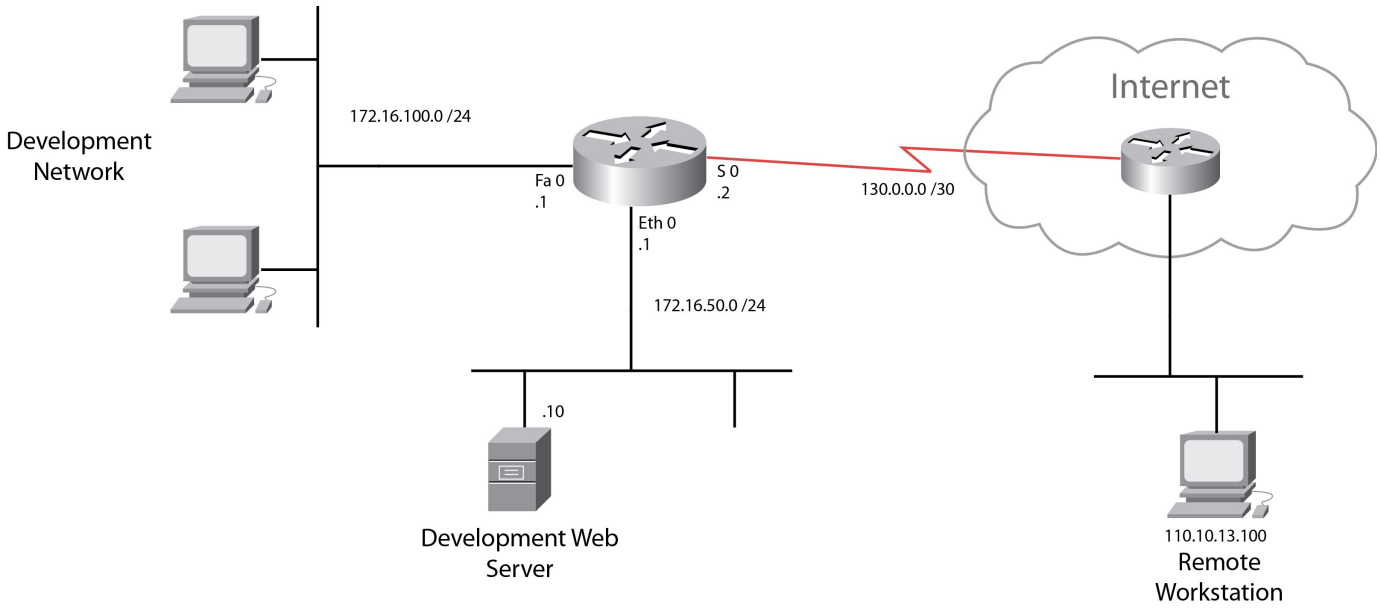
Web Development Network with NVI

(By Angel Cool; Sat 04/Aug 12)



Topology Layout

Introduction

The goal of this setup is to allow users in the Development Network and in the Internet to use the local router's S0 IP address (130.0.0.2) to access the Development Web Server. We'll use *NAT Virtual Interface* for the translations; NVI removes the *inside* and *outside* terminology, thus translations can happen between any combination of interfaces. Before, two *inside* interfaces could not have translation between each other. Using the same IP permits DNS entries (static in HOST file) to work in the local and remote hosts.

Configuration Steps

1.- The following commands will specify what interface participate in NAT:

(config)# **interface FastEthernet0**
(config-if)# **ip nat enable**
(config)# **interface Ethernet0**
(config-if)# **ip nat enable**
(config)# **interface Serial0**
(config-if)# **ip nat enable**

2.- We'll create an ACL to specify what addresses will be translated to the internet trough Serial0 for outgoing connections, after creating the access-list we will create the translation.

(config)# **access-list 50 permit 172.16.100.0 0.0.0.255** //Development Network
(config)# **access-list 50 permit 172.16.50.0 0.0.0.255** //Development Servers
(config)# **ip nat source list 50 interface Serial0 overload** //Create translations. All hosts will be seen with S0's IP.

2.- Create a static translation for incoming requests to the Development Web Server. Hosts in the Internet will type 130.0.0.2 to access the web server :

(config)#**ip nat source static tcp 172.16.50.10 80 interface Serial0 80**

3.- Create a translation from the Development Network to the Development Web Server. Hosts in the Development Network will type 130.0.0.2 to access the server.

(config)#**access-list 125 permit ip 172.16.100.0 0.0.0.255 host 130.0.0.2**
(config)#**ip nat source list 125 interface Ethernet0 overload**

3.- OPTIONAL. Create an ACL to protect the two LANs

//Only allow tcp connections to be initianed from the LANs (unless otherwise specified)
(config)#**access-list 100 permit tcp any host 130.0.0.2 gt 1023 established**
//Permit incoming requests to the development server (could use lock-and-key ACL)
(config)#**access-list 100 permit tcp any host 130.0.0.2 eq www**
//Allow DNS connections
(config)#**access-list 100 permit udp any host 130.0.0.2 gt 1023**
//Record number of denied connections
(config)#**access-list 100 deny ip any any**
//Apply ACL
(config)#**int serial 0**
(config-if)#**ip access-group 100 in**

Conclusion

Users in the the Development Network and the Internet can access the Development Web Server using the same IP, thus using the same domain name (eg. *developing.ourbusiness.com*). We can set up a lock-and-key ACL to permit only authorized hosts to access the Development Server.