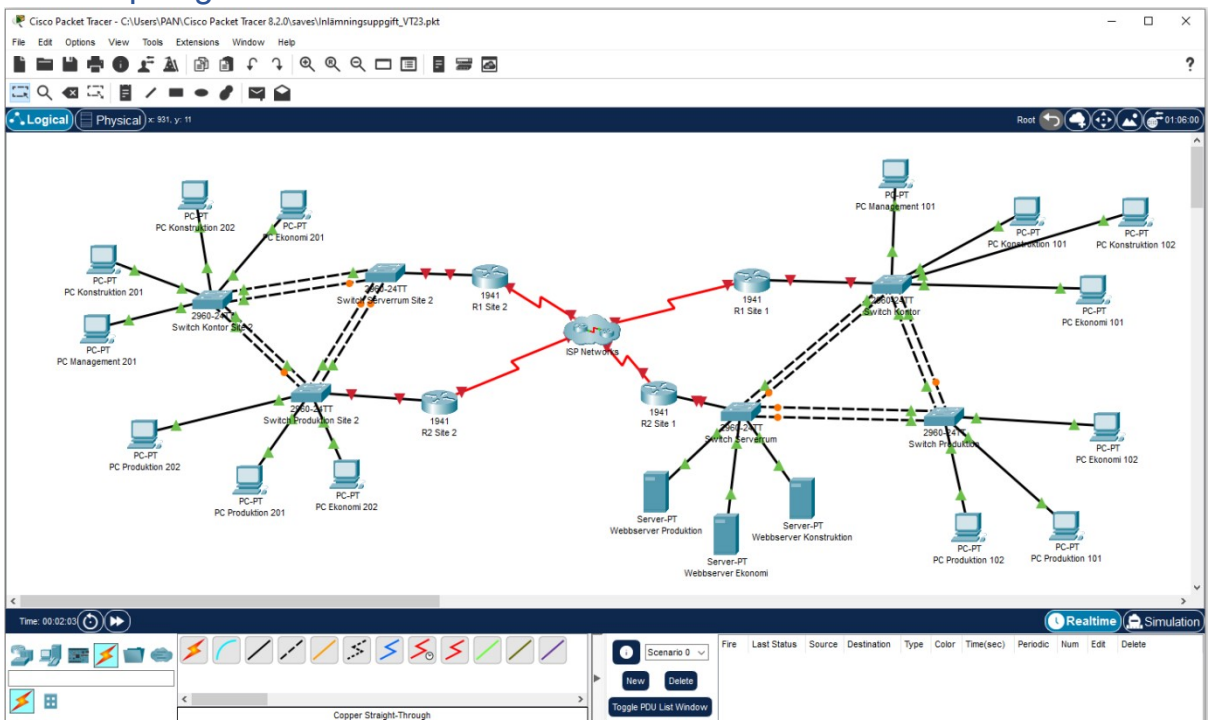
Inlämningsuppgift i kursen Nätverk CCNA 7.5 hp HT23

Detta dokument innehåller information/krav som ni behöver för att lösa inlämningsuppgiften. Det skall ni också använda som ”mall” för det dokument ni skall lämna in i tillägg till vad ni konfigurerat upp i Packet Tracer. Det får också tas med vid redovisningstillfället.

- bestämma vilka VLAN som behövs
- ta fram ett ip-adresschema
- utföra ip-adresstilldelning till routrar, switchar, servrar och hostar
- konfigurera GRE-tunnlar mellan siterna
- konfigurera routing, statisk och/eller dynamisk, inom och mellan siterna
- konfigurera redundans för default gateway
- konfigurera länkaggregering
- bestämma önskvärda L2-topologier och konfigurera STP för att uppnå dessa
- skapa ACL:er för att uppfylla krav på säkerhet samt applicera dessa på lämpliga interface
- aktivera lämplig variant av NAT/PAT

1. Topologi



2. WAN-länkar, ip-adresser och abonnemangstyp

Följande IP-nät är tilldelade från dina ISP:er för att användas mellan dina routrar och ”ISP Networks”

ISP-router	Lokal router	IP-nät
ISP1_1	R1 Site 1	133.10.5.0/30
ISP2_1	R2 Site 1	79.15.82.128/30

ISP1_2	R1 Site 2	148.99.2.0/30
ISP2_2	R2 Site 2	81.22.4.252/30

Observera att dina ISP:er har allokerat den första hostadressen i respektive ip-nät till sina routrar och den andra hostadressen är avsedd för dina routrar.

