Project Documentation: Secure Inter-Branch Communication

---

1. Introduction

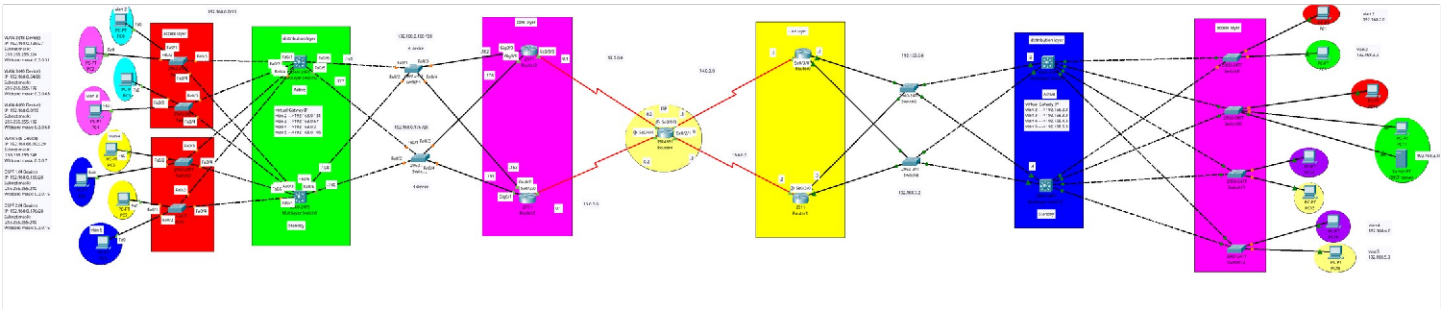
- **Project Title**: Secure Inter-Branch Communication
- **Project Objective**:
  The aim of this project is to establish a secure communication channel between two branches using VPN tunneling and advanced Cisco security features. This solution ensures secure data transmission over potentially untrusted networks, while providing strong network segmentation and internal security within each branch.
- **Scope**:
  The project implements a secure VPN tunnel for inter-branch communication, VLAN segmentation for internal network management, OSPF for dynamic routing, and Cisco security features like Port Security, BPDU Guard, DHCP Snooping, and NAT.
- **Network Topology Overview**:
  The network connects two branches through a secure VPN tunnel, with an ISP router providing internet access. The branches use multiple switches (access and multilayer) and routers configured with OSPF for dynamic routing and NAT for external communication.

---

2. Network Design

2.1 Network Diagram

Below is the logical topology for the "Secure Inter-Branch Communication" project:



The topology shows the secure VPN connection between two branches, detailing various VLANs, core routers, switches, and an ISP providing internet connectivity.

2.2 IP Addressing Scheme

Device	Interface	IP Address	Subnet Mask	Role
R1 Core Router	GigabitEthernet0/0	192.168.0.162	255.255.255.240	OSPF, Internal Interface
R1 Core Router	Serial0/3/0	12.0.0.1	255.0.0.0	NAT Outside, ISP Link
Multilayer SW	FastEthernet0/5	192.168.0.177	255.255.255.240	OSPF Interface
Active Multilayer SW2	FastEthernet0/5	192.168.6.2	255.255.255.0	OSPF Interface
ISP Router	Serial0/1/0	12.0.0.2	255.0.0.0	ISP Link

---

3. Device Configuration

This section includes the detailed configurations of the various devices used in the network.

3.1 Configuration for Branch Switches (SW0, SW1, SW9, SW10)

```
ip arp inspection vlan 2-3
!
ip dhcp snooping vlan 2-3
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 ip arp inspection trust
 ip dhcp snooping trust
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/2
 ip arp inspection trust
 ip dhcp snooping trust
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/3
```

```
 switchport access vlan 2
 ip dhcp snooping limit rate 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 5
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0001.97CC.22B5
 spanning-tree bpduguard enable
!
interface FastEthernet0/4
 switchport access vlan 3
 ip dhcp snooping limit rate 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 5
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 000C.CFC3.40C6
 spanning-tree bpduguard enable
no cdp run
```

Configuration for Branch Switches (SW3, SW4, SW11, SW12)

```
ip arp inspection vlan 4-5
!
ip dhcp snooping vlan 4-5
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk native vlan 999
```

```
 ip arp inspection trust
 ip dhcp snooping trust
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport trunk native vlan 999
 ip arp inspection trust
 ip dhcp snooping trust
 switchport mode trunk
 switchport nonegotiate

interface FastEthernet0/3
 switchport access vlan 4
 ip dhcp snooping limit rate 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 5
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0060.5C3D.446D
 spanning-tree bpduguard enable
!
interface FastEthernet0/4
 switchport access vlan 5
 ip dhcp snooping limit rate 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 5
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 000A.41B7.59E8
```

```
 spanning-tree bpduguard enable

no cdp run
```

