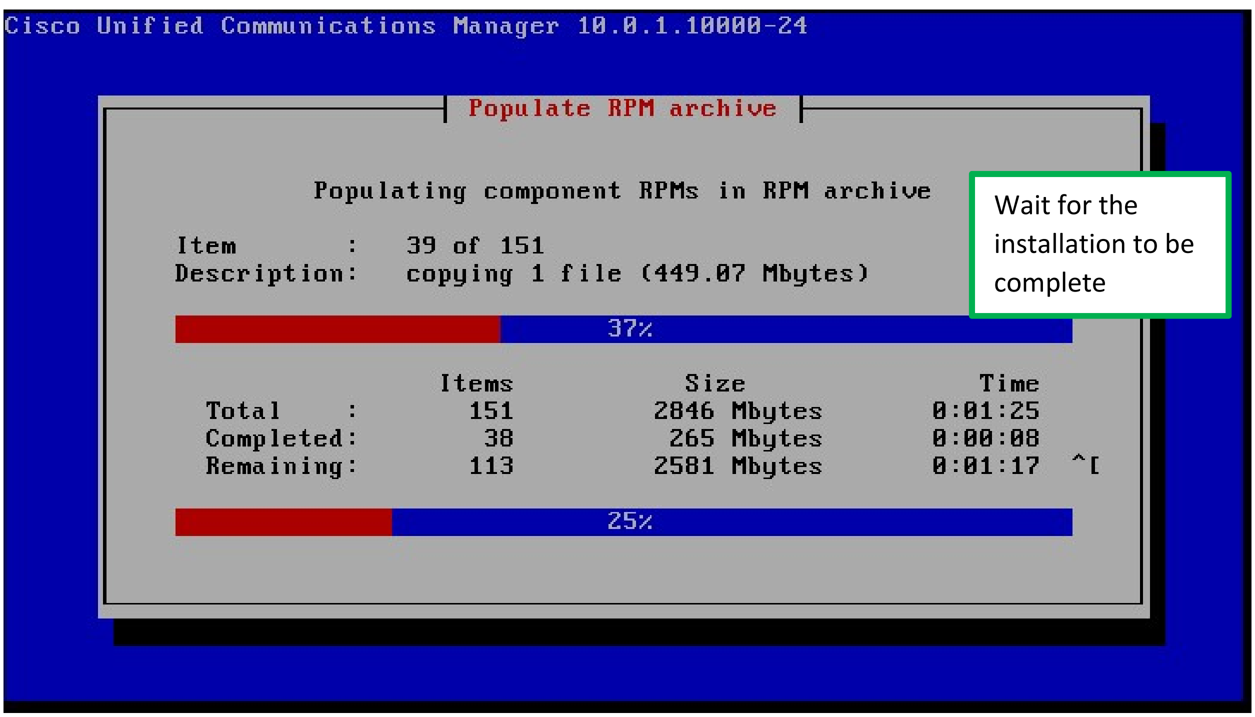

Cisco Unified Communications Manager 10.0.1.10000-24
Application User Configuration
Create a Username and Password then Click OK
The Application User username and password are used to log into the Application administrative webpage(s).
Application User Username
Application User Password
Confirm Application User Password
admin
OK
Back
Help
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

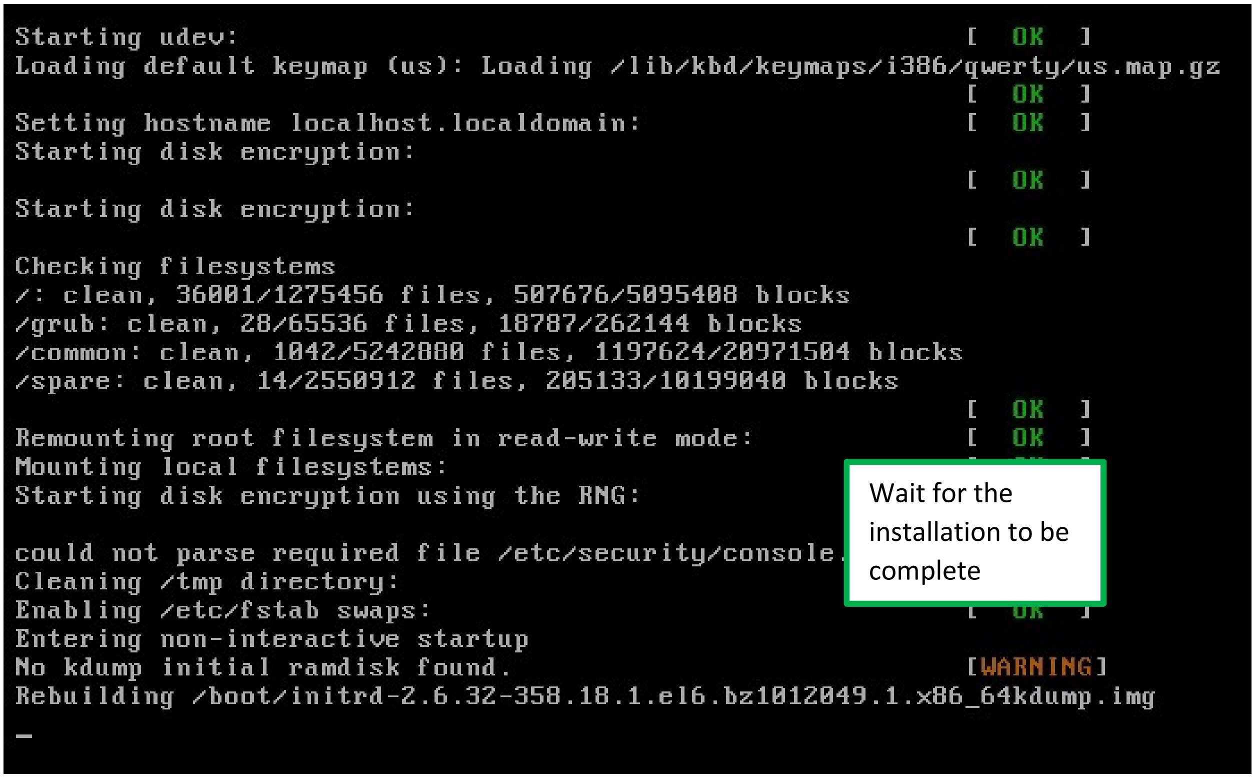

Cisco Unified Communications Manager 10.0.1.10000-24
Platform Configuration Confirmation
The Platform Configuration is complete.
Select OK to continue or Back to change the configuration.
Warning: Once you select OK, you will no longer be able to modify the Platform Configuration.
Click OK
OK
Back
Cancel
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

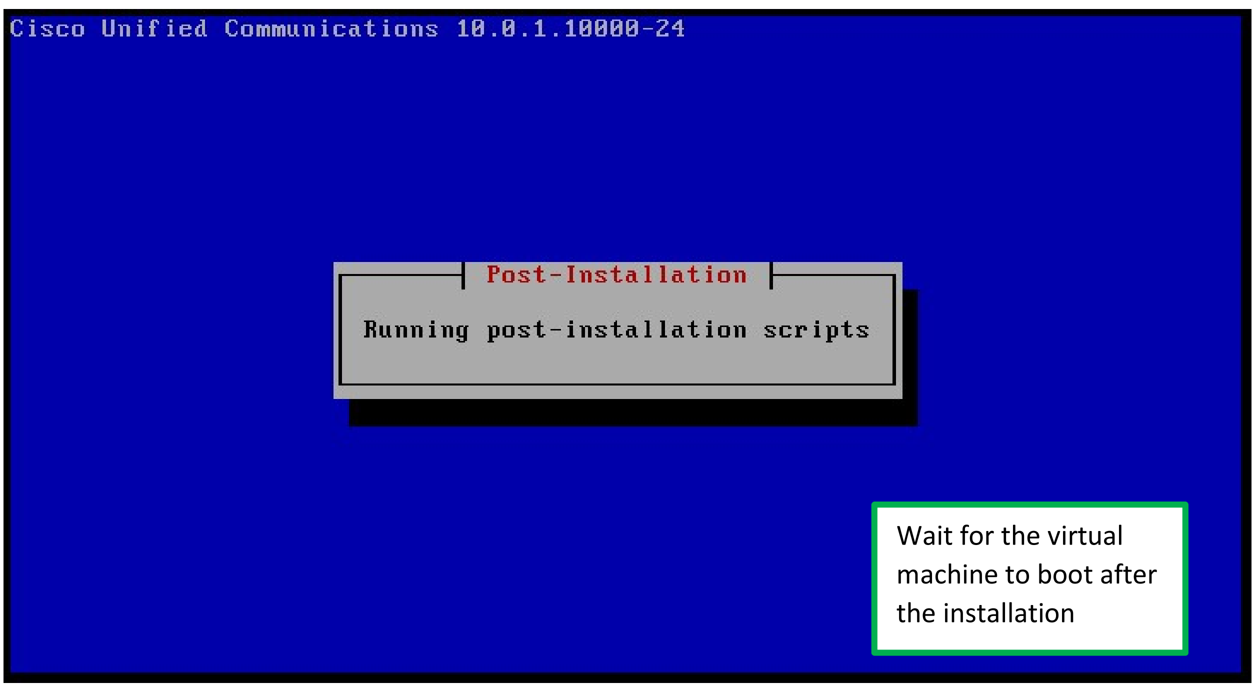

Cisco Unified Communications 10.0.1.10000-24
Package Installation
22%
Packages completed: 127 of 512
Installing vim-common-7.2.411-1.6.el6.x86_64 (16 MB)
The common files needed by any version of the VIM editor
Wait for the installation to be complete
<Tab>/<Shift,Tab> between elements | <Space> selects

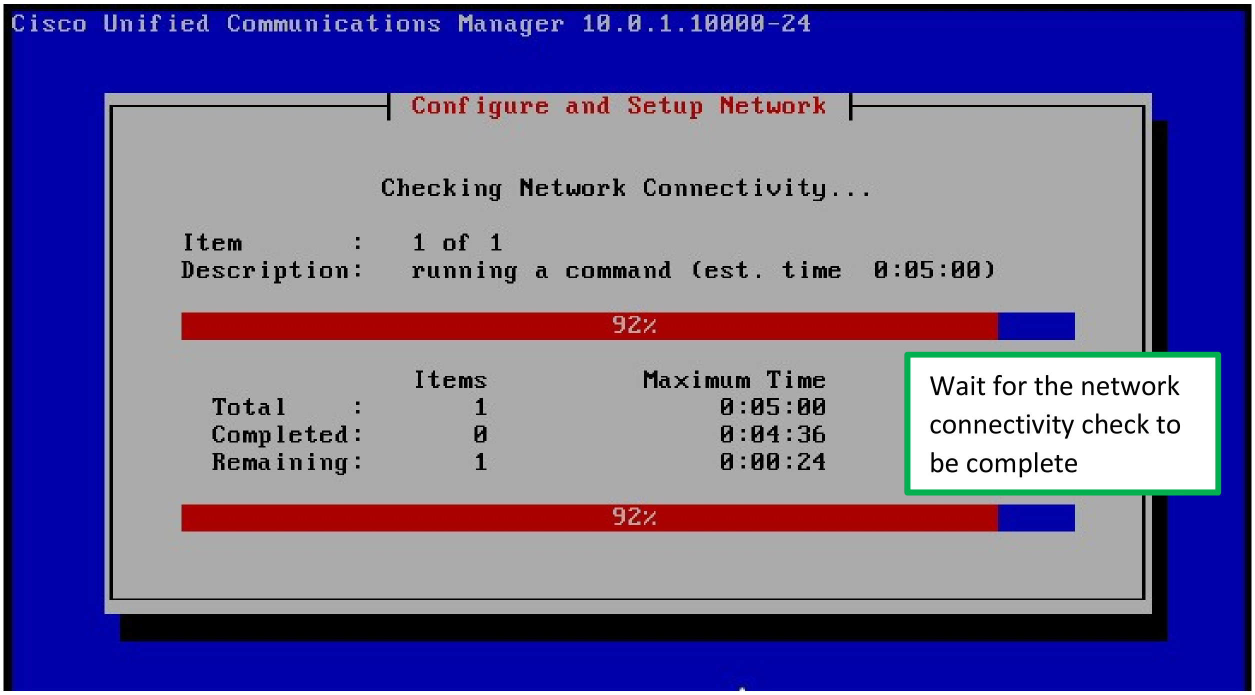

Cisco Unified Communications 10.0.1.10000-24
Formatting
Creating ext4 filesystem on /dev/sdb1
Wait for the installation to be complete
<Tab>/<Shift,Tab> between elements | <Space> selects

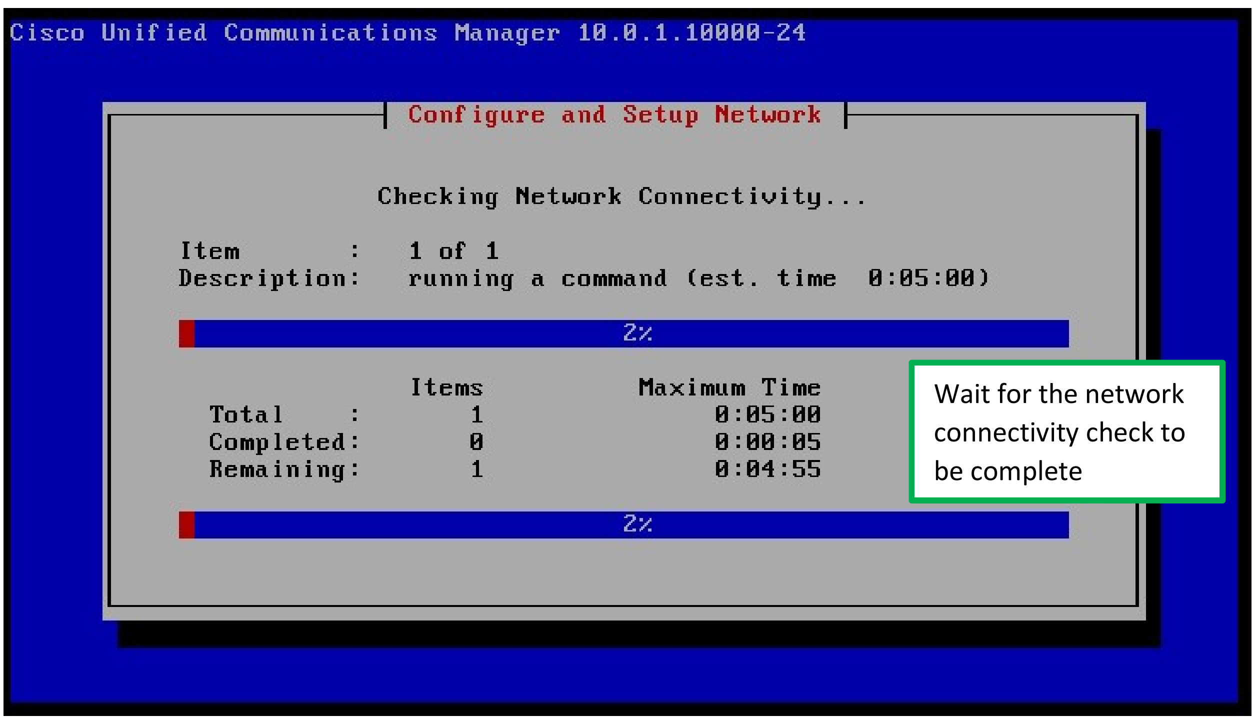

Cisco Unified Communications Manager 10.0.1.10000-24
Populate RPM archive
Populating hardware RPMs in RPM archive
Item : 8 of 8
Description: copying 1 file (3932.00 bytes)
100%
Items Size Time
Total : 8 3660124 bytes 0:00:00
Completed: 8 3660124 bytes 0:00:00
Remaining: 0 0 bytes 0:00:00
100%
"Populating hardware RPMs in RPM archive": Done
Wait for the installation to be complete

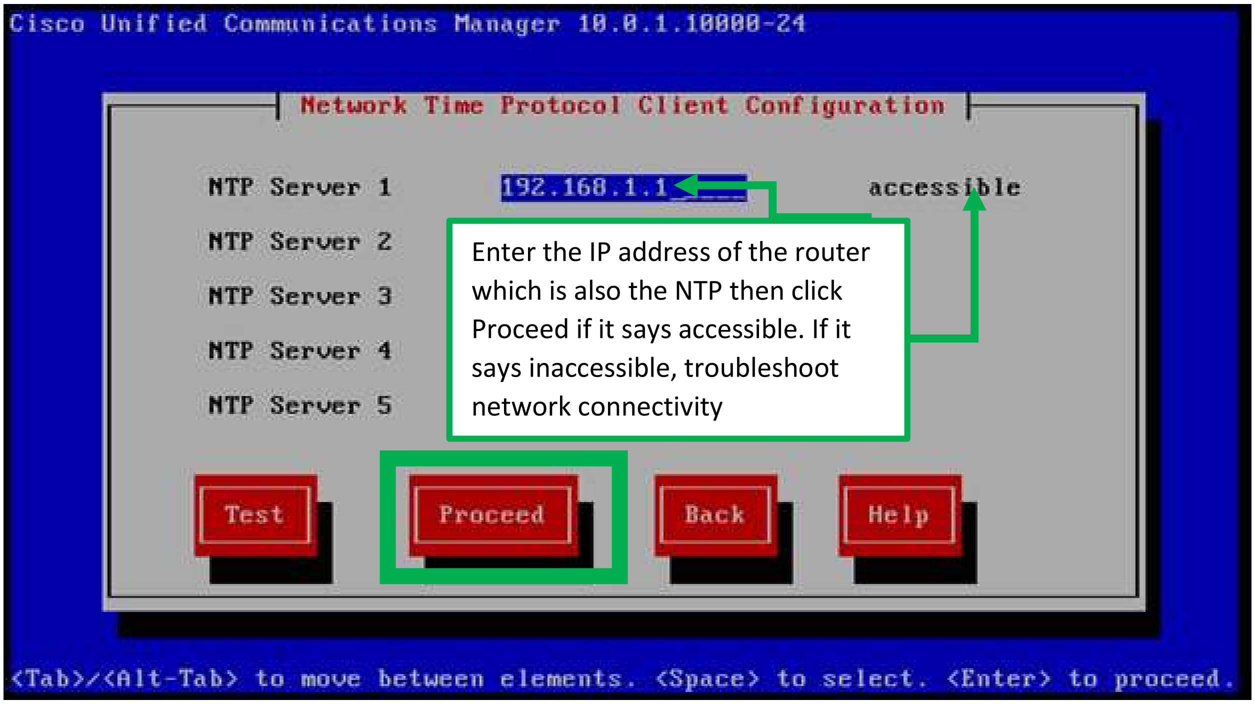

Cisco Unified Communications Manager 10.0.1.10000-24
Populate RPM archive
Populating component RPMs in RPM archive
Item : 39 of 151
Description: copying 1 file (449.07 Mbytes)
37%
Items Size Time
Total : 151 2846 Mbytes 0:01:25
Completed: 38 265 Mbytes 0:00:08
Remaining: 113 2581 Mbytes 0:01:17 ^[
25%
Wait for the installation to be complete

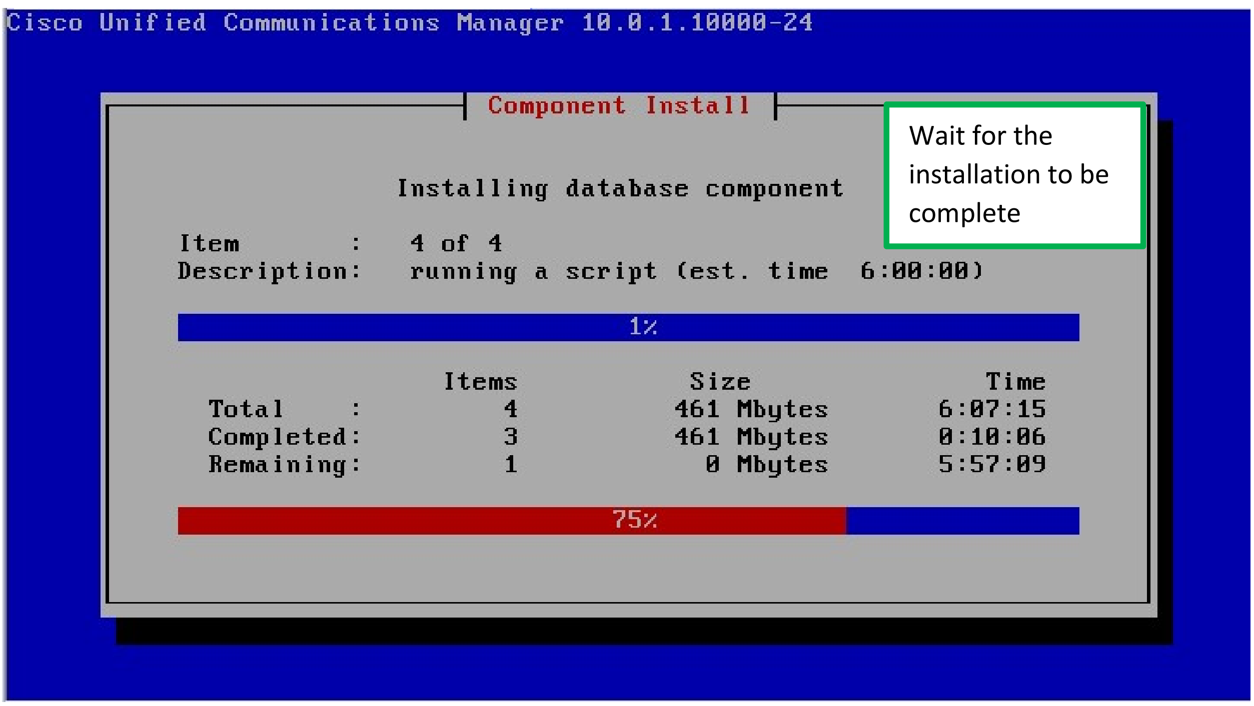

Starting udev: [OK]
Loading default keymap (us): Loading /lib/kbd/keymaps/i386/qwerty/us.map.gz
[OK]
Setting hostname localhost.localdomain: [OK]
Starting disk encryption:
[OK]
Starting disk encryption:
[OK]
Checking filesystems
/: clean, 36001/1275456 files, 507676/5095408 blocks
/grub: clean, 28/65536 files, 18787/262144 blocks
/common: clean, 1042/5242880 files, 1197624/20971504 blocks
/spare: clean, 14/2550912 files, 205133/10199040 blocks
[OK]
Remounting root filesystem in read-write mode: [OK]
Mounting local filesystems:
Starting disk encryption using the RNG:
could not parse required file /etc/security/console.
Cleaning /tmp directory:
Enabling /etc/fstab swaps:
Entering non-interactive startup
No kdump initial ramdisk found. [WARNING]
Rebuilding /boot/initrd-2.6.32-358.18.1.el6.bz1012049.1.x86_64kdump.img
Wait for the installation to be complete

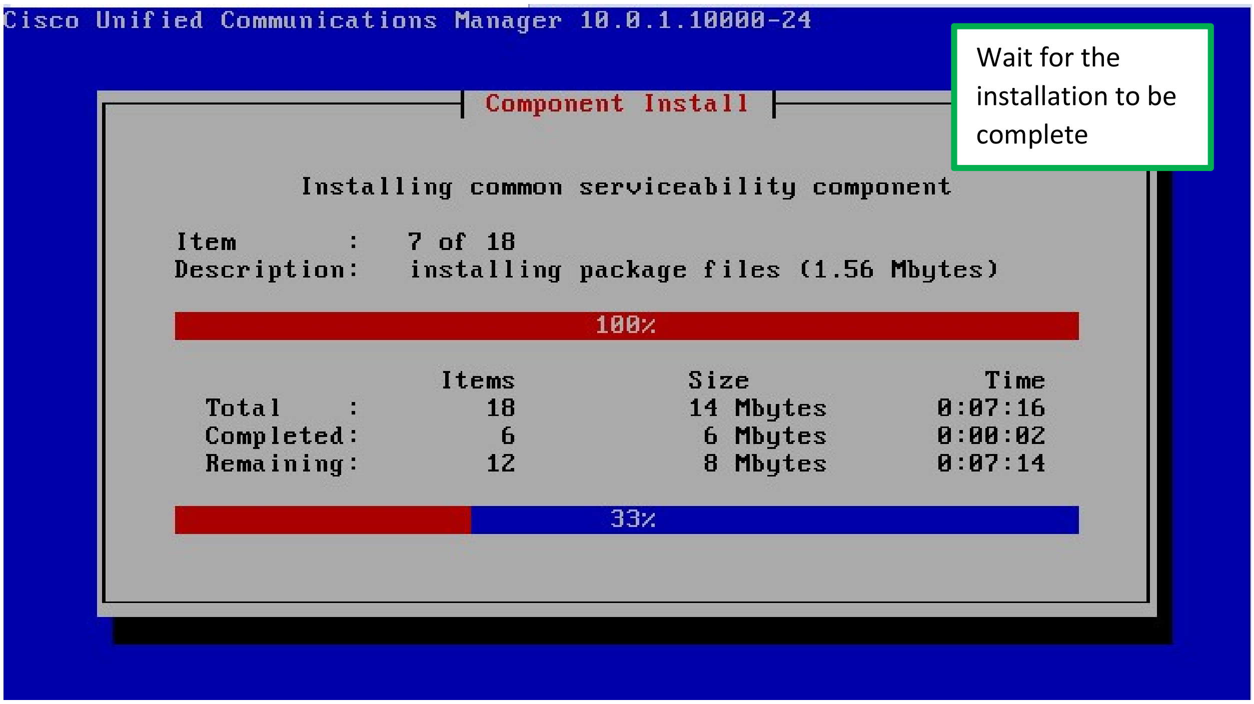

Cisco Unified Communications 10.0.1.10000-24
Post-Installation
Running post-installation scripts
Wait for the virtual machine to boot after the installation

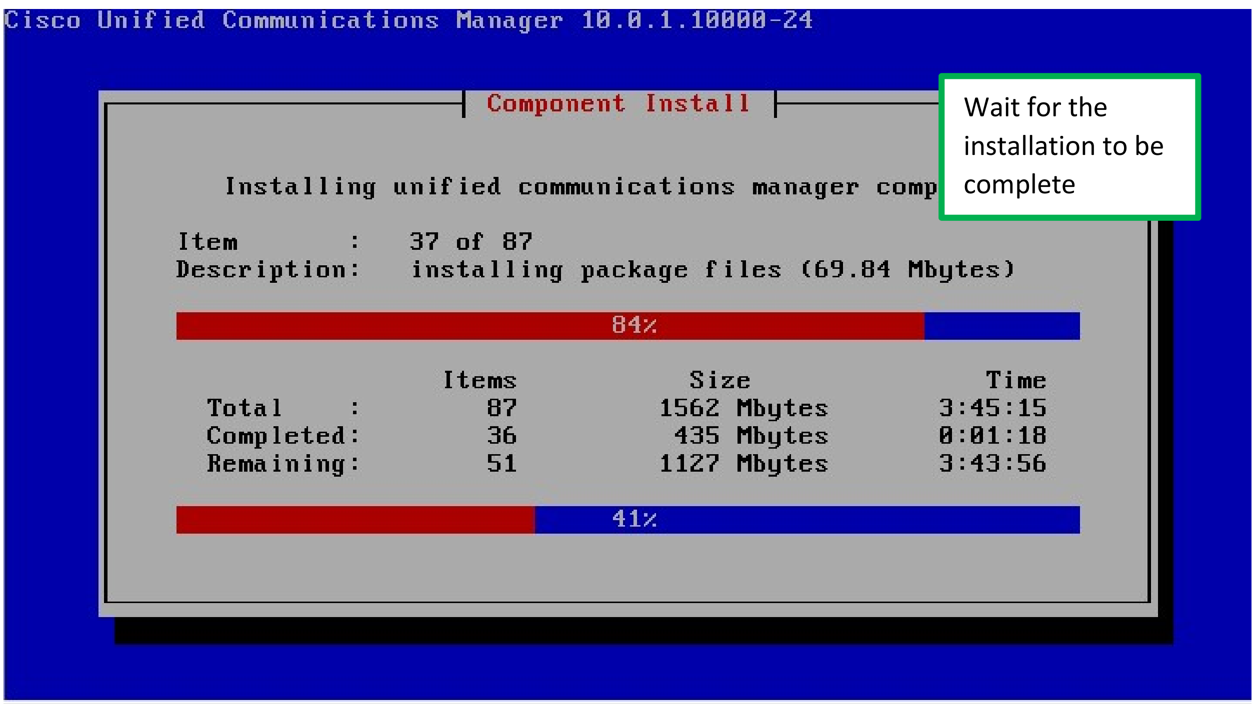

Cisco Unified Communications Manager 10.0.1.10000-24
Configure and Setup Network
Checking Network Connectivity...
Item : 1 of 1
Description: running a command (est. time 0:05:00)
92%
Items Maximum Time
Total : 1 0:05:00
Completed: 0 0:04:36
Remaining: 1 0:00:24
92%
Wait for the network connectivity check to be complete

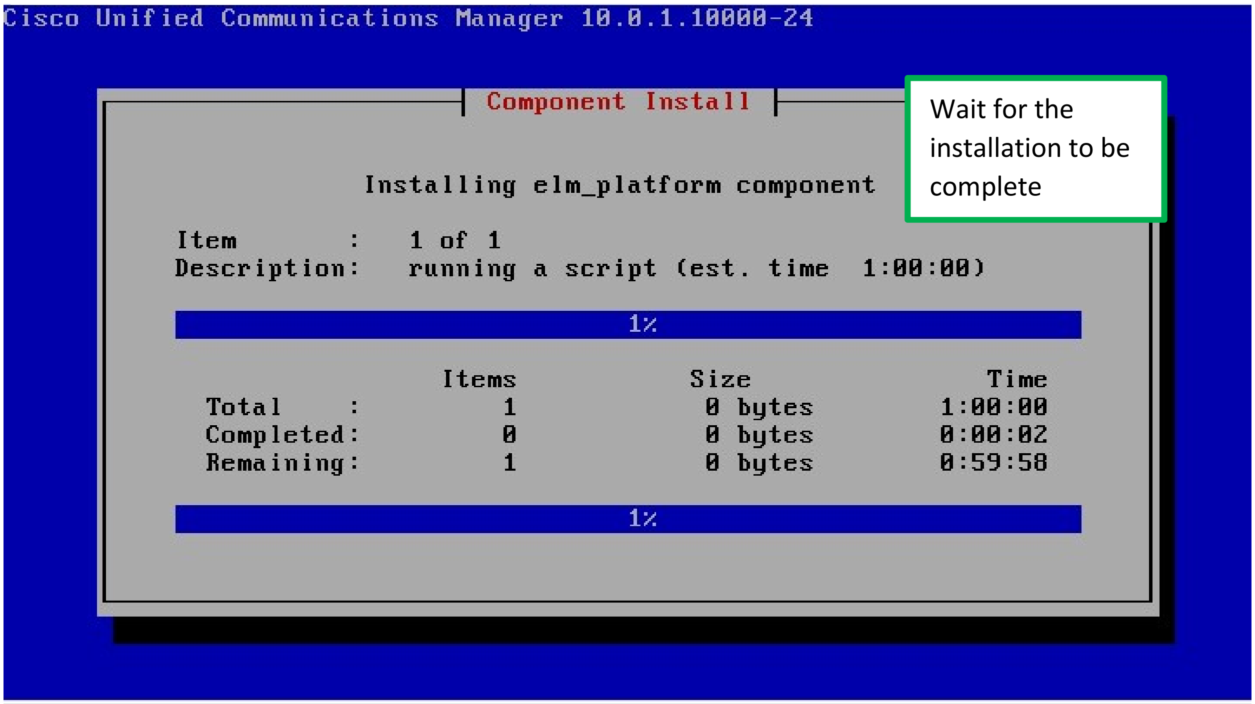

Cisco Unified Communications Manager 10.0.1.10000-24
Configure and Setup Network
Checking Network Connectivity...
Item : 1 of 1
Description: running a command (est. time 0:05:00)
2%
Items Maximum Time
Total : 1 0:05:00
Completed: 0 0:00:05
Remaining: 1 0:04:55
2%
Wait for the network connectivity check to be complete

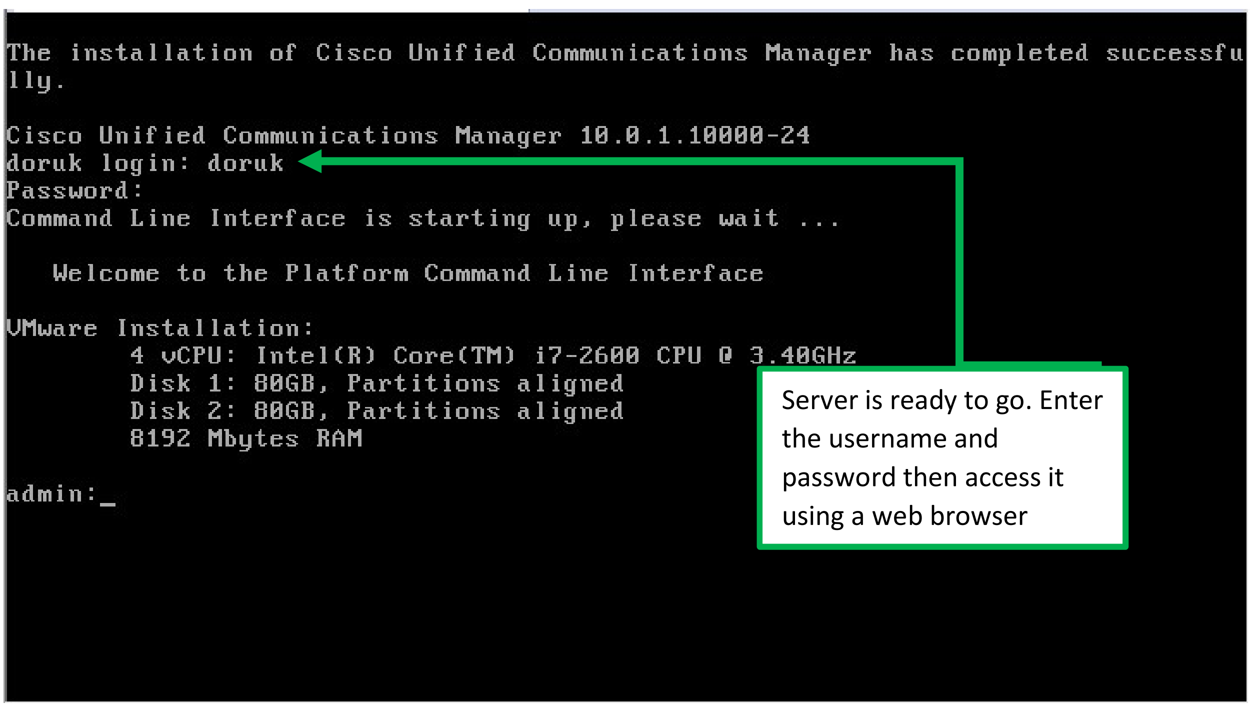

Cisco Unified Communications Manager 10.0.1.10000-24
Network Time Protocol Client Configuration
NTP Server 1
192.168.1.1
accessible
NTP Server 2
NTP Server 3
NTP Server 4
NTP Server 5
Enter the IP address of the router which is also the NTP then click Proceed if it says accessible. If it says inaccessible, troubleshoot network connectivity
Test
Proceed
Back
Help
<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

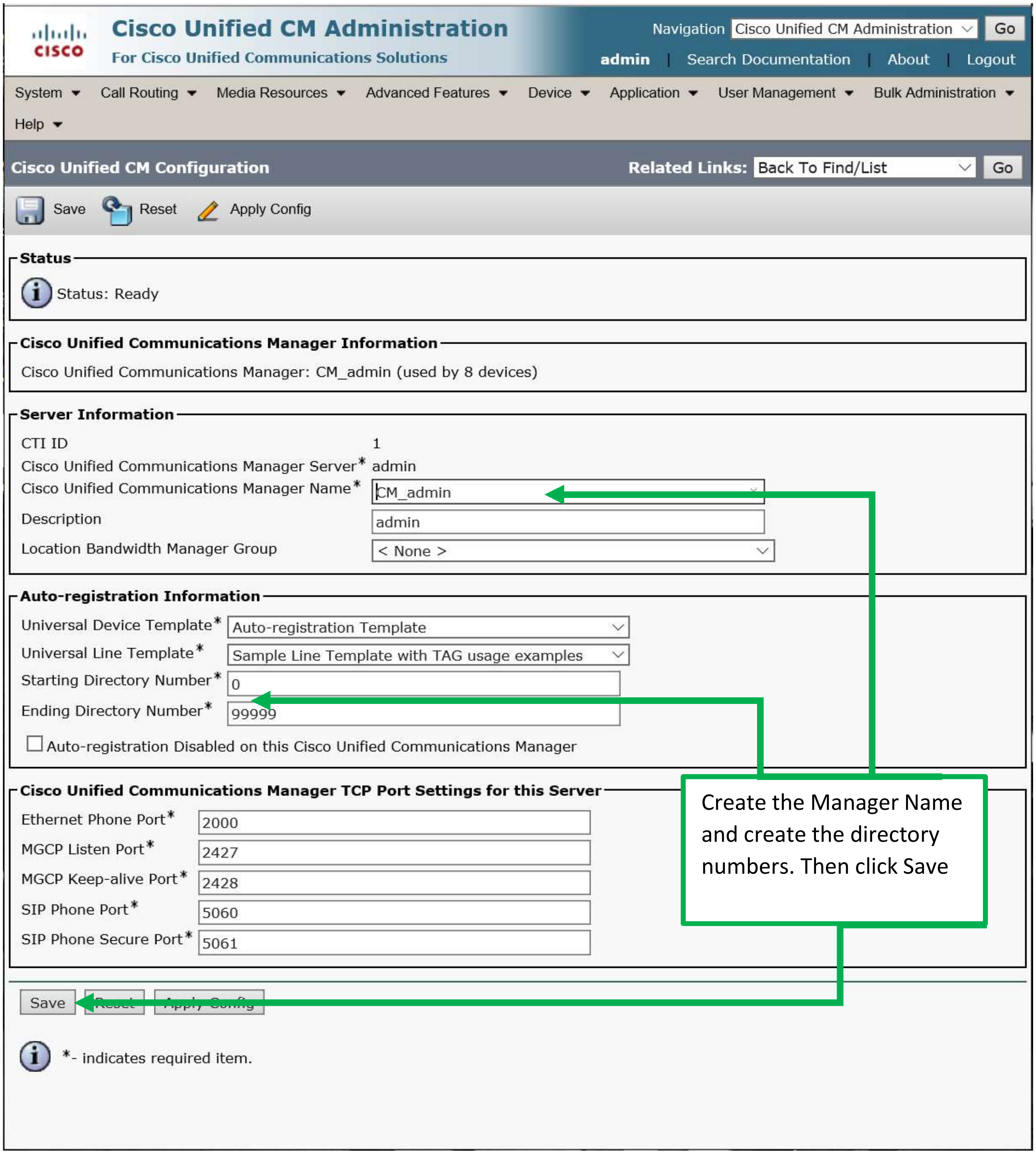

Cisco Unified Communications Manager 10.0.1.10000-24
Component Install
Wait for the installation to be complete
Installing database component
Item : 4 of 4
Description: running a script (est. time 6:00:00)
1%
Items Size Time
Total : 4 461 Mbytes 6:07:15
Completed: 3 461 Mbytes 0:10:06
Remaining: 1 0 Mbytes 5:57:09
75%


Cisco Unified Communications Manager 10.0.1.10000-24
Component Install
Installing common serviceability component
Item : 7 of 18
Description: installing package files (1.56 Mbytes)
100%
Items Size Time
Total : 18 14 Mbytes 0:07:16
Completed: 6 6 Mbytes 0:00:02
Remaining: 12 8 Mbytes 0:07:14
33%
Wait for the installation to be complete


Cisco Unified Communications Manager 10.0.1.10000-24
Component Install
Installing unified communications manager comp
Item : 37 of 87
Description: installing package files (69.84 Mbytes)
84%
Items Size Time
Total : 87 1562 Mbytes 3:45:15
Completed: 36 435 Mbytes 0:01:18
Remaining: 51 1127 Mbytes 3:43:56
41%
Wait for the installation to be complete

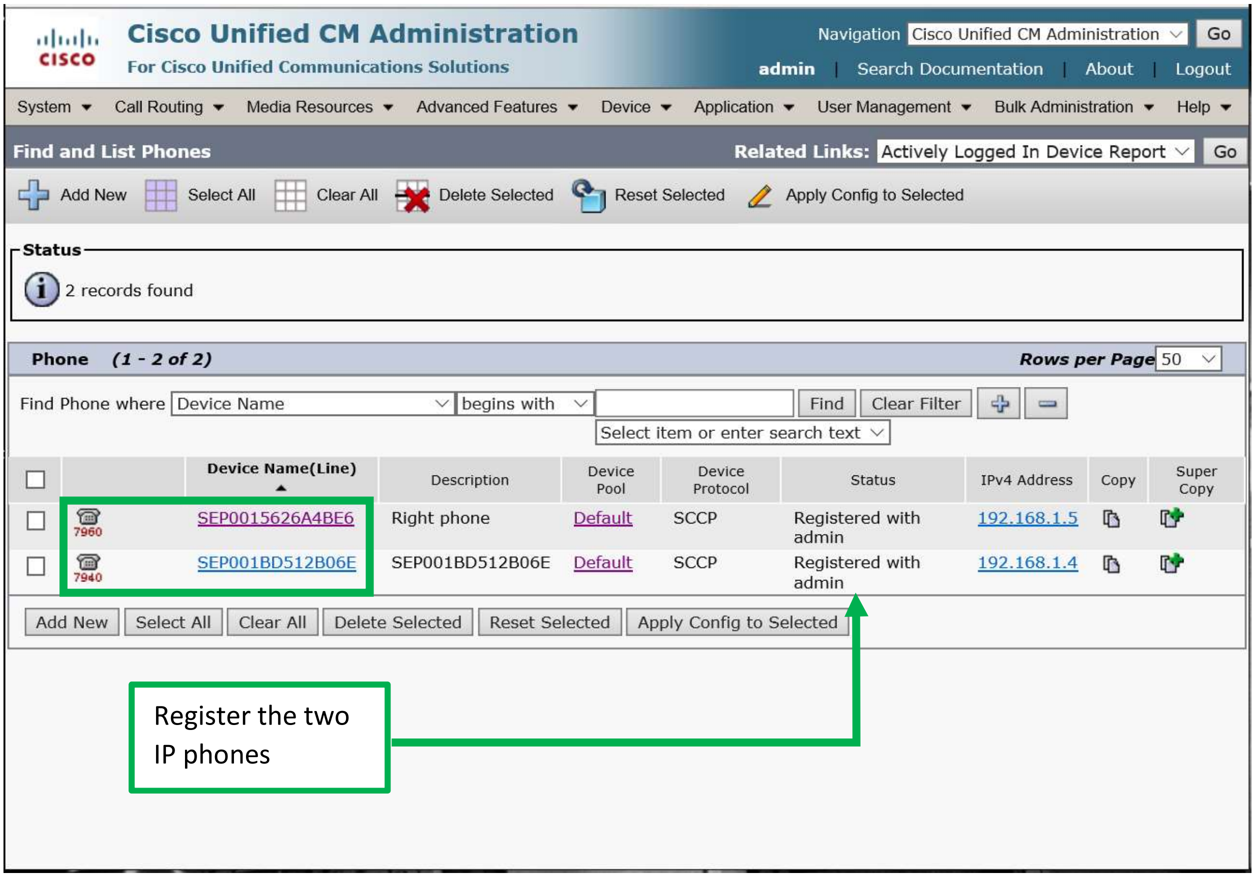

Cisco Unified Communications Manager 10.0.1.10000-24
Component Install
Installing elm_platform component
Item : 1 of 1
Description: running a script (est. time 1:00:00)
1%
Items Size Time
Total : 1 0 bytes 1:00:00
Completed: 0 0 bytes 0:00:02
Remaining: 1 0 bytes 0:59:58
1%
Wait for the installation to be complete

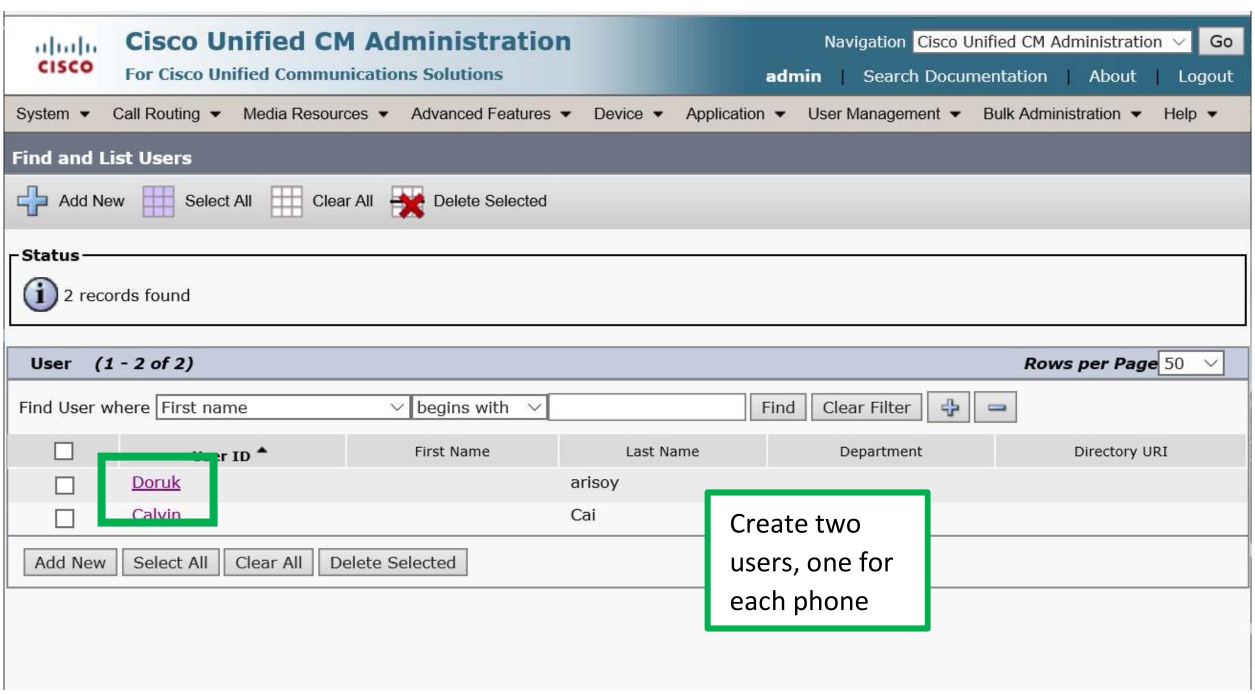

The installation of Cisco Unified Communications Manager has completed successfully.
Cisco Unified Communications Manager 10.0.1.10000-24
doruk login: doruk
Password:
Command Line Interface is starting up, please wait ...
Welcome to the Platform Command Line Interface
VMware Installation:
4 vCPU: Intel(R) Core(TM) i7-2600 CPU @ 3.40GHz
Disk 1: 80GB, Partitions aligned
Disk 2: 80GB, Partitions aligned
8192 Mbytes RAM
admin:_
Server is ready to go. Enter the username and password then access it using a web browser