ISP:erna tillåter inte några privata ip-adresser (RFC1918) på sina nätverk.

Redundans är viktigt, därför har vi två olika routrar på varje site med internetanslutning. R1routrarna har en uppkoppling med högre bandbredd än R2-rotrarna. Detta abonnemang har även en ”flat rate”-prissättning, d.v.s. det tillkommer inga trafikavgifter utöver abonnemangskostnaden. R2routrarna har däremot en anslutning med mycket lägre bandbredd, och trafikavgifter tillkommer för det data som överförs. Därför skall R1-routrarnas internetuppkoppling användas primärt, och R2routrarna användas endast om R1-routrarna går ned eller förlorar sin uppkoppling.

3. Webbserver på internet

För att kontrollera access till tjänster på internet finns det en webbserver/http-server tillgänglig på ”internet”. Den har ip-adressen 112.4.8.23/32

4. VLAN och ip-adresser för de två LAN:en, ”Site 1” och ”Site 2”

Tag fram, för respektive site, de VLAN ni behöver för att lösa uppgiften. Tag även fram vilka ip-nät som ni skall använda för dessa. Privata ip-adresser (RFC1918) skall användas för alla interna nätverk.

Behövs fler ip-nät på siterna? Tag fram dessa också.

Observera att komplexiteten för implementeringen av routing på de båda siterna kan påverkas av hur ni designar ditt ip-adresschema. Ett ”smart” val kan göra implementeringen av routing mycket enklare.

Dokumentera, för respektive site, alla VLAN och ip-nät via två lämpliga tabeller som det brukar vara gjort i labb-pm och på examinationer. Observera att alla ip-nät ni använder skall vara med. Ange även en kort beskrivning vart de används, exempelvis *VLAN10* eller *GRE-tunnel R1-R1*.

Skapa sedan två tabeller, en per site, där ni gör ip-adresstilldelning för respektive enhet/host ni har i dina nätverk som det brukar vara gjort i labb-pm och på examinationer.

Kraven för antal hostar och servrar per avdelning är följande:

Avdelning	Hostar/Workstations	Servrar
Ekonomi (Site 1)	50	10
Konstruktion (Site 1)	80	10
Produktion (Site 1)	350	10
Management (Site 1)	10	50 (inkl. routrar/switchar/m.m.)
Ekonomi (Site 2)	20	-
Konstruktion (Site 2)	20	-
Produktion (Site 2)	450	-
Management (Site 2)	10	50 (inkl. routrar/switchar/m.m.)

IP-adressschema

Site-1

Enheter	Gränssnitt	IP-adress	Subnätmask	Default Gateway	Standby IP/Virtual Default Gateway
R1	g0/0.10	10.10.1.62	255.255.255.192		10.10.1.1
	g0/0.20	10.20.2.126	255.255.255.128		10.20.1.1
	g0/0.30	10.30.1.62	255.255.255.192		10.30.1.1
	g0/0.40	10.40.11.253	255.255.254.0		10.40.10.1
	s0/0/0	133.10.5.2	255.255.255.252		
R2	g0/0.10	10.10.1.61	255.255.255.192		10.10.1.1
	g0/0.20	10.20.1.125	255.255.255.128		10.20.1.1
	g0/0.30	10.30.1.61	255.255.255.192		10.30.1.1
	g0/0.40	10.40.11.254	255.255.254.0		10.40.10.1
	s0/0/0	79.15.82.130	255.255.255.252		
PC Management 101		10.30.1.5	255.255.255.192	10.30.1.1	
PC Konstruktion 101		10.20.1.2	255.255.255.128	10.20.1.1	
PC Konstruktion 102		10.20.1.3	255.255.255.128	10.20.1.1	
PC Ekonomi 101		10.10.1.2	255.255.255.192	10.10.1.1	
PC Ekonomi 102		10.10.1.3	255.255.255.192	10.10.1.1	
PC Produktion 101		10.40.10.2	255.255.254.0	10.40.10.1	
PC Produktion 102		10.40.10.3	255.255.254.0	10.40.1.1	
Webbserver Konstr.		10.20.1.4	255.255.255.128	10.20.1.1	
Webbserver Ekonomi		10.10.1.4	255.255.255.192	10.10.1.1	
Webbserver Prod.		10.40.10.4	255.255.254.0	10.40.1.1	
Switch-Kontor		10.30.1.2	255.255.255.192	10.30.1.1	
Switch-Serverrum		10.30.1.4	255.255.255.192	10.30.1.1	

