

Packet Tracer – Konfigurowanie rozszerzonych list ACL – Scenariusz 2

Topologia

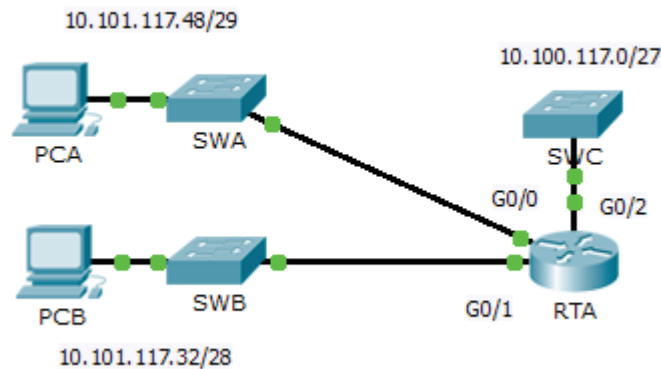


Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
RTA	G0/0	10.101.117.49	255.255.255.248	Nie dotyczy
	G0/1	10.101.117.33	255.255.255.240	Nie dotyczy
	G0/2	10.101.117.1	255.255.255.224	Nie dotyczy
PCA	Karta sieciowa	10.101.117.51	255.255.255.248	10.101.117.49
PCB	Karta sieciowa	10.101.117.35	255.255.255.240	10.101.117.33
SWC	VLAN1	10.101.117.2	255.255.255.224	10.101.117.1

Cele

Część 1: Konfigurowanie, zastosowanie i weryfikacja rozszerzonych numerowanych list ACL

Część 2: Pytania do przemyślenia

Wprowadzenie / Scenariusz

W tym scenariuszu, urządzenia z jednej sieci LAN mają zdalny dostęp do urządzeń w innej sieci LAN za pomocą protokołu telnet. Poza pakietami ICMP, cały ruch z innych sieci jest zabroniony.

Część 1: Konfigurowanie, zastosowanie i weryfikacja rozszerzonych numerowanych list ACL

Skonfiguruj, zastosuj i zweryfikuj ACL, tak aby spełnione zostały następujące zasady:

- Ruch telnet z urządzeń w sieci 10.101.117.32/28 jest dozwolony do urządzeń znajdujących się w sieciach 10.100.117.0/27.
- Ruch pakietów ICMP jest dozwolony z dowolnego źródła do dowolnego miejsca przeznaczenia.
- Cały pozostały ruch jest zablokowany.

Krok 1: Skonfiguruj rozszerzoną listę ACL.

- a. Aby skonfigurować listę ACL, użyj ostatniego ważnego numeru dla rozszerzonej listy ACL w odpowiednim trybie konfiguracji na **RTA**. Wykonaj następujące kroki w celu skonstruowania pierwszej instrukcji ACL:
 - 1) Ostatni numer dla listy rozszerzonej to 199.
 - 2) Protokołem jest TCP.
 - 3) Sieć źródłowa to 10.101.117.32.
 - 4) Maskę blankietową można ustalić poprzez odjęcie 255.255.255.240 od 255.255.255.255.
 - 5) Sieć docelowa to 10.101.117.0.
 - 6) Maskę blankietową można ustalić poprzez odjęcie 255.255.255.224 od 255.255.255.255.
 - 7) Protokołem jest telnet.Jaka jest pierwsza instrukcja ACL?
- b. ICMP jest dozwolone i dlatego potrzebna jest druga instrukcja ACL. Użyj tego samego numeru listy kontroli dostępu ACL aby zezwolić na cały ruch ICMP, niezależnie od adresu źródłowego lub docelowego. Jaka będzie druga instrukcja ACL? (Wskazówka: użyj słów kluczowych "any")
- c. Domyślnie cały pozostały ruch IP jest zabroniony.

Krok 2: Zastosuj rozszerzoną listę ACL.

Ogólna zasada zaleca umieszczanie rozszerzonych list ACL w pobliżu źródła. Jednakże lista kontroli dostępu ACL 199 dotyczy ruchu pochodzącego z obu sieci 10.101.117.48/29 i 10.101.117.32/28 i dlatego najlepszym miejscem na jej umieszczenie może być interfejs Gigabit Ethernet 0/2 w kierunku wychodzącym. Jakie jest polecenie, aby zastosować listę ACL 199 na interfejsie Gigabit Ethernet 0/2?

Krok 3: Sprawdź implementację rozszerzonej listy ACL.

- a. Użyj polecenia ping z **PCB** do wszystkich innych adresów IP w sieci. Jeśli pingi zakończą się niepowodzeniem, to sprawdź adresy IP przed dalszym kontynuowaniem.
- b. Połącz się protokołem telnet z **PCB** do **SWC**. Hasło dostępu do routera to **cisco**.
- c. Wyjdź z usługi telnet na **SWC**.
- d. Użyj polecenia ping z **PCA** do wszystkich innych adresów IP w sieci. Jeśli pingi zakończą się niepowodzeniem, to sprawdź adresy IP przed dalszym kontynuowaniem.
- e. Połącz się protokołem telnet z **PCA** do **SWC**. Lista kontroli dostępu ACL powoduje, że router odrzuca połączenie.
- f. Połącz się protokołem telnet z **PCA** do **SWB**. Lista kontroli dostępu ACL umieszczona jest na interfejsie **G0/2** w związku z czym nie wpływa na to połączenie.
- g. Po zalogowaniu się do **SWB**, nie wylogowuj się. Połącz się protokołem telnet z **SWC**.

Część 2: Pytania do przemyślenia

1. Dlaczego PCA był w stanie obejść listę kontroli dostępu ACL 199 i połączyć się protokołem telnet z SWC?
2. Co można było zrobić, aby uniemożliwić PCA dostęp do SWC pośrednio, a jednocześnie pozwolić PCB łączyć się telnetem z SWC?
3. Tabela sugerowanej punktacji

Sekcja ćwiczenia	Lokalizacja pytania	Maksymalna liczba punktów do uzyskania	Uzyskana liczba punktów
Część 1: Konfigurowanie, zastosowanie i weryfikacja rozszerzonych numerowanych list ACL	Krok 1a	4	
	Krok 1b	4	
	Krok 2	4	
Część 1 Razem		12	
Część 2: Pytania do przemyślenia	Pytanie 1	4	
	Pytanie 2	4	
Część 2 Razem		8	
Punktacja PacketTracer		80	
Suma punktów		100	