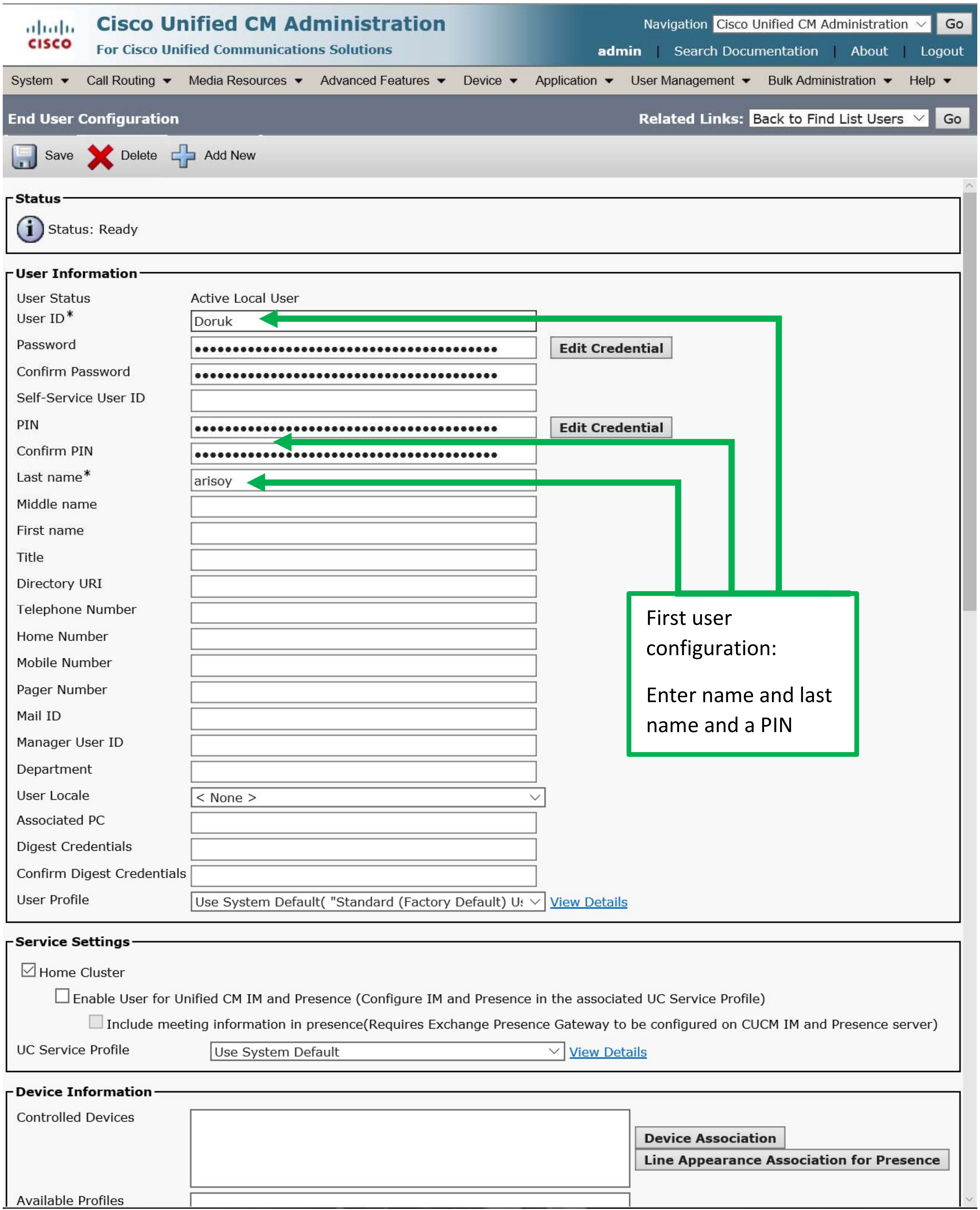


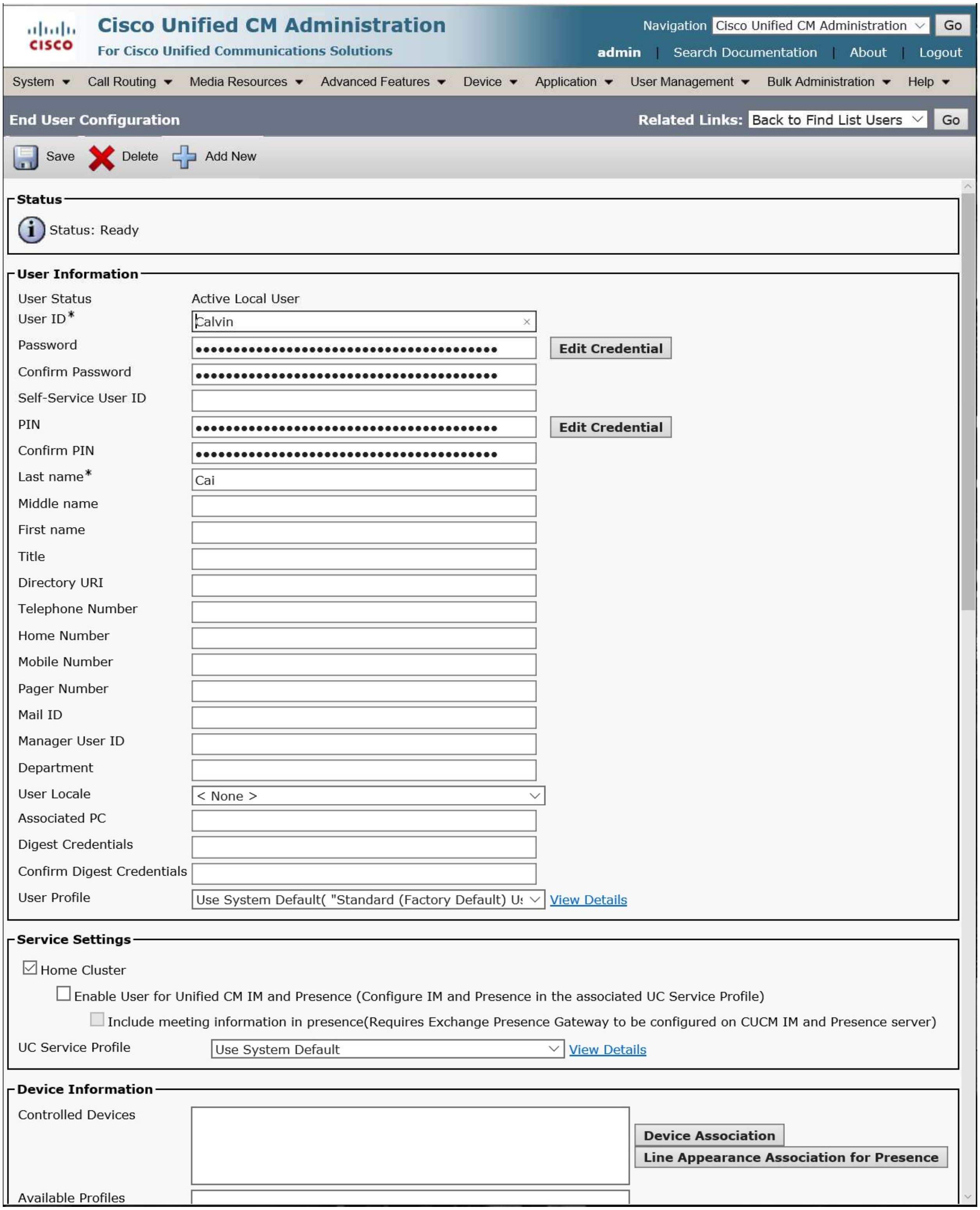
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Cisco Unified CM Configuration
Related Links: Back To Find/List Go
Save Reset Apply Config
Status
Status: Ready
Cisco Unified Communications Manager Information
Cisco Unified Communications Manager: CM_admin (used by 8 devices)
Server Information
CTI ID 1
Cisco Unified Communications Manager Server* admin
Cisco Unified Communications Manager Name* CM_admin
Description admin
Location Bandwidth Manager Group < None >
Auto-registration Information
Universal Device Template* Auto-registration Template
Universal Line Template* Sample Line Template with TAG usage examples
Starting Directory Number* 0
Ending Directory Number* 99999
Auto-registration Disabled on this Cisco Unified Communications Manager
Cisco Unified Communications Manager TCP Port Settings for this Server
Ethernet Phone Port* 2000
MGCP Listen Port* 2427
MGCP Keep-alive Port* 2428
SIP Phone Port* 5060
SIP Phone Secure Port* 5061
Create the Manager Name and create the directory numbers. Then click Save
Save Reset Apply Config
*- indicates required item.

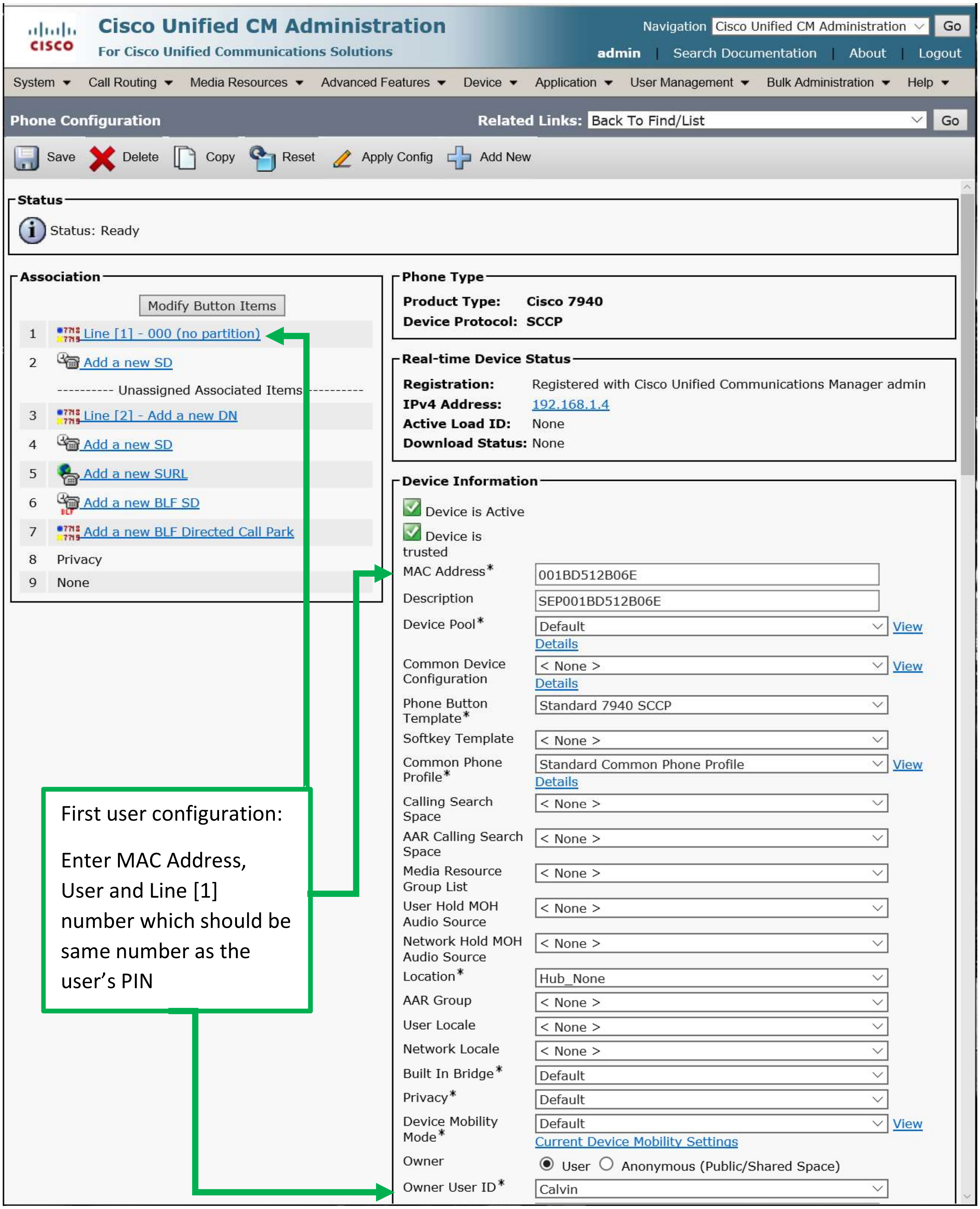

Save
Set to Default
Refresh
Status:
Ready
Select Server
Server*
admin--CUCM Voice/Video
Go
Check All Services
In the Cisco Unified OS Administration, enable all services
CM Services
Service Name
Activation Status
Cisco CallManager
Activated
Cisco Unified Mobile Voice Access Service
Activated
Cisco IP Voice Media Streaming App
Activated
Cisco CTIManager
Activated
Cisco Extension Mobility
Activated
Cisco Extended Functions
Activated
Cisco DHCP Monitor Service
Activated
Cisco Intercluster Lookup Service
Activated
Cisco Location Bandwidth Manager
Activated
Cisco Directory Number Alias Sync
Activated
Cisco Directory Number Alias Lookup
Activated
Cisco Dialed Number Analyzer Server
Activated
Cisco Dialed Number Analyzer
Activated
Cisco Tftp
Activated
CTI Services
Service Name
Activation Status
Cisco IP Manager Assistant
Activated
Cisco WebDialer Web Service
Activated
Self Provisioning IVR
Activated
CDR Services
Service Name
Activation Status
Cisco SOAP - CDRonDemand Service
Activated
Cisco CAR Web Service
Activated
Database and Admin Services
Service Name
Activation Status
Cisco Bulk Provisioning Service
Activated
Cisco AXL Web Service
Activated
Cisco UXL Web Service
Activated
Cisco TAPS Service
Activated
Performance and Monitoring Services
Service Name
Activation Status
Cisco Serviceability Reporter
Activated
Cisco CallManager SNMP Service
Activated
Security Services
Service Name
Activation Status
Cisco CTL Provider
Activated
Cisco Certificate Authority Proxy Function
Activated
Directory Services
Service Name
Activation Status
Cisco DirSync
Activated

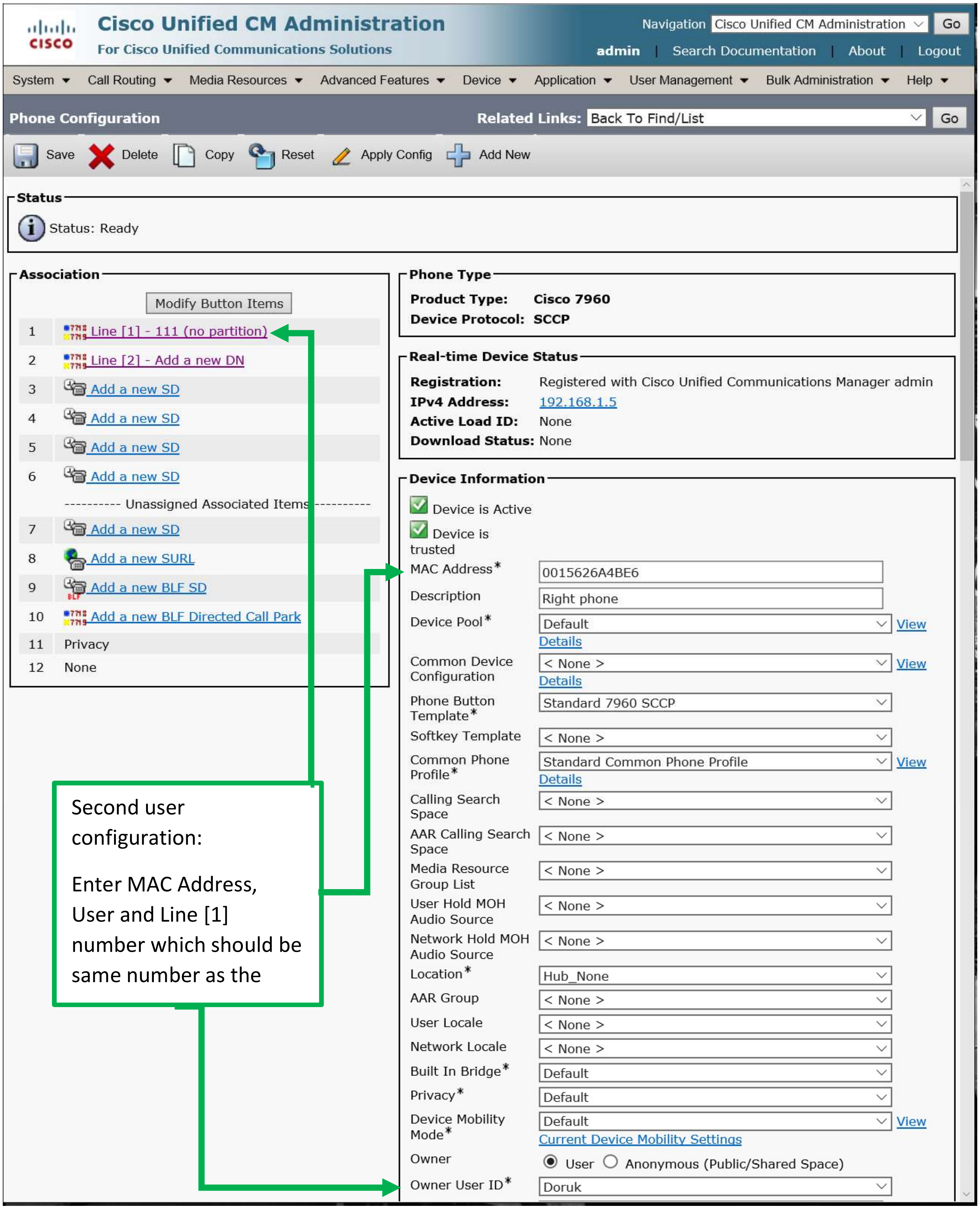

Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Find and List Phones
Related Links: Actively Logged In Device Report Go
Add New Select All Clear All Delete Selected Reset Selected Apply Config to Selected
Status
2 records found
Phone (1 - 2 of 2)
Rows per Page 50
Find Phone where Device Name begins with Find Clear Filter
Select item or enter search text
Device Name(Line) Description Device Pool Device Protocol Status IPv4 Address Copy Super Copy
7960 SEP0015626A4BE6 Right phone Default SCCP Registered with admin 192.168.1.5
7940 SEP001BD512B06E SEP001BD512B06E Default SCCP Registered with admin 192.168.1.4
Add New Select All Clear All Delete Selected Reset Selected Apply Config to Selected
Register the two IP phones


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Find and List Users
Add New Select All Clear All Delete Selected
Status
2 records found
User (1 - 2 of 2)
Rows per Page 50
Find User where First name begins with Find Clear Filter
First Name Last Name Department Directory URI
Doruk arisoy
Calvin Cai
Add New Select All Clear All Delete Selected
Create two users, one for each phone


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
End User Configuration
Related Links: Back to Find List Users Go
Save Delete Add New
Status
Status: Ready
User Information
User Status Active Local User
User ID* Doruk
Password
Edit Credential
Confirm Password
Self-Service User ID
PIN
Edit Credential
Confirm PIN
Last name* arisoy
Middle name
First name
Title
Directory URI
Telephone Number
Home Number
Mobile Number
Pager Number
Mail ID
Manager User ID
Department
User Locale < None >
Associated PC
Digest Credentials
Confirm Digest Credentials
User Profile Use System Default("Standard (Factory Default) U: View Details
First user configuration:
Enter name and last name and a PIN
Service Settings
Home Cluster
Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)
Include meeting information in presence(Requires Exchange Presence Gateway to be configured on CUCM IM and Presence server)
UC Service Profile Use System Default View Details
Device Information
Controlled Devices
Device Association
Line Appearance Association for Presence
Available Profiles


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
End User Configuration
Related Links: Back to Find List Users Go
Save Delete Add New
Status
Status: Ready
User Information
User Status Active Local User
User ID* Calvin
Password
Edit Credential
Confirm Password
Self-Service User ID
PIN
Edit Credential
Confirm PIN
Last name* Cai
Middle name
First name
Title
Directory URI
Telephone Number
Home Number
Mobile Number
Pager Number
Mail ID
Manager User ID
Department
User Locale < None >
Associated PC
Digest Credentials
Confirm Digest Credentials
User Profile Use System Default("Standard (Factory Default) U: View Details
Service Settings
Home Cluster
Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)
Include meeting information in presence(Requires Exchange Presence Gateway to be configured on CUCM IM and Presence server)
UC Service Profile Use System Default View Details
Device Information
Controlled Devices
Device Association
Line Appearance Association for Presence
Available Profiles


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Phone Configuration
Related Links: Back To Find/List Go
Save Delete Copy Reset Apply Config Add New
Status
Status: Ready
Association
Modify Button Items
1 Line [1] - 000 (no partition)
2 Add a new SD
---------- Unassigned Associated Items ----------
3 Line [2] - Add a new DN
4 Add a new SD
5 Add a new SURL
6 Add a new BLF SD
7 Add a new BLF Directed Call Park
8 Privacy
9 None
Phone Type
Product Type: Cisco 7940
Device Protocol: SCCP
Real-time Device Status
Registration: Registered with Cisco Unified Communications Manager admin
IPv4 Address: 192.168.1.4
Active Load ID: None
Download Status: None
Device Information
Device is Active
Device is trusted
MAC Address* 001BD512B06E
Description SEP001BD512B06E
Device Pool* Default View Details
Common Device Configuration < None > View Details
Phone Button Template* Standard 7940 SCCP
Softkey Template < None >
Common Phone Profile* Standard Common Phone Profile View Details
Calling Search Space < None >
AAR Calling Search Space < None >
Media Resource Group List < None >
User Hold MOH Audio Source < None >
Network Hold MOH Audio Source < None >
Location* Hub_None
AAR Group < None >
User Locale < None >
Network Locale < None >
Built In Bridge* Default
Privacy* Default
Device Mobility Mode* Default View Current Device Mobility Settings
Owner User Anonymous (Public/Shared Space)
Owner User ID* Calvin
First user configuration:
Enter MAC Address, User and Line [1] number which should be same number as the user's PIN

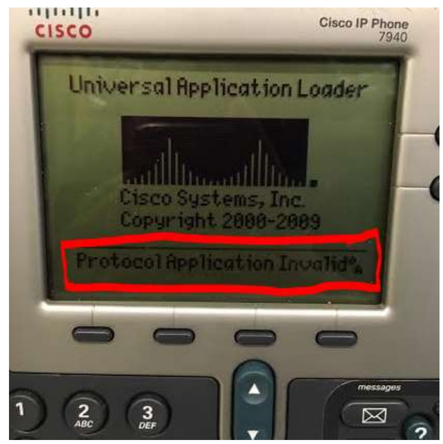


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Phone Configuration
Related Links: Back To Find/List Go
Save Delete Copy Reset Apply Config Add New
Status
Status: Ready
Association
Modify Button Items
1 Line [1] - 111 (no partition)
2 Line [2] - Add a new DN
3 Add a new SD
4 Add a new SD
5 Add a new SD
6 Add a new SD
---------- Unassigned Associated Items ----------
7 Add a new SD
8 Add a new SURL
9 Add a new BLF SD
10 Add a new BLF Directed Call Park
11 Privacy
12 None
Phone Type
Product Type: Cisco 7960
Device Protocol: SCCP
Real-time Device Status
Registration: Registered with Cisco Unified Communications Manager admin
IPv4 Address: 192.168.1.5
Active Load ID: None
Download Status: None
Device Information
Device is Active
Device is trusted
MAC Address* 0015626A4BE6
Description Right phone
Device Pool* Default View Details
Common Device Configuration < None > View Details
Phone Button Template* Standard 7960 SCCP
Softkey Template < None >
Common Phone Profile* Standard Common Phone Profile View Details
Calling Search Space < None >
AAR Calling Search Space < None >
Media Resource Group List < None >
User Hold MOH Audio Source < None >
Network Hold MOH Audio Source < None >
Location* Hub_None
AAR Group < None >
User Locale < None >
Network Locale < None >
Built In Bridge* Default
Privacy* Default
Device Mobility Mode* Default View
Current Device Mobility Settings
Owner User Anonymous (Public/Shared Space)
Owner User ID* Doruk
Second user configuration:
Enter MAC Address, User and Line [1] number which should be same number as the

Problems

Our first problem started with the finding the right version of the server. We tried creating a virtual machine from all three software that was given to us but none of them worked. We lost plenty of time waiting for them to load just to learn that they are not compatible with our virtual machine. We then discovered that we were also given templates to create the virtual machine and eventually the server. We had a couple of different templates we finally found the right one but it wasted our time. Template then asked for us to choose from the 3 soft wares that were given to us. We tried all three and finally one of them did not give a “Halt” message after downloading for almost hours. We finished the creation of the virtual machine and were finally able to move on to the installation of the server.

The only problem we came across during the installation was that our NTP server and the router were inaccessible and we were not able to continue the installation. We went back to the router and looked at the configurations but we couldn’t find any problem and our NTP server was working just fine. We decided to reset the port that is going to the virtual machine and the virtual machine itself which took a lot of time. After we reset those two we were finally able to get the message from the virtual machine that the NTP server was accessible. However resetting the virtual machine took really long and wasted a whole day.



After almost a week of work, we finally managed to install the server and access it but we were facing a big problem now. One of our phones didn’t have image or any software in it. We decided that we needed to download new image on the phone. We researched online, and downloaded the software but then we had to somehow get it on to the phone using the server. We researched that the software upload or update can only be done using the server user interface but our server wasn’t able to see the phone. We tried to solve that problem for couple of days but we couldn’t get our server to see the phone. We finally decided that we weren’t going to have enough time to actually do the lab and decided to get a new phone that had image and software on it.

As we were trying to fix the phone without the software, our virtual machine suddenly stopped responding and our server crashed. We restarted the virtual machine but the server was still not responding. We no other option but to recreate the virtual machine and install the software again. We lost a day on installing the server all over again.

After our server was running again and both of our phones working properly, we finally moved onto configuring them. Our phones both got IP address and we were able to ping both but they were not being registered. We tried everything from checking the software to deleting and adding the phones again to the server’s system. After looking around everywhere, we realized that the problem was with our TFTP server command that was set under the DHCP on the router. The IP address we set for the TFTP server was not an IP address from our network. We deleted that command and set it again so the TFTP server belonged to the same network as everything else. After doing that our phones were finally registered and were able to call and talk to one another.

Conclusion

Voice over IP was a completely new topic for me. I have never configured it before. I learned how it worked during CCNA Routing & Switching course but configuring it for the first time was a completely different experience. It is not easy as it sounds. We had a hard time finding resources on how to do it and came across quite a few problems. Besides configuring VoIP and NTP, I learned how to trouble shoot new and different problems. I think I learned how to configure a really important protocol that can be used in any kind of business and small-office home-office network and I believe that I am going to use this knowledge many times I the future.

VoIP part 2

Purpose

The first purpose of this lab is to set up custom ring tone and hold on music. The second purpose of this lab is dial out and call a cell phone using and IP phones.

Background information

On IP phones, a ringtone is a brief audio file played to indicate an incoming call. A contemporary ringtone might consist of several bars of a familiar musical tune. IP phones and the CUCM server doesn't work with any type of music format. It has to be in a specific format. For example, the ring tone has to be in .raw file before it's sent to the IP phones from the CUCM server.

Music on hold (MOH) is the business practice of playing recorded music to fill the silence that would be heard by telephone callers who have been placed on hold. It is especially common in situations involving customer service. In order to upload a music, one has to convert the .mp3 file into .wav format so that it can play on hold. The IP phones can only play .wav files, so it curtails that the uploaded file is converted to .wav format.

Server and the IP phones are people who can only speak one language. One can communicate with a monolingual person with only one language. In this case the server and the phones are monolingual and in order to give them a ring tone or a hold on music one has to speak the same language that they are speaking. In this case there are no languages but there are file formats. The music that is being uploaded to the network has to be the same format so that the system can understand it and play the song.

The Voice over IP network we created was internal, meaning that the phones in the network could only call the other IP phones in the same network. In order to be able to call any phone number in the world, we had to be able to dial-out of the network. The traditional phone lines use analog line while our network uses digital. So we need a router that can convert digital line into analog. One needs to use a router that acts like a H323 gateway in order to make that conversion. A router has to follow the H323 standards in order to be a H323 gateway.

H.323 is a standard approved by the International Telecommunication Union to promote compatibility in videoconference transmissions over IP networks. H.323 was originally promoted as a way to provide consistency in audio, video and data packet transmissions in the event that a local area network (LAN) did not provide guaranteed service quality (QoS). It is now considered to be the standard for interoperability in audio, video and data transmissions as well as Internet phone and voice-over-IP (VoIP) because it addresses call control and management for both point-to-point and multipoint conferences as well as gateway administration of media traffic, bandwidth and user participation.

There are specific ports that have to be on a H323 gateway. They are either FXO or FXS ports and it is critical to connect the phone line to the right port. Foreign exchange subscriber (FXS) interface is the port that actually delivers the analog line to the subscriber. In other words it is the "plug on the wall" that delivers a dial tone, battery current and ring voltage. Foreign exchange office (FXO) interface is the port that receives the analog line. It is the plug on the phone or fax machine, or the plug(s) on your analog phone system. It delivers an on-hook/off-hook indication (loop closure). Since the FXO port is attached to a device, such as a fax or phone, the device is often called the "FXO device". In this lab we used FXS ports to attach the phone line to the router.

Lab Summary

In this lab, we had our server pre-installed from the previous lab and had two IP phones configured. The two phones were able to call each other but we had to change the ring tone and add a hold on music. To do that we first had to download .wav files from the internet to upload to the server so the phones. We used the program Audacity and opened the files there. Changed the quality which is determined by Hertz and adjusted the sample numbers. Then we exported the ringtone as a special uncompressed file. That uncompressed file head a RAW (header-less) header and a U-Law encoding. In the screen that popped up we removed all tags. So we saved the file in .raw format this way. Then we went to the CUCM server, go to the “TFTP File Management” section and uploaded the .raw file that we created using Audacity. Then we opened up Tftpd64 on the PC and configured it a client. While we do this, the server transferred the .raw file into an .xml file and we got that on our PC using TFTP. We opened the file on a WordPad, just kept the things between <CiscoIPPhoneRingList> and deleted everything else. Then we saved the file and uploaded it back to CUCM. After the file was finally converted and uploaded to the server we then sent it to the IP phones using TFTP. When the file was sent, we went to the IP phones and selected the ring tone.

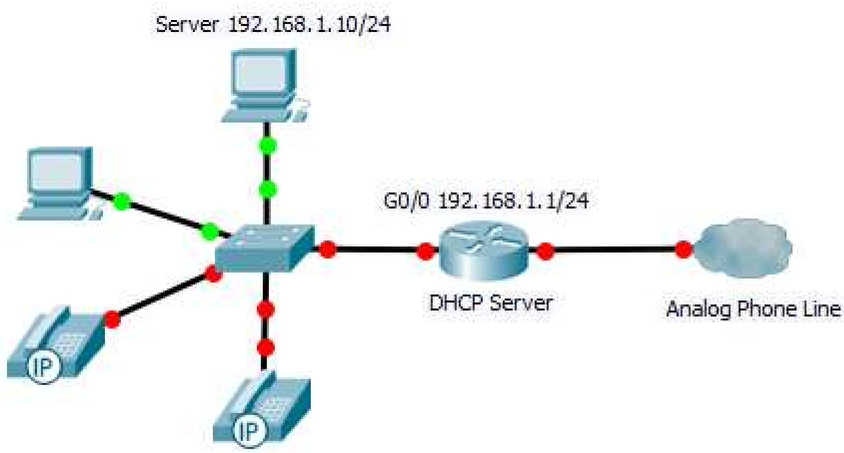
For the hold on music, the idea was similar. We first converted the .mp3 files into .wav files using Audacity and then uploaded the files to the CUCM server from the “Music on Hold Audio File Manager”. After we did that, we went to the “Music on Hold Audio Source” and defined which phones were going to get the music on hold audio and added the source file name. Then we reset the phones and the music on hold was good to go.

Then we moved on to the final step of the lab which is to dial out and call a cell phone. In order to do this we needed to use the router with the voice ports which are RJ11 ports. We first enabled VoIP on the router, set up a calling patter and assigned that patter to the voice port that was connected to the analog line. Then we set up the server. We first added the router as a H323 gateway and created the same call router we did on the router. At the end we were able to dial out to any phone number in the world.

Lab Commands

`voice service voip`	This command enables the VoIP service over the router and goes in to the VoIP configuration mode.
`allow-connections h323 to h323`	This command allows connections between H.323 endpoints which are the routers that are responsible for VoIP.
`h323-gateway voip interface`	This command is entered under the interface and it identifies that interface as a VoIP gateway interface that goes to a network that uses VoIP.
`h323-gateway voip bind srcaddr` *`192.168.1.1`*	This command is also entered under the interface and is used to specify the gateway address for VoIP of the interface which is the same as the interface’s original IP address.
`dial-peer voice` *`1`* **`pots`**	This command enters to the dial-peer mode, to set dialing pattern and ports for router to use VoIP at.
`destination-pattern` *`9..........`*	This command specifies telephone number to match for a dial peer.
`port` *`0/3/0`*	This command assigns this port to the dial-peer and use the dialing pattern from that port.
`forward-digits all`	This command implies that all the digits of the called party number are sent to analog phone line connection.

Network Diagram



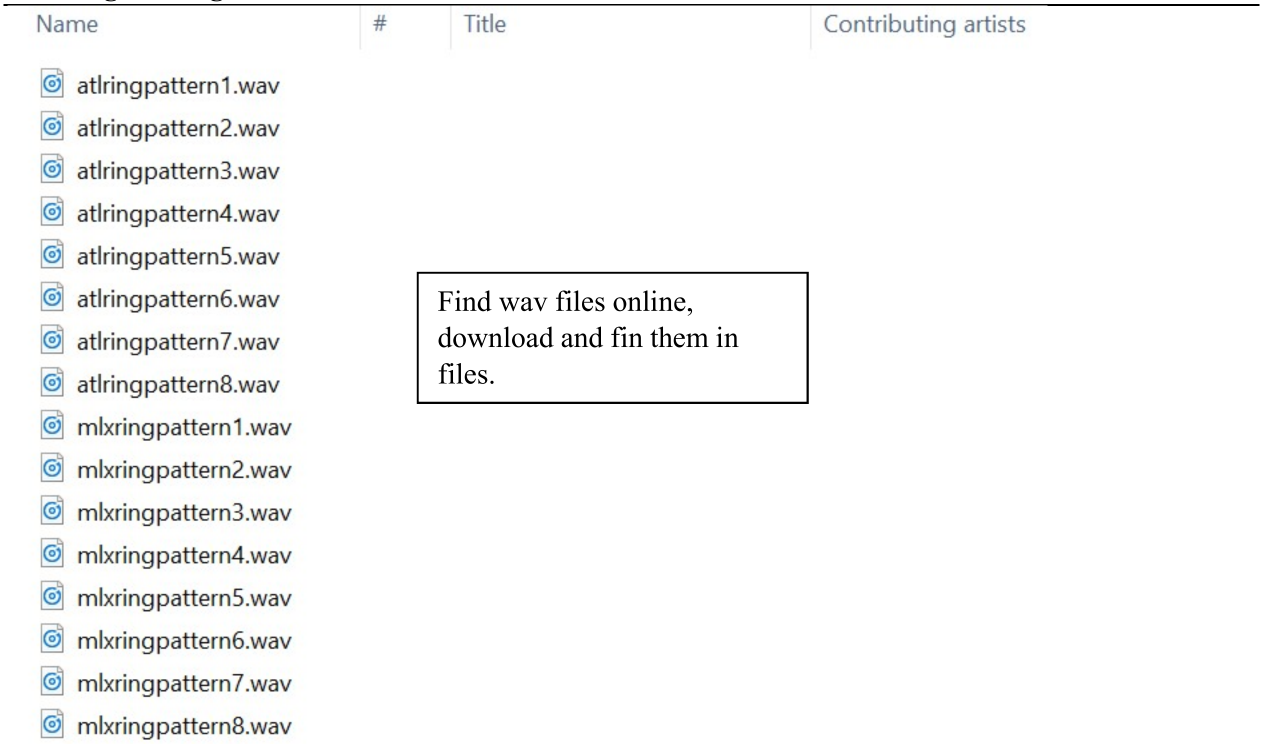
Configuration

DHCPserver
show run

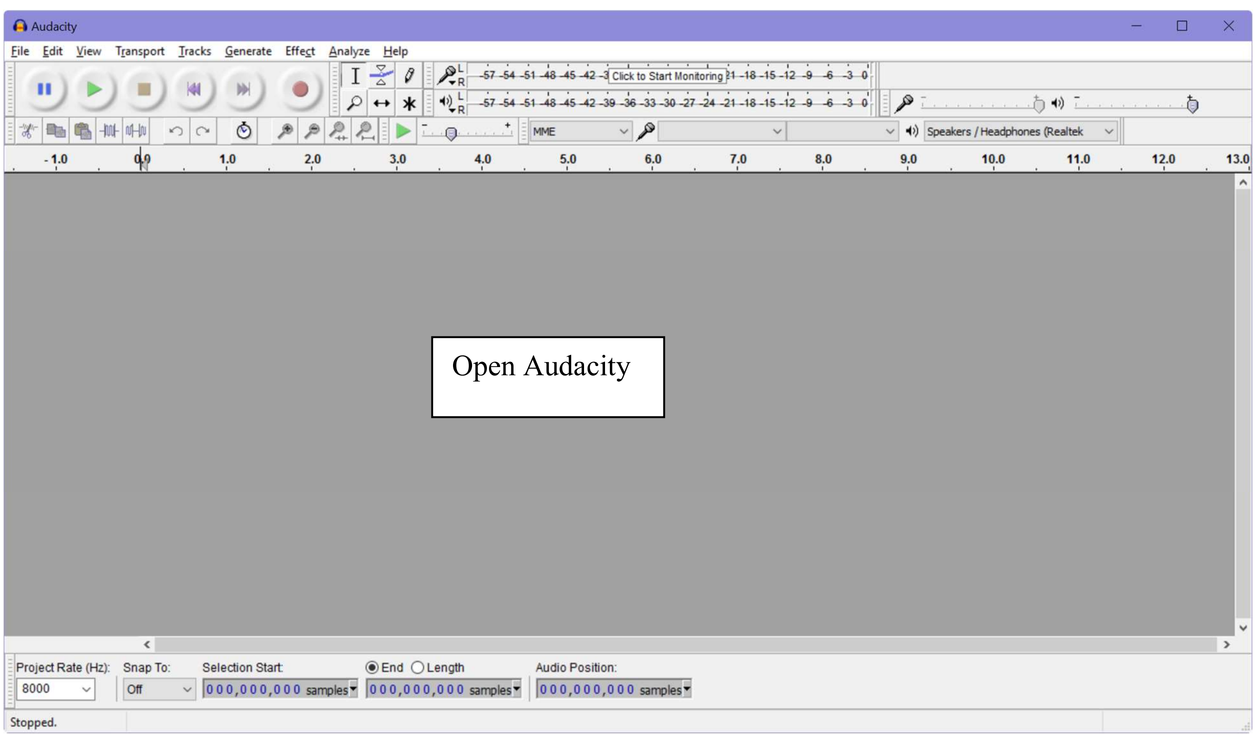
```
Current configuration : 1845 bytes
! Last configuration change at 00:05:09 UTC Thu Dec 29 2011
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname DHCPserver
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
memory-size iomem 10
no network-clock-participate slot 1
ip subnet-zero
ip cef
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.1.7 192.168.1.11
ip dhcp pool nam
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.1
   dns-server 192.168.1.1
   domain-name calvin.com
   option 150 ip 192.168.1.10
ip domain name calvin.com
voice-card 0
 no dspfarm
voice-card 1
 no dspfarm
voice service voip
 allow-connections h323 to h323
interface FastEthernet0/0
```

```
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 h323-gateway voip bind srcaddr 192.168.1.1
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet0/1/0
interface FastEthernet0/1/1
interface FastEthernet0/1/2
interface FastEthernet0/1/3
interface FastEthernet0/1/4
interface FastEthernet0/1/5
interface FastEthernet0/1/6
interface FastEthernet0/1/7
interface FastEthernet0/1/8
interface Serial0/2/0
 no ip address
 shutdown
interface Vlan1
 no ip address
ip classless
ip http server
no ip http secure-server
tftp-server flash:calvin
control-plane
voice-port 0/3/0
voice-port 0/3/1
voice-port 0/3/2
voice-port 0/3/3
voice-port 1/0/0
voice-port 1/0/1
dial-peer voice 1 pots
 destination-pattern 9..........
 port 0/3/0
 forward-digits all
gateway
 timer receive-rtp 1200
line con 0
line aux 0
line vty 0 4
 login
scheduler allocate 20000 1000
ntp master
ntp server 192.168.1.1
end
```

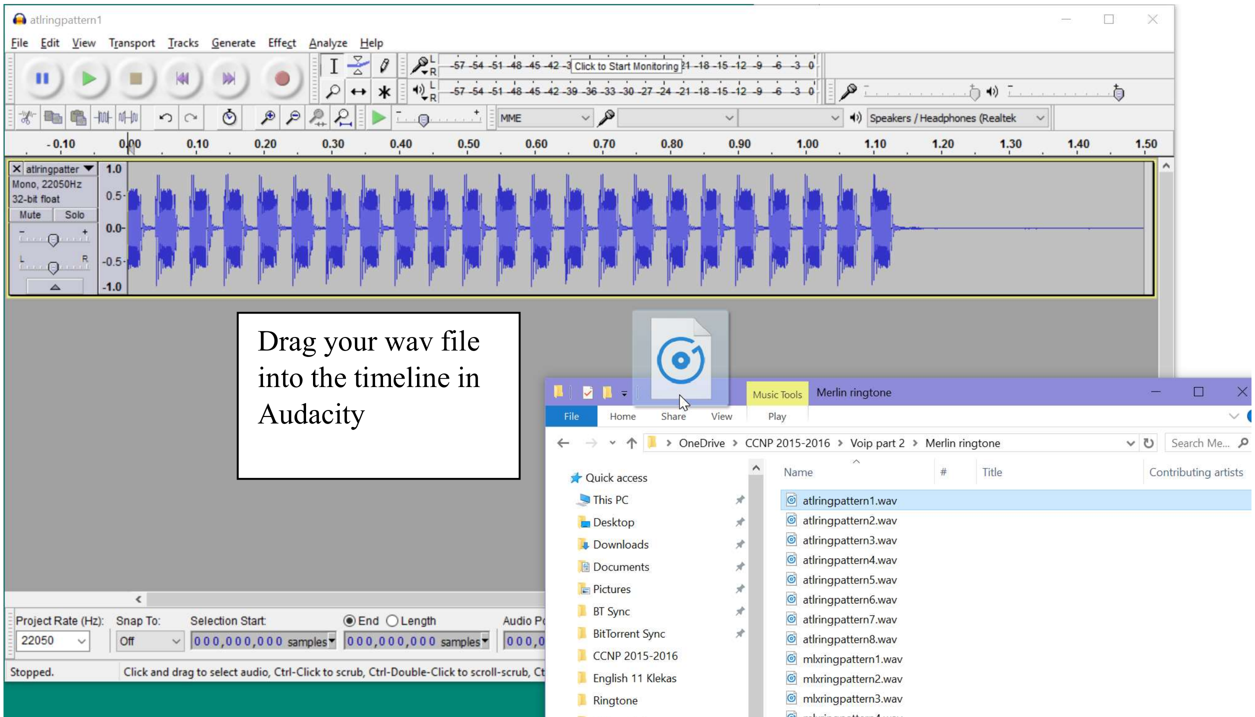
Creating the ringtone

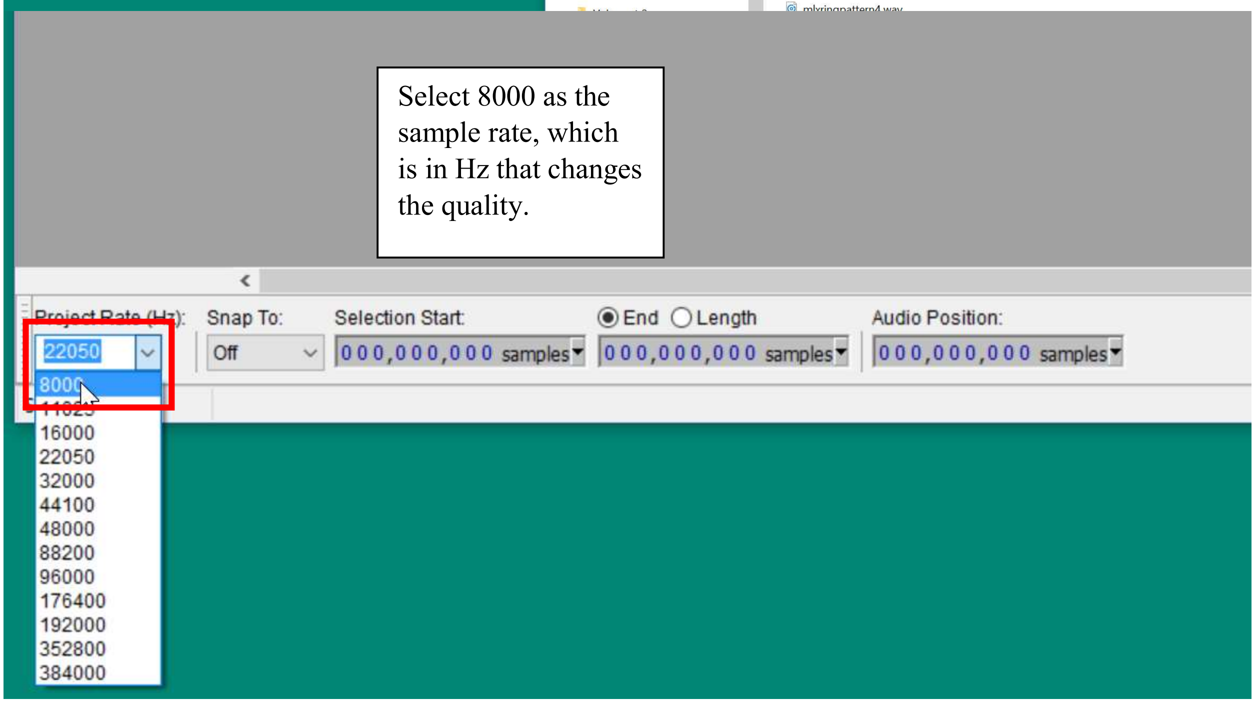


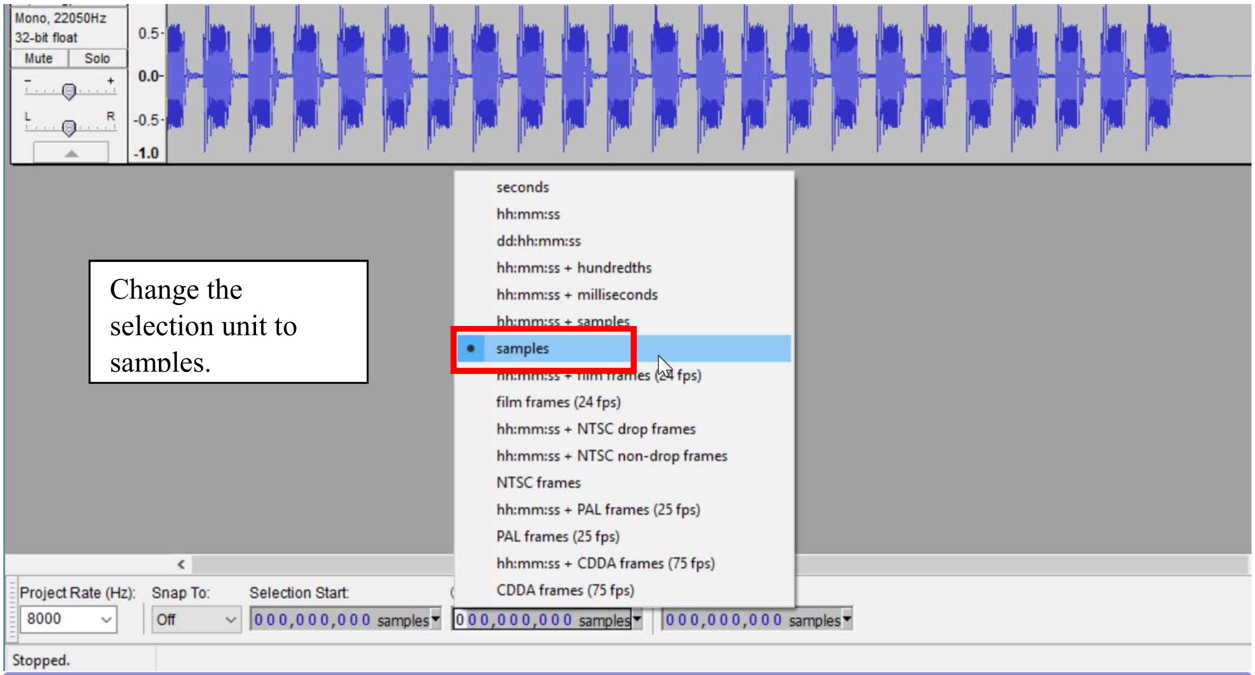
Find wav files online, download and fin them in files.