Switch-Produktion		10.30.1.3	255.255.255.192	10.30.1.1	

Site 2:

Enheter	Gränssnitt	IP-adress	Subnätmask	Default Gateway	Standby IP/Virtual Default Gateway
R1	g0/0.10	10.10.2.30	255.255.255.224		10.10.2.1
	g0/0.20	10.20.2.30	255.255.255.224		10.20.2.1
	g0/0.30	10.30.2.62	255.255.255.192		10.30.2.1
	g0/0.40	10.40.3.253	255.255.254.0		10.40.2.1
	s0/0/0	148.99.2.2	255.255.255.252		
R2	g0/0.10	10.10.2.29	255.255.255.224		10.10.2.1
	g0/0.20	10.20.2.29	255.255.255.224		10.20.2.1
	g0/0.30	10.30.2.61	255.255.255.192		10.30.2.1
	g0/0.40	10.40.3.254	255.255.254.0		10.40.3.1
	s0/0/0	81.22.4.254	255.255.255.252		
PC Management 201		10.30.2.5	255.255.255.192	10.30.2.1	
PC Konstruktion 201		10.20.2.2	255.255.255.224	10.20.2.1	
PC Konstruktion 202		10.20.2.3	255.255.255.224	10.20.2.1	
PC Ekonomi 201		10.10.2.2	255.255.255.224	10.10.2.1	
PC Ekonomi 202		10.10.2.3	255.255.255.224	10.10.2.1	
PC Produktion 201		10.40.2.2	255.255.254.0	10.40.2.1	
PC Produktion 202		10.40.2.3	255.255.254.0	10.40.2.1	

5. DHCP

Ni behöver INTE använda DHCP för att dela ut ip-adresser till hostarna utan ni kan använda statisk ip-adresstilldelning. Vill ni använda DHCP så måste ni ange de olika DHCP-konfigurationerna i detta kapitel.

<Om ni använder DHCP, kopiera konfigurationerna från Packet Tracer och klistra in här>

6. Site-to-site VPN

För att emulera en ” Site-to-site VPN”-lösning implementerar ni minst två olika GRE-tunnlar. Observera att primärt skall tunneln mellan R1-routrarna användas. Tunneln mellan R2-routrarna skall vara för backup om tunneln mellan de två R1-routrarna går ned.

R1 Site 1:

interface Tunnel0
Tunnel mode gre ip
ip address 192.168.1.2 255.255.255.0
tunnel source Serial0/0/0
tunnel destination 148.99.2.2

R2 Site 1:

interface Tunnel1
tunnel mode gre ip
ip address 192.168.2.2 255.255.255.0
tunnel source Serial0/0/0
tunnel destination 81.22.4.254

R1 Site 2:

interface Tunnel0
tunnel mode gre ip
ip address 192.168.1.2 255.255.255.0
tunnel source Serial0/0/0
tunnel destination 133.10.5.2

R2 Site 2:

interface Tunnel1
tunnel mode gre ip
ip address 192.168.2.1 255.255.255.0
tunnel source Serial0/0/0
tunnel destination 79.15.82.130

Hur ni löser att ”rätt” GRE-tunnel används anger ni under *10 Routing inom och mellan de två ”siterna”*.

7. Redundans för ”Default Gateway”

För att få redundans på ”Default Gateway” för hostarna skall ett ”First Hop Redundancy Protocol” användas. Det är sedan tidigare beslutat att HSRP, Hot Standby Router Protocol, skall användas för detta. HSRP skall användas på alla ip-nät där det finns hostar/servrar.