3.2 Configuration for Active Multilayer Switch

```
ip dhcp excluded-address 192.168.0.129
ip dhcp excluded-address 192.168.0.131
ip dhcp excluded-address 192.168.0.130
ip dhcp excluded-address 192.168.0.65 192.168.0.67
ip dhcp excluded-address 192.168.0.1 192.168.0.3
ip dhcp excluded-address 192.168.0.193 192.168.0.195

ip dhcp pool 2
 network 192.168.0.128 255.255.255.224
 default-router 192.168.0.131
 dns-server 8.0.0.20
 domain-name depi.com

ip dhcp pool 3
 network 192.168.0.64 255.255.255.192
 default-router 192.168.0.67
 dns-server 8.0.0.20
 domain-name depi.com

ip dhcp pool 4
 network 192.168.0.0 255.255.255.192
 default-router 192.168.0.3
 dns-server 8.0.0.20
 domain-name depi.com

ip dhcp pool 5
 network 192.168.0.192 255.255.255.248
 default-router 192.168.0.195
 dns-server 8.0.0.20
 domain-name depi.com

ip routing
spanning-tree mode pvst
```

3.3 Configuration for Router R1 on Layer Core 1

```
spanning-tree mode pvst

interface Tunnel0
 ip address 100.0.0.1 255.0.0.0
 mtu 1476
 tunnel source Serial0/3/0
 tunnel destination 14.0.0.2

interface GigabitEthernet0/0
 ip address 192.168.0.162 255.255.255.240
 ip ospf 1 area 0
 ip nat inside
 duplex auto
```

```
 speed auto

interface GigabitEthernet0/1
 ip address 192.168.0.178 255.255.255.240
 ip ospf 1 area 0
 ip nat inside
 duplex auto
 speed auto

interface Serial0/3/0
 ip address 12.0.0.1 255.0.0.0
 ip nat outside

router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
 default-information originate

ip nat inside source list 10 interface Serial0/3/0 overload
ip route 0.0.0.0 0.0.0.0 Serial0/3/0

access-list 10 permit 192.168.0.0 0.0.0.255
```

3.4 Configuration for ISP Router

```
interface Serial0/1/0
 ip address 12.0.0.2 255.0.0.0
 clock rate 2000000

interface Serial0/2/0
 ip address 14.0.0.1 255.0.0.0

router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
```

---

4. Security Features

The project implements the following security features to protect the network:

1. **VPN Tunneling**:
   A secure tunnel is established between the two branches to ensure encrypted communication over the internet.
2. **Port Security**:
   Enforces limits on the number of MAC addresses allowed on each access port. Configured to allow up to 5 addresses per port, and unknown addresses are restricted.
3. **BPDU Guard**:
   Enables protection against potential loops by disabling ports when BPDU packets are received on access ports.

4. **DHCP Snooping**:
   Helps prevent rogue DHCP servers from providing incorrect IP addresses by inspecting DHCP messages and allowing only legitimate servers.
5. **IP DHCP Snooping Trust**:
   Applied to trusted trunk links to allow DHCP messages only from legitimate DHCP servers.
6. **ARP Inspection**:
   Protects the network from ARP spoofing attacks by inspecting ARP packets and only allowing valid IP-to-MAC address bindings.

---

5. Testing and Verification

The following steps were taken to verify the successful implementation of the project:

1. **Ping Tests**:
   The connectivity between the branches was tested using ICMP ping. Both secure VPN communication and standard branch-to-branch communication were verified.
2. **Security Feature Testing**:
   - **Port Security**: Attempts to connect more than 5 devices to a single port triggered the configured port security measures.
   - **BPDU Guard**: Introducing a potential loop to the network correctly disabled the affected port.
   - **DHCP Snooping and ARP Inspection**: Successfully prevented unauthorized DHCP servers and ARP spoofing attempts.
3. **VPN Tunnel**:
   Verified that the VPN tunnel was active and passing encrypted traffic between the two branches.

---

6. Challenges and Solutions

- **Challenge**: VPN tunnel stability and configuration.
  - **Solution**: Adjusting the MTU and ensuring the correct source and destination interfaces were configured for the tunnel interface.
- **Challenge**: Ensuring that DHCP snooping and ARP inspection didn't block legitimate traffic.
  - **Solution**: Fine-tuning the DHCP snooping trust settings and ensuring ARP inspection was correctly configured on trusted ports.

---

7. Conclusion

The "Secure Inter-Branch Communication" project successfully achieved its goal of establishing a secure VPN tunnel between two branches, alongside implementing robust internal network security. By utilizing Cisco's security features and routing protocols, the project ensured both encrypted external communication and a well-segmented internal network.