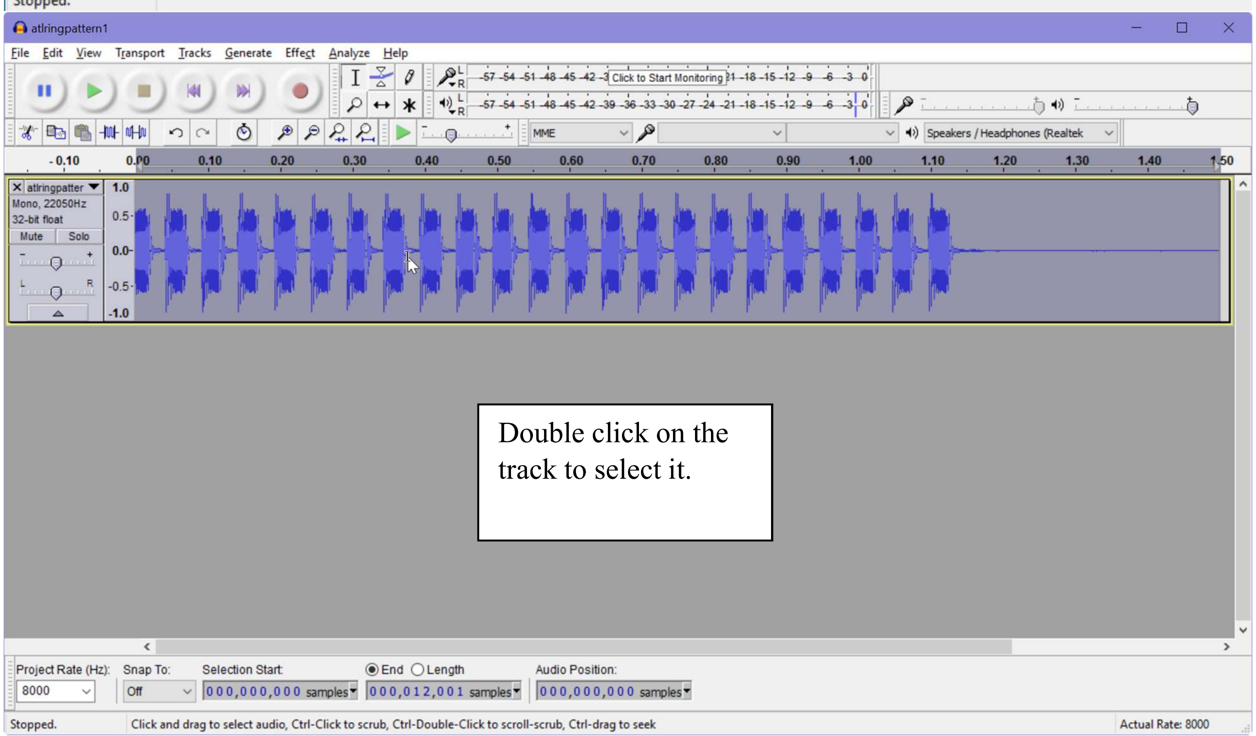


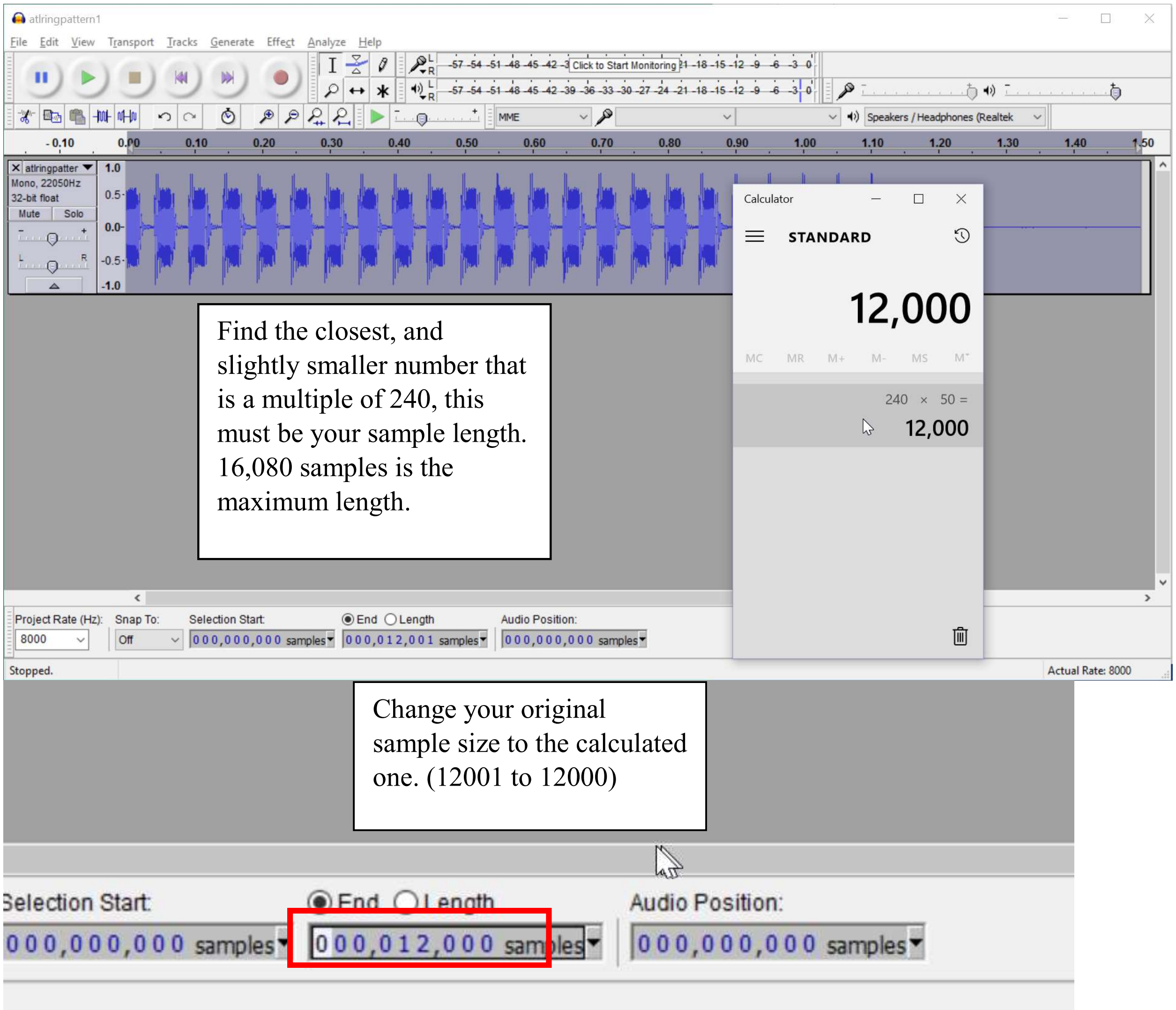
Open Audacity

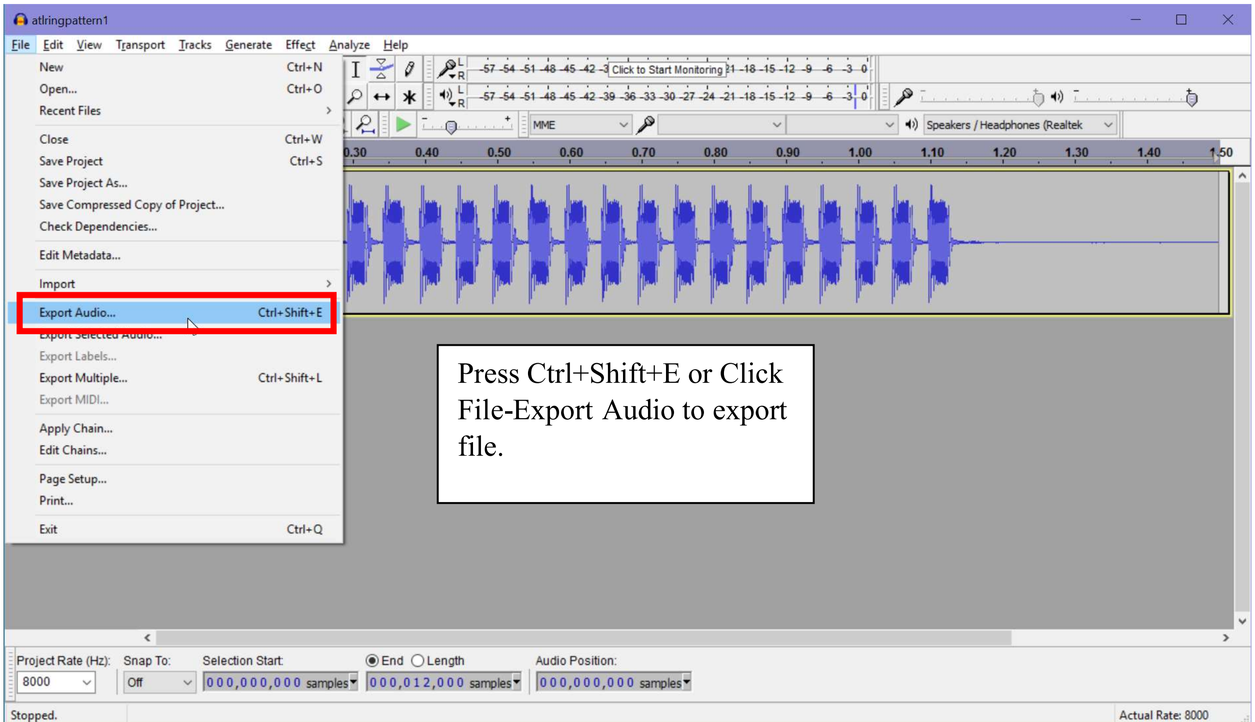

Drag your wav file into the timeline in Audacity

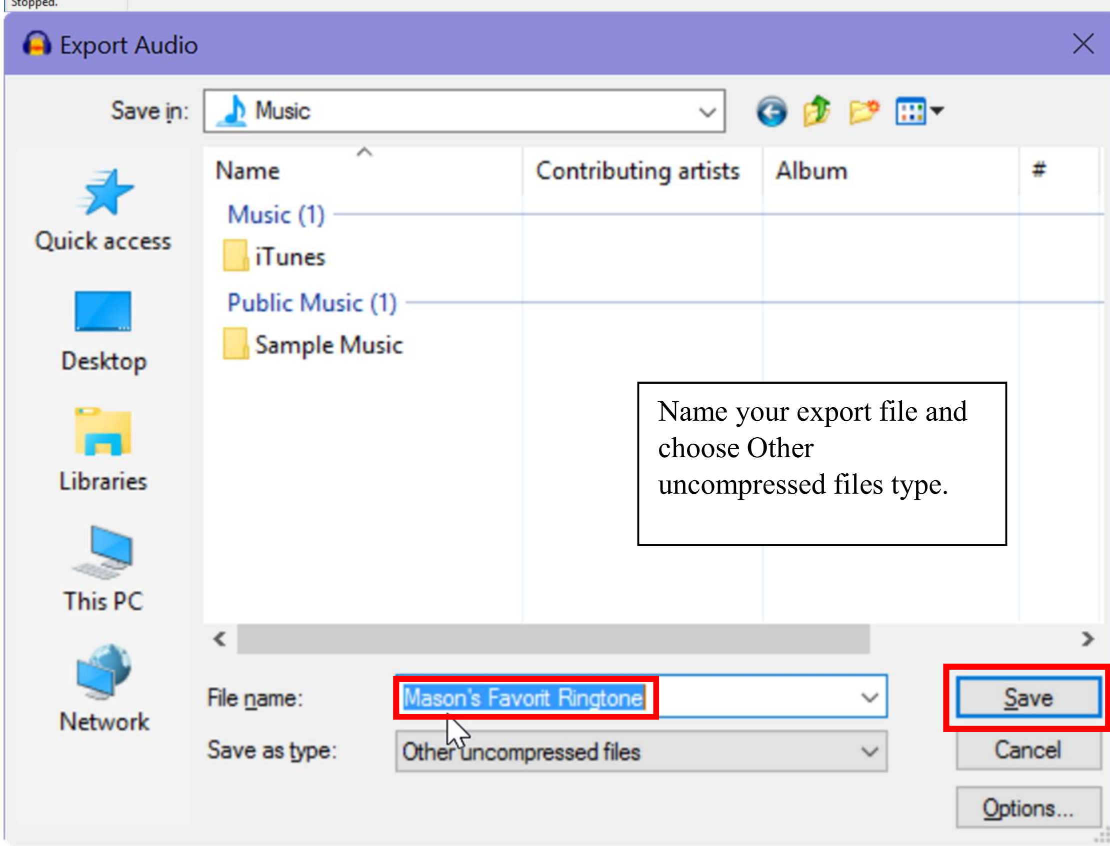

Select 8000 as the sample rate, which is in Hz that changes the quality.

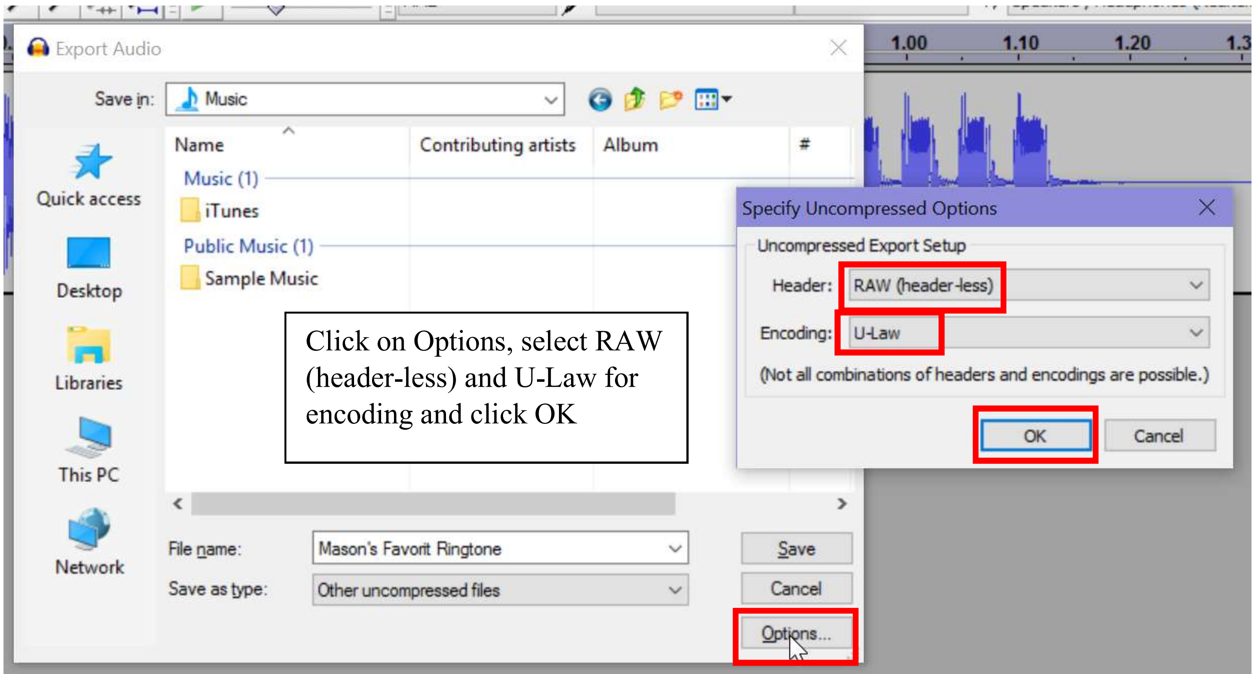

Mono, 22050Hz
32-bit float
Mute
Solo
seconds
hh:mm:ss
dd:hh:mm:ss
hh:mm:ss + hundredths
hh:mm:ss + milliseconds
hh:mm:ss + samples
samples
film frames (24 fps)
hh:mm:ss + NTSC drop frames
hh:mm:ss + NTSC non-drop frames
NTSC frames
hh:mm:ss + PAL frames (25 fps)
PAL frames (25 fps)
hh:mm:ss + CDDA frames (75 fps)
CDDA frames (75 fps)
Change the selection unit to samples.
Project Rate (Hz):
8000
Snap To:
Off
Selection Start:
000,000,000 samples
000,000,000 samples
000,000,000 samples
Stopped.


atlringpattern1
File
Edit
View
Transport
Tracks
Generate
Effect
Analyze
Help
Click to Start Monitoring
MME
Speakers / Headphones (Realtek
atlringpatter
Mono, 22050Hz
32-bit float
Mute
Solo
Double click on the track to select it.
Project Rate (Hz):
8000
Snap To:
Off
Selection Start:
End
Length
Audio Position:
000,000,000 samples
000,012,001 samples
000,000,000 samples
Stopped.
Click and drag to select audio, Ctrl-Click to scrub, Ctrl-Double-Click to scroll-scrub, Ctrl-drag to seek
Actual Rate: 8000

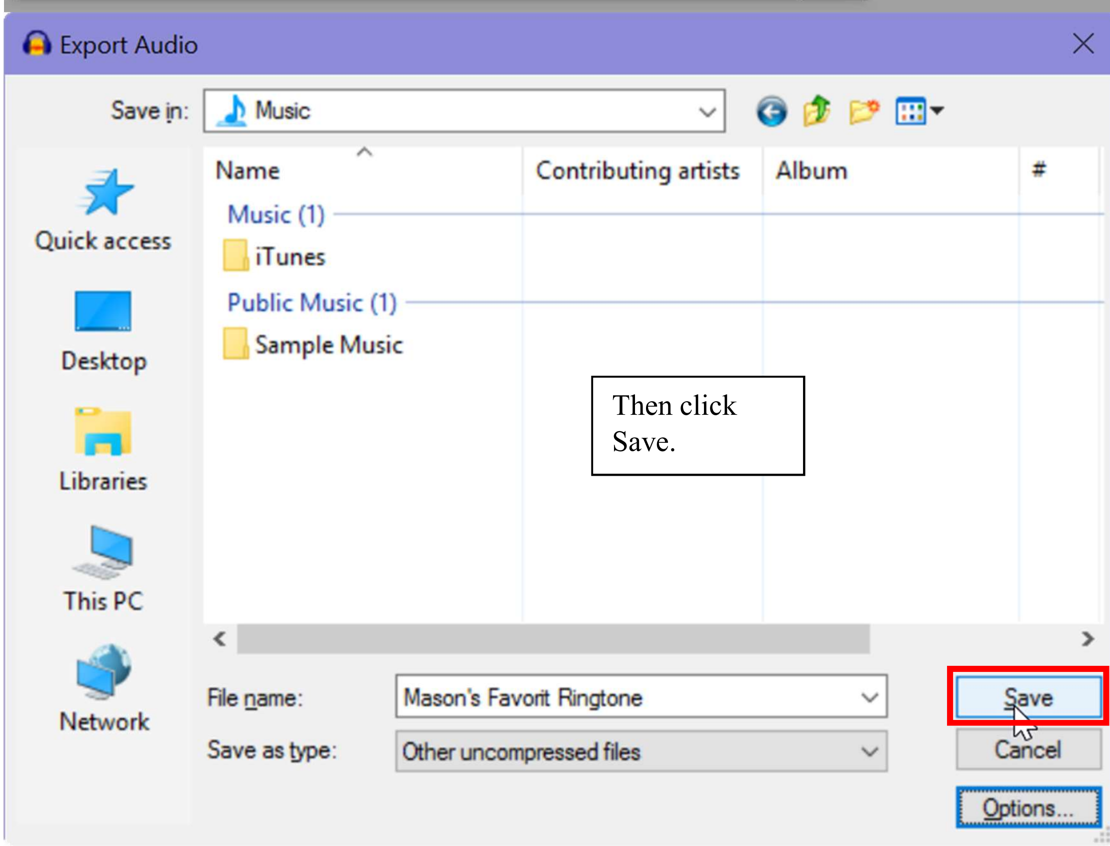

atlringpattern1
File Edit View Transport Tracks Generate Effect Analyze Help
Click to Start Monitoring
Calculator
STANDARD
12,000
240 × 50 =
12,000
Find the closest, and slightly smaller number that is a multiple of 240, this must be your sample length. 16,080 samples is the maximum length.
Project Rate (Hz): 8000
Snap To: Off
Selection Start: 000,000,000 samples
End Length 000,012,001 samples
Audio Position: 000,000,000 samples
Stopped.
Actual Rate: 8000
Change your original sample size to the calculated one. (12001 to 12000)
Selection Start: 000,000,000 samples
End Length 000,012,000 samples
Audio Position: 000,000,000 samples


atlringpattern1
File Edit View Transport Tracks Generate Effect Analyze Help
New Ctrl+N
Open... Ctrl+O
Recent Files
Close Ctrl+W
Save Project Ctrl+S
Save Project As...
Save Compressed Copy of Project...
Check Dependencies...
Edit Metadata...
Import
Export Audio... Ctrl+Shift+E
Export Labels...
Export Multiple... Ctrl+Shift+L
Export MIDI...
Apply Chain...
Edit Chains...
Page Setup...
Print...
Exit Ctrl+Q
Press Ctrl+Shift+E or Click File-Export Audio to export file.
Project Rate (Hz): 8000
Snap To: Off
Selection Start:
Audio Position:
Stopped.
Actual Rate: 8000

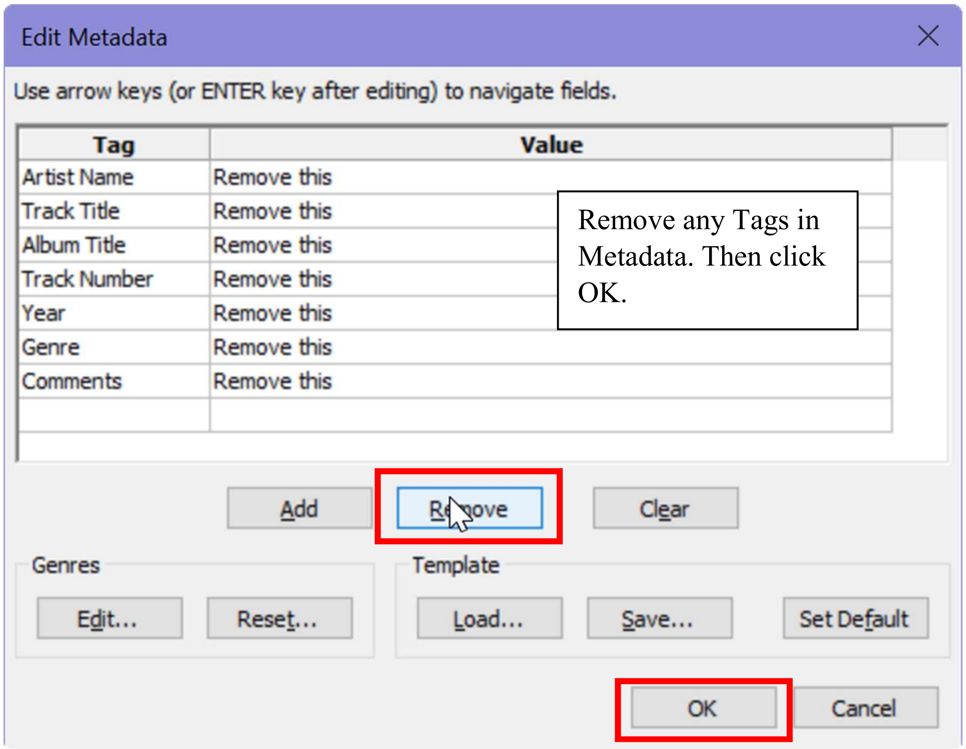

Export Audio
Save in: Music
Quick access
Desktop
Libraries
This PC
Network
Name
Contributing artists
Album
#
Music (1)
iTunes
Public Music (1)
Sample Music
Name your export file and choose Other uncompressed files type.
File name: Mason's Favorit Ringtone
Save as type: Other uncompressed files
Save
Cancel
Options...

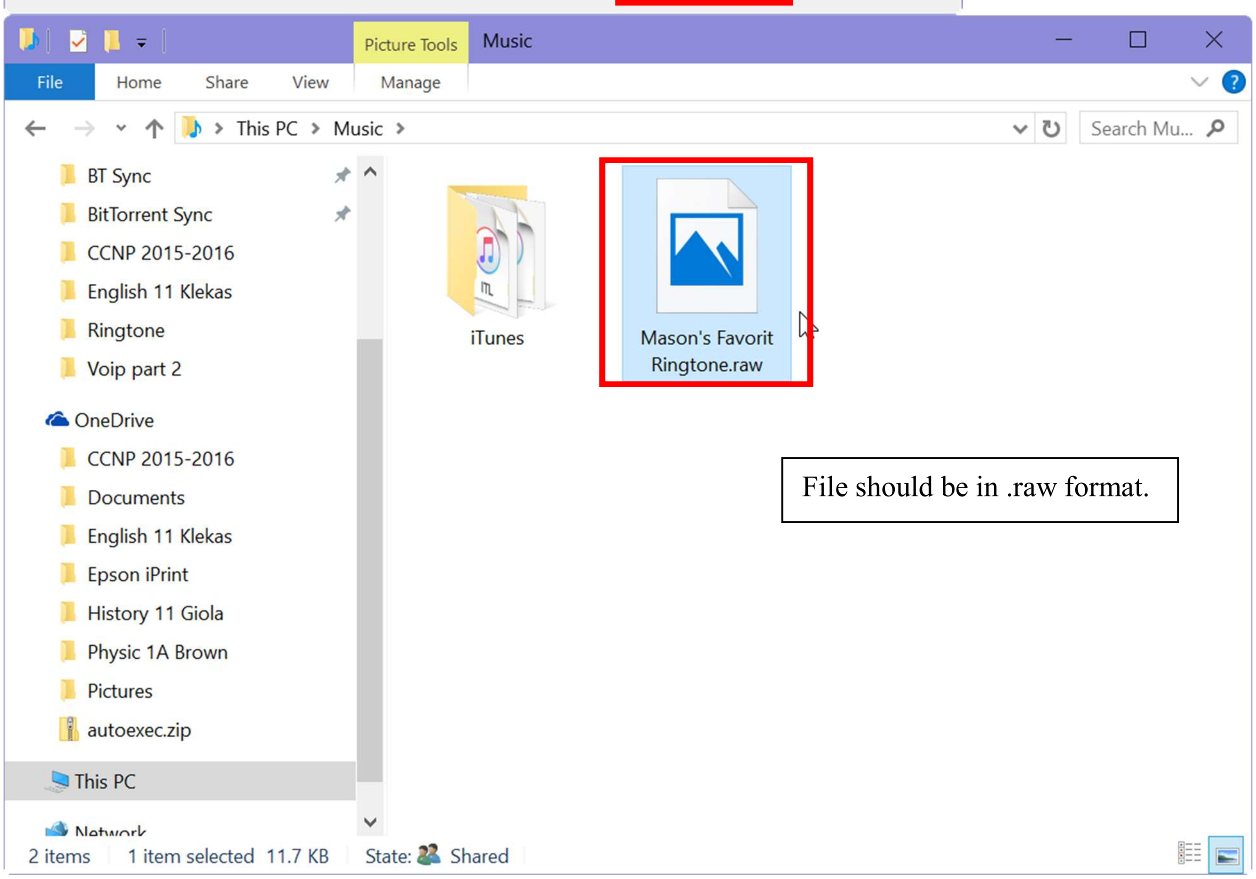


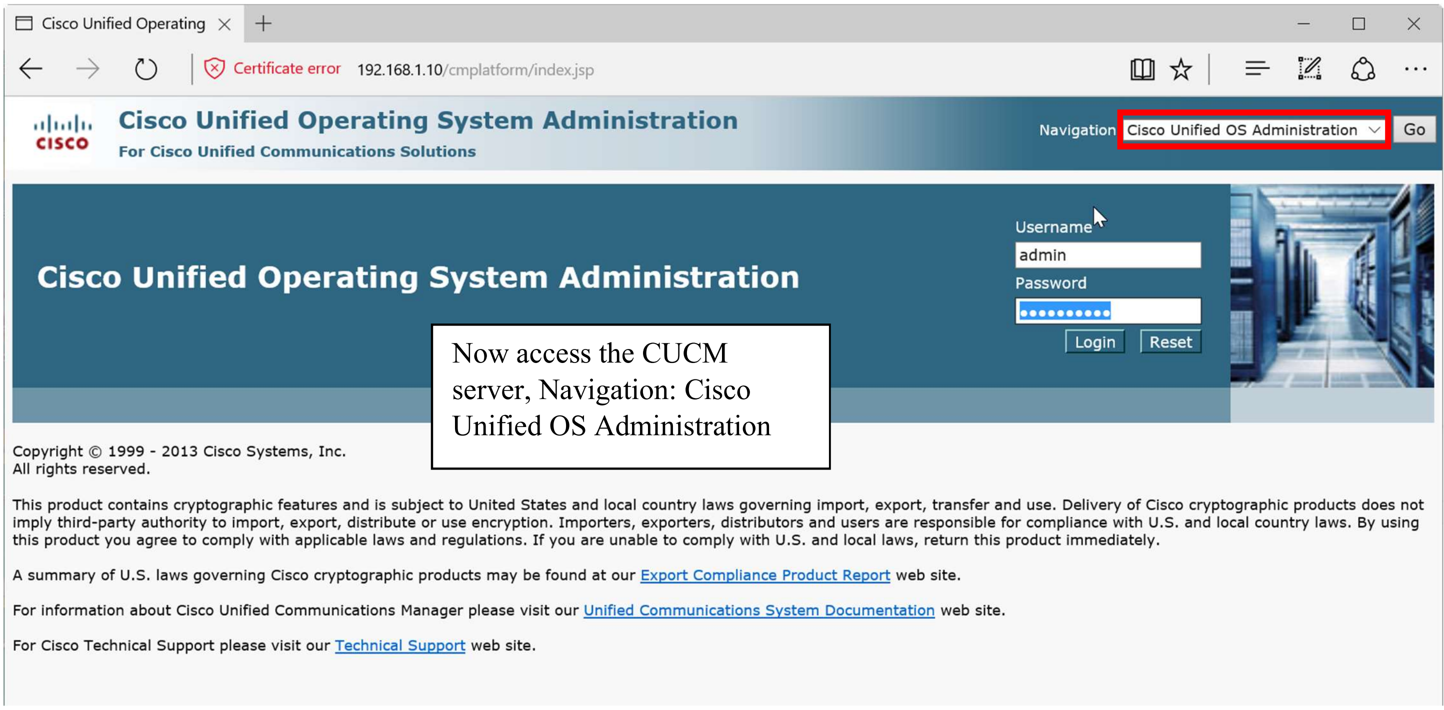
Export Audio
Save in: Music
Quick access
Desktop
Libraries
This PC
Network
Name
Contributing artists
Album
#
Music (1)
iTunes
Public Music (1)
Sample Music
Click on Options, select RAW (header-less) and U-Law for encoding and click OK
File name: Mason's Favorit Ringtone
Save as type: Other uncompressed files
Save
Cancel
Options...
1.00
1.10
1.20
Specify Uncompressed Options
Uncompressed Export Setup
Header: RAW (header-less)
Encoding: U-Law
(Not all combinations of headers and encodings are possible.)
OK
Cancel

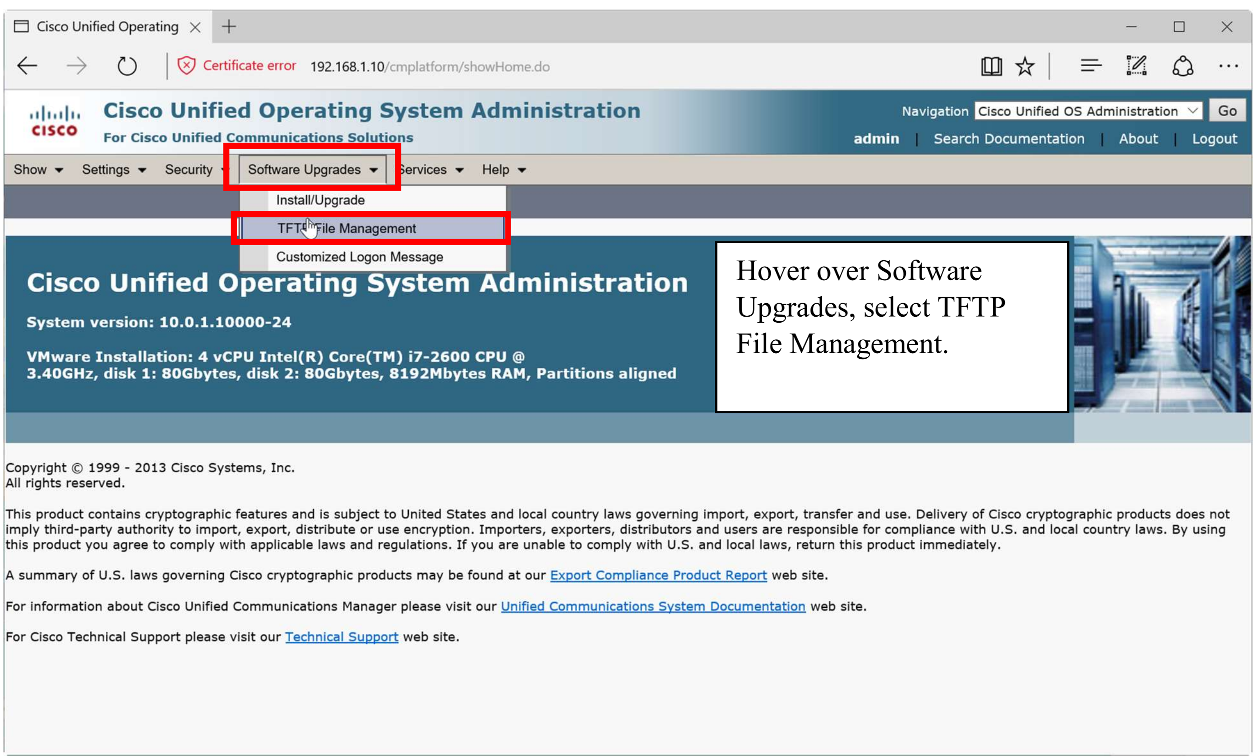


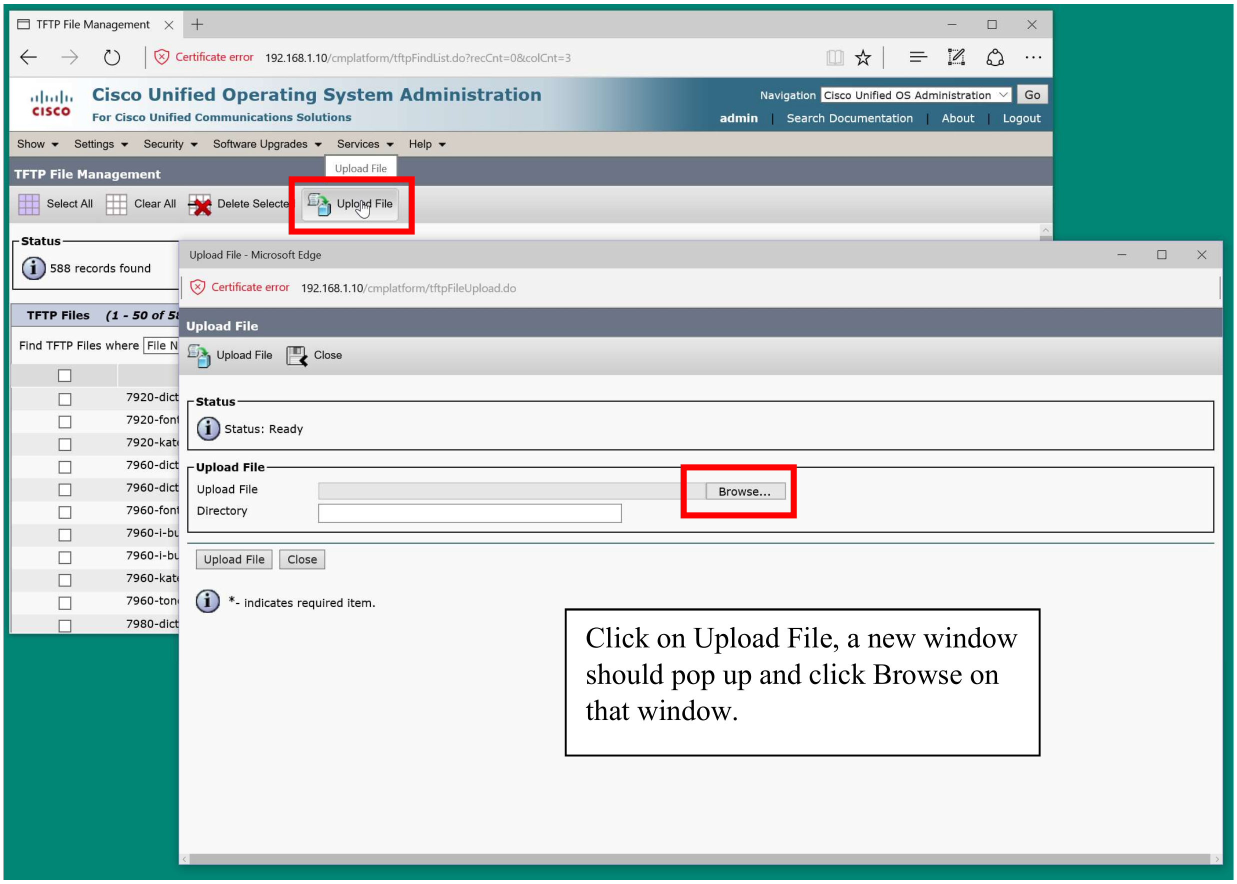
Export Audio
Save in: Music
Quick access
Desktop
Libraries
This PC
Network
Name
Contributing artists
Album
#
Music (1)
iTunes
Public Music (1)
Sample Music
Then click Save.
File name: Mason's Favorit Ringtone
Save as type: Other uncompressed files
Save
Cancel
Options...

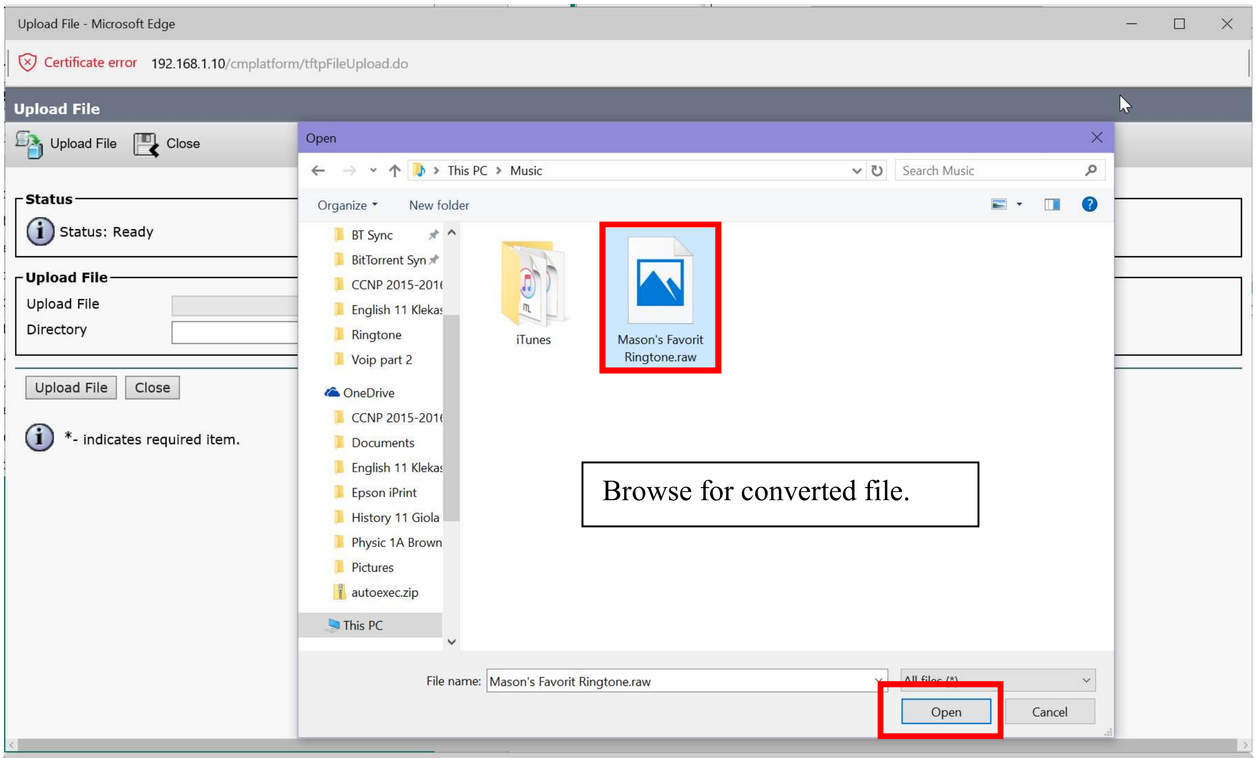

Edit Metadata
Use arrow keys (or ENTER key after editing) to navigate fields.
Tag
Value
Artist Name
Remove this
Track Title
Remove this
Album Title
Remove this
Track Number
Remove this
Year
Remove this
Genre
Remove this
Comments
Remove this
Remove any Tags in Metadata. Then click OK.
Add
Remove
Clear
Genres
Edit...
Reset...
Template
Load...
Save...
Set Default
OK
Cancel

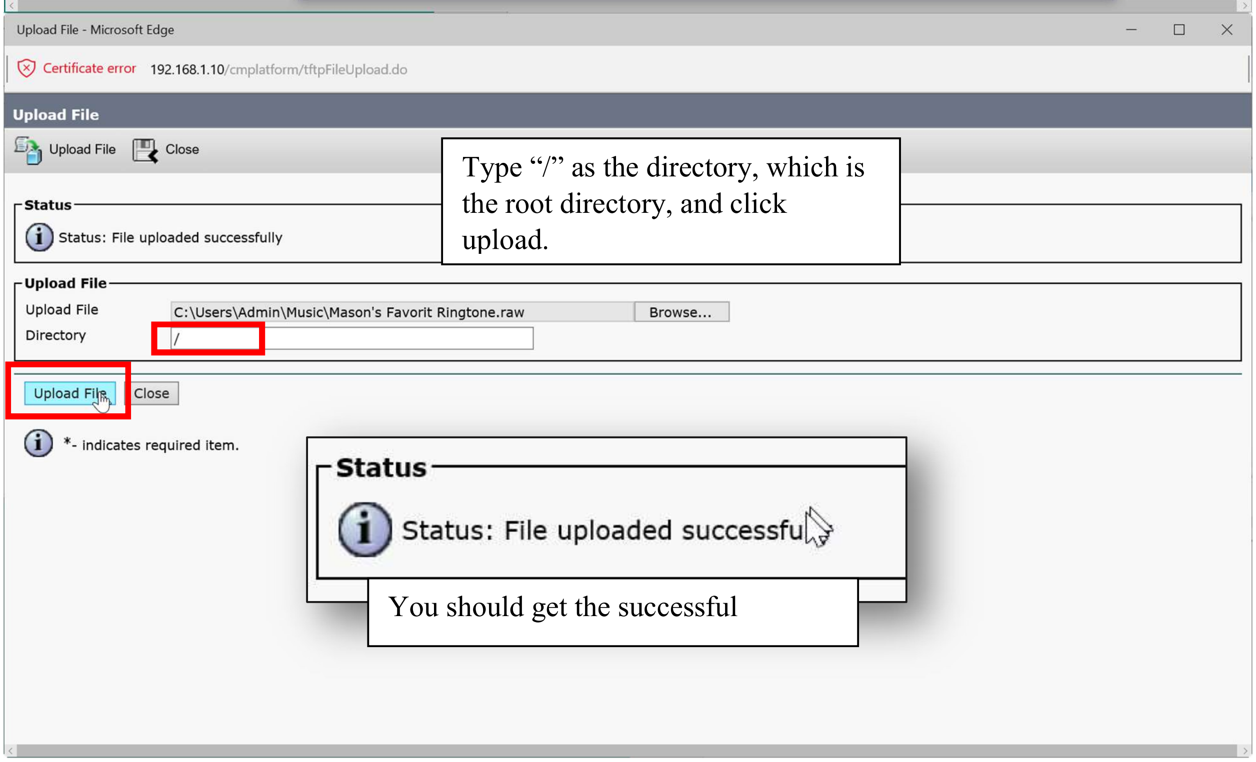

Picture Tools
Music
File
Home
Share
View
Manage
This PC
Music
Search Mu...
BT Sync
BitTorrent Sync
CCNP 2015-2016
English 11 Klekas
Ringtone
Voip part 2
OneDrive
CCNP 2015-2016
Documents
English 11 Klekas
Epson iPrint
History 11 Giola
Physic 1A Brown
Pictures
autoexec.zip
This PC
iTunes
Mason's Favorit Ringtone.raw
File should be in .raw format.
2 items
1 item selected 11.7 KB
State:
Shared

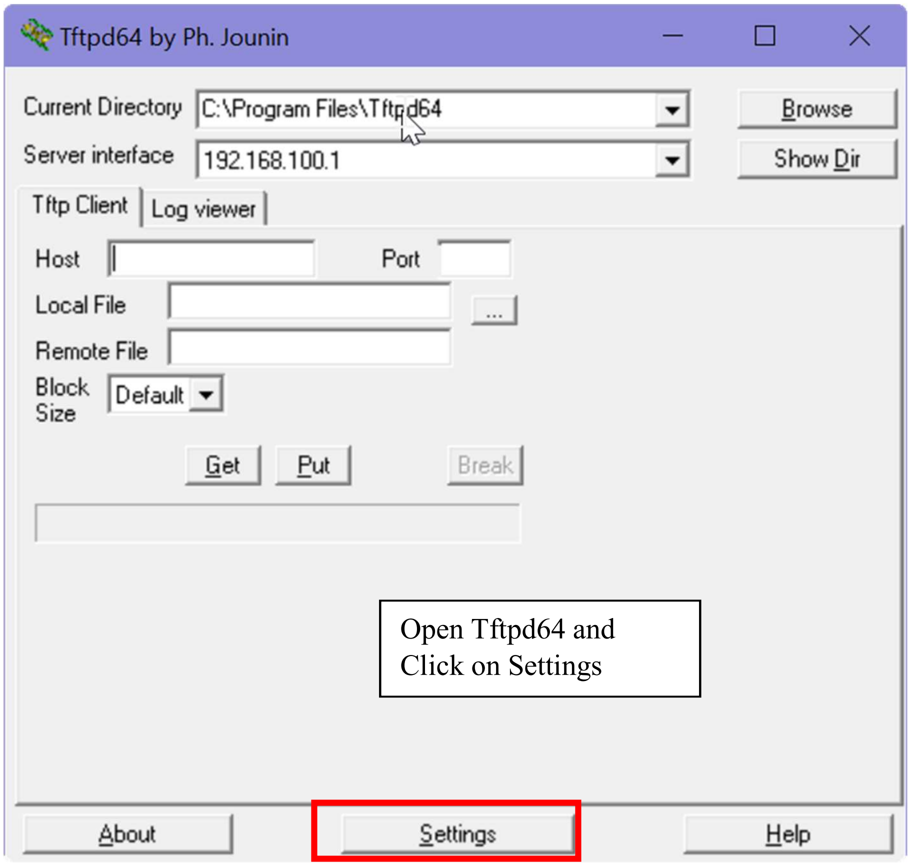

Cisco Unified Operating
Certificate error
192.168.1.10/cmplatform/index.jsp
Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Navigation
Cisco Unified OS Administration
Go
Cisco Unified Operating System Administration
Username
admin
Password
Login
Reset
Now access the CUCM server, Navigation: Cisco Unified OS Administration
Copyright © 1999 - 2013 Cisco Systems, Inc.
All rights reserved.
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance Product Report web site.
For information about Cisco Unified Communications Manager please visit our Unified Communications System Documentation web site.
For Cisco Technical Support please visit our Technical Support web site.