<Kopiera konfigurationerna för HSRP från Packet Tracer och klistra in här. Det räcker att ni i detta dokument endast anger konfigurationerna för HSRP på ”Site 1”:s routrar. >

R1 Site 1:

interface GigabitEthernet0/0.10
encapsulation dot1Q 10

```
ip address 10.10.1.62 255.255.255.192
ip access-group 100 in
ip nat inside
standby version 2
standby 10 ip 10.10.1.1
standby 10 priority 150
standby 10 preempt
!
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 10.20.1.126 255.255.255.128
ip access-group 100 in
ip nat inside
standby version 2
standby 20 ip 10.20.1.1
standby 20 priority 150
standby 20 preempt
!
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 10.30.1.62 255.255.255.192
ip access-group 100 in
ip nat inside
standby version 2
standby 30 ip 10.30.1.1
standby 30 priority 150
standby 30 preempt
!
interface GigabitEthernet0/0.40
encapsulation dot1Q 40
ip address 10.40.11.253 255.255.254.0
ip access-group 100 in
standby version 2
standby 40 ip 10.40.10.1
standby 40 priority 150
standby 40 preempt
```

R2 Site 1:

```
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 10.10.1.61 255.255.255.192
ip access-group 100 in
ip nat inside
standby version 2
standby 10 ip 10.10.1.1
!
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 10.20.1.125 255.255.255.128
```

```
ip access-group 100 in
ip nat inside
standby version 2
standby 20 ip 10.20.1.1
!
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 10.30.1.61 255.255.255.192
ip access-group 100 in
ip nat inside
standby version 2
standby 30 ip 10.30.1.1
!
interface GigabitEthernet0/0.40
encapsulation dot1Q 40
ip address 10.40.11.254 255.255.254.0
ip access-group 100 in
standby version 2
standby 40 ip 10.40.10.1
```

R1 Site 2:

```
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 10.10.2.30 255.255.255.224
ip access-group 100 in
ip nat inside
standby version 2
standby 10 ip 10.10.2.1
standby 10 priority 150
standby 10 preempt
!
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 10.20.2.30 255.255.255.224
ip access-group 100 in
ip nat inside
standby version 2
standby 20 ip 10.20.2.1
standby 20 priority 150
standby 20 preempt
!
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 10.30.2.62 255.255.255.192
ip access-group 100 in
ip nat inside
standby version 2
standby 30 ip 10.30.2.1
standby 30 priority 150
standby 30 preempt
!
```

```
interface GigabitEthernet0/0.40
encapsulation dot1Q 40
ip address 10.40.3.253 255.255.254.0
ip access-group 100 in
standby version 2
standby 40 ip 10.40.2.1
standby 40 priority 150
standby 40 preempt
```

R2 Site 2:

```
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 10.10.2.29 255.255.255.224
ip access-group 100 in
ip nat inside
standby version 2 standby 10
ip 10.10.2.1
!
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 10.20.2.29 255.255.255.224
ip access-group 100 in
ip nat inside
standby version 2
standby 20 ip 10.20.2.1
!
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 10.30.2.61 255.255.255.192
ip access-group 100 in
ip nat inside
standby version 2
standby 30 ip 10.30.2.1
!
interface GigabitEthernet0/0.40
encapsulation dot1Q 40
ip address 10.40.3.254 255.255.254.0
ip access-group 100 in
standby version 2
standby 40 ip 10.40.2.1
```

8. Länkaggregering

Länkaggregering skall användas mellan alla switchar på båda siterna. För närvarande använder vi endast Cisco-switchar, men i framtiden kan andra fabrikat komma att användas.

Vilket länkaggregeringsprotokoll väljer ni att använda och varför? Motivera!

LACP är en open standard, vilket gör anslutningarna mer anpassningsbara eftersom PAgP endast gäller på Cisco-switchar.

<Kopiera konfigurationerna för länkaggregering från Packet Tracer och klistra in här. Det räcker att ni i detta dokument endast anger konfigurationerna för länkaggregering mellan "Switch Kontor" och "Switch Serverrum" på "Site 1">

Switch kontor site 1:
Show etherchannel sum
1 Po1(SU) LACP Fa0/1(P) Fa0/2(P)
2 Po2(SU) LACP Fa0/3(P) Fa0/4(P)

Site 1:

***Switch-Kontor**:*

Interface range f0/1-2
switchport mode trunk
switchport trunk native vlan 1000
switchport trunk allowed vlan 10,20,30,40,500,1000

Channel-group 1 mode active

***Switch-Serverrum**:*

Interface range f0/1-2 switchport
mode trunk switchport trunk
native vlan 1000
switchport trunk allowed vlan 10,20,30,40,500,1000

Channel-group 1 mode active

Switch-Kontor:
Interface range fa0/3-4
Switchport mode trunk
switchport trunk native vlan 1000
switchport trunk allowed vlan
10,20,30,40,500,1000
channel-group 2 mode active

Switch Produktion:
Interface range fa0/1-2
Switchport mode trunk
switchport trunk native vlan 1000
switchport trunk allowed vlan
10,20,30,40,500,1000
channel-group 2 mode active

Switch-Serverrum:
Interface range fa0/3-4

Switchport mode trunk
switchport trunk native vlan 1000
switchport trunk allowed vlan
10,20,30,40,500,1000
channel-group 3 mode active

Switch-Produktion:
Interface range fa0/3-4
Switchport mode trunk
switchport trunk native vlan 1000
switchport trunk allowed vlan 10,20,30,40,500,1000
channel-group 3 mode active

9. STP, Spanning Tree Protocol

Eftersom vi vill använda redundanta vägar på våra L2-topologier är det viktigt att switcharna stödjer STP. Just nu har vi endast Cisco-switchar och har, för snabb konvergering, valt att STP-protokollet Rapid PVST+ skall användas. Rapid PVST+ är Cisco-proprietärt men det är kompatibelt med exempelvis STP-protokollen RSTP och MSTP, vilka båda är IEEE-standarder. Detta ger möjlighet att använda switchar från andra tillverkare i framtiden.

Ni skall också implementera ”Spanning-Tree PortFast” på alla switchportar mot hostar/servrar.

Vilken switch bör vara primär root-brygga för respektive VLAN på ”Site 1”? Motivera ditt val för varje VLAN som används.

Vi valde Switch-serverrum som root bridge eftersom mycket trafikflöde ska mot webbservrarna och denna switch ligger närmast.

Vilken switch bör vara sekundär root-brygga för respektive VLAN på ”Site 1”? Motivera ditt val för varje VLAN som används.

Switch-Kontor bör vara sekundär root bridge eftersom den ligger närmast den primära routern där all trafik kommer flödas.

Vilken switch bör vara primär root-brygga för respektive VLAN på ”Site 2”? Motivera ditt val för varje VLAN som används.

Switch-serverrum site 2 bör vara den primära root bridge eftersom den ligger närmast den primära routern där trafiken ska flödas.

Vilken switch bör vara sekundär root-brygga för respektive VLAN på ”Site 2”? Motivera ditt val för varje VLAN som används.

Den sekundära root bryggan bör placeras på Switch-kontor där port fa0/3-4 är blockade så att trafiken som flödas ut switch-produktion färdas direkt till switch-serverrum och in till router R1 Site 2.

<Kopiera konfigurationerna för Rapid PVST+ från Packet Tracer och klistra in här. Det räcker att ni i detta dokument endast anger konfigurationerna för ett av VLAN:en på ”Site 1”>

Switch-Kontor Site 1:

spanning-tree mode rapid-pvst
spanning-tree vlan 10,20,30,40 priority 28672

Spanning-tree portfast på alla PC:s och
webbservrar.

Switch-Serverrum Site 1:

spanning-tree mode rapid-pvst
spanning-tree vlan 10,20,30,40 priority 24576
Lägst prioritet till root bridge.