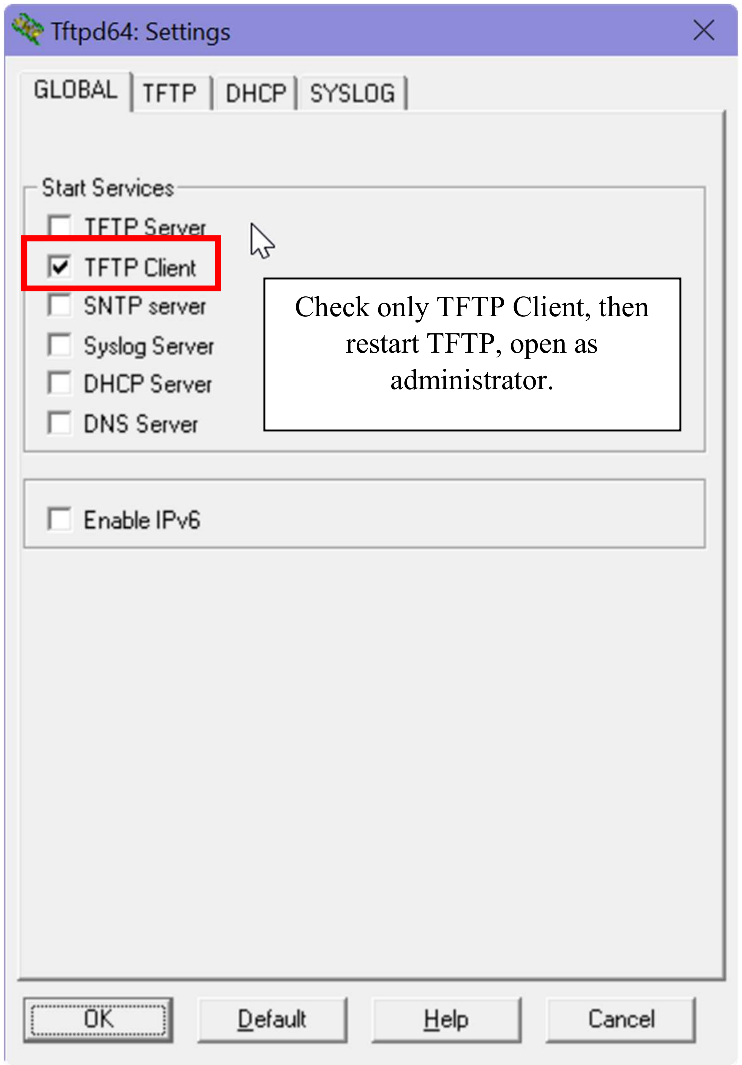

Cisco Unified Operating
Certificate error
192.168.1.10/cmplatform/showHome.do
Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Navigation
Cisco Unified OS Administration
Go
admin
Search Documentation
About
Logout
Show
Settings
Security
Software Upgrades
Services
Help
Install/Upgrade
TFTP File Management
Customized Logon Message
Cisco Unified Operating System Administration
System version: 10.0.1.10000-24
VMware Installation: 4 vCPU Intel(R) Core(TM) i7-2600 CPU @ 3.40GHz, disk 1: 80Gbytes, disk 2: 80Gbytes, 8192Mbytes RAM, Partitions aligned
Hover over Software Upgrades, select TFTP File Management.
Copyright © 1999 - 2013 Cisco Systems, Inc.
All rights reserved.
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance Product Report web site.
For information about Cisco Unified Communications Manager please visit our Unified Communications System Documentation web site.
For Cisco Technical Support please visit our Technical Support web site.

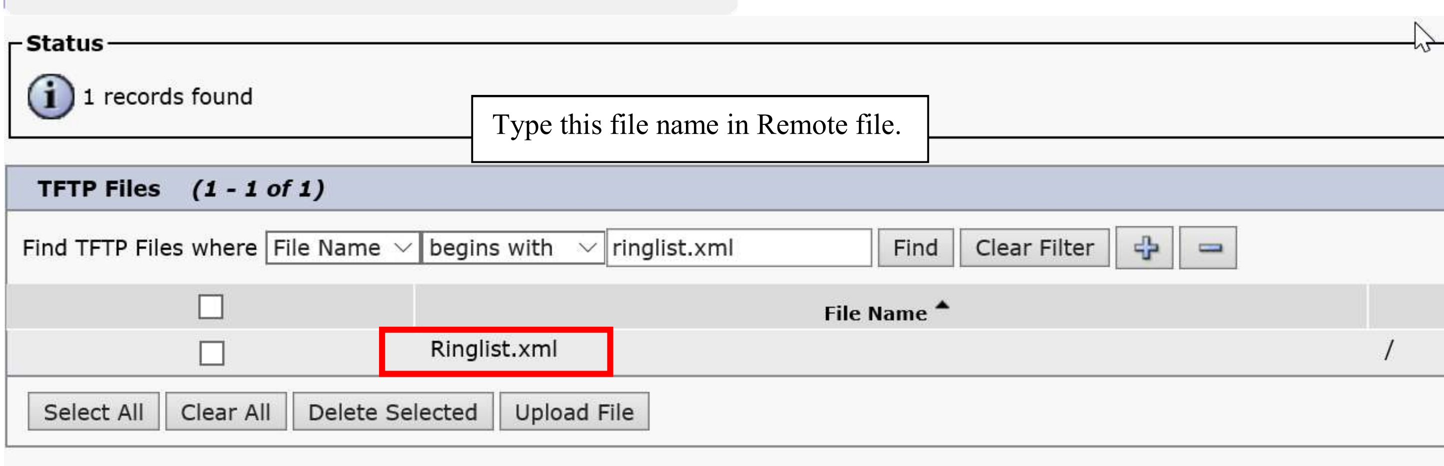

TFTP File Management
Certificate error 192.168.1.10/cmplatform/tftpFindList.do?recCnt=0&colCnt=3
Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified OS Administration Go
admin | Search Documentation | About | Logout
Show Settings Security Software Upgrades Services Help
TFTP File Management
Select All Clear All Delete Selected Upload File
Status
588 records found
Upload File - Microsoft Edge
Certificate error 192.168.1.10/cmplatform/tftpFileUpload.do
Upload File
Upload File Close
Status
Status: Ready
Upload File
Upload File
Directory
Browse...
Upload File Close
*- indicates required item.
Click on Upload File, a new window should pop up and click Browse on that window.

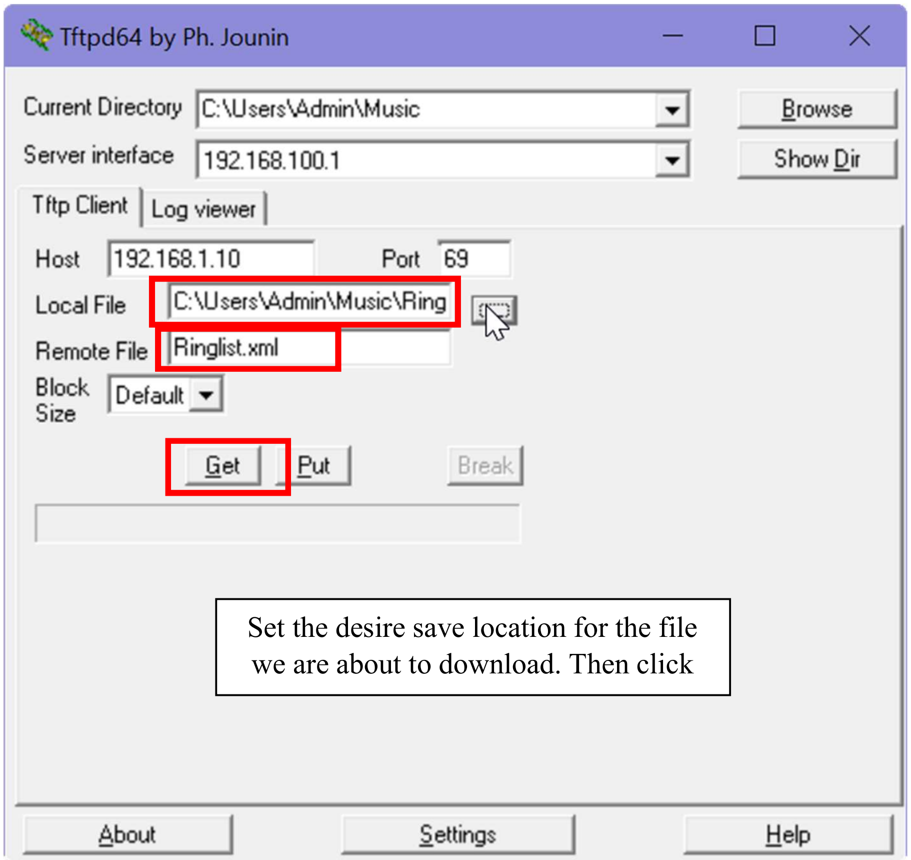

Upload File - Microsoft Edge
Certificate error 192.168.1.10/cmplatform/tftpFileUpload.do
Upload File
Open
This PC > Music
Search Music
Organize New folder
BT Sync
BitTorrent Syn
CCNP 2015-201
English 11 Klekas
Ringtone
Voip part 2
OneDrive
Documents
Epson iPrint
History 11 Giola
Physic 1A Brown
Pictures
autoexec.zip
This PC
iTunes
Mason's Favorit Ringtone.raw
Browse for converted file.
Status
Status: Ready
Upload File
Directory
Close
*- indicates required item.
File name: Mason's Favorit Ringtone.raw
Open
Cancel

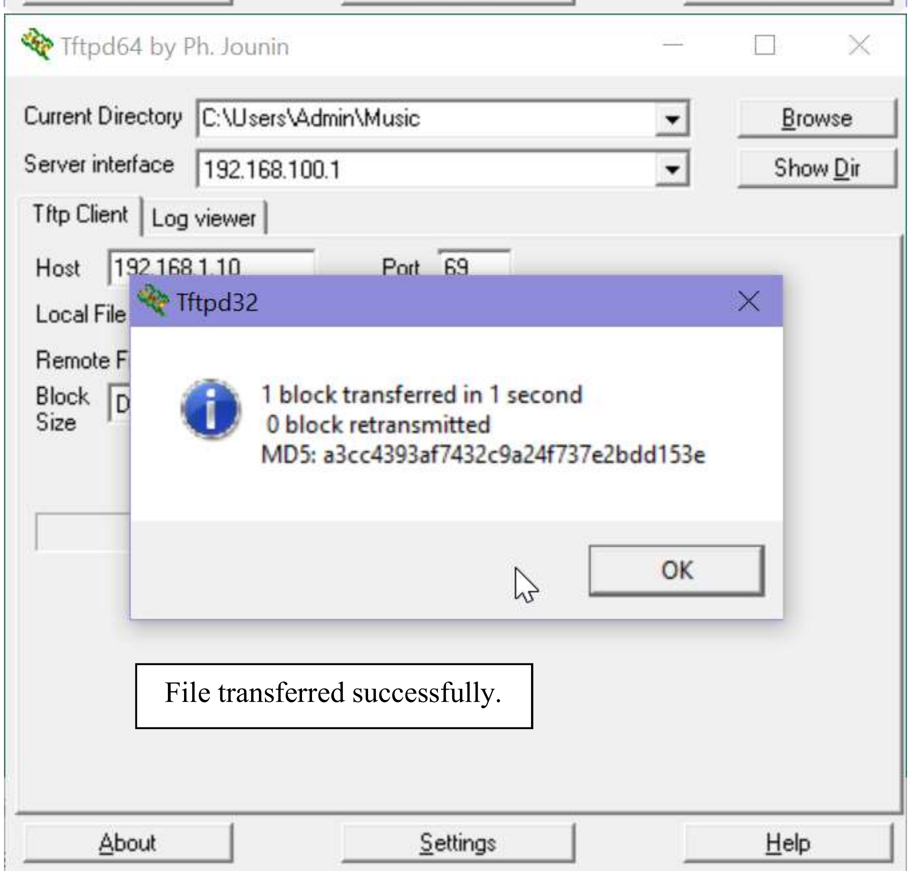

Upload File - Microsoft Edge
Certificate error 192.168.1.10/cmplatform/tftpFileUpload.do
Upload File
Close
Type "/" as the directory, which is the root directory, and click upload.
Status
Status: File uploaded successfully
Upload File
C:\Users\Admin\Music\Mason's Favorit Ringtone.raw
Browse...
Directory
/
*- indicates required item.
Status: File uploaded successfu
You should get the successful

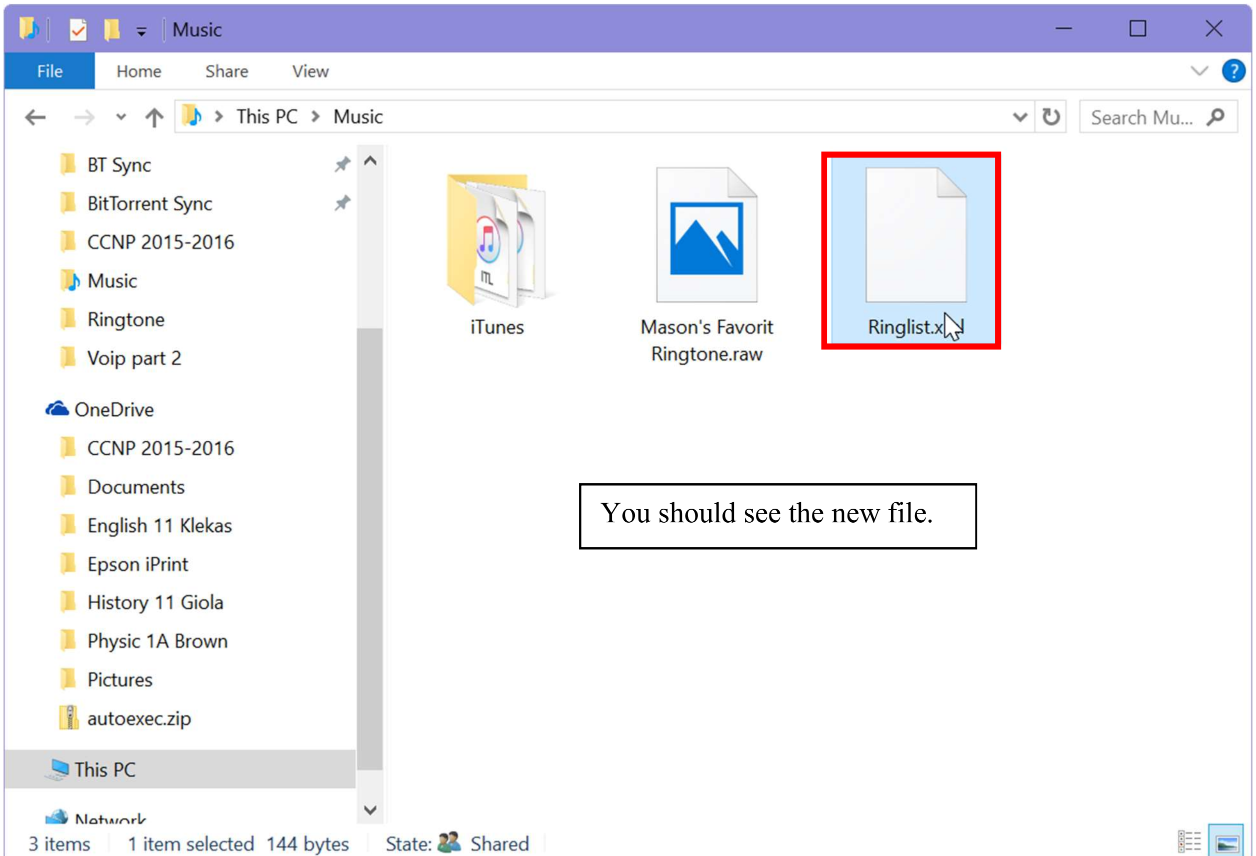

Tftpd64 by Ph. Jounin
Current Directory
C:\Program Files\Tftpd64
Browse
Server interface
192.168.100.1
Show Dir
Tftp Client
Log viewer
Host
Port
Local File
...
Remote File
Block Size
Default
Get
Put
Break
Open Tftpd64 and Click on Settings
About
Settings
Help


Tftpd64: Settings
GLOBAL
TFTP
DHCP
SYSLOG
Start Services
TFTP Server
TFTP Client
SNTP server
Syslog Server
DHCP Server
DNS Server
Check only TFTP Client, then restart TFTP, open as administrator.
Enable IPv6
OK
Default
Help
Cancel


Status
1 records found
Type this file name in Remote file.
TFTP Files (1 - 1 of 1)
Find TFTP Files where File Name begins with ringlist.xml Find Clear Filter
File Name
Ringlist.xml
/
Select All
Clear All
Delete Selected
Upload File

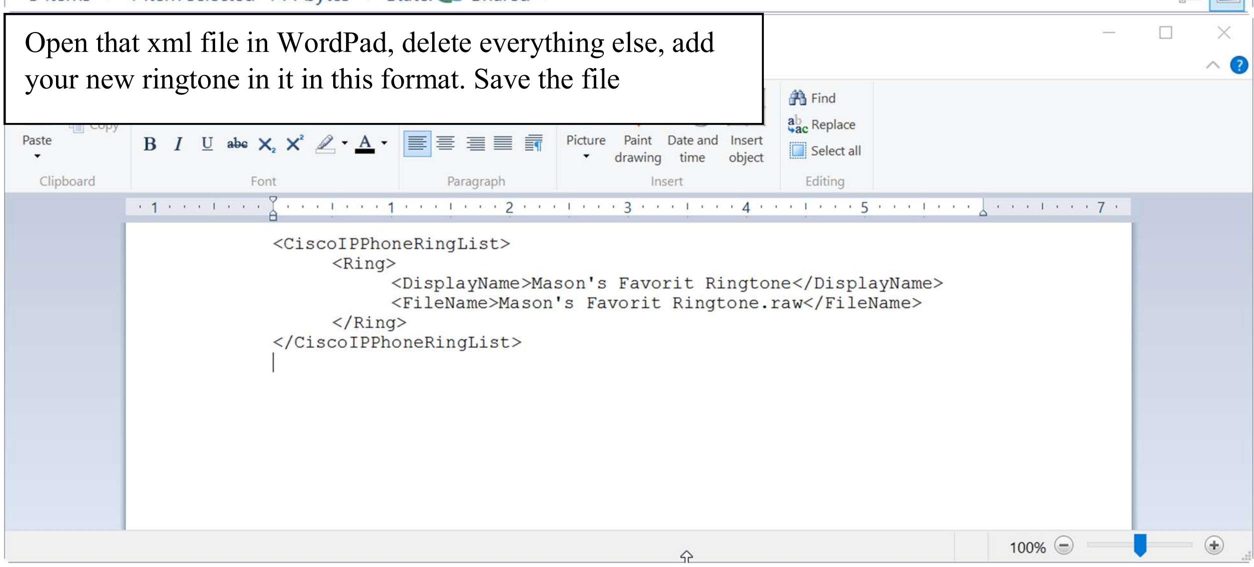

Tftpd64 by Ph. Jounin
Current Directory
C:\Users\Admin\Music
Browse
Server interface
192.168.100.1
Show Dir
Tftp Client
Log viewer
Host
192.168.1.10
Port
69
Local File
C:\Users\Admin\Music\Ring
Remote File
Ringlist.xml
Block Size
Default
Get
Put
Break
Set the desire save location for the file we are about to download. Then click
About
Settings
Help

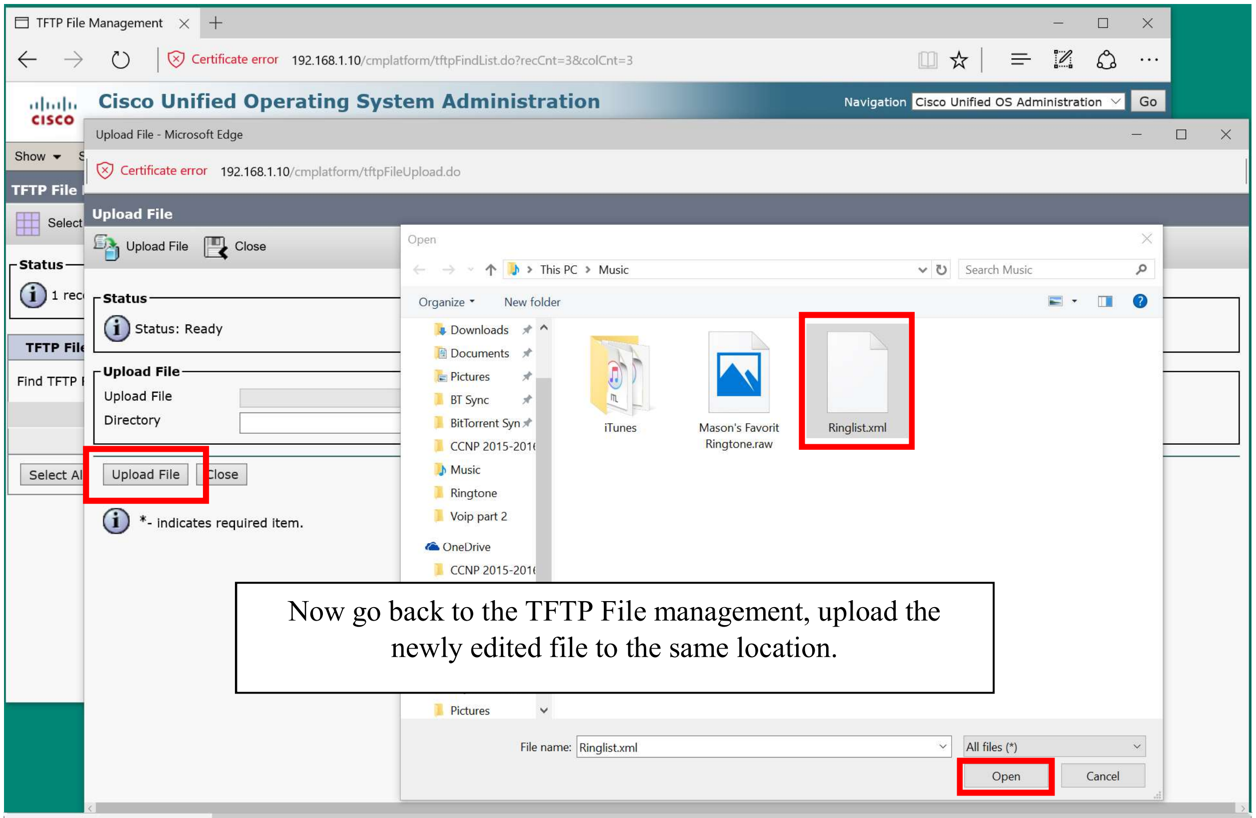

Tftpd64 by Ph. Jounin
Current Directory
C:\Users\Admin\Music
Browse
Server interface
192.168.100.1
Show Dir
Tftp Client
Log viewer
Host
Port
Local File
Remote F
Block Size
Tftpd32
1 block transferred in 1 second
0 block retransmitted
MD5: a3cc4393af7432c9a24f737e2bdd153e
OK
File transferred successfully.
About
Settings
Help

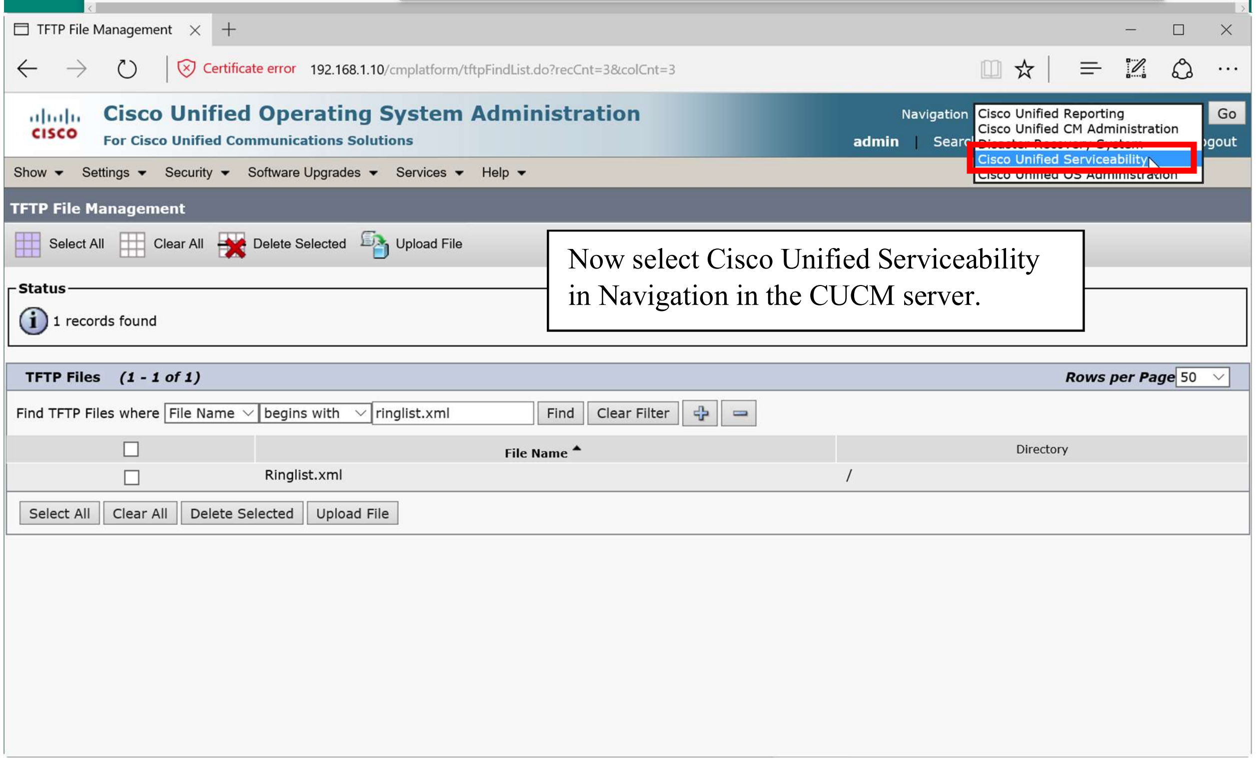


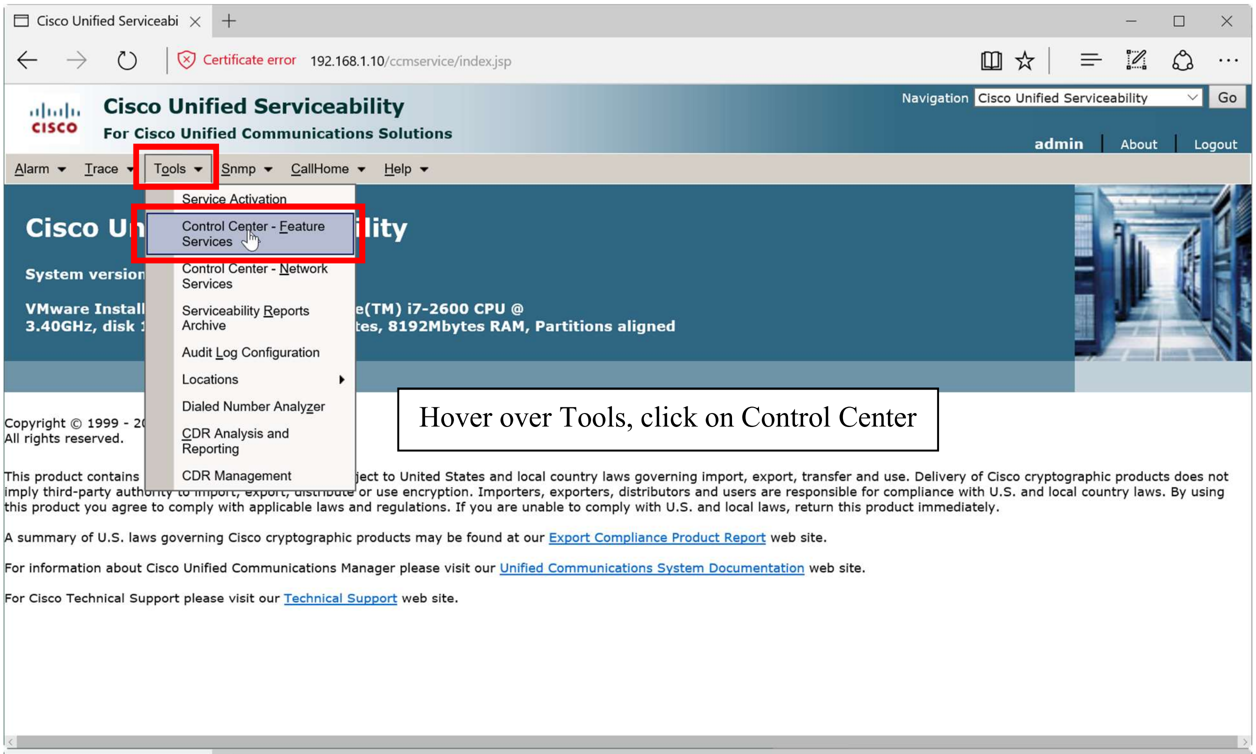
You should see the new file.

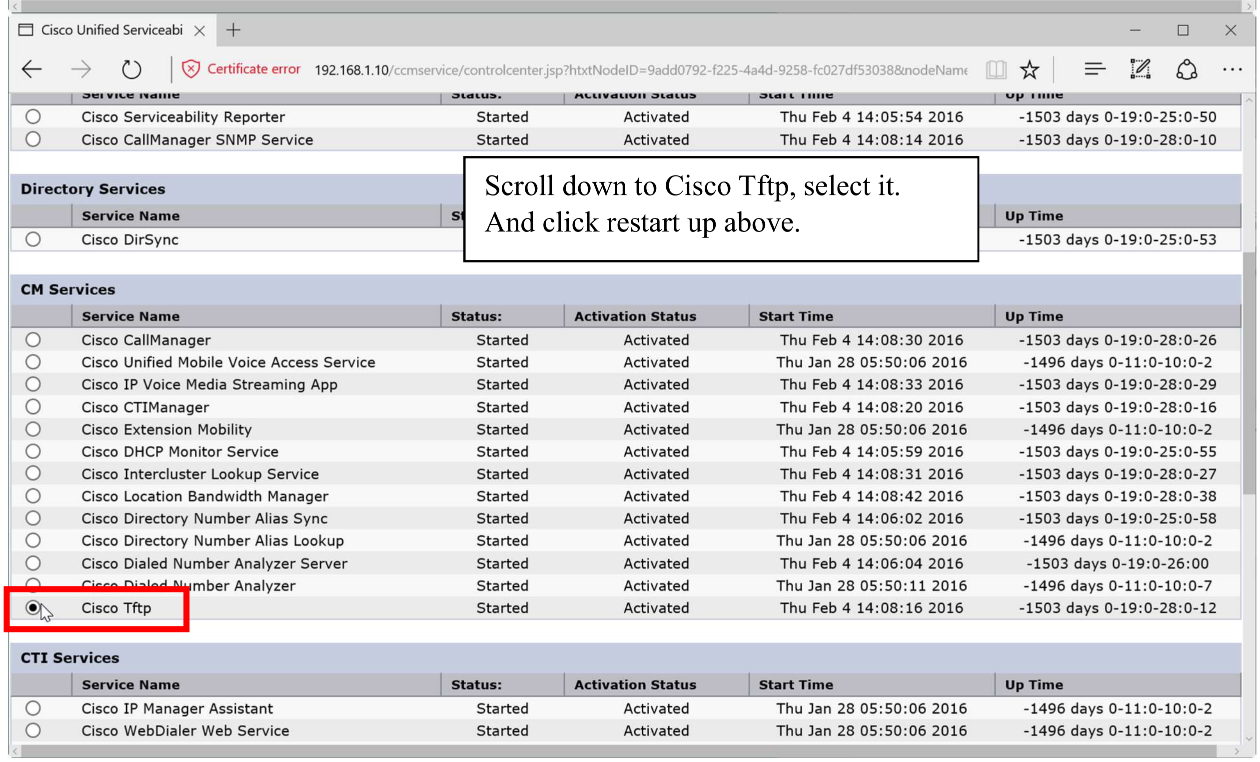
Open that xml file in WordPad, delete everything else, add your new ringtone in it in this format. Save the file

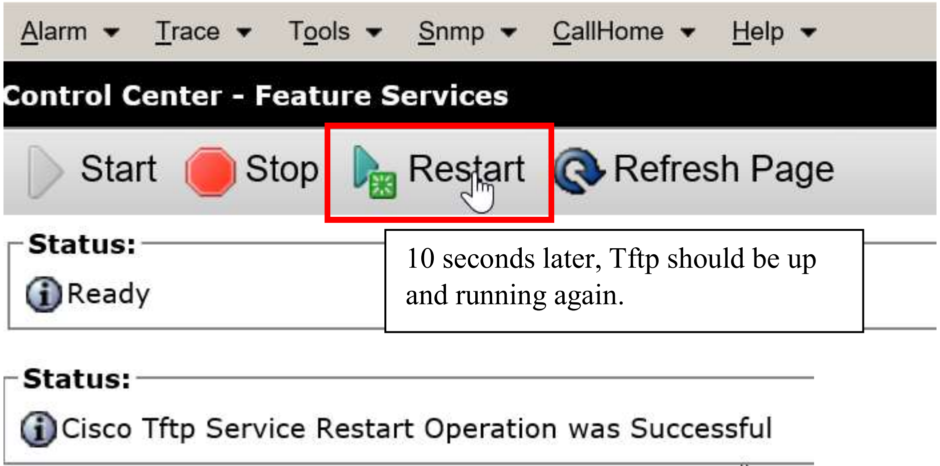



TFTP File Management
Cisco Unified Operating System Administration
Upload File - Microsoft Edge
Upload File
Status: Ready
Upload File
Close
Open
Ringlist.xml
Now go back to the TFTP File management, upload the newly edited file to the same location.

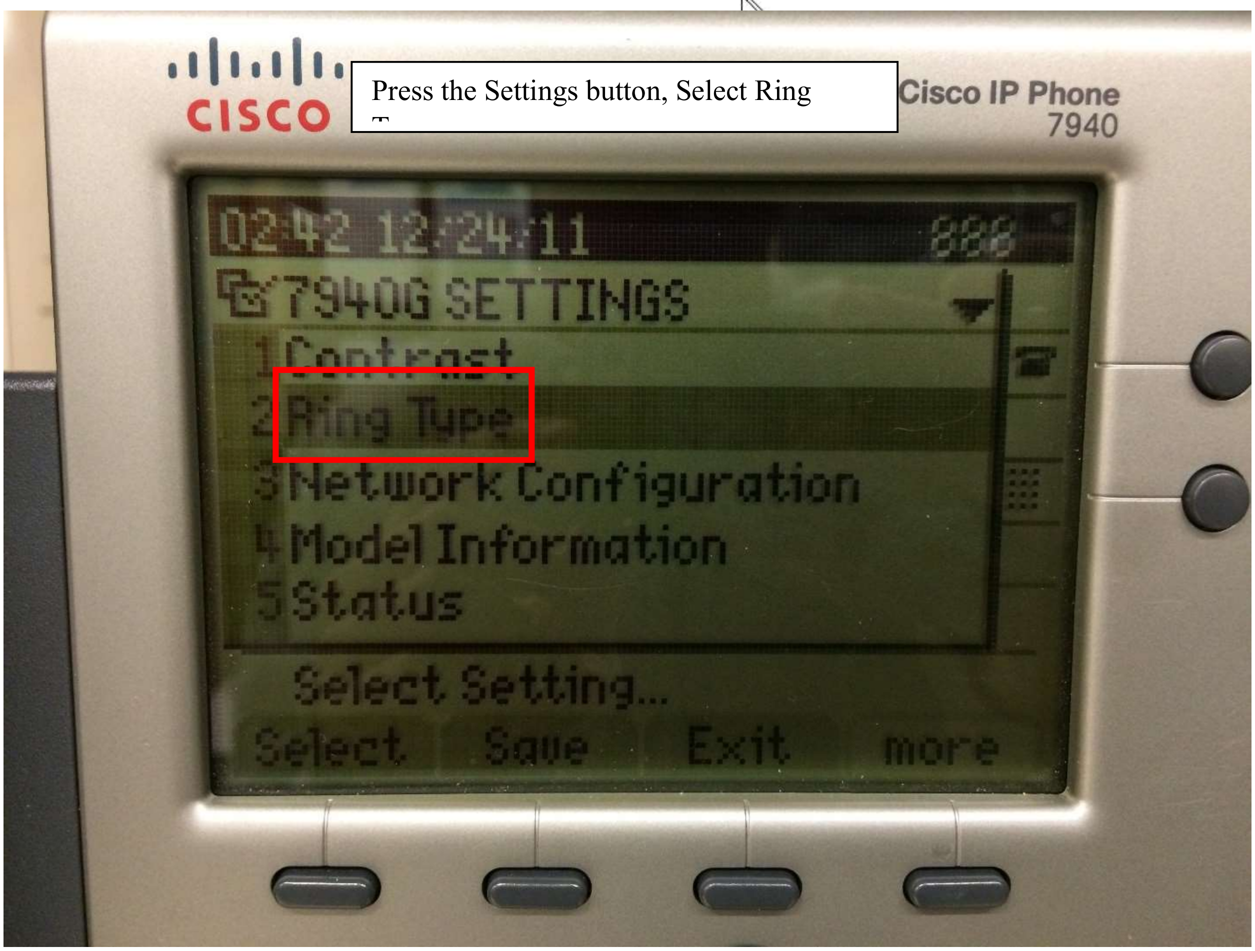

TFTP File Management
Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Cisco Unified Reporting
Cisco Unified CM Administration
Cisco Unified Serviceability
Now select Cisco Unified Serviceability in Navigation in the CUCM server.
1 records found
Ringlist.xml


Cisco Unified Serviceabi
Certificate error 192.168.1.10/ccmservice/index.jsp
Cisco Unified Serviceability
For Cisco Unified Communications Solutions
Navigation Cisco Unified Serviceability Go
admin About Logout
Alarm Trace Tools Snmp CallHome Help
Service Activation
Control Center - Feature Services
Control Center - Network Services
Serviceability Reports Archive
Audit Log Configuration
Locations
Dialed Number Analyzer
CDR Analysis and Reporting
CDR Management
Hover over Tools, click on Control Center
A summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance Product Report web site.
For information about Cisco Unified Communications Manager please visit our Unified Communications System Documentation web site.
For Cisco Technical Support please visit our Technical Support web site.

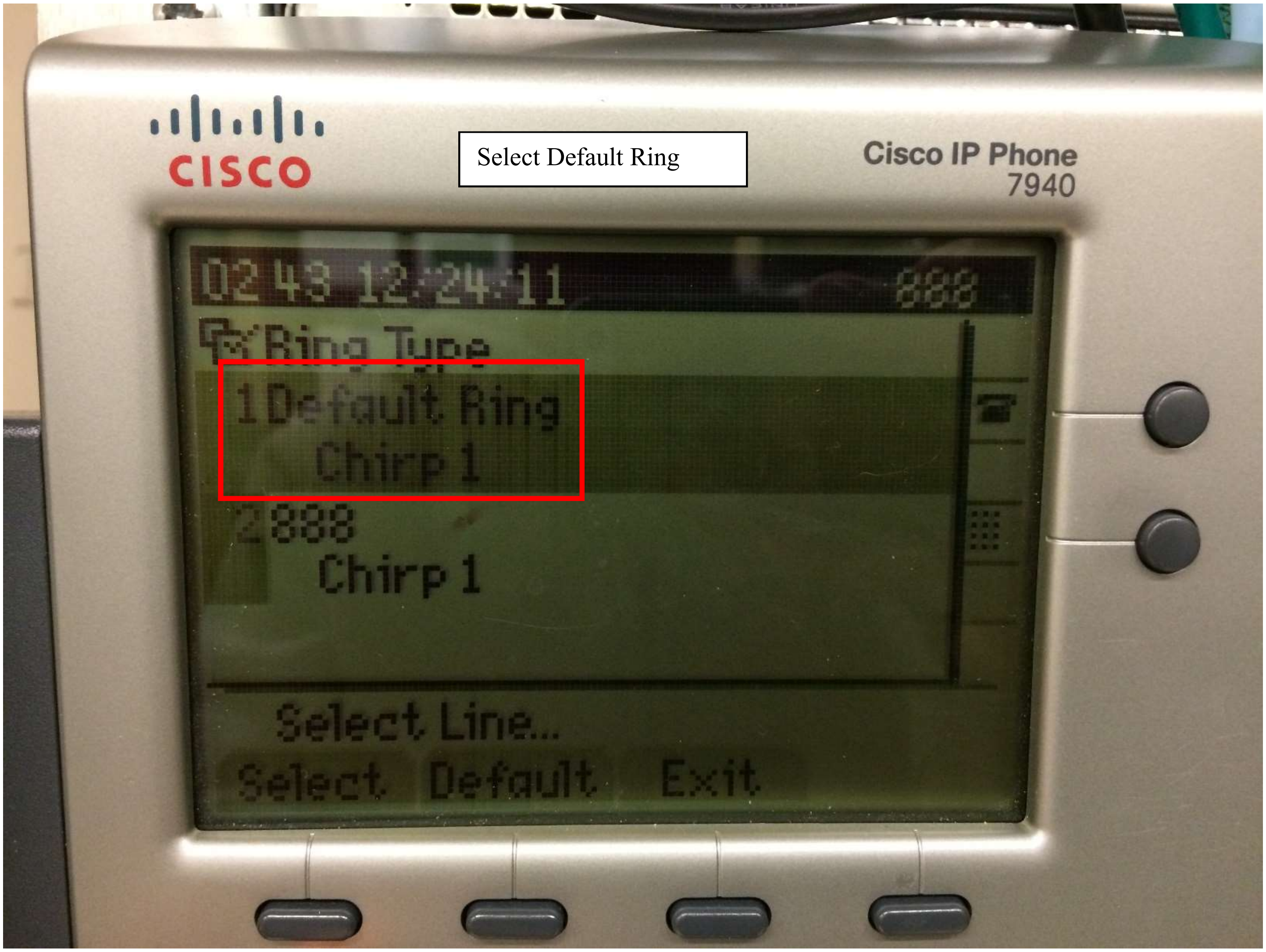

Cisco Unified Serviceabi
Certificate error 192.168.1.10/ccmservice/controlcenter.jsp?htxtNodeID=9add0792-f225-4a4d-9258-fc027df53038&nodeName
Cisco Serviceability Reporter Started Activated Thu Feb 4 14:05:54 2016 -1503 days 0-19:0-25:0-50
Cisco CallManager SNMP Service Started Activated Thu Feb 4 14:08:14 2016 -1503 days 0-19:0-28:0-10
Scroll down to Cisco Tftp, select it.
And click restart up above.
Directory Services
Cisco DirSync -1503 days 0-19:0-25:0-53
CM Services
Service Name Status: Activation Status Start Time Up Time
Cisco CallManager Started Activated Thu Feb 4 14:08:30 2016 -1503 days 0-19:0-28:0-26
Cisco Unified Mobile Voice Access Service Started Activated Thu Jan 28 05:50:06 2016 -1496 days 0-11:0-10:0-2
Cisco IP Voice Media Streaming App Started Activated Thu Feb 4 14:08:33 2016 -1503 days 0-19:0-28:0-29
Cisco CTIManager Started Activated Thu Feb 4 14:08:20 2016 -1503 days 0-19:0-28:0-16
Cisco Extension Mobility Started Activated Thu Jan 28 05:50:06 2016 -1496 days 0-11:0-10:0-2
Cisco DHCP Monitor Service Started Activated Thu Feb 4 14:05:59 2016 -1503 days 0-19:0-25:0-55
Cisco Intercluster Lookup Service Started Activated Thu Feb 4 14:08:31 2016 -1503 days 0-19:0-28:0-27
Cisco Location Bandwidth Manager Started Activated Thu Feb 4 14:08:42 2016 -1503 days 0-19:0-28:0-38
Cisco Directory Number Alias Sync Started Activated Thu Feb 4 14:06:02 2016 -1503 days 0-19:0-25:0-58
Cisco Directory Number Alias Lookup Started Activated Thu Jan 28 05:50:06 2016 -1496 days 0-11:0-10:0-2
Cisco Dialed Number Analyzer Server Started Activated Thu Feb 4 14:06:04 2016 -1503 days 0-19:0-26:00
Cisco Dialed Number Analyzer Started Activated Thu Jan 28 05:50:11 2016 -1496 days 0-11:0-10:0-7
Cisco Tftp Started Activated Thu Feb 4 14:08:16 2016 -1503 days 0-19:0-28:0-12
CTI Services
Service Name Status: Activation Status Start Time Up Time
Cisco IP Manager Assistant Started Activated Thu Jan 28 05:50:06 2016 -1496 days 0-11:0-10:0-2
Cisco WebDialer Web Service Started Activated Thu Jan 28 05:50:06 2016 -1496 days 0-11:0-10:0-2

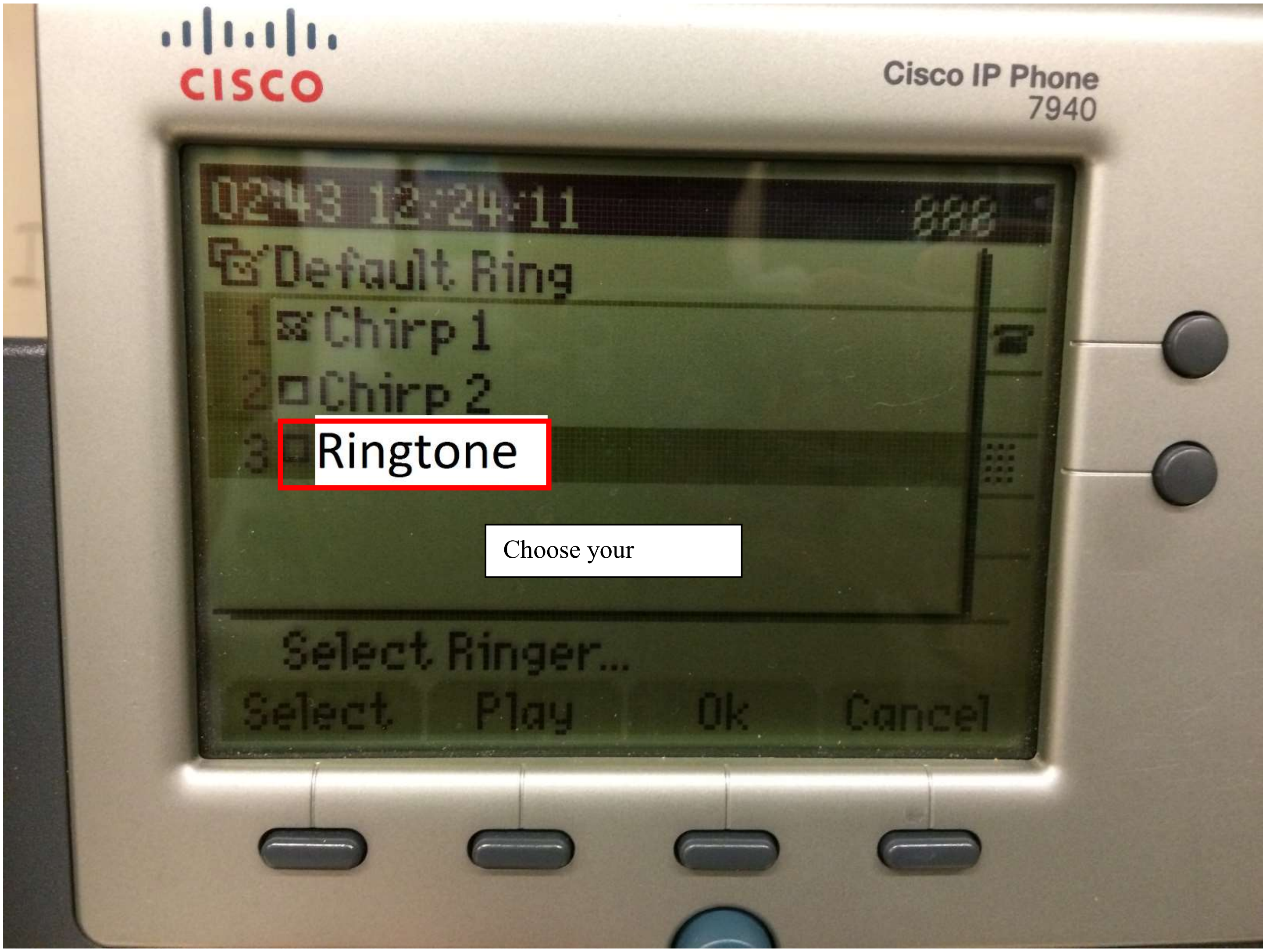


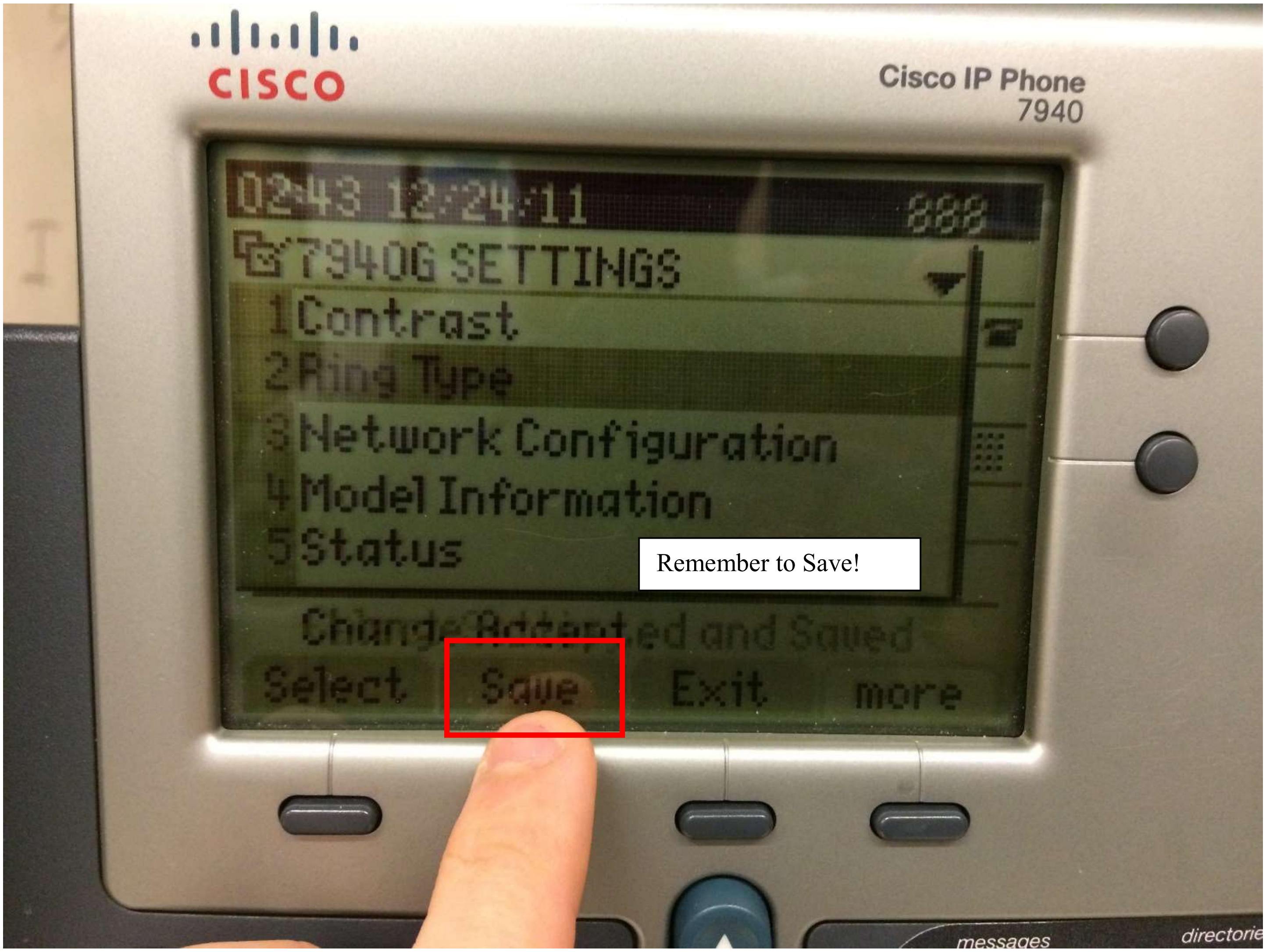
10 seconds later, Tftp should be up and running again.



Press the Settings button, Select Ring


Select Default Ring
Cisco IP Phone
7940
Ring Type
1 Default Ring
Chirp 1
2 888
Chirp 1
Select Line...
Select
Default
Exit


CISCO
Cisco IP Phone
7940
02:43 12/24/11
Default Ring
1 Chirp 1
2 Chirp 2
3 Ringtone
Choose your
Select Ringer...
Select
Play
Ok
Cancel



Problems

This lab was full of problems. When we first started the lab we decided to add shortcuts so that we could call the phones with pressing only one button. After doing that, we reset the phones and somehow phones were never able to open the server. On the displays of the phones it said "Opening 192.168.1.1" which was the IP address of the router but it was supposed to open the server. For some reason the phones couldn't see the server. We later realized that the server stopped working. So we had to restart the server which took a while and after restarting, the phones were able to connect to the server. They were registered.

After the phones were registered, we tried to call one from the other one but the phones were dropping the calls. Everything was looking right. From the settings on the phones to the server. After checking settings with groups whose phones were working, we realized that the partition on the lines have to have none partition. We had partition for our lines, so we had to change the partition to none. After we made the change and applied the configuration to the phones, we were able to call from one phone to the other.

We then started doing the music on hold. We decided to set it up from the "Music on Hold Server". We selected the file and save the configuration. We were trying to check if the music on hold was working or not, so we tried to call the other phone but we were coming across an error message. The message said that the call was dropped because the maximum call number in the network was reached. But there were no ongoing calls on the network. We change the number of maximum possible calls in the network but that did not fix the problem. When we looked at the switch we were using, we saw the port lights were flashing as fast as they could. We realized that something was generating a broadcast message in the network that was taking up all the bandwidth and not letting us make calls. We decided to capture the packets from a PC using Wireshark. As soon as we started the capture, packets started flowing in our screen, we stopped the capture and looked at the sources of these broadcast packets. They were coming from the server. We couldn't figure out where in the server the packets were coming from. We looked in the server for hours and finally realized that "Music on Hold Server" that we created earlier was generating the unwanted broadcast packets. We immediately disabled the server. The switch's lights' flashing rate was back to normal and we were able to make phone calls once again. We also learned that "Music on Hold Server" is not how to configure music on hold on IP phones.

After we managed to configure and successfully upload new music on hold and ring tone we started configuring the dialing-out portion of the lab. We were first entering the commands so that we can configure the router to convert the analog line into digital line. While configuring, we had to figure out which voice port the line was going into, but the ports' numbers were not labeled on the router. So we spent some time going back and forth between the CLI and the router trying to figure out which port we were connected to. After trying a couple of ports we finally figured out which port we were connected to and were able to turn it on.

When the configuration on the router was done, we moved on to the dial-out configuration on the server. We configured everything. From the H323 gateway configurations to the call routing but we weren't able to dial out. We then realized that our server was not seeing the router. There was no IP address for the server that represented the router on the CUCM server. We changed the settings so that the server's name was the router's IP address but not "admin". However that did not solve our problem. We still weren't able to dial-out of our network. Then we realized that in the H323 gateway set up we had to type the IP address of the router again into the description. After doing that our problem was fixed. The server was able to see the router and we were able to dial out and call our own cell phones.

Conclusion

This lab was a more challenging than the first past of this lab. When we started the lab, we were using our pre-configured and pre-registered IP phones however we made mistakes and we went back on our progress. We lost a lot of time to just get the phones to register again and working. Converting the file types was a challenge, took some time but I learned how to use Audacity. Dialing out looked simple in the beginning but we came across simple problems that took more time than they should to solve. I think I learned really important skills despite all the problems we had. I learned how to make a custom ring tone and hold on music. Most importantly, I learned how to dial-out to traditional phones that use analog line from an IP phones that uses digital line.

CCNA Security

CISCO CERTIFIED
CCNA
SECURITY

ASA 5505 Reset

Purpose

The purpose lab was to do password recovery on Cisco ASA 5505, update ASA ASDM versions and launch ASDM image on PC.

Background information on lab concepts:

The Cisco ASA 5505 is a full-featured firewall for small business, branch, and enterprise teleworker environments. It delivers high-performance firewall, SSL and IPsec VPN, and rich networking services in a modular, immediately operational appliance. Using the integrated graphical Cisco Adaptive Security Device Manager (ASDM), the Cisco ASA 5505 can be rapidly deployed and easily managed, helping businesses reduce operational costs. It features a flexible 8-port 10/100 Fast Ethernet switch whose ports can be dynamically grouped to create up to three separate VLANs for home, business, and Internet traffic for improved network segmentation and security.

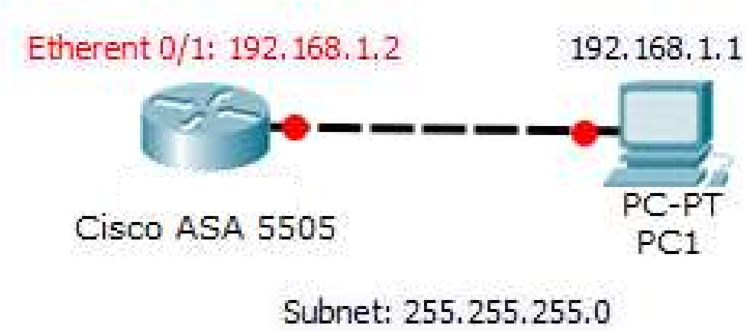
Lab Summary:

Password recovery: We first went into the ASA rommon mode, entered confreg 0x41 and then booted the ASA to remove the existing password.
ASDM image load (TFTP server): To upgrade the ASDM version, we sent the file via TFTP and then deleted the existing image. We entered "copy tftp flash" with the host IP address and file name.
Launching ASDM: We first enabled http server in the ASA, and loaded Java Flash on the PC. Then we went to web browser https://192.168.1.2/admin clicked on launch ASDM. We downloaded the ASDM to the PC, opened the program, entered ASA IP address username and password. ASDM was up and running.

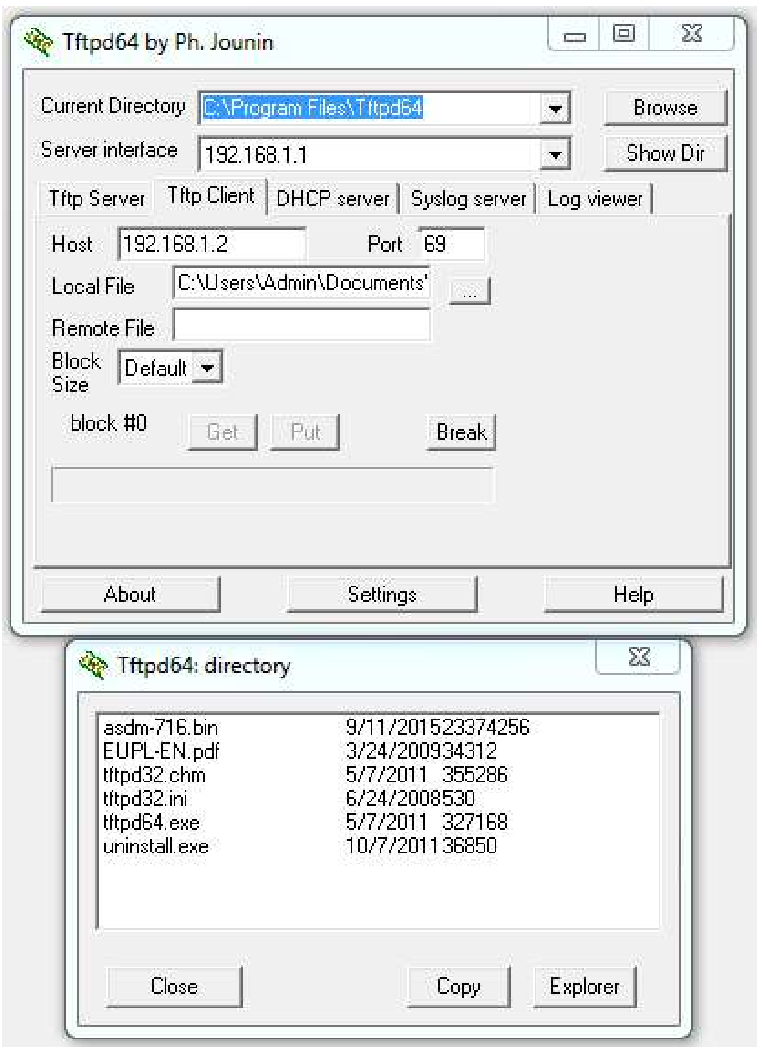
Lab commands:

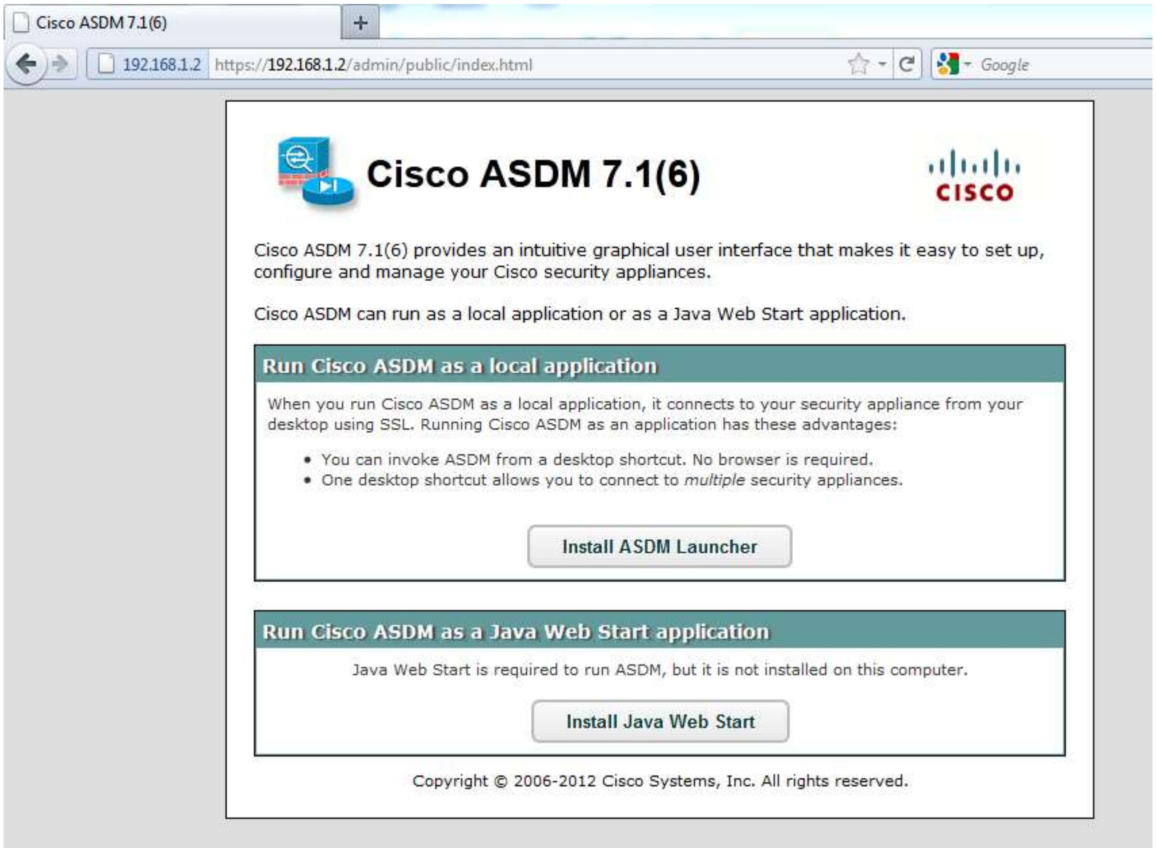
`rommon #0>confreg 0x41`	This command deletes the existing password that blocks users to change modes in the ASA.
`rommon #1>boot`	With this command, the ASA exits the rommon mode and boots up the device.
`copy tftp flash`	This command uploads the file to the ASA that was sent from the TFTP server.
`http server enable`	This command enables the Cisco ASA to be a web server including the Cisco web browser user interface.
`http` *`192.168.1.0 255.255.255.`***`0 management`**	This command defines networks that can access the Cisco web browser user interface.
`username` *`admin`* **`password`** *`cisco`* **`privilege 15`**	This command sets an username and password for remote users to access the Cisco ASA 5505's web browser user interface.
`asdm image` *`asdm-716.bin`*	This command changes the running ASDM image on the ASA with a file (asdm-716.bin, in this case) that is uploaded to the ASA earlier.

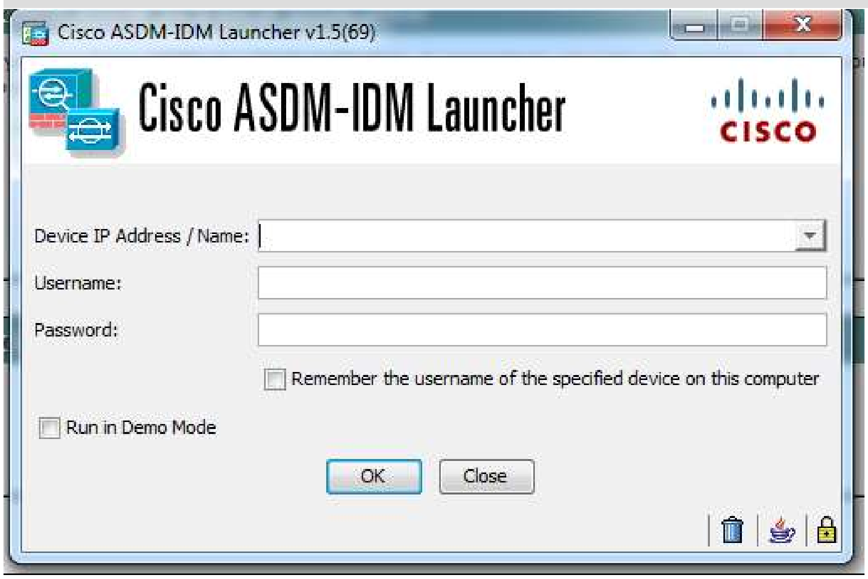
Network Diagram:

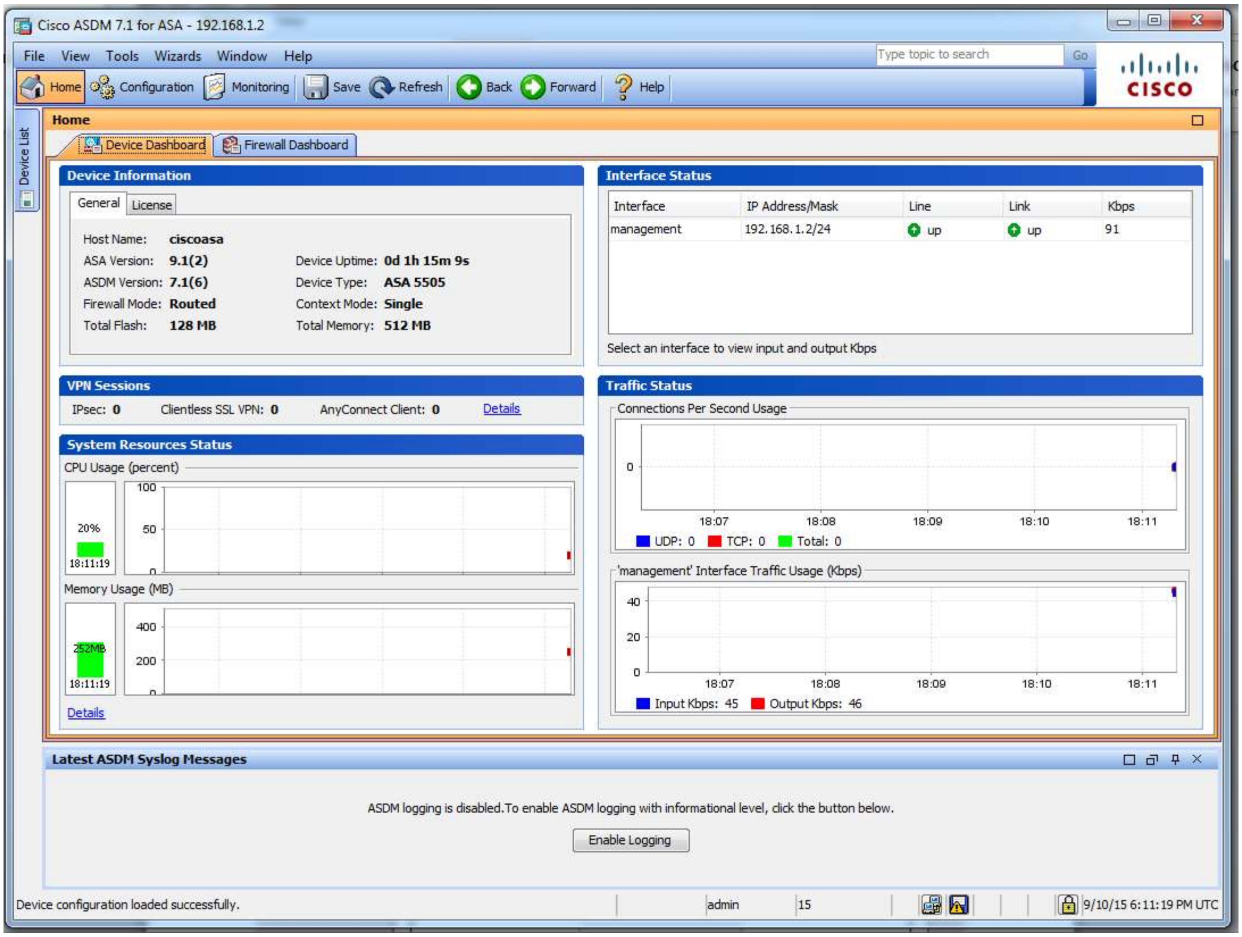


ASDM settings:




Cisco ASDM 7.1(6)
192.168.1.2 https://192.168.1.2/admin/public/index.html
Google
Cisco ASDM 7.1(6)
CISCO
Cisco ASDM 7.1(6) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco security appliances.
Cisco ASDM can run as a local application or as a Java Web Start application.
Run Cisco ASDM as a local application
When you run Cisco ASDM as a local application, it connects to your security appliance from your desktop using SSL. Running Cisco ASDM as an application has these advantages:
• You can invoke ASDM from a desktop shortcut. No browser is required.
• One desktop shortcut allows you to connect to multiple security appliances.
Install ASDM Launcher
Run Cisco ASDM as a Java Web Start application
Java Web Start is required to run ASDM, but it is not installed on this computer.
Install Java Web Start
Copyright © 2006-2012 Cisco Systems, Inc. All rights reserved.


Cisco ASDM-IDM Launcher v1.5(69)
Cisco ASDM-IDM Launcher
CISCO
Device IP Address / Name:
Username:
Password:
Remember the username of the specified device on this computer
Run in Demo Mode
OK
Close


Cisco ASDM 7.1 for ASA - 192.168.1.2
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Home
Device Dashboard
Firewall Dashboard
Device Information
General License
Host Name: ciscoasa
ASA Version: 9.1(2)
Device Uptime: 0d 1h 15m 9s
ASDM Version: 7.1(6)
Device Type: ASA 5505
Firewall Mode: Routed
Context Mode: Single
Total Flash: 128 MB
Total Memory: 512 MB
Interface Status
Interface IP Address/Mask Line Link Kbps
management 192.168.1.2/24 up up 91
Select an interface to view input and output Kbps
VPN Sessions
IPsec: 0 Clientless SSL VPN: 0 AnyConnect Client: 0 Details
Traffic Status
Connections Per Second Usage
UDP: 0 TCP: 0 Total: 0
System Resources Status
CPU Usage (percent)
Memory Usage (MB)
Details
'management' Interface Traffic Usage (Kbps)
Input Kbps: 45 Output Kbps: 46
Latest ASDM Syslog Messages
ASDM logging is disabled.To enable ASDM logging with informational level, click the button below.
Enable Logging
Device configuration loaded successfully.
admin
15
9/10/15 6:11:19 PM UTC

ASA

Show run

```
ASA Version 9.1(2)
hostname ciscoasa
domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
names

interface Ethernet0/0
 shutdown
interface Ethernet0/1
interface Ethernet0/2
interface Ethernet0/3
interface Ethernet0/4
interface Ethernet0/5
interface Ethernet0/6
interface Ethernet0/7
interface Vlan1
 nameif management
 security-level 0
 ip address 192.168.1.2 255.255.255.0
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
pager lines 24
mtu management 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-716.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
```

```
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
username admin password f3UhLvUj1QsXsuK7 encrypted privilege 15
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:3ca8f79396fb78cd9465f86adfd33c59
: end
```

Show ip route:

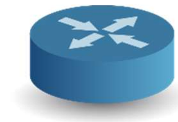
```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, 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 not set

C    192.168.1.0 255.255.255.0 is directly connected, management
```

Problems

We had a hard time sending the asdm file via tftp but we finally sent it. Then we had another problem. The ASA was still using the old asdm image. Then we did some research and found out that we have to put in the “asdm image asdm-716.bin” command.
When we were going to download the asdm on the PC and had to enter the ip address of the asa to the browser we forgot to put https:// in the url bar. We were not able to access the asa for a while because of that but we figured it out after some research.

Conclusion

This lab was challenging in the beginning since I did not have any knowledge of the ASA. It was easy to figure out how to do password recovery however figuring out what ASDM was and how it worked was really challenging. After our hard work, I now understand how ASA’s work and how to set up ASDM. Steps to set up the ASDM can be tricky while doing it for the first time but after doing it once, I realized that it was easy and required couple of simple steps.



Site-to-Site VPN

Purpose

The purpose of this lab was to create site-to-site VPN between two ASA 5505s and encrypt the traffic in between.

Background Information

Site-to-site Virtual Private Network (VPN) is a secure way connect remote networks using the internet's infrastructure. For example a company that has buildings around the world can use VPN to securely connect their networks in different continents.

Two sites that are connected with Site-to-Site VPN use can use Cisco ASA5505s. One ASA encrypts the information that is sent from the one local site so that the information cannot be seen by anyone who is connected to the internet. And the second ASA that is receiving the information from the first local site decrypts the information makes it available for the hosts in the second local site.

Site-to-site VPN can be viewed like an imaginary tunnel in a highway. The highway represents the internet and the cars are the packets going through. VPN is like an imaginary tunnel and no one can see the see the cars that are going through that tunnel and the tunnel is almost indestructible. The entrance and the exit to the tunnel is like the ASAs.

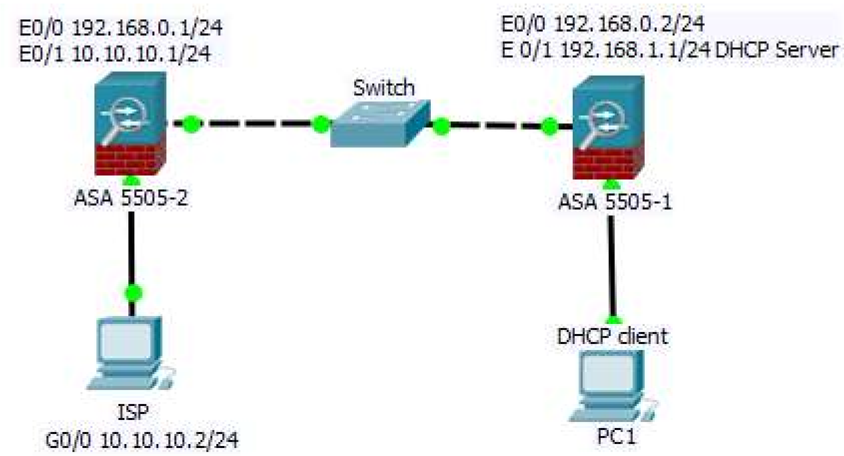
Lab Summary

In order to do this lab, we needed two Cisco ASA 5505's. We already had one ASA with latest version software but the other ASA we grabbed was an old version so we first installed the new software for the new ASA we got and for its ASDM too. We cabled the two firewalls, two PCs and a switch. We first configured and established connectivity between PCs by configuring OSPF on both ASAs. Once we configured OSPF we started configuring the Site-to-site VPN. We launched ASDM on the first ASA and from the ASDM we used the wizard to set up a Site-to-site VPN connection with a remote network which was using the second ASDM. We also used wizard on the second ASA using the ASDM and used the remote network as the network PC1 and ASA 1 is in. After setting up site to site-to-site VPN in both sides we saw on the ASDM that there was an IPsec connection. We then connected a laptop to the switch, launched Wireshark on the laptop and started monitoring the traffic between the two ASAs. All the packets we got were encrypted including the ping packets that were going between two hosts which meant that the site-to-site VPN was successful.

Lab Commands

monitor session *1* **source interface** *Fa0/1*	This command is used in the switch and it allows the device that is connected to fa0/1 to monitor the traffic that is going through the switch.
access-list inside_access_in extended permit icmp any any	This command allows the ping access through the ASA.
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac	This command tells the router to use IPsec and IKEv1 to do cryptography (or encryption which is the same thing) and to also use 3 transform sets which use ESP, AES-128, SHA; ESP, AES; and ESP, SHA, HMAC.
crypto ikev2 policy *1*	This command creates a IKEv2 policy and gives at a name (1 in this case). It also enters the IKEv2 policy configuration mode.
encryption aes-256	This command enables the AES-256 which is a type of encryption in the policy.
integrity sha	This command defines what type of integrity hash algorithm the policy is going to be using, which is “sha” in this case.
group *5 2*	This command specifies the Diffie-Hellman (DH) (a protocol used for two users to generate a shared private key) group. 5 specifies 1536-bit DH and 2 specifies 1024-bit DH.
prf sha	This command defines what type of Pseudo-Random Function (PRF)algorithm the policy is going to be using, which is “sha” in this case.
lifetime seconds *86400*	This command specifies the lifetime for the IKEv2 Security Association (SA) in seconds.
crypto ipsec ikev2 ipsec-proposal AES256	This command is telling the ASA to use IPsec and IKEv2 protocol to do cryptography (or encryption which is the same thing) and also to use the AES256 encryption algorithm.
protocol esp encryption aes-256	This command uses the AES-256 encryption, that belongs to Encapsulating Security Payload (ESP) which is a member of the IPsec protocol suite, to encrypt the traffic.
protocol esp integrity sha-1 md5	This command uses MD5 hashing algorithm and SHA-1, which both belong to ESP, as the type of integrity for the site-to-site VPN.

Network Diagram



Configurations

Switch
Show run:

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname Switch
ip subnet-zero
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
interface FastEthernet0/1
 no ip address
interface FastEthernet0/2
 no ip address
interface FastEthernet0/3
 no ip address
interface FastEthernet0/4
 no ip address
interface FastEthernet0/5
 no ip address
interface FastEthernet0/6
 no ip address
interface FastEthernet0/7
 no ip address
interface FastEthernet0/8
 no ip address
interface FastEthernet0/9
 no ip address
```

```
interface FastEthernet0/10
 no ip address
interface FastEthernet0/11
 no ip address
interface FastEthernet0/12
 no ip address
interface FastEthernet0/13
 no ip address
interface FastEthernet0/14
 no ip address
interface FastEthernet0/15
 no ip address
interface FastEthernet0/16
 no ip address
interface FastEthernet0/17
 no ip address
interface FastEthernet0/18
 no ip address
interface FastEthernet0/19
 no ip address
interface FastEthernet0/20
 no ip address
interface FastEthernet0/21
 no ip address
interface FastEthernet0/22
 no ip address
interface FastEthernet0/23
 no ip address
interface FastEthernet0/24
 no ip address
interface GigabitEthernet0/1
 no ip address
interface GigabitEthernet0/2
 no ip address
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
ip http server
line con 0
line vty 5 15
monitor session 1 source interface Fa0/1
monitor session 1 destination interface Fa0/3 encapsulation dot1q
end
```

ASA 5505-1
Show run:

```
: Saved
: Serial Number: JMX1617Z2JE
: Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
ASA Version 9.2(4)
```

```
hostname ciscoasa1
enable password 8Ry2YjIyt7RRXU24 encrypted
names
interface Ethernet0/0
 switchport access vlan 2
interface Ethernet0/1
interface Ethernet0/2
interface Ethernet0/3
interface Ethernet0/4
interface Ethernet0/5
interface Ethernet0/6
interface Ethernet0/7
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
interface Vlan2
 nameif outside
 security-level 0
 ip address 192.168.0.2 255.255.255.0
ftp mode passive
object network obj_any
 subnet 0.0.0.0 0.0.0.0
access-list inside_access_in extended permit icmp any any
access-list inside_access_in extended permit tcp any any eq www
access-list inside_access_in extended permit ip any any
access-list global_access extended permit icmp any any
access-list global_access extended permit tcp any any eq www
access-list outside_access_in extended permit icmp any any
access-list outside_access_in extended permit tcp any any eq www
access-list outside_access_in extended permit ip any any
access-list outside_cryptomap extended permit ip 192.168.1.0
255.255.255.0 10.10.10.0 255.255.255.0
pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group inside_access_in in interface inside
access-group outside_access_in in interface outside
access-group global_access global
router ospf 1
 network 192.168.0.0 255.255.255.0 area 0
 network 192.168.1.0 255.255.255.0 area 0
 log-adj-changes
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
```

```
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
http 192.168.1.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-
hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-
hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-
hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-
hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS esp-aes esp-
sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS esp-aes esp-
md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS esp-aes-192
esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS esp-aes-192
esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS esp-aes-256
esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS esp-aes-256
esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS esp-3des esp-sha-
hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS esp-3des esp-md5-
hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
```

```
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS esp-des esp-sha-
hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS esp-des esp-md5-
hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS mode transport
crypto ipsec ikev2 ipsec-proposal DES
 protocol esp encryption des
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal 3DES
 protocol esp encryption 3des
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES
 protocol esp encryption aes
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES192
 protocol esp encryption aes-192
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec security-association pmtu-aging infinite
crypto map outside_map 1 match address outside_cryptomap
crypto map outside_map 1 set peer 192.168.0.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA ESP-
AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-
256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto map outside_map 1 set ikev2 ipsec-proposal AES256 AES192 AES
3DES DES
crypto map outside_map interface outside
crypto ca trustpool policy
crypto ikev2 policy 1
 encryption aes-256
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 10
 encryption aes-192
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 20
 encryption aes
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 30
 encryption 3des
 integrity sha
```

```
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 40
 encryption des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 enable outside
crypto ikev1 enable outside
crypto ikev1 policy 10
 authentication crack
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 20
 authentication rsa-sig
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 30
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 40
 authentication crack
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 50
 authentication rsa-sig
 encryption aes-192
 hash sha
group 2
 lifetime 86400
crypto ikev1 policy 60
 authentication pre-share
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 70
 authentication crack
 encryption aes
 hash sha
 group 2
```

```
 lifetime 86400
crypto ikev1 policy 80
 authentication rsa-sig
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 90
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 100
 authentication crack
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 110
 authentication rsa-sig
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 120
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 130
 authentication crack
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 140
 authentication rsa-sig
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 150
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
no ssh stricthostkeycheck
ssh timeout 5
```

```
ssh key-exchange group dh-group1-sha1
console timeout 0
dhcpd auto_config outside
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
threat-detection basic-threat
threat-detection statistics port
threat-detection statistics protocol
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
group-policy GroupPolicy_192.168.0.1 internal
group-policy GroupPolicy_192.168.0.1 attributes
 vpn-tunnel-protocol ikev1 ikev2
username admin password f3UhLvUj1QsXsuK7 encrypted
tunnel-group 192.168.0.1 type ipsec-l2l
tunnel-group 192.168.0.1 general-attributes
 default-group-policy GroupPolicy_192.168.0.1
tunnel-group 192.168.0.1 ipsec-attributes
 ikev1 pre-shared-key *****
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
Cryptochecksum:fb887c986d6a6129c7b5d4d87b3195f9
: end
```

Show route:

```
O        10.10.10.0 255.255.255.0 [110/20] via 192.168.0.1, 00:28:49,
outside
C        192.168.0.0 255.255.255.0 is directly connected, outside
L        192.168.0.2 255.255.255.255 is directly connected, outside
C        192.168.1.0 255.255.255.0 is directly connected, inside
L        192.168.1.1 255.255.255.255 is directly connected, inside
```

Cisco ASA 5505-2
Show run:

```
: Saved
: Serial Number: JMX1237Z0AT
: Hardware:   ASA5505, 1024 MB RAM, CPU Geode 500 MHz
ASA Version 9.2(4)
hostname ciscoasa2
enable password 8Ry2YjIyt7RRXU24 encrypted
names
interface Ethernet0/0
 switchport access vlan 2
interface Ethernet0/1
interface Ethernet0/2
interface Ethernet0/3
interface Ethernet0/4
interface Ethernet0/5
interface Ethernet0/6
interface Ethernet0/7
interface Vlan1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
interface Vlan2
 nameif outside
 security-level 0
 ip address 192.168.0.1 255.255.255.0
ftp mode passive
object network obj_any
 subnet 0.0.0.0 0.0.0.0
access-list inside_access_in extended permit icmp any any
access-list inside_access_in extended permit ip any any
access-list global_access extended permit icmp any any
access-list outside_access_in extended permit icmp any any
access-list outside_access_in extended permit ip any any
access-list outside_cryptomap extended permit ip 10.10.10.0
255.255.255.0 192.168.1.0 255.255.255.0
pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
```

```
no arp permit-nonconnected
access-group inside_access_in in interface inside
access-group outside_access_in in interface outside
access-group global_access global
router ospf 1
 network 10.10.10.0 255.255.255.0 area 0
 network 192.168.0.0 255.255.255.0 area 0
 log-adj-changes
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
http 192.168.1.0 255.255.255.0 inside
http 10.10.10.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-
hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-
hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-
hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-
hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS esp-aes esp-
sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS esp-aes esp-
md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS esp-aes-192
esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS esp-aes-192
esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS esp-aes-256
esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS esp-aes-256
esp-md5-hmac
```

```
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS esp-3des esp-sha-
hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS esp-3des esp-md5-
hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS esp-des esp-sha-
hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS esp-des esp-md5-
hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS mode transport
crypto ipsec ikev2 ipsec-proposal DES
 protocol esp encryption des
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal 3DES
 protocol esp encryption 3des
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES
 protocol esp encryption aes
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES192
 protocol esp encryption aes-192
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec security-association pmtu-aging infinite
crypto map outside_map 1 match address outside_cryptomap
crypto map outside_map 1 set peer 192.168.0.2
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA ESP-
AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-
256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto map outside_map 1 set ikev2 ipsec-proposal AES256 AES192 AES
3DES DES
crypto map outside_map interface outside
crypto ca trustpool policy
crypto ikev2 policy 1
 encryption aes-256
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 10
 encryption aes-192
 integrity sha
 group 5 2
```

```
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 20
 encryption aes
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 30
 encryption 3des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 40
 encryption des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 enable outside
crypto ikev1 enable outside
crypto ikev1 policy 10
 authentication crack
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 20
 authentication rsa-sig
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 30
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 40
 authentication crack
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 50
 authentication rsa-sig
 encryption aes-192
 hash sha
group 2
 lifetime 86400
```

```
crypto ikev1 policy 60
 authentication pre-share
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 70
 authentication crack
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 80
 authentication rsa-sig
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 90
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 100
 authentication crack
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 110
 authentication rsa-sig
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 120
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 130
 authentication crack
 encryption des
 hash sha
group 2
 lifetime 86400
crypto ikev1 policy 140
 authentication rsa-sig
 encryption des
 hash sha
```

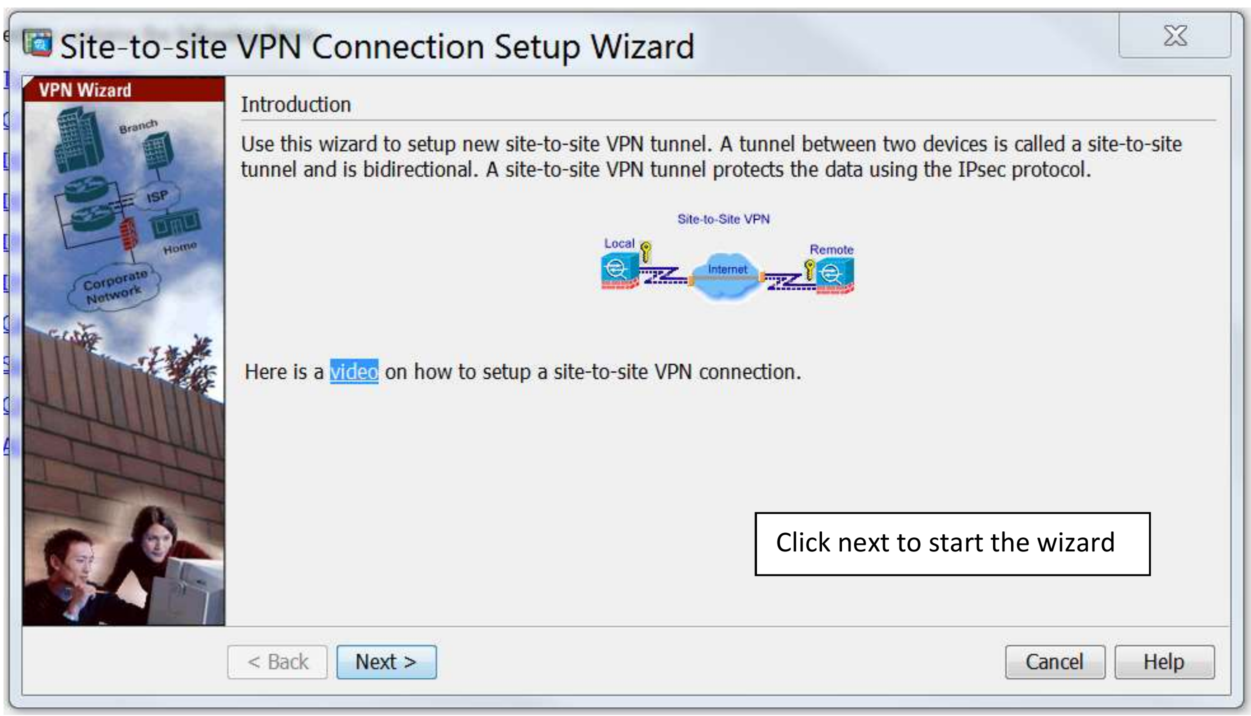
```
 group 2
 lifetime 86400
crypto ikev1 policy 150
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
no ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
group-policy GroupPolicy_192.168.0.2 internal
group-policy GroupPolicy_192.168.0.2 attributes
 vpn-tunnel-protocol ikev1 ikev2
username admin password f3UhLvUj1QsXsuK7 encrypted
tunnel-group 192.168.0.2 type ipsec-l2l
tunnel-group 192.168.0.2 general-attributes
 default-group-policy GroupPolicy_192.168.0.2
tunnel-group 192.168.0.2 ipsec-attributes
 ikev1 pre-shared-key *****
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
 inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
service-policy global_policy global
prompt hostname context
```

```
call-home reporting anonymous prompt 1
Cryptochecksum:7ca3fd27bb0a68ec05f4a5722995901e
: end
```

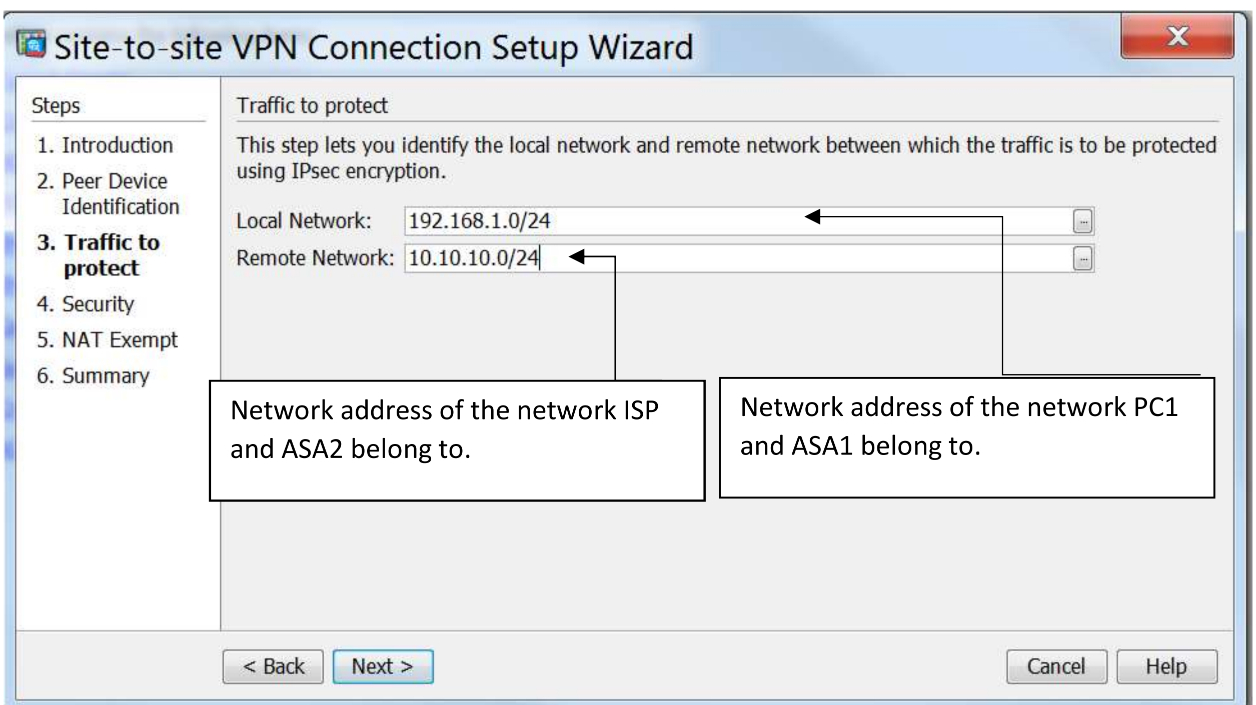
Show route

```
C        10.10.10.0 255.255.255.0 is directly connected, inside
L        10.10.10.1 255.255.255.255 is directly connected, inside
C        192.168.0.0 255.255.255.0 is directly connected, outside
L        192.168.0.1 255.255.255.255 is directly connected, outside
O     192.168.1.0 255.255.255.0 [110/20] via 192.168.0.2, 00:29:09,
outside
```

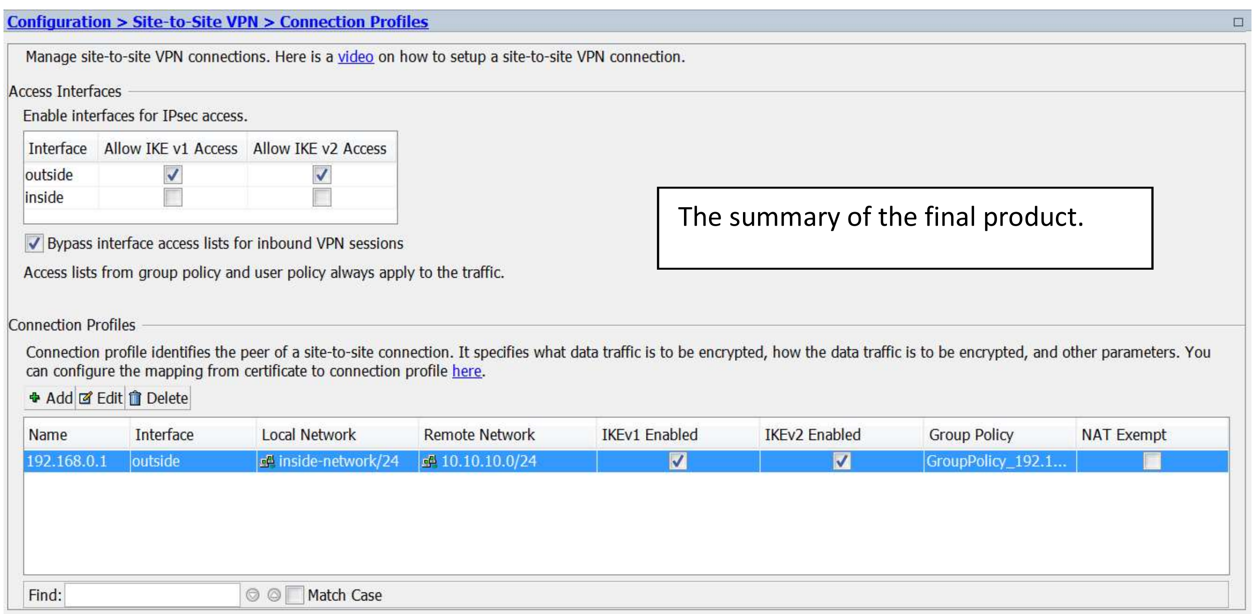
Setting up the Wizard on *ASA 5505-1*



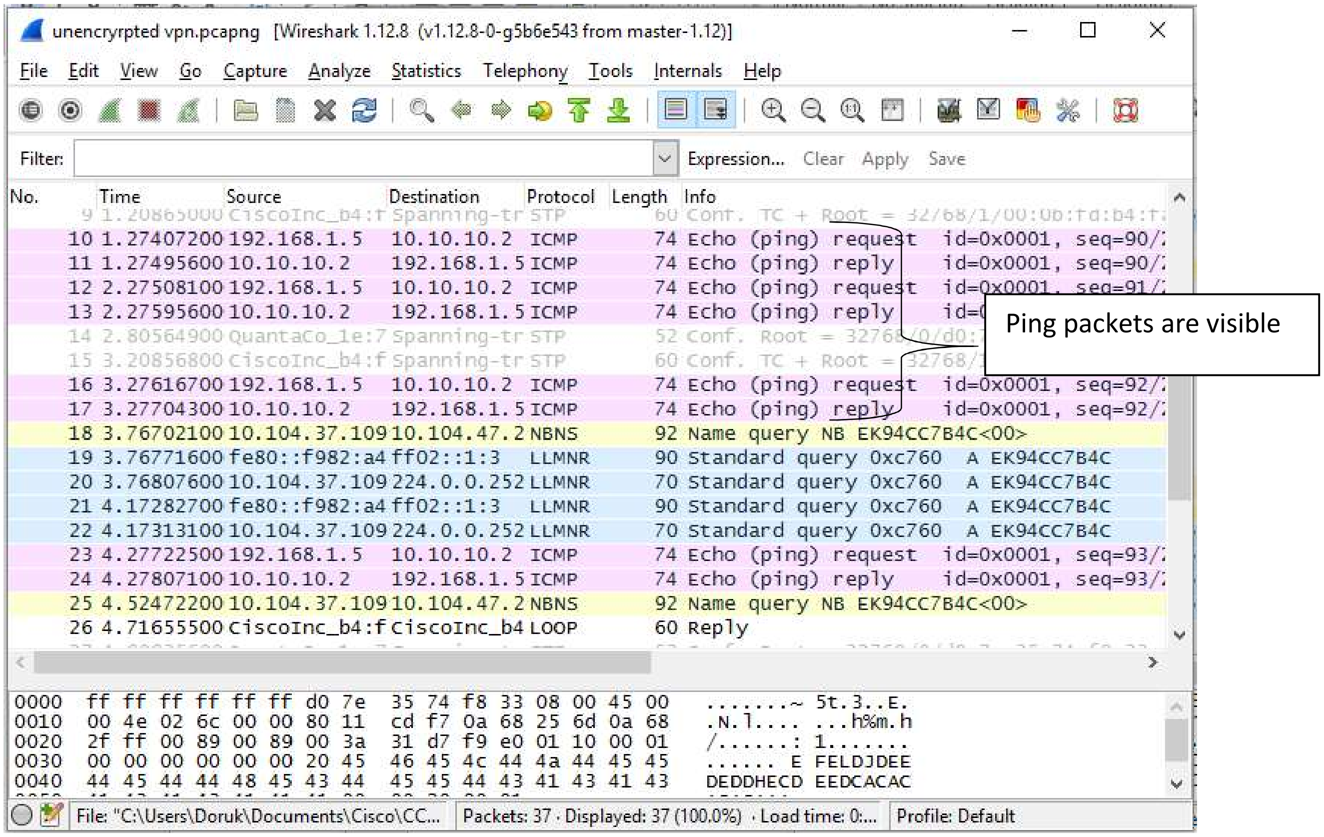

Site-to-site VPN Connection Setup Wizard
Steps
1. Introduction
2. Peer Device Identification
3. Traffic to protec
4. Security
5. NAT Exempt
6. Summary
Peer Device Identification
This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.
Peer IP Address: 192.168.0.1
VPN Access Interface: outside
Use the IP address of the outside interface of the remote network that you are trying to establish VPN connection with.
< Back
Next >
Cancel
Help


Site-to-site VPN Connection Setup Wizard
Steps
1. Introduction
2. Peer Device Identification
3. Traffic to protect
4. Security
5. NAT Exempt
6. Summary
Traffic to protect
This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption.
Local Network: 192.168.1.0/24
Remote Network: 10.10.10.0/24
Network address of the network ISP and ASA2 belong to.
Network address of the network PC1 and ASA1 belong to.
< Back
Next >
Cancel
Help

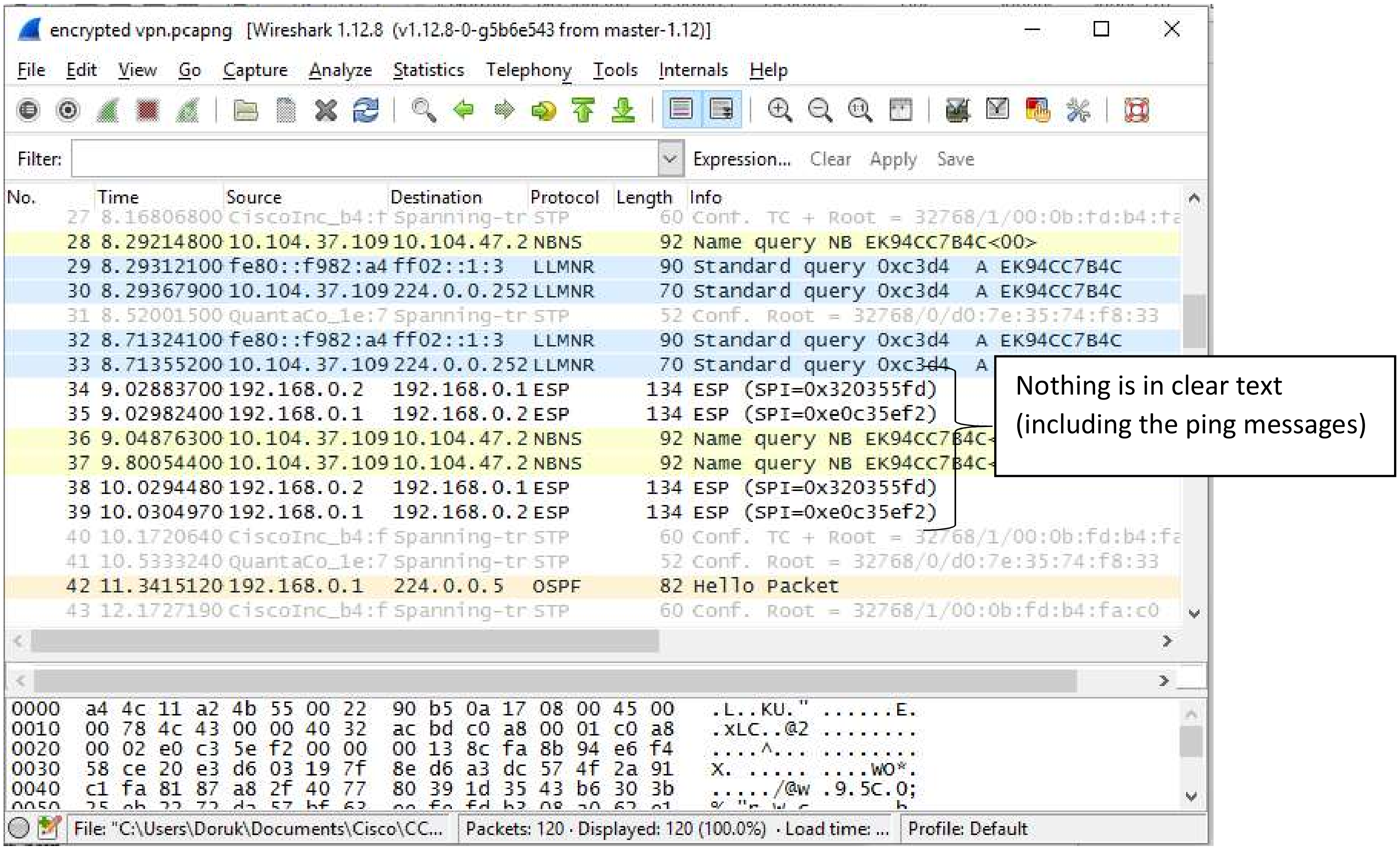

Site-to-site VPN Connection Setup Wizard
Steps
1. Introduction
2. Peer Device Identification
3. Traffic to protec
4. Security
5. NAT Exempt
6. Summary
Security
This step lets you secure the selected traffic.
Simple Configuration
ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer.
Pre-shared Key: •••••
Set up a password that is the same as the one on the other ASA.
Customized Configuration
You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.
< Back
Next >
Cancel
Help


Configuration > Site-to-Site VPN > Connection Profiles
Manage site-to-site VPN connections. Here is a video on how to setup a site-to-site VPN connection.
Access Interfaces
Enable interfaces for IPsec access.
Interface
Allow IKE v1 Access
Allow IKE v2 Access
outside
inside
Bypass interface access lists for inbound VPN sessions
Access lists from group policy and user policy always apply to the traffic.
The summary of the final product.
Connection Profiles
Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be encrypted, and other parameters. You can configure the mapping from certificate to connection profile here.
Add
Edit
Delete
Name
Interface
Local Network
Remote Network
IKEv1 Enabled
IKEv2 Enabled
Group Policy
NAT Exempt
192.168.0.1
outside
inside-network/24
10.10.10.0/24
GroupPolicy_192.1...
Find:
Match Case

Not encrypted Wireshark capture between ASA 5505-1 and DHCP client:



Encrypted Wireshark capture between ASA 5505-1 and ASA 5505-2:



Problems

First day:
Host cannot ping 10.10.10.1
Router can ping 10.10.10.1 cannot ping 192.168.1.1
removed the dhcp setroute command still not working
set access rules for permitting icmp any to any still not working

Second day:
G0/0 port was down
We were configuring a different router
Switch the cables
working

same problem as yesterday

decided to use dhcp
asa couldn't get an ip from dhcp
forgot to change router from 10.10.10.2 to 192.168.0.1
working

made an access rule to permimt any to any icmp host able to ping 192.168.0.1 but not the dhcp ip

Third day:
pings were working
only have icmp packets

Fourth day:
host cannot ping 192.168.0.1
tried removing VPN commands didn't work
isolated the switch and it works
there's a problem with the switch
reload switch
there were saved crypto configs on switch

Fifth day:
host cannot ping 10.10.10.1 (can’t get access to asdm)
reload asa
working

host can ping 192.168.1.1 but can’t access asdm
re-download the launcher
working

Sixth day:
host cannot ping 10.10.10.2

no sessions after configuration
after #show crypto isakmp sa
there is an entry dest: 192.168.0.3 src 192.168.0.1 but the status is ACTIVE (deleted)

Seventh day:
Added a router at the end
didn't work

Eighth day:
Added an ASA
ASA wouldn't update from 9.1 to the 924 version after we load the image in
updated ASDM from 7.1 to 7.5 version

ASA2 cannot access asdm
show run
http command wrong network address

Ninth day:
PC can ping ASA but not the opposite PC
deleted NAT rule in ASDM
able to ping

We first started the lab with trying to configure site-to-site VPN between a router and a Cisco ASA 5505 however after tries many different configurations and starting over and over again, we couldn't establish VPN between two sites because they were using two different encryption types. So instead of using a router we decided to use another ASA and changed our topology.

While we were using the router, we lost one day because of wrong cabling. Then we lost couple of more days trying to ping the router from the PC that is on the ASA's network. We got rid of DHCP and tried assigning IP addresses but that did not solve the problem so we configured DHCP again. We also thought it might have been a firewall problem but that didn't solve the problem either. After trying for almost a week and checking every option, we decided to delete everything on the ASA and start from starch. We tried configuring site-to-site VPN, on the ASA we were able to see that there were encrypted packets but we weren't able to establish the VPN connection between the ASA and the router. We made more research and tried different configurations for a VPN connection between a Cisco Router and ASA 5505. We tried at least 4 different versions but none of them worked. The encryption types in the ASA and the router were different and we couldn't get them to talk to each other. So we decided to replace the router with an ASA at the end.

After we connected a new ASA we couldn't do anything because the ASA and ASDM software was old and we had to upgrade it. We then upgraded the ASA and set the IP address as well as the OSPF network commands but we then came across connectivity problems. We were able to connect to the ASDM but we couldn't establish the end-to-end connectivity of the network before configuring the VPN. No traffic was going through the ASA, we checked firewall, permitted all traffic, checked the IP addresses and the OSPF but nothing was solving the problem. Then we enabled syslog messages looked at the error messages we got and saw that there was a NAT problem. We went into NAT and saw that there were NAT rules entered by default. We deleted them all and that solved our problem. Now we had end to end connectivity.

Conclusion

I have never configured a VPN connection before. I learned what it is in CCNA routing and switching but it was my first time configuring site-to-site between two remote sites. It was more challenging than I expected to be. The commands that are used in this lab is not easy, short commands. This lab was challenging from the beginning. It took really long and the problems kept coming. Almost every day we came across a different problem and spent the whole day trying to fix it. We made a major change through the lab by adding another Cisco ASA 5505 instead of a router. After weeks of hard work we finally configured site-to-site VPN between two Cisco ASA 5505s. This lab was mostly about troubleshooting and finding new ways to solve problems I have never faced before. I learned a lot in this lab including the configuration of VPN.

Anyconnect VPN

Purpose

The purpose of this lab was to create Cisco Anyconnect VPN between a Cisco ASA 5505 and a remote PC and encrypt the traffic in between.

Background Information

Cisco Anyconnect is a software that uses SSL VPN. It can empower employees of any big company to allow them to work from anywhere, on corporate laptops as well as personal mobile devices, regardless of physical location. And provide the security necessary to help ensure that the company's or the organization's data is safe and protected. Cisco AnyConnect is a unified agent that delivers multiple security services to protect the enterprise. It provides the visibility and the control you need to identify who and what is accessing the extended enterprise before, during, and after an attack. The AnyConnect Client software offers a comprehensive endpoint security platform with remote access functionality, posture enforcement, and web security features. AnyConnect gives the IT departments of big companies and organizations all the secure-access features necessary to provide a robust, user-friendly, and highly secure mobile experience.

Anyconnect is a type of SSL VPN. An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser. In contrast to the traditional Internet Protocol Security (IPsec) VPN, an SSL VPN does not require the installation of specialized client software on the end user's computer. It's used to give remote users with access to Web applications, client/server applications and internal network connections.

A virtual private network (VPN) provides a secure communications mechanism for data and other information transmitted between two endpoints. An SSL VPN consists of one or more VPN devices to which the user connects by using his Web browser. The traffic between the Web browser and the SSL VPN device is encrypted with the SSL protocol.

One can think of VPN like an island in a huge ocean. There are thousands of other islands all around the person who lives in one island, some very close and others farther away. The normal way to travel is to take a ferry from an island to whichever island the person wishes to visit. Traveling on a ferry means that the person has almost no privacy. Anything the person does can be seen by someone else.

Assume that each island represents a private LAN and the ocean is the Internet. When the person travel by ferry, it is similar to when he/she connects to a web server or to another device through the Internet. They have no control over the wires and routers that make up the Internet, just like they have no control over the other people on the ferry. This leaves the person susceptible to security issues if they try to connect between two private networks using a public resource.

The person decides to build a bridge to another island from his/her island so that there is an easier, more secure and direct way for people to travel between the two. It is expensive to build and maintain the bridge, even though the island they are connecting with is very close. But the need for a reliable, secure path is so great that they do it anyway. The person would like to connect to a second island that is much farther away, but they decide that it is too expensive.

This situation is very much like having a leased line. The bridges (leased lines) are separate from the ocean (Internet), yet they are able to connect the islands (LANs). Many companies have chosen this route because of the need for security and reliability in connecting their remote offices. However, if the offices are very far apart, the cost can be prohibitively high - just like trying to build a bridge that spans a great distance. In the cases of long distances, companies can use the existing bridges with their private vehicles which represent the packets going through a network.

Lab Summary

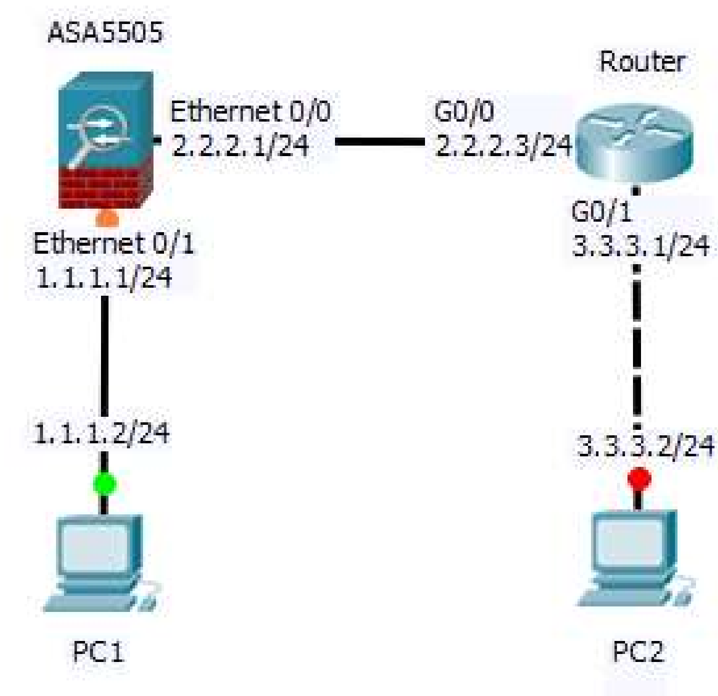
In this lab we first established end to end connectivity between two PCs before we configured and installed Cisco Anyconnect. We had a Cisco ASA 5505 and a router. We set the IP addresses on the PCs and the interfaces on both the router and the ASA. Then we configured OSPF on the ASA and the router and we had connectivity between the PCs after doing that. Then we installed Anyconnect Client software on the PC with the IP address 3.3.3.2. After we installed the software, we had to restart the computer in order for Anyconnect client to work. Then we had to configure the ASA as an Anyconnect server. In order to do that we used the Cisco Anyconnect VPN wizard on the ASDM. We accessed the ASDM, then started the wizard. In the wizard, we first specified that the Anyconnect will serve on the outside interface of the ASA. Then we selected only SSL for the ASA to use and also specified which software the client is going to be using. We then used a local AAA server to configure the usernames and passwords. We also created a new address pool for clients to get IP addresses from, give it a name and enter the starting and ending IP addresses and subnet mask. Since we did not use DNS in this lab, we just skipped the part where the wizard asks for a DNS address. Then we exempted VPN traffic from network address translation. After that was done, the wizard was completed and Anyconnect server on the ASA was configured. Then we went back to the PC to establish the connection. To do that, we entered the outside IP address of the ASA, a username and the password that is associated with that username. We then waited for the client software to connect and after a couple of seconds the VPN connection between the ASA and the client was established.

Lab Commands

Webvpn	This command is used on the ASA to go into the VPN configuration mode to configure SSL VPN.
enable outside	This command enables VPN on the outside interface of the ASA.
anyconnect image disk0:/anyconnect-win-3.1.04066-k9.pkg 1	This command tells the ASA which software the clients are going to be using.
anyconnect enable	This command enables Anyconnect VPN on the ASA.
tunnel-group-list enable	This command is used under the WebVPN configuration mode and enables tunnel groups which consists of a set of records that contain tunnel connection policies.
group-policy GroupPolicy_*doruk* **internal**	To configure a default group policy the GroupPolicy_doruk has to be specified as internal.
group-policy GroupPolicy_*doruk* **attributes**	This command is used to change any of the attributes of the group policy, use this command to enter attributes mode, then specify the commands to change whatever attributes that you want to modify.
tunnel-group *doruk* **type remote-access**	This command is used to creat a remote-access connection profile named doruk.
tunnel-group *doruk* **general-attributes**	This command is used to go into the general-attributes configuration mode to configure general attributes.
address-pool *doruk*	This command assigns IP addresses to VPN clients using the address pool “doruk”.

default-group-policy GroupPolicy_*doruk*	This command specifies the name of the default group policy.
tunnel-group *doruk* **webvpn-attributes**	To specify the attributes of a clientless SSL VPN tunnel-group, enter tunnel-group webvpn-attributes mode by entering this command.
group-alias *doruk* **enable**	To specify alternative names for the group and enable that group, use this command.

Network Diagram



Configurations

Router
Show run:

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX1520806Y
license accept end user agreement
license boot module c2900 technology-package uck9
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 2.2.2.3 255.255.255.0
 duplex auto
 speed auto
 no shutdown
interface GigabitEthernet0/1
 ip address 3.3.3.1 255.255.255.0
 duplex auto
 speed auto
 no shutdown
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 duplex auto
 speed auto
router ospf 1
 network 2.2.2.0 0.0.0.255 area 0
 network 3.3.3.0 0.0.0.255 area 0
```

```
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Show ip route:

```
Gateway of last resort is not set

      1.0.0.0/24 is subnetted, 1 subnets
O        1.1.1.0 [110/11] via 2.2.2.1, 01:28:54, GigabitEthernet0/0
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.2.2.0/24 is directly connected, GigabitEthernet0/0
L        2.2.2.3/32 is directly connected, GigabitEthernet0/0
      3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        3.3.3.0/24 is directly connected, GigabitEthernet0/1
L        3.3.3.1/32 is directly connected, GigabitEthernet0/1
```

ASA 5505

Show run:

```
: Saved
: Serial Number: JMX1617Z2JE
: Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
ASA Version 9.2(4)
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
ip local pool doruk 4.4.4.1-4.4.4.254 mask 255.255.255.0
interface Ethernet0/0
 switchport access vlan 2
interface Ethernet0/1
interface Ethernet0/2
interface Ethernet0/3
interface Ethernet0/4
interface Ethernet0/5
interface Ethernet0/6
```

```
interface Ethernet0/7
interface Vlan1
 nameif inside
 security-level 100
 ip address 1.1.1.1 255.255.255.0
interface Vlan2
 nameif outside
 security-level 0
 ip address 2.2.2.1 255.255.255.0
ftp mode passive
object network obj_any
 subnet 0.0.0.0 0.0.0.0
object network NETWORK_OBJ_4.4.4.0_24
 subnet 4.4.4.0 255.255.255.0
object network NETWORK_OBJ_1.1.1.0_24
 subnet 1.1.1.0 255.255.255.0
access-list inside_access_in extended permit ip any any
access-list inside_access_in extended permit icmp any any
access-list inside_access_in extended permit tcp any any eq www
access-list inside_access_in extended permit tcp any any eq https
access-list global_access extended permit ip any any
access-list global_access extended permit icmp any any
access-list global_access extended permit tcp any any eq www
access-list global_access extended permit tcp any any eq https
access-list outside_access_in extended permit ip any any
access-list outside_access_in extended permit tcp any any eq www
access-list outside_access_in extended permit tcp any any eq https
access-list outside_access_in extended permit icmp any any
pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
nat (outside,outside) source static any any destination static
NETWORK_OBJ_4.4.4.0_24 NETWORK_OBJ_4.4.4.0_24 no-proxy-arp route-
lookup
nat (inside,outside) source static NETWORK_OBJ_1.1.1.0_24
NETWORK_OBJ_1.1.1.0_24 destination static NETWORK_OBJ_4.4.4.0_24
NETWORK_OBJ_4.4.4.0_24 no-proxy-arp route-lookup
nat (inside,outside) source static any any destination static
NETWORK_OBJ_4.4.4.0_24 NETWORK_OBJ_4.4.4.0_24 no-proxy-arp route-
lookup
object network obj_any
 nat (inside,outside) dynamic interface
access-group inside_access_in in interface inside
access-group outside_access_in in interface outside
access-group global_access global
router ospf 1
```

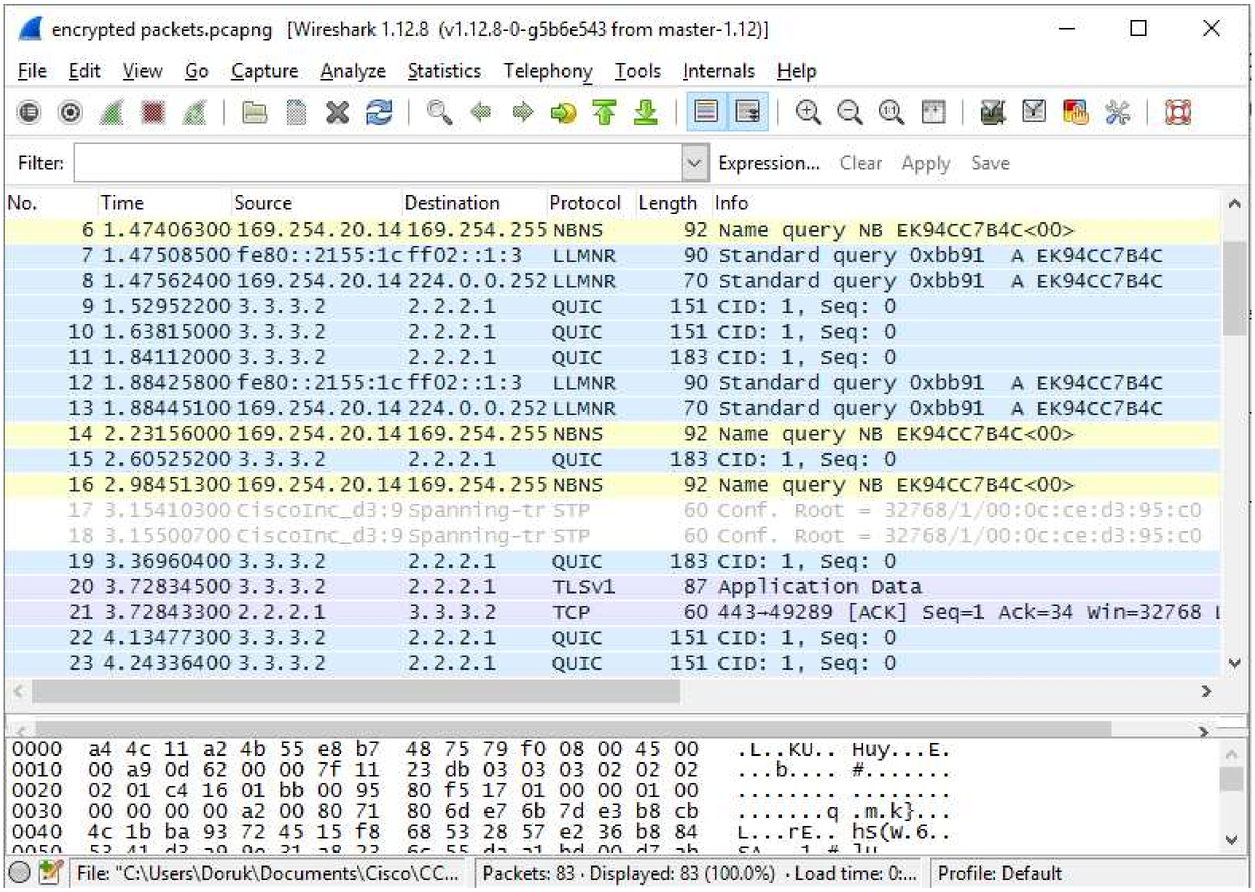
```
 network 1.1.1.0 255.255.255.0 area 0
 network 2.2.2.0 255.255.255.0 area 0
 log-adj-changes
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
http 192.168.1.0 255.255.255.0 inside
http 1.1.1.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
no ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.04066-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
group-policy GroupPolicy_doruk internal
group-policy GroupPolicy_doruk attributes
 wins-server none
 dns-server none
 vpn-tunnel-protocol ssl-client
 default-domain none
username admin password f3UhLvUj1QsXsuK7 encrypted
username doruk password dMmeFSbg9dksQIY8 encrypted
username laurissa password 55TLrsc6HFUw5SJH encrypted
tunnel-group doruk type remote-access
tunnel-group doruk general-attributes
 address-pool doruk
 default-group-policy GroupPolicy_doruk
tunnel-group doruk webvpn-attributes
 group-alias doruk enable
class-map inspection_default
 match default-inspection-traffic
```

```
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
service-policy global_policy global
prompt hostname context
call-home reporting anonymous prompt 2
Cryptochecksum:398d5bdfd512da3fd5b66eb7d8a98d6c
: end
```

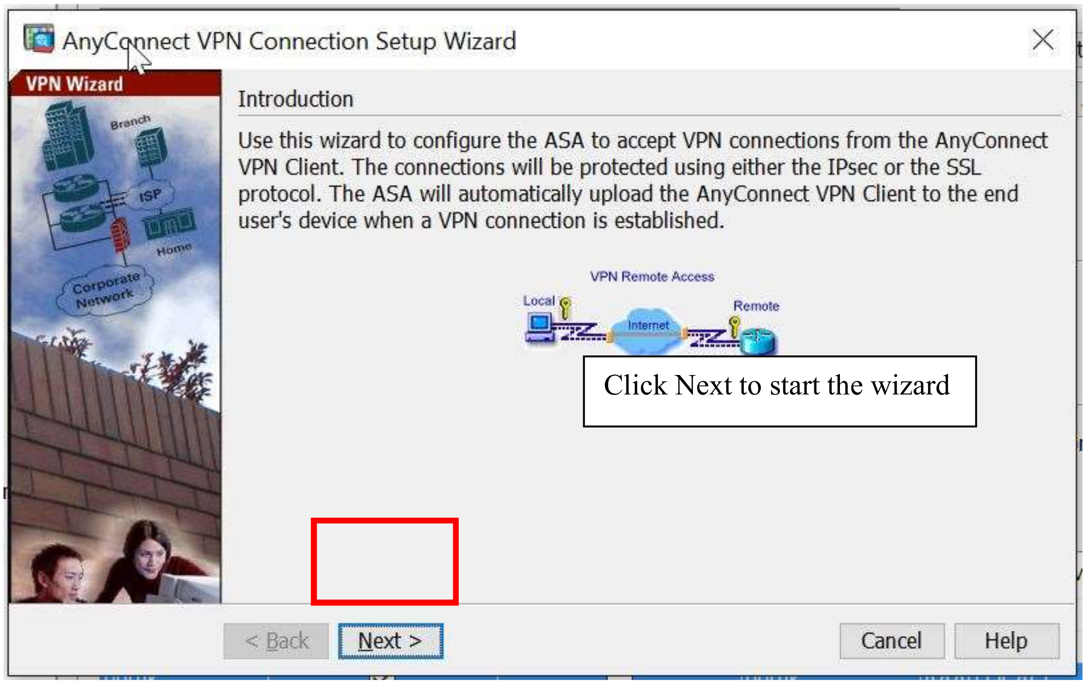
Show route:

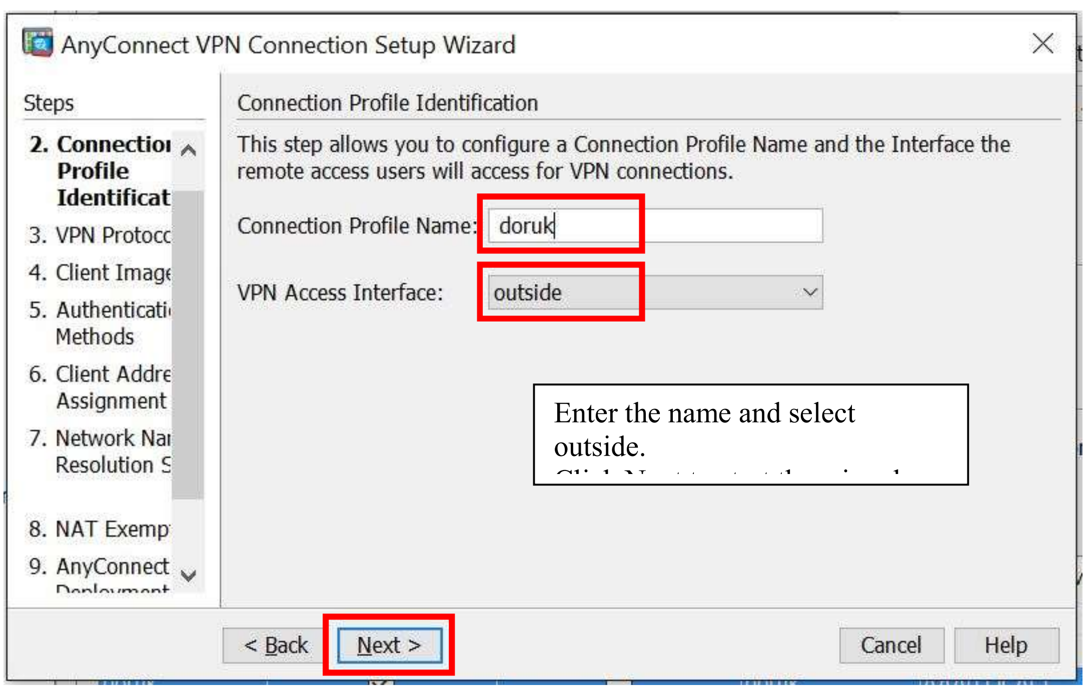
```
Gateway of last resort is not set

C        1.1.1.0 255.255.255.0 is directly connected, inside
L        1.1.1.1 255.255.255.255 is directly connected, inside
C        2.2.2.0 255.255.255.0 is directly connected, outside
L        2.2.2.1 255.255.255.255 is directly connected, outside
O        3.3.3.0 255.255.255.0 [110/11] via 2.2.2.3, 01:27:54, outside
S        4.4.4.1 255.255.255.255 [1/0] via 2.2.2.3, outside
```

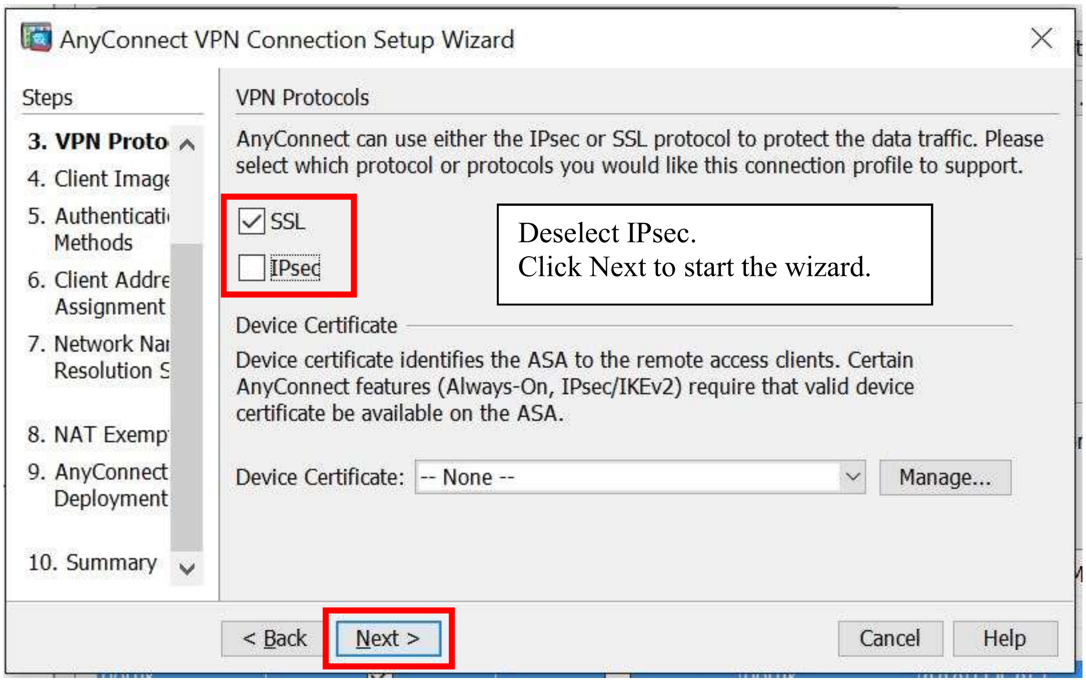
Encrypted Wireshark capture between the ASA 5505 and Router.

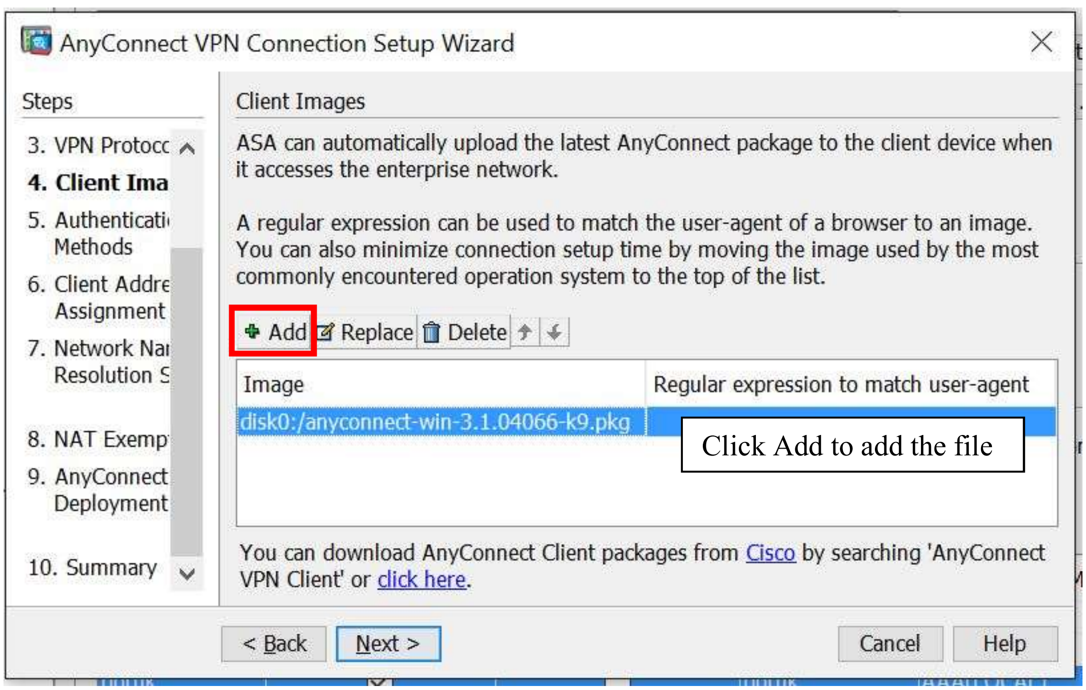


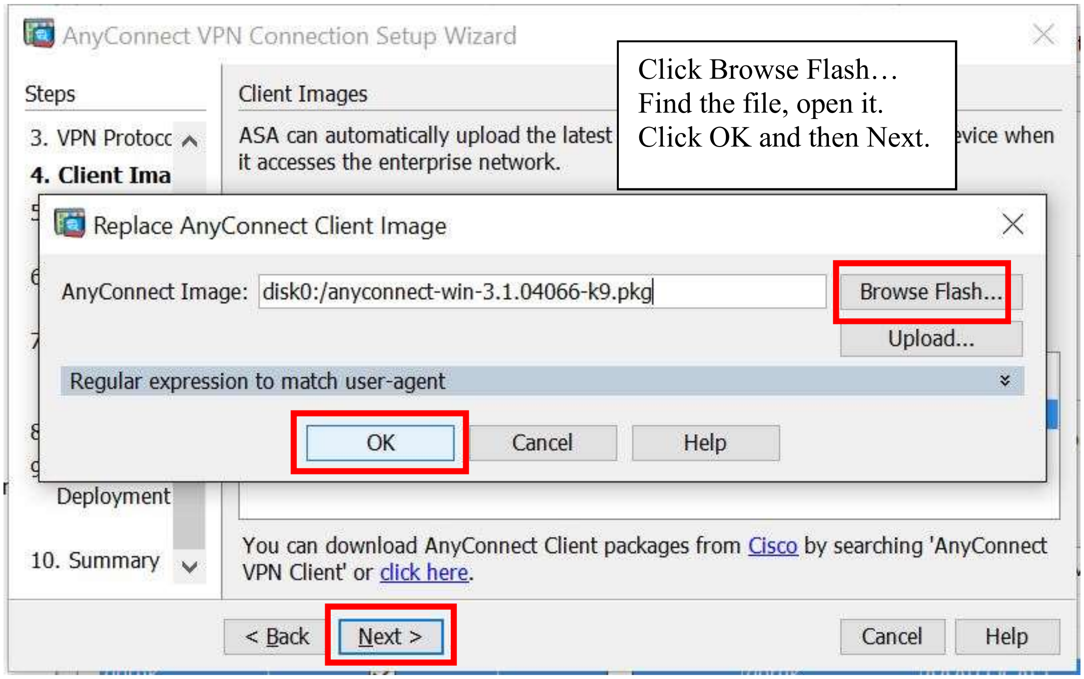
Setting up the Wizard on *ASA 5505*

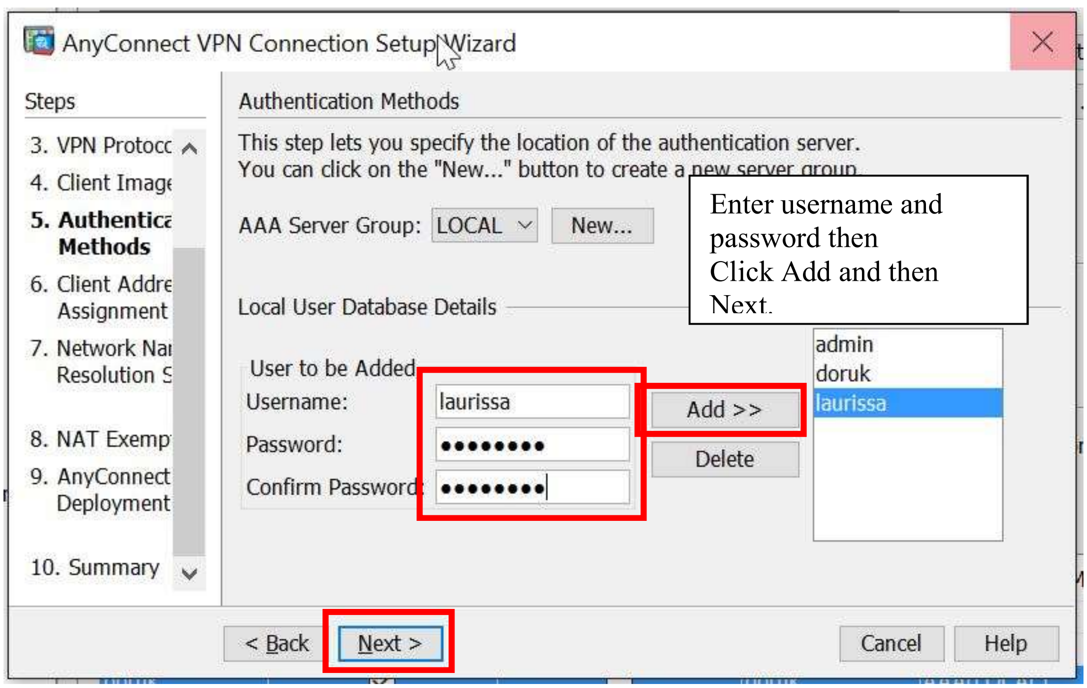


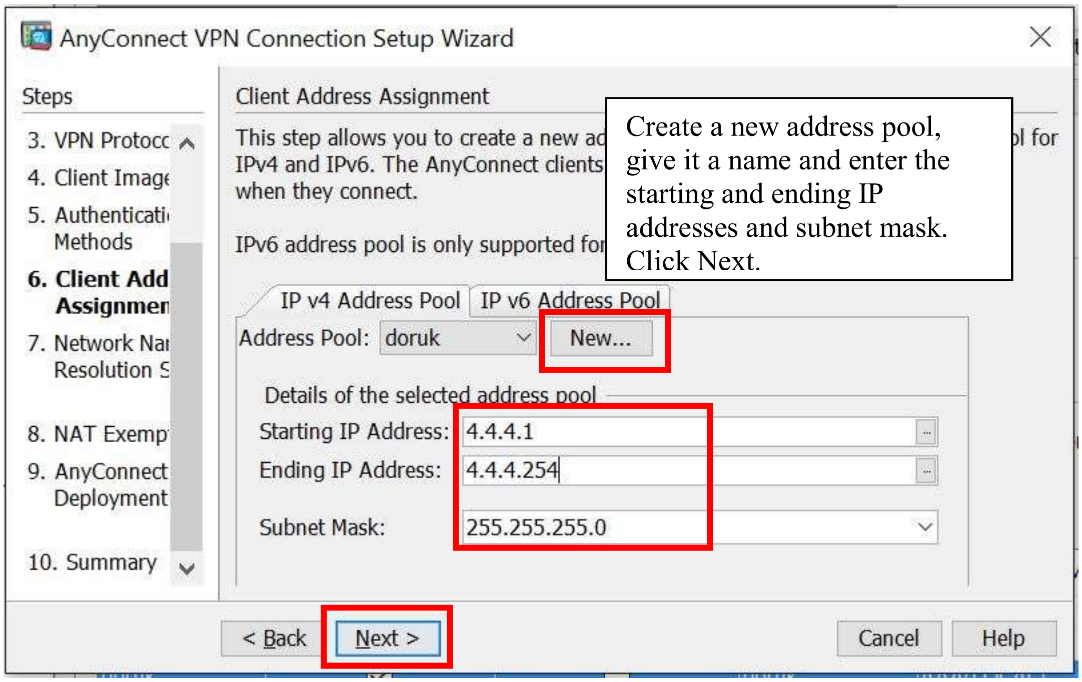


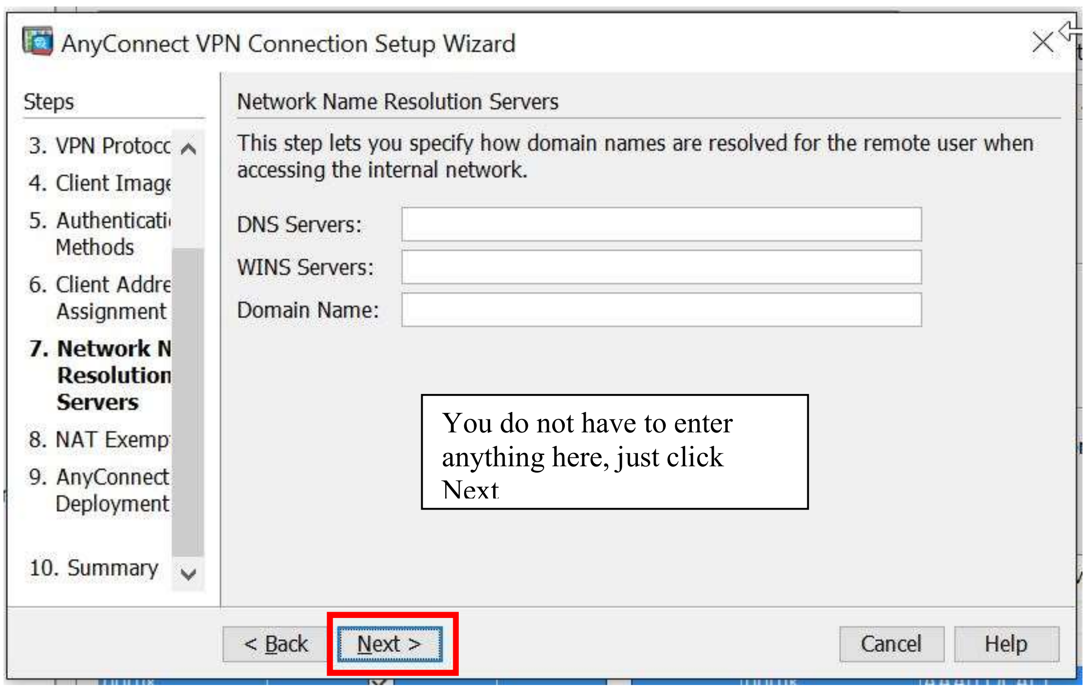

AnyConnect VPN Connection Setup Wizard
Steps
3. VPN Proto
4. Client Image
5. Authenticati Methods
6. Client Addre Assignment
7. Network Nar Resolution S
8. NAT Exemp
9. AnyConnect Deployment
10. Summary
VPN Protocols
AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to support.
SSL
IPsec
Deselect IPsec.
Click Next to start the wizard.
Device Certificate
Device certificate identifies the ASA to the remote access clients. Certain AnyConnect features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA.
Device Certificate: -- None --
Manage...
< Back
Next >
Cancel
Help

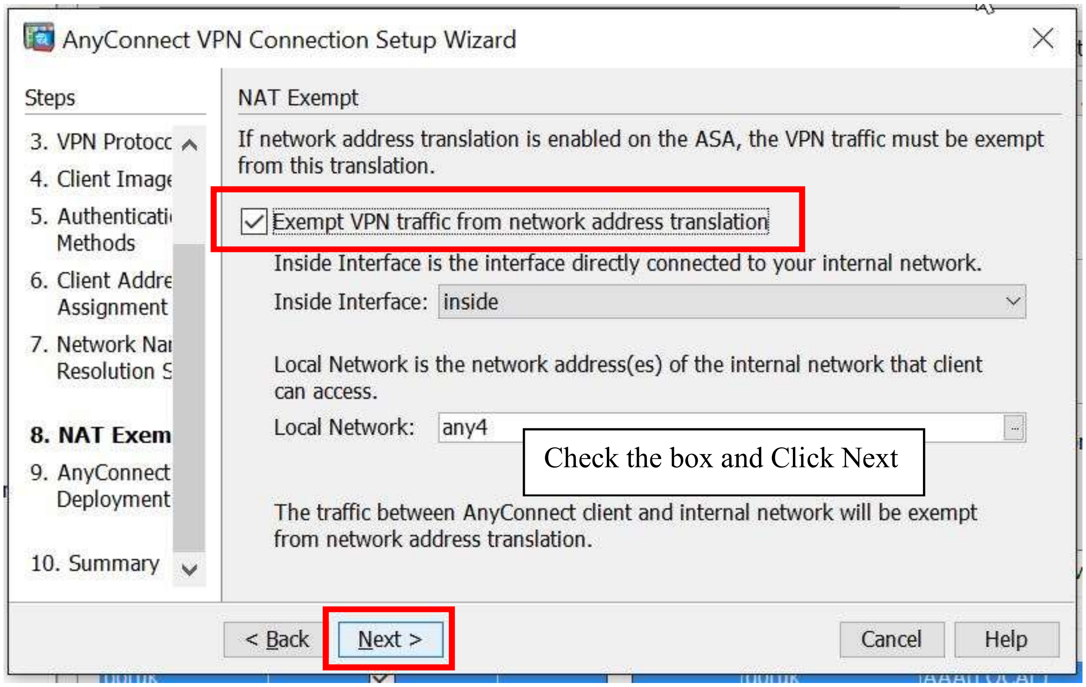

AnyConnect VPN Connection Setup Wizard
Steps
3. VPN Protoc
4. Client Ima
5. Authenticati Methods
6. Client Addre Assignment
7. Network Nar Resolution S
8. NAT Exemp
9. AnyConnect Deployment
10. Summary
Client Images
ASA can automatically upload the latest AnyConnect package to the client device when it accesses the enterprise network.
A regular expression can be used to match the user-agent of a browser to an image. You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.
Add
Replace
Delete
Image
Regular expression to match user-agent
disk0:/anyconnect-win-3.1.04066-k9.pkg
Click Add to add the file
You can download AnyConnect Client packages from Cisco by searching 'AnyConnect VPN Client' or click here.
< Back
Next >
Cancel
Help

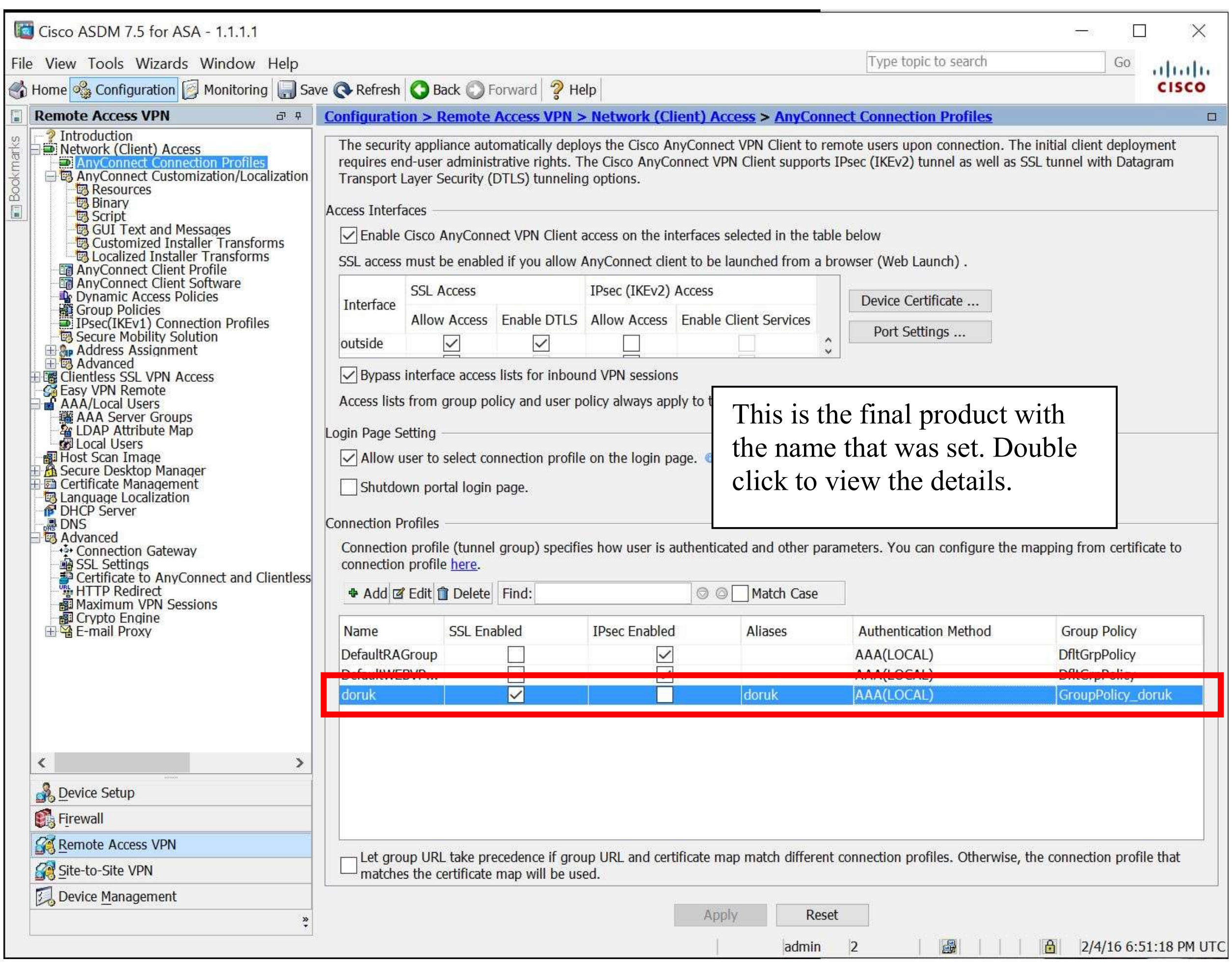

AnyConnect VPN Connection Setup Wizard
Steps
3. VPN Protocc
4. Client Ima
Deployment
10. Summary
Client Images
ASA can automatically upload the latest
it accesses the enterprise network.
evice when
Click Browse Flash…
Find the file, open it.
Click OK and then Next.
Replace AnyConnect Client Image
AnyConnect Image: disk0:/anyconnect-win-3.1.04066-k9.pkg
Browse Flash...
Upload...
Regular expression to match user-agent
OK
Cancel
Help
You can download AnyConnect Client packages from Cisco by searching 'AnyConnect VPN Client' or click here.
< Back
Next >
Cancel
Help

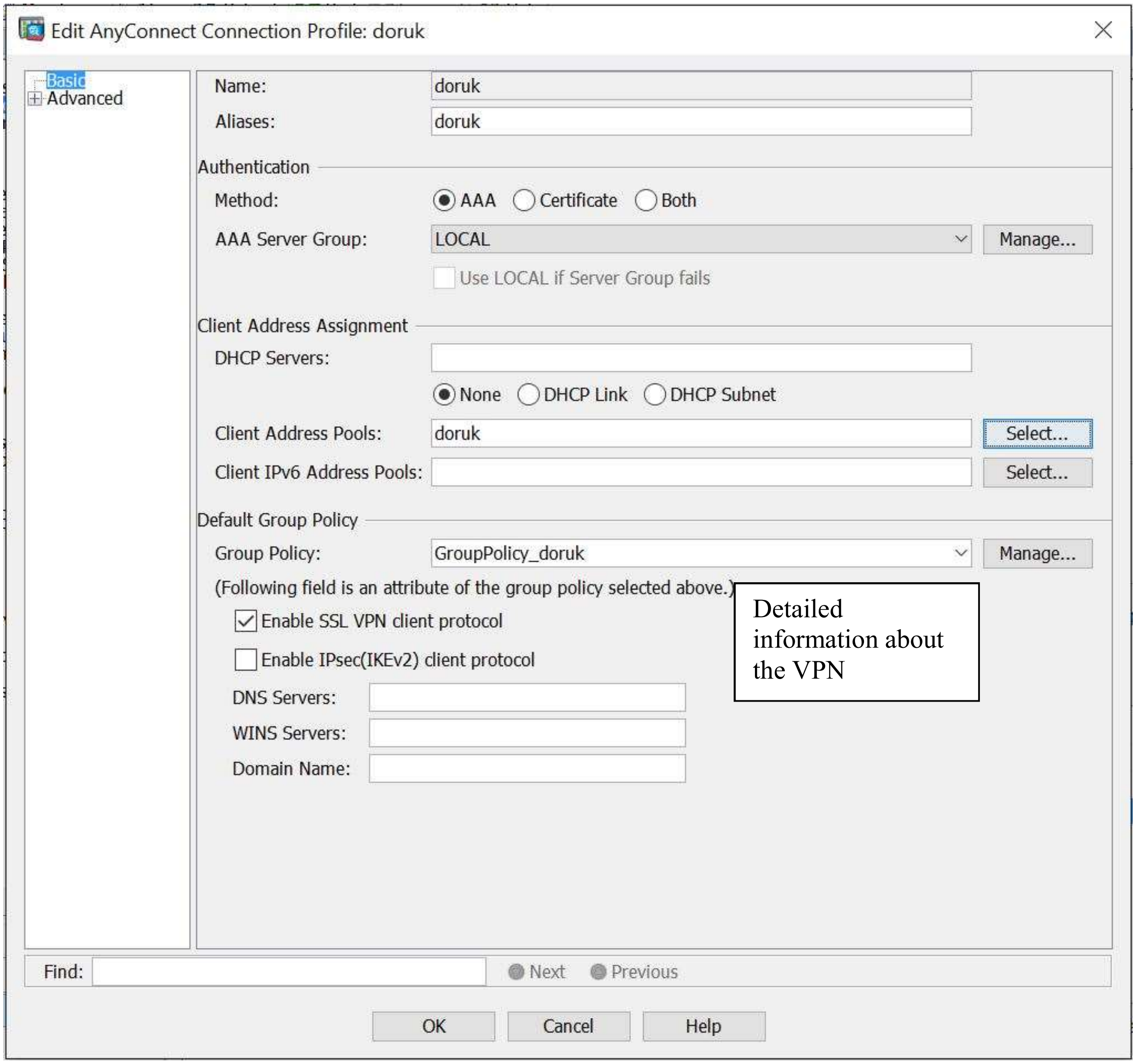

AnyConnect VPN Connection Setup Wizard
Steps
3. VPN Protocc
4. Client Image
5. Authentica Methods
6. Client Addre Assignment
7. Network Nai Resolution S
8. NAT Exemp
9. AnyConnect Deployment
10. Summary
Authentication Methods
This step lets you specify the location of the authentication server.
You can click on the "New..." button to create a new server group.
AAA Server Group: LOCAL
New...
Enter username and password then Click Add and then Next.
Local User Database Details
User to be Added
Username: laurissa
Password:
Confirm Password:
Add >>
Delete
admin
doruk
laurissa
< Back
Next >
Cancel
Help

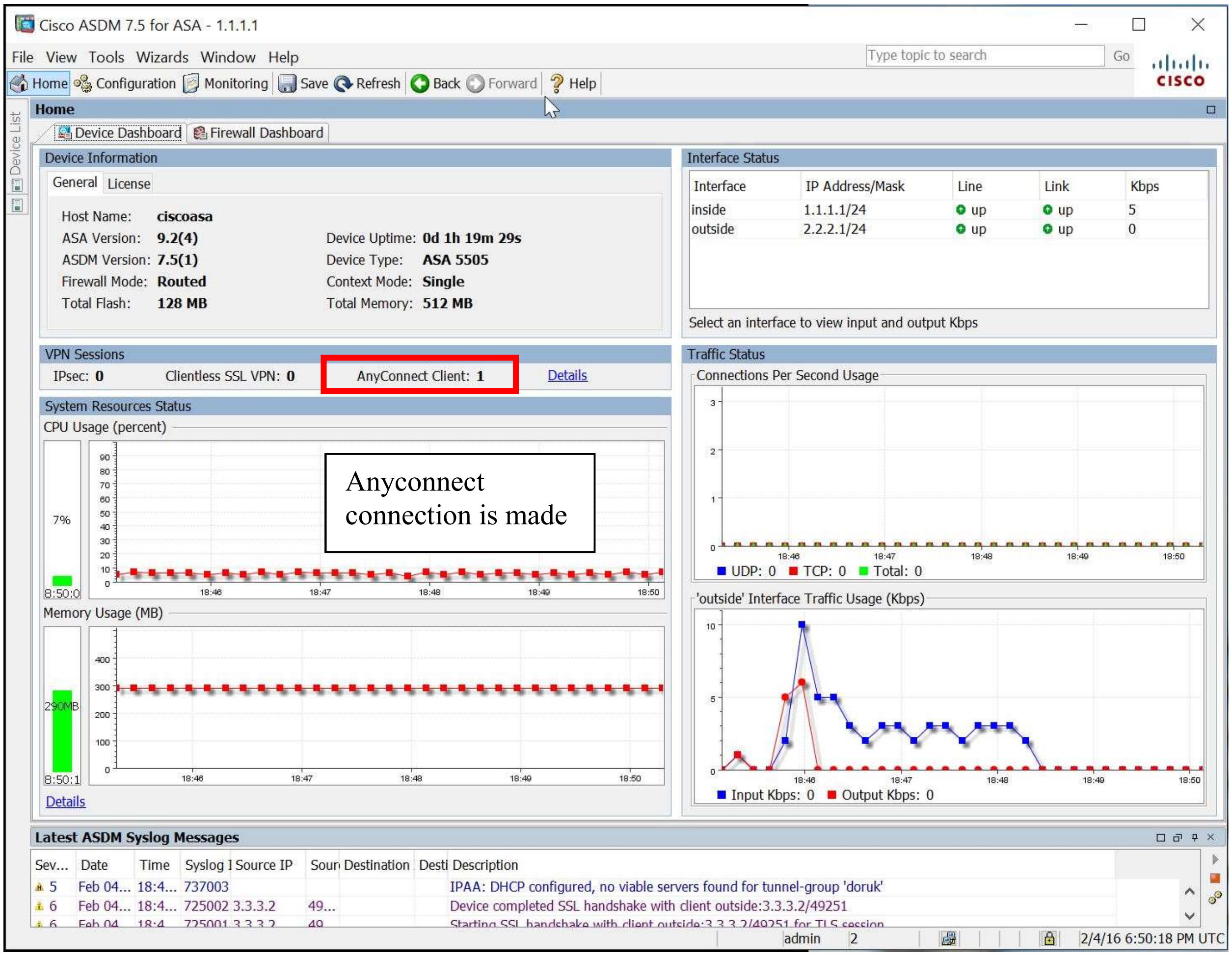

AnyConnect VPN Connection Setup Wizard
Steps
3. VPN Protoco
4. Client Image
5. Authenticati Methods
6. Client Add Assignmen
7. Network Na Resolution S
8. NAT Exemp
9. AnyConnect Deployment
10. Summary
Client Address Assignment
This step allows you to create a new ad
IPv4 and IPv6. The AnyConnect clients
when they connect.
IPv6 address pool is only supported fo
Create a new address pool, give it a name and enter the starting and ending IP addresses and subnet mask. Click Next.
IP v4 Address Pool
IP v6 Address Pool
Address Pool: doruk
New...
Details of the selected address pool
Starting IP Address: 4.4.4.1
Ending IP Address: 4.4.4.254
Subnet Mask: 255.255.255.0
< Back
Next >
Cancel
Help


AnyConnect VPN Connection Setup Wizard
Steps
3. VPN Protoco
4. Client Image
5. Authenticati Methods
6. Client Addre Assignment
7. Network N Resolution Servers
8. NAT Exemp
9. AnyConnect Deployment
10. Summary
Network Name Resolution Servers
This step lets you specify how domain names are resolved for the remote user when accessing the internal network.
DNS Servers:
WINS Servers:
Domain Name:
You do not have to enter anything here, just click Next
< Back
Next >
Cancel
Help

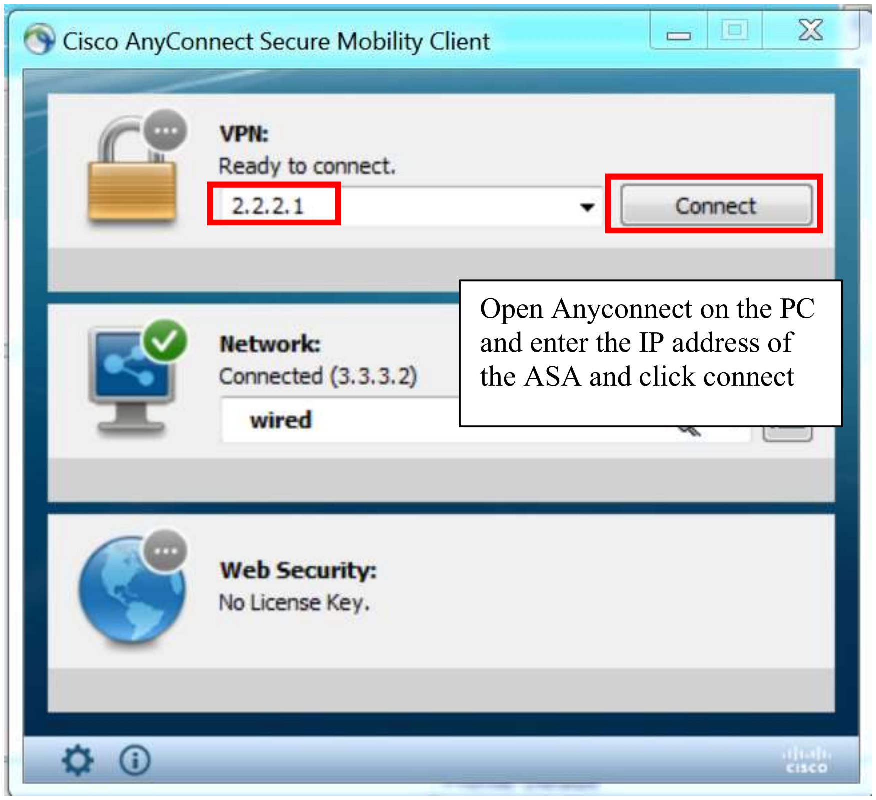

AnyConnect VPN Connection Setup Wizard
Steps
3. VPN Protocc
4. Client Image
5. Authenticati Methods
6. Client Addre Assignment
7. Network Nai Resolution S
8. NAT Exem
9. AnyConnect Deployment
10. Summary
NAT Exempt
If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.
Exempt VPN traffic from network address translation
Inside Interface is the interface directly connected to your internal network.
Inside Interface: inside
Local Network is the network address(es) of the internal network that client can access.
Local Network: any4
Check the box and Click Next
The traffic between AnyConnect client and internal network will be exempt from network address translation.
< Back
Next >
Cancel
Help

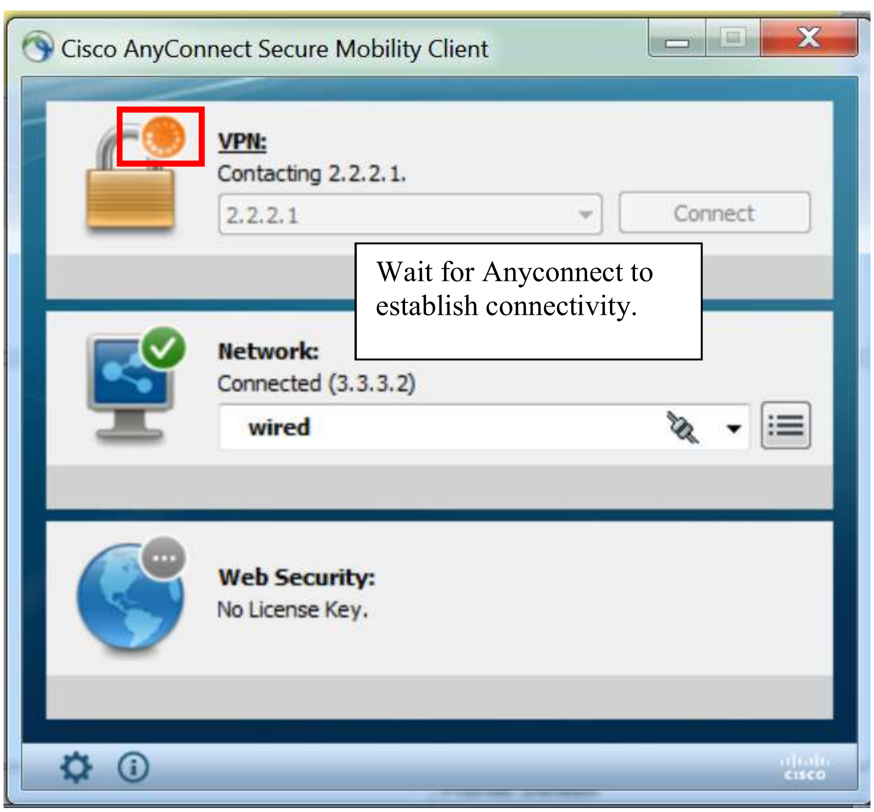

Cisco ASDM 7.5 for ASA - 1.1.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
Resources
Binary
Script
GUI Text and Messages
Customized Installer Transforms
Localized Installer Transforms
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
Easy VPN Remote
AAA/Local Users
AAA Server Groups
LDAP Attribute Map
Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
DHCP Server
DNS
Advanced
Connection Gateway
SSL Settings
Certificate to AnyConnect and Clientless
HTTP Redirect
Maximum VPN Sessions
Crypto Engine
E-mail Proxy
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.
Access Interfaces
Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below
SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .
Interface
SSL Access
Allow Access
Enable DTLS
IPsec (IKEv2) Access
Allow Access
Enable Client Services
outside
Device Certificate ...
Port Settings ...
Bypass interface access lists for inbound VPN sessions
Access lists from group policy and user policy always apply to t
Login Page Setting
Allow user to select connection profile on the login page.
Shutdown portal login page.
This is the final product with the name that was set. Double click to view the details.
Connection Profiles
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here.
Add Edit Delete Find: Match Case
Name
SSL Enabled
IPsec Enabled
Aliases
Authentication Method
Group Policy
DefaultRAGroup
AAA(LOCAL)
DfltGrpPolicy
doruk
doruk
AAA(LOCAL)
GroupPolicy_doruk
Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.
Apply
Reset
admin
2
2/4/16 6:51:18 PM UTC


Edit AnyConnect Connection Profile: doruk
Basic
Advanced
Name:
doruk
Aliases:
doruk
Authentication
Method:
AAA
Certificate
Both
AAA Server Group:
LOCAL
Manage...
Use LOCAL if Server Group fails
Client Address Assignment
DHCP Servers:
None
DHCP Link
DHCP Subnet
Client Address Pools:
doruk
Select...
Client IPv6 Address Pools:
Select...
Default Group Policy
Group Policy:
GroupPolicy_doruk
Manage...
(Following field is an attribute of the group policy selected above.)
Enable SSL VPN client protocol
Enable IPsec(IKEv2) client protocol
DNS Servers:
WINS Servers:
Domain Name:
Detailed information about the VPN
Find:
Next
Previous
OK
Cancel
Help

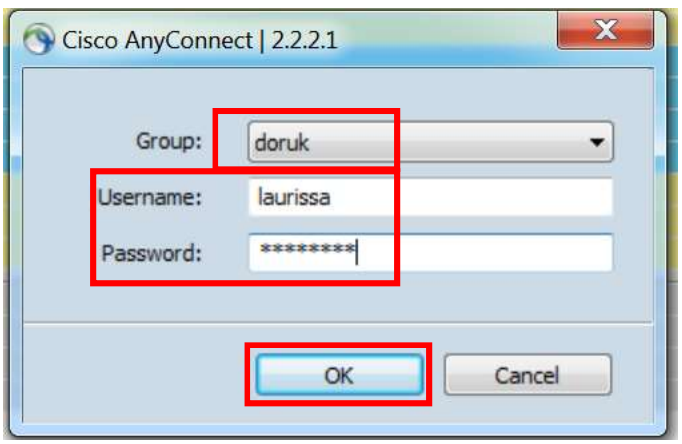

Cisco ASDM 7.5 for ASA - 1.1.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device Dashboard Firewall Dashboard
Device Information
Host Name: ciscoasa
ASA Version: 9.2(4)
ASDM Version: 7.5(1)
Firewall Mode: Routed
Total Flash: 128 MB
Device Uptime: 0d 1h 19m 29s
Device Type: ASA 5505
Context Mode: Single
Total Memory: 512 MB
Interface Status
inside 1.1.1.1/24 up up 5
outside 2.2.2.1/24 up up 0
Select an interface to view input and output Kbps
VPN Sessions
IPsec: 0 Clientless SSL VPN: 0 AnyConnect Client: 1 Details
Anyconnect connection is made
System Resources Status
CPU Usage (percent)
Memory Usage (MB)
Traffic Status
Connections Per Second Usage
UDP: 0 TCP: 0 Total: 0
'outside' Interface Traffic Usage (Kbps)
Input Kbps: 0 Output Kbps: 0
Latest ASDM Syslog Messages
IPAA: DHCP configured, no viable servers found for tunnel-group 'doruk'
Device completed SSL handshake with client outside:3.3.3.2/49251
2/4/16 6:50:18 PM UTC

Connecting to the VPN from the Client





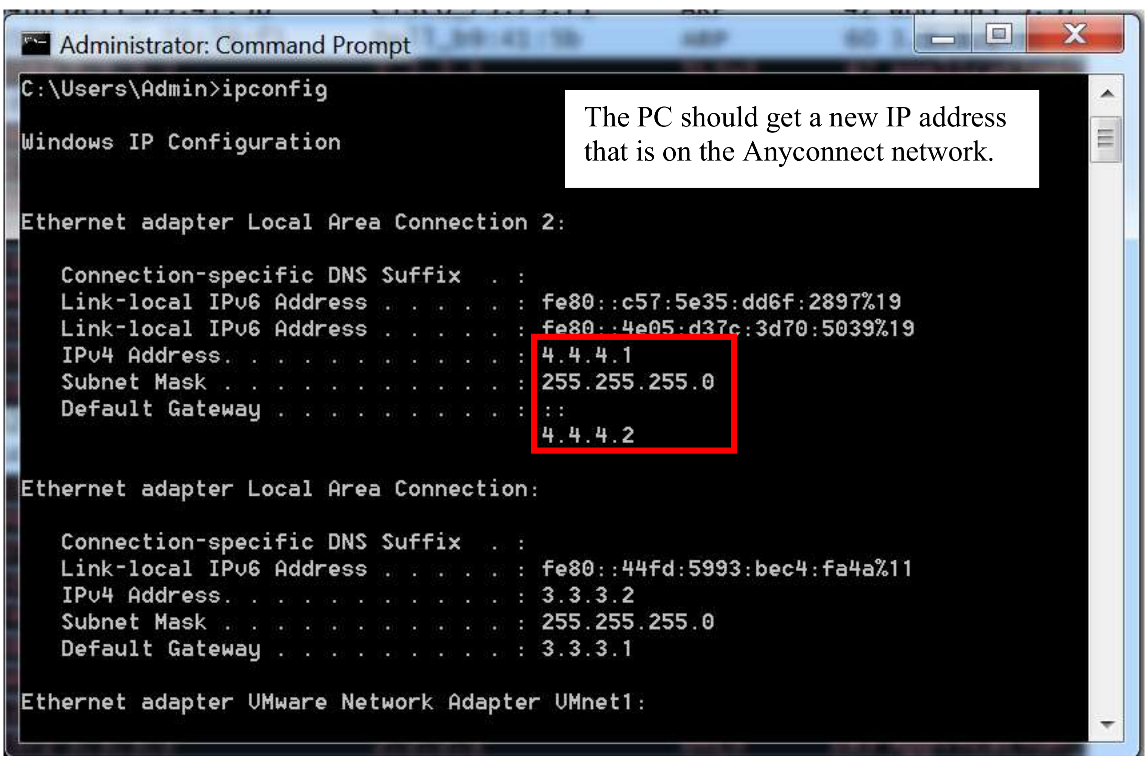
Click Connect Anyway



Select the Group, enter username, password and click OK

Once the connection is successfully established, this message should pop


Cisco AnyConnect Secure Mobility Client
VPN:
Connected to 2.2.2.1.
2.2.2.1
Disconnect
00:00:33
Once the connection is established, Anyconnect should say "connected" and to what server it is connected to.
wired
Web Security:
No License Key.


Administrator: Command Prompt
C:\Users\Admin>ipconfig
Windows IP Configuration
The PC should get a new IP address that is on the Anyconnect network.
Ethernet adapter Local Area Connection 2:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::c57:5e35:dd6f:2897%19
Link-local IPv6 Address . . . . . : fe80::4e05:d37c:3d70:5039%19
IPv4 Address. . . . . : 4.4.4.1
Subnet Mask . . . . : 255.255.255.0
Default Gateway . . . . : ::
4.4.4.2
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::44fd:5993:bec4:fa4a%11
IPv4 Address. . . . . : 3.3.3.2
Subnet Mask . . . . : 255.255.255.0
Default Gateway . . . . : 3.3.3.1
Ethernet adapter VMware Network Adapter VMnet1:

Problems

While doing this lab, we only faced a couple of problems. The first problem had to do with the Cisco Anyconnect Client software. We first wanted to install the software on a PC that was running Windows 10. However the software we had was compatible with Windows 7 and 8 but not 10. We still installed the software on the PC. The software told us to restart the PC. So we did. But the PC did not start normally. There was no login page. When we tried to go to the Windows login page, we were just getting a blank page. We then looked at the software on the other PC that was running Windows 7. We went to the properties of the software and realized that it was not compatible with Windows 10 and that was causing the problem. We somehow had to delete the software but we did not have access to the computer. So we decided to start the PC in recovery mode. In the recovery mode, we found a troubleshooting tool for the startup of the PC. The troubleshooting tool found the corrupted files that were causing the problem and gave us the option to delete them. So we deleted the Windows 7 and 8 compatible Anyconnect client software from the PC that was running Windows 10. Then we restarted the PC again, and it was working just like it was supposed to. To fix this client software issue, we had two options. We had the option to find the Windows 10 version of the Cisco Anyconnect client software and the option to install the Windows 7 version onto the PC that was running Windows 7. We lost enough time trying to fix the PC that was running, so instead of spending more time trying to find the right software, we just changed the places of the two PCs in our topology and installed the client software on the PC that was running Windows 7. Then we were able to move on to the Anyconnect server configuration.

We second and the last problem we had was after configuring everything. We configured the ASA as a Cisco Anyconnect server and a PC as a client. We had end to end connectivity and all we had to do is connect the client and the server. To establish the connection, we had to enter the IP address of the outside interface of the ASA. We thought we were entering the right IP address, but we were not able to establish the VPN connectivity. After checking the IP addresses it turned out that we were entering the IP address of the inside interface of the server not the outside. We then entered the right IP address and the software didn't let us connect. It said that the server we were trying to connect to is an untrusted server and therefore client software can't connect to it. Then we went to the settings and disabled a setting that did not let the client to connect to untrusted servers. After that, we were able to connect to the server with no problem and create the Cisco Anyconnect VPN connection.

Conclusion

In this lab, we configured Cisco Anyconnect Clientless SSL VPN for the first time. We have configured IPSec site-to-site VPN before but this was the first time we have configured a SSL VPN. Though they are both a type of VPN, the configuration was quite different. Configuration of Cisco Anyconnect was easier than configuring site-to-site VPN. We just needed to establish end-to-end connectivity in the network and once that was done, we installed the software on PC and configured Anyconnect on the ASA using the wizard. After doing those steps, we created the Cisco Anyconnect VPN. We did not have many problems. This simple tool is very common and useful in the outside world, since a lot of companies use it for their employers who work from home.

SSL VPN

Purpose

The purpose of this lab was to create a SSL server and connect to it from a remote PC and access a HTTP server.

Background Information

An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser. In contrast to the traditional Internet Protocol Security (IPsec) VPN, an SSL VPN does not require the installation of specialized client software on the end user's computer. It's used to give remote users with access to Web applications, client/server applications and internal network connections.

A virtual private network (VPN) provides a secure communications mechanism for data and other information transmitted between two endpoints. An SSL VPN consists of one or more VPN devices to which the user connects by using his Web browser. The traffic between the Web browser and the SSL VPN device is encrypted with the SSL protocol or its successor, the Transport Layer Security (TLS) protocol.

SSL Portal VPN allows for a single SSL connection to a Web site so the end user can securely access multiple network services. The site is called a portal because it is one door (a single page) that leads to many other resources. The remote user accesses the SSL VPN gateway using any modern Web browser, identifies himself or herself to the gateway using an authentication method supported by the gateway and is then presented with a Web page that acts as the portal to the other services.

One can think of VPN like an island in a huge ocean. There are thousands of other islands all around the person who lives in one island, some very close and others farther away. The normal way to travel is to take a ferry from an island to whichever island the person wishes to visit. Traveling on a ferry means that the person has almost no privacy. Anything the person does can be seen by someone else.

Assume that each island represents a private LAN and the ocean is the Internet. When the person travels by ferry, it is similar to when he/she connects to a web server or to another device through the Internet. They have no control over the wires and routers that make up the Internet, just like they have no control over the other people on the ferry. This leaves the person susceptible to security issues if they try to connect between two private networks using a public resource.

The person decides to build a bridge to another island from his/her island so that there is an easier, more secure and direct way for people to travel between the two. It is expensive to build and maintain the bridge, even though the island they are connecting with is very close. But the need for a reliable, secure path is so great that they do it anyway. The person would like to connect to a second island that is much farther away, but they decide that it is too expensive.

This situation is very much like having a leased line. The bridges (leased lines) are separate from the ocean (Internet), yet they are able to connect the islands (LANs). Many companies have chosen this route because of the need for security and reliability in connecting their remote offices. However, if the offices are very far apart, the cost can be prohibitively high - just like trying to build a bridge that spans a great distance. In the cases of long distances, companies can use the existing bridges with their private vehicles which represent the packets going through a network.

Lab Summary

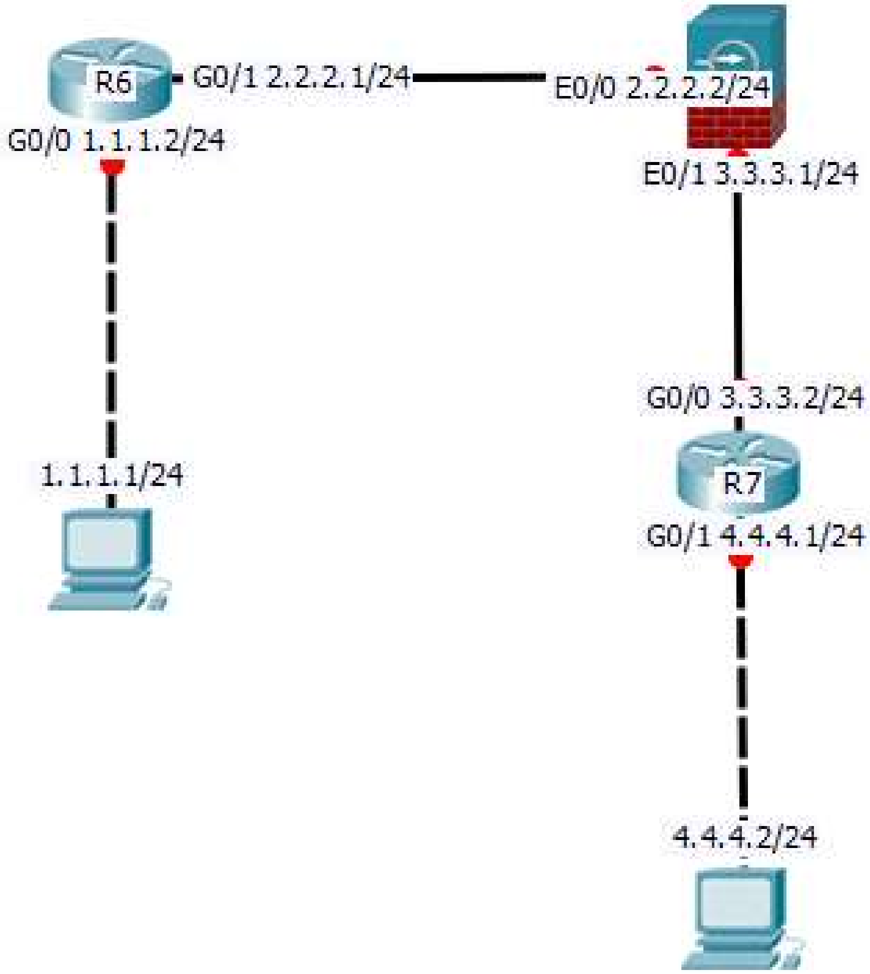
In this lab we had, an ASA as the SSL VPN server, a router that will connect the remote host and the ASA and another router that will act like the HTTP server on the inside network of the ASA. We first made sure that we had end to end connectivity. To do that we used OSPF. We configured OSPF on the routers and the ASA. We also allowed IP traffic on the ASA firewall. When we had end to end connectivity we created the HTTP server on R7 so that the remote host could connect to is using the SSL VPN.

Once we could ping between all the hosts we moved into configuring the SSL VPN server on the ASA. We used the wizard to set up the VPN. We defined the users that could access the VPN, created the group policy. It was pretty easy to setup the VPN server. Once we were done, we opened a web browser on the remote host. We entered the address of the outside interface of the ASA. Then we entered our username and password to gain access to the SSL VPN connection. After we got in, we were able to enter the IP address of the HTTP server on the URL bar of the SSL VPN portal. Then we entered the username and password for the HTTP server and we were able to connect to the HTTP server successfully using the SSL VPN portal through our ASA. Our lab was complete.

Lab Commands

default-group-policy GroupPolicy_*doruk*	This command specifies the name of the default group policy.
tunnel-group *doruk* **webvpn-attributes**	To specify the attributes of a clientless SSL VPN tunnel-group, enter tunnel-group webvpn-attributes mode by entering this command.
group-alias *doruk* **enable**	To specify alternative names for the group and enable that group, use this command.
group-policy GroupPolicy_*doruk* **attributes**	This command is used to change any of the attributes of the group policy, use this command to enter attributes mode, then specify the commands to change whatever attributes that you want to modify.
tunnel-group *doruk* **type remote-access**	This command is used to creat a remote-access connection profile named doruk.
tunnel-group *doruk* **general-attributes**	This command is used to go into the general-attributes configuration mode to configure general attributes.

Network Diagram



ASA-5055
Show run

```
: Saved
: Serial Number: JMX1617Z2JE
: Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
ASA Version 9.2(4)
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
interface Ethernet0/0
 switchport access vlan 2
interface Ethernet0/1
interface Ethernet0/2
 shutdown
interface Ethernet0/3
 shutdown
interface Ethernet0/4
 shutdown
interface Ethernet0/5
 shutdown
interface Ethernet0/6
 shutdown
interface Ethernet0/7
 shutdown
interface Vlan1
 nameif inside
 security-level 100
 ip address 3.3.3.1 255.255.255.0
interface Vlan2
 nameif outside
 security-level 0
 ip address 2.2.2.2 255.255.255.0
ftp mode passive
access-list inside_access_in extended permit ip any any
access-list inside_access_in extended permit tcp any any eq www
access-list inside_access_in extended permit tcp any any eq https
access-list inside_access_in extended permit icmp any any
access-list global_access extended permit ip any any
access-list global_access extended permit tcp any any eq www
access-list global_access extended permit tcp any any eq https
access-list global_access extended permit icmp any any
access-list outside_access_in extended permit ip any any
access-list outside_access_in extended permit tcp any any eq www
access-list outside_access_in extended permit tcp any any eq https
access-list outside_access_in extended permit icmp any any
pager lines 24
mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
```

```
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group inside_access_in in interface inside
access-group outside_access_in in interface outside
access-group global_access global
router ospf 1
 network 2.2.2.0 255.255.255.0 area 0
 network 3.3.3.0 255.255.255.0 area 0
 log-adj-changes
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
http 4.4.4.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
 enable outside
group-policy SSL internal
group-policy SSL attributes
 vpn-tunnel-protocol ssl-clientless
 webvpn
  url-list none
username admin password f3UhLvUj1QsXsuK7 encrypted
username doruk password dMmeFSbg9dksQIY8 encrypted privilege 0
username doruk attributes
 vpn-group-policy SSL
username laurissa password CriVx1UAp7.OqGMD encrypted privilege 0
username laurissa attributes
 vpn-group-policy SSL
tunnel-group Cisco type remote-access
tunnel-group Cisco general-attributes
```

```
 default-group-policy SSL
prompt hostname context
call-home reporting anonymous prompt 2
call-home
 profile CiscoTAC-1
  no active
  destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:d362cba772c1dc9d400566e8a3a2d8ab
: end
```

R6
Show run

```
Current configuration : 1532 bytes
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R6
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX1520806Z
license accept end user agreement
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 1.1.1.2 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 2.2.2.1 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0/0
```

```
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 duplex auto
 speed auto
router ospf 1
 network 1.1.1.0 0.0.0.255 area 0
 network 2.2.2.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
End
```

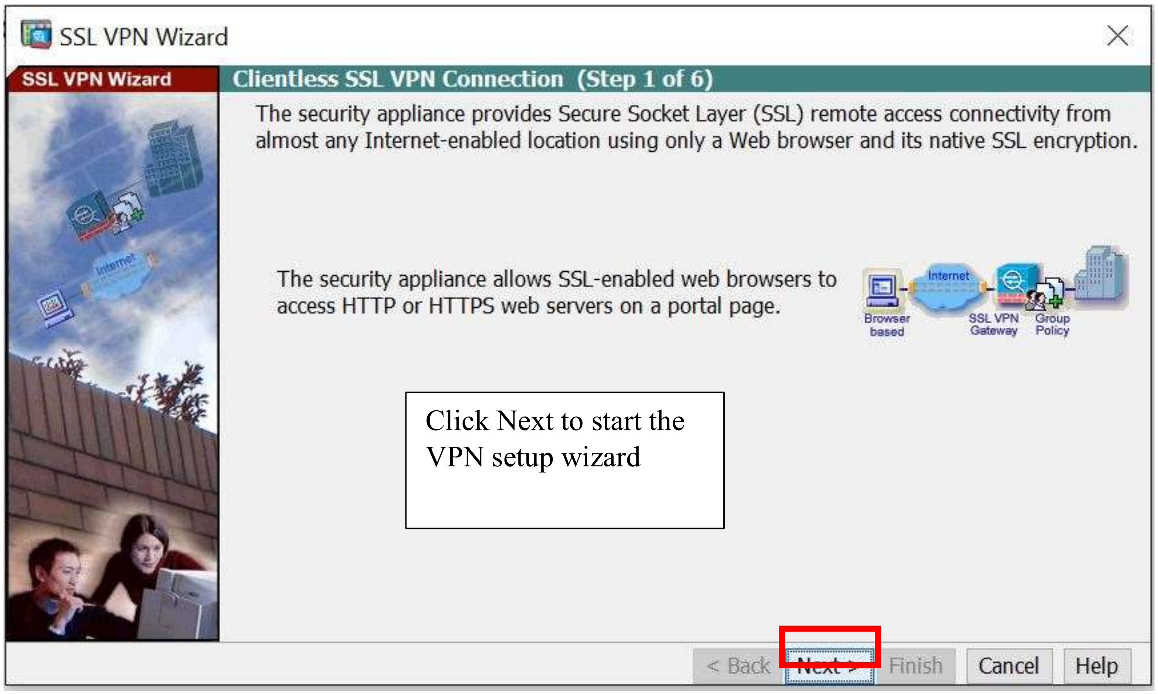
R7
show run:

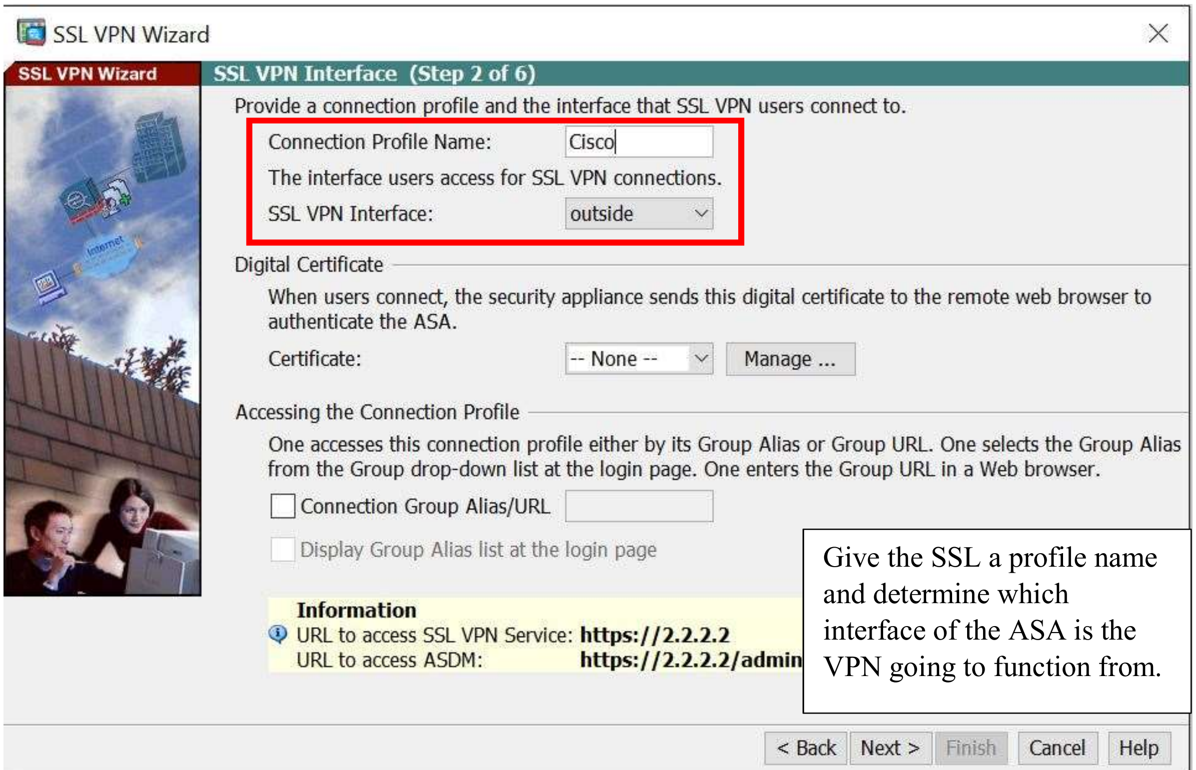
```
Current configuration : 1645 bytes Last configuration change at
18:54:27 UTC Thu Apr 14 2016
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R7
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 10
ip cef
no ipv6 cef
```

```
multilink bundle-name authenticated
voice-card 0
license udi pid CISCO2901/K9 sn FTX152885RE
license accept end user agreement
license boot module c2900 technology-package uck9
vtp domain cisco
vtp mode transparent
username admin privilege 15 password 0 cisco
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 3.3.3.2 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 4.4.4.1 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
interface GigabitEthernet0/1/0
 no ip address
 shutdown
 duplex auto
 speed auto
router ospf 1
 network 3.3.3.0 0.0.0.255 area 0
 network 4.4.4.0 0.0.0.255 area 0
ip forward-protocol nd
ip http server
ip http authentication local
no ip http secure-server
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
```

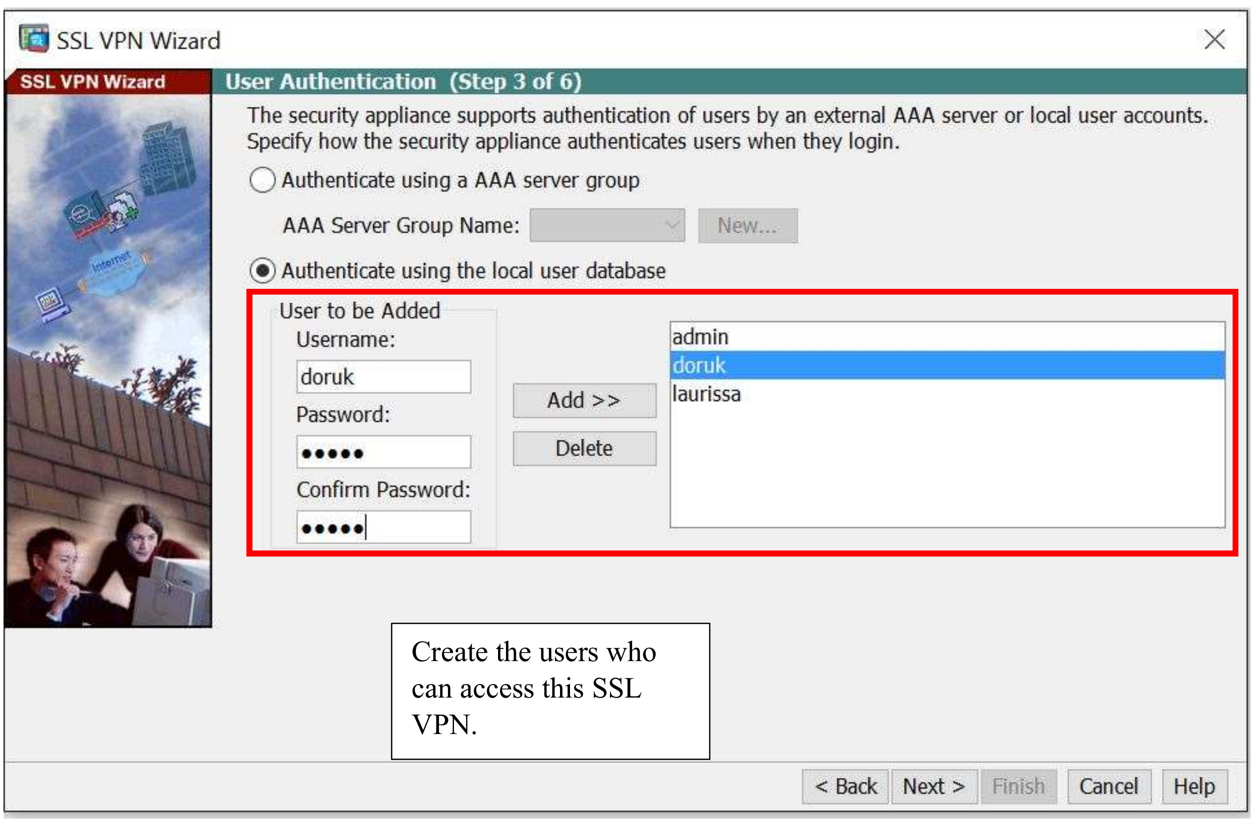
```
line vty 0 4
 login
 transport input all
scheduler allocate 20000 1000
end
```

Setting up SSL VPN

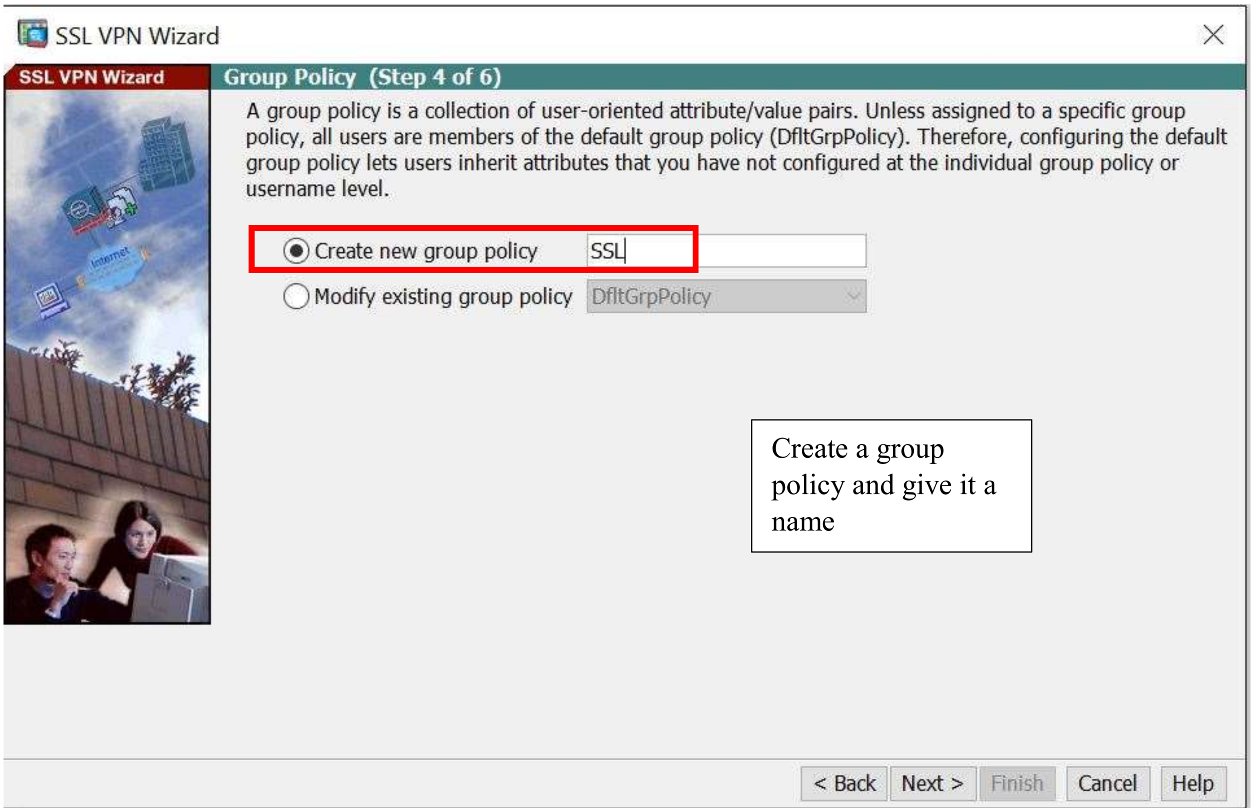


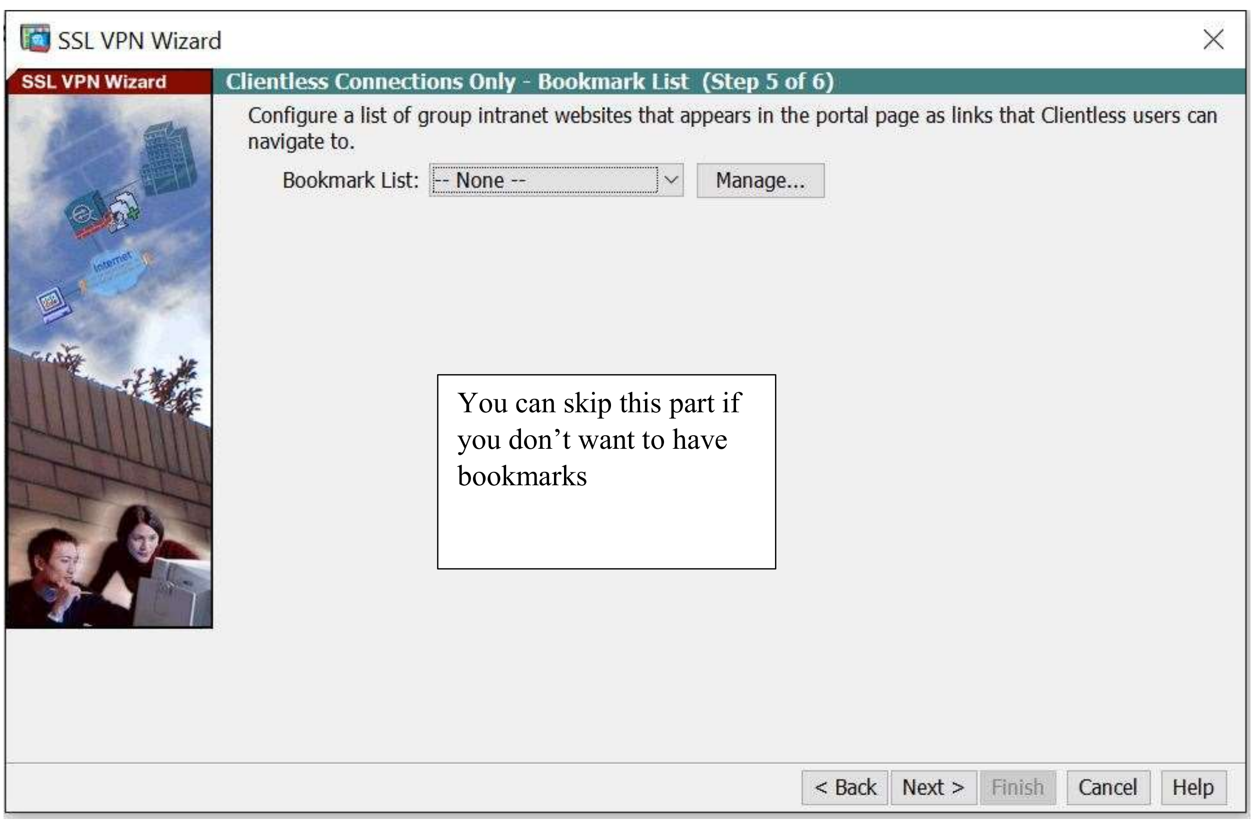


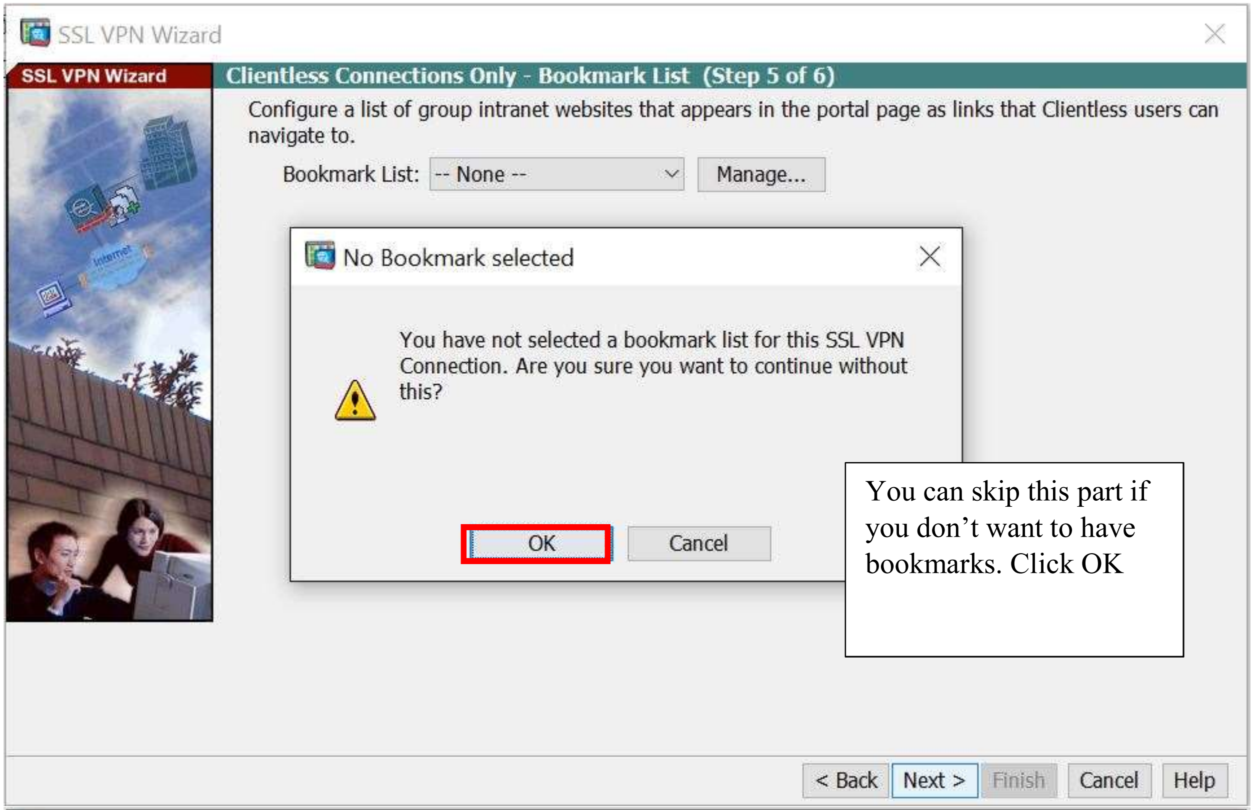
Give the SSL a profile name and determine which interface of the ASA is the VPN going to function from.

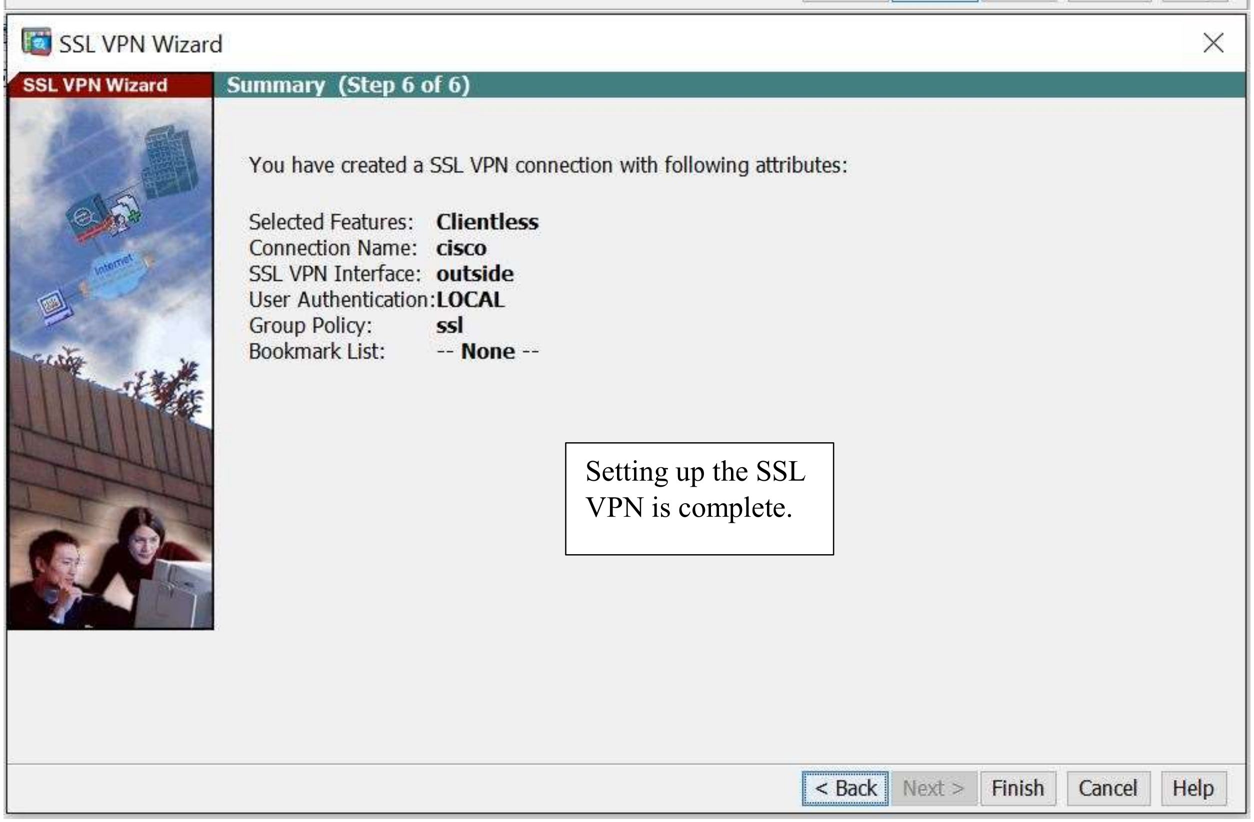


Create the users who can access this SSL VPN.

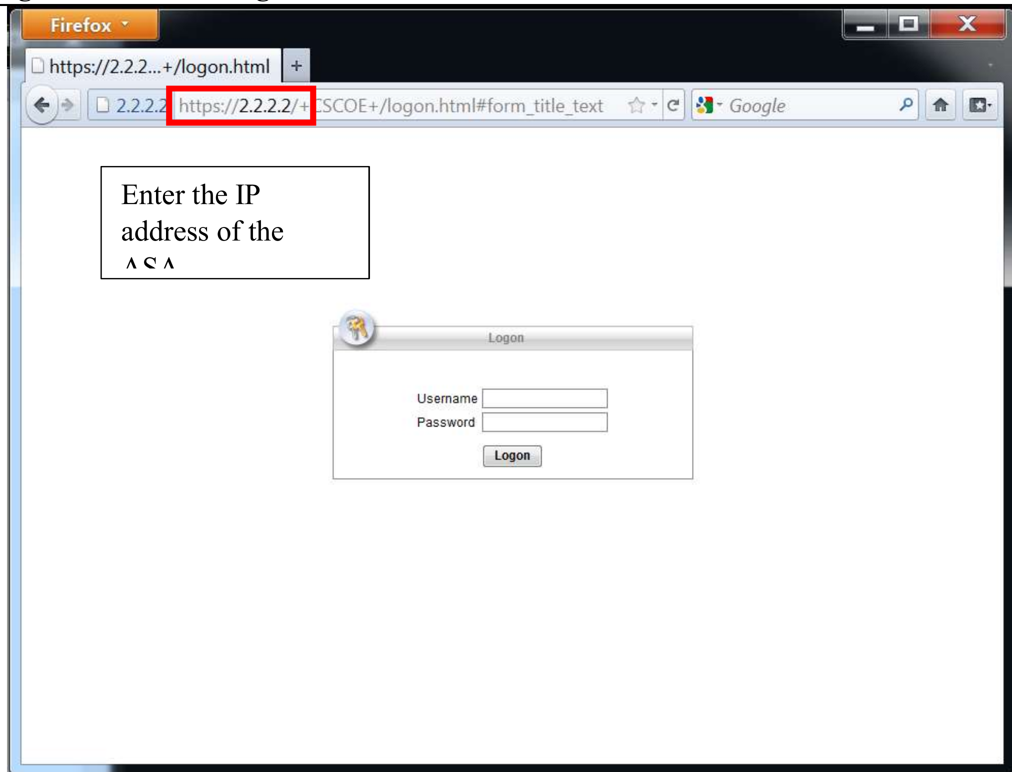

SSL VPN Wizard
SSL VPN Wizard
Group Policy (Step 4 of 6)
A group policy is a collection of user-oriented attribute/value pairs. Unless assigned to a specific group policy, all users are members of the default group policy (DfltGrpPolicy). Therefore, configuring the default group policy lets users inherit attributes that you have not configured at the individual group policy or username level.
Create new group policy
SSL
Modify existing group policy
DfltGrpPolicy
Create a group policy and give it a name
< Back
Next >
Finish
Cancel
Help

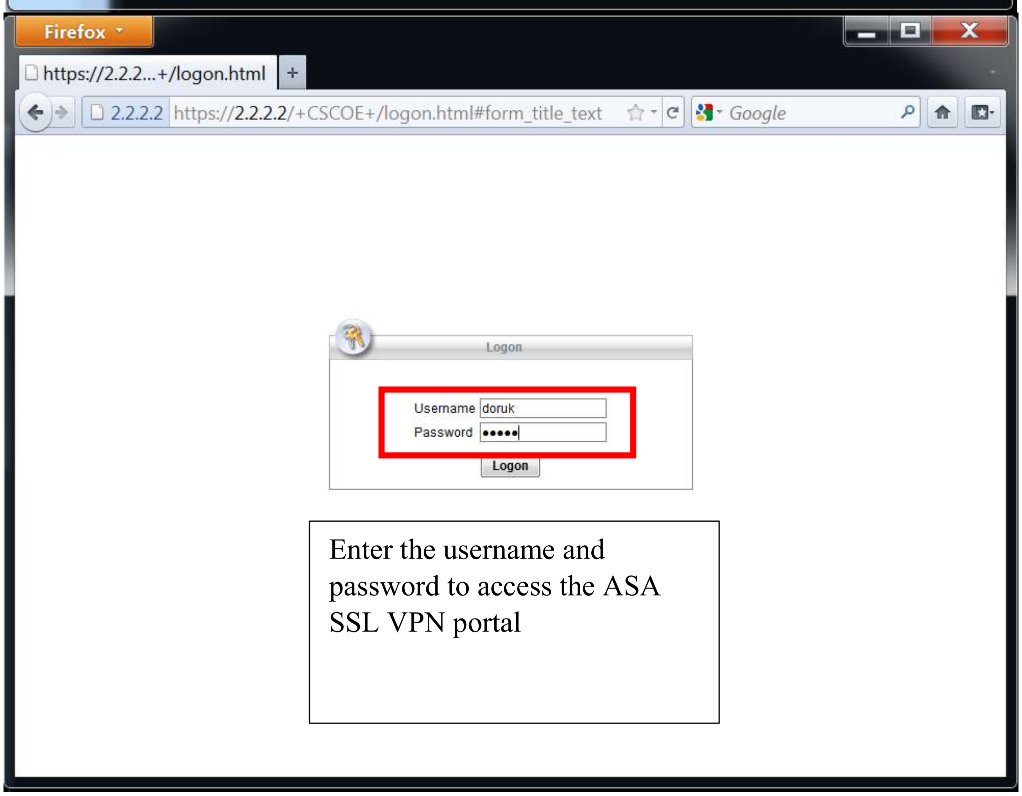

SSL VPN Wizard
SSL VPN Wizard
Clientless Connections Only - Bookmark List (Step 5 of 6)
Configure a list of group intranet websites that appears in the portal page as links that Clientless users can navigate to.
Bookmark List:
-- None --
Manage...
You can skip this part if you don't want to have bookmarks
< Back
Next >
Finish
Cancel
Help

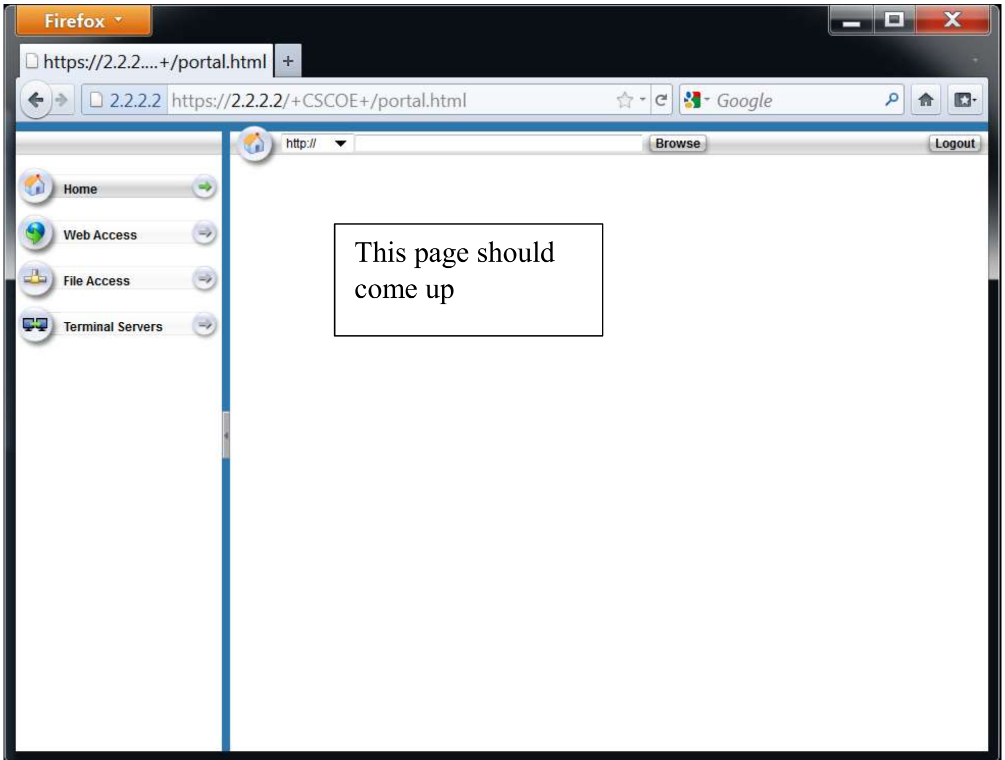

SSL VPN Wizard
SSL VPN Wizard
Clientless Connections Only - Bookmark List (Step 5 of 6)
Configure a list of group intranet websites that appears in the portal page as links that Clientless users can navigate to.
Bookmark List: -- None --
Manage...
No Bookmark selected
You have not selected a bookmark list for this SSL VPN Connection. Are you sure you want to continue without this?
OK
Cancel
You can skip this part if you don't want to have bookmarks. Click OK
< Back
Next >
Finish
Cancel
Help

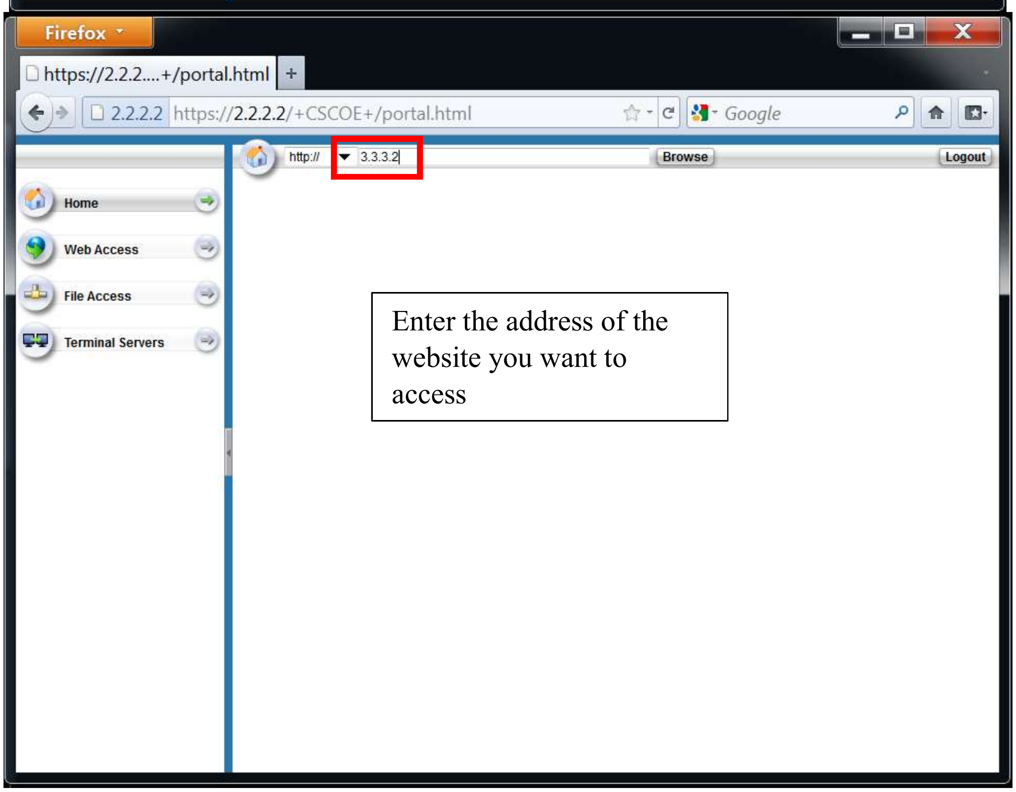

SSL VPN Wizard
SSL VPN Wizard
Summary (Step 6 of 6)
You have created a SSL VPN connection with following attributes:
Selected Features: Clientless
Connection Name: cisco
SSL VPN Interface: outside
User Authentication: LOCAL
Group Policy: ssl
Bookmark List: -- None --
Setting up the SSL VPN is complete.
< Back
Next >
Finish
Cancel
Help

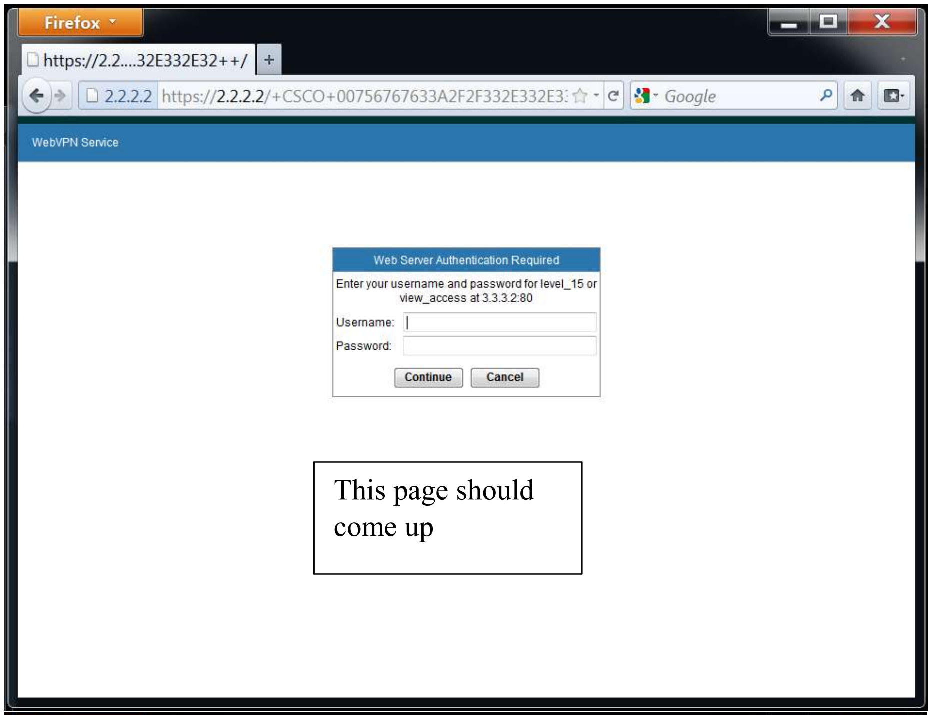
Connecting to the server using SSL VPN

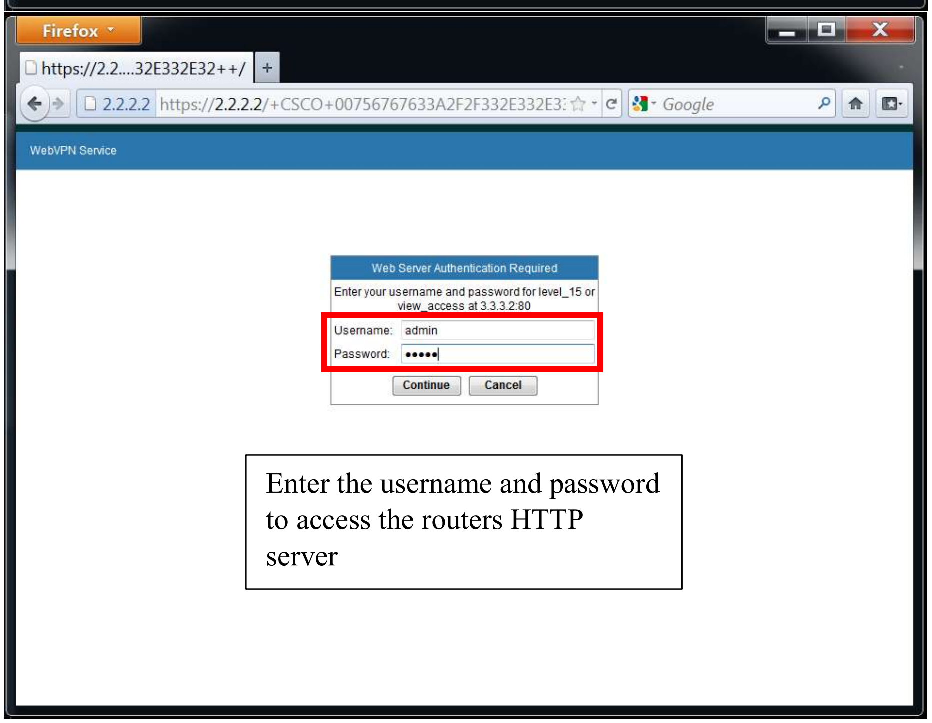


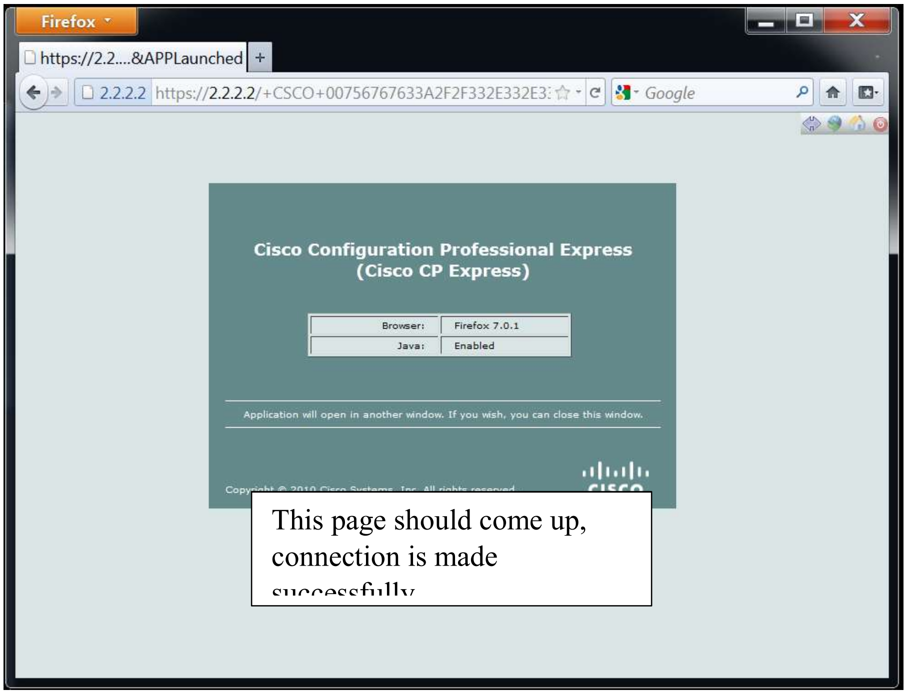



Firefox
https://2.2.2....+/portal.html
2.2.2.2 https://2.2.2.2/+CSCOE+/portal.html
Google
http://
Browse
Logout
Home
Web Access
File Access
Terminal Servers
This page should come up


Firefox
https://2.2.2....+/portal.html
2.2.2.2 https://2.2.2.2/+CSCOE+/portal.html
Google
http://
3.3.3.2
Browse
Logout
Home
Web Access
File Access
Terminal Servers
Enter the address of the website you want to access


Firefox
https://2.2....32E332E32++/
2.2.2.2 https://2.2.2.2/+CSCO+00756767633A2F2F332E332E3
Google
WebVPN Service
Web Server Authentication Required
Enter your username and password for level_15 or view_access at 3.3.3.2:80
Username:
Password:
Continue
Cancel
This page should come up


Firefox
https://2.2....32E332E32++/
2.2.2.2 https://2.2.2.2/+CSCO+00756767633A2F2F332E332E3
Google
WebVPN Service
Web Server Authentication Required
Enter your username and password for level_15 or view_access at 3.3.3.2:80
Username: admin
Password:
Continue
Cancel
Enter the username and password to access the routers HTTP server



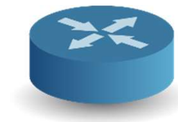
Problems

This lab was one of the labs where we had almost no problems and thigs went really smooth. We configured everything right the first time, however there was something we forgot to do. We had the VPN created, fully functional and running but we didn't have a website we could try to connect to, to prove that the VPN was working.

We spent some time discussing where to place the HTTP server and we finally decided that we would put it on the inside network of the ASA. We configured the router as a HTTP server, set a username and a password to access it and configured OSPF on it so that it could have connectivity with the other devices in the network. After doing that we were able to access the HTTP server using the SSL VPN we configured on the ASA and we were able to prove that it was working properly. After fixing that small problem, our lab was complete. We didn't have any other problems and everything ran smoothly.

Conclusion

This lab was a really easy and quick lab. Configuring SSL VPN was really similar to configuring and setting up Cisco Anyconnect VPN. It took me a really short time to configure and finish the lab. Even though it was an easy lab, I believe that I learned a really important skill because more and more people are starting to use and prefer SSL VPN these days over any type of VPNS. I didn't run into many problems while doing this lab except for having to add a router to the topology. I think I learned a lot.



Thank you for reading!

Contact info: doruk.arisoy@gmail.com