Switch-Produktion Site 1:

spanning-tree mode rapid-pvst

Switch Kontor site 2:

spanning-tree mode rapid-pvst
spanning-tree vlan 10,20,30,40 priority 28672

Switch-Serverrum site 2:

spanning-tree mode rapid-pvst
spanning-tree vlan 10,20,30,40 priority 24576

Switch Produktion site 2:
spanning-tree mode rapid-pvst

10. Routing inom och mellan de två ”siterna”

Hur väljer ni att implementera routing inom, och mellan siterna, **statiskt** och/eller dynamiskt? Beskriv din lösning som ni tänker implementera. Observera att för trafik mellan siterna skall GREtunneln mellan R1-routrarna användas. För trafik mot internet skall respektive R1-router användas. R2-routrarna är endast för backuplänkar om någon R1-router går ned, eller dess länk mot internet går ned. Troligtvis måste någon ”floating static route” användas för detta.

Observera att komplexiteten för detta moment kan till stor del bero på hur ni har gjort ditt ipadresschema. Ett ”smart” val tidigare kan göra detta moment enklare.

<Beskriv ditt val för impementering av routing. Dynamisk, statisk eller en kombination. Om dynamisk, vilket routingprotokoll väljer ni att använda och vilka nätverk annonseras via detta. Vilka statiska routes implementerar ni? Floating static routes, vilka?>

*Vi har vald en **default static route** som skickar all okänd* IP till motsvarande router i klustret. Den andra skickar till den andra änden av tunneln för nätverket 10.0.0.0 255.0.0.0 för trafik som ska till den andra siten.

<Kopiera konfigurationerna för routing från Packet Tracer och klistra in här. Kopiera in för alla dina routrar>

R1 Site 1:

ip route 0.0.0.0 0.0.0.0 133.10.5.1
ip route 10.0.0.0 255.0.0.0 192.168.1.2

R2 Site 1:
ip route 0.0.0.0 0.0.0.0 79.15.82.129 ip
route 10.0.0.0 255.0.0.0 192.168.2.1

R1 Site 2:
ip route 0.0.0.0 0.0.0.0 148.99.2.1
ip route 10.0.0.0 255.0.0.0
192.168.1.1

R2 Site 2:
ip route 0.0.0.0 0.0.0.0 81.22.4.253 ip
route 10.0.0.0 255.0.0.0 192.168.1.2

<Kopiera routingtabellerna från Packet Tracer och klistra in här. Kopiera in för alla dina routrar. Kontrollera att alla nätverk är annonserade, antingen individuellt eller summerade router>

R1 site 1:
10.0.0.0/8 is variably subnetted, 9 subnets, 5 masks
S 10.0.0.0/8 [1/0] via 192.168.1.2
C 10.10.1.0/26 is directly connected, GigabitEthernet0/0.10
L 10.10.1.62/32 is directly connected, GigabitEthernet0/0.10
C 10.20.1.0/25 is directly connected, GigabitEthernet0/0.20
L 10.20.1.126/32 is directly connected, GigabitEthernet0/0.20
C 10.30.1.0/26 is directly connected, GigabitEthernet0/0.30
L 10.30.1.62/32 is directly connected, GigabitEthernet0/0.30
C 10.40.10.0/23 is directly connected, GigabitEthernet0/0.40
L 10.40.11.253/32 is directly connected, GigabitEthernet0/0.40
133.10.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 133.10.5.0/30 is directly connected, Serial0/0/0
L 133.10.5.2/32 is directly connected, Serial0/0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, Tunnel0
L 192.168.1.1/32 is directly connected, Tunnel0
S* 0.0.0.0/0 [1/0] via 133.10.5.1

R2 Site 1:
10.0.0.0/8 is variably subnetted, 9 subnets, 5 masks
S 10.0.0.0/8 [1/0] via 192.168.2.1
C 10.10.1.0/26 is directly connected, GigabitEthernet0/0.10
L 10.10.1.61/32 is directly connected, GigabitEthernet0/0.10
C 10.20.1.0/25 is directly connected, GigabitEthernet0/0.20
L 10.20.1.125/32 is directly connected, GigabitEthernet0/0.20
C 10.30.1.0/26 is directly connected, GigabitEthernet0/0.30
L 10.30.1.61/32 is directly connected, GigabitEthernet0/0.30

C 10.40.10.0/23 is directly connected, GigabitEthernet0/0.40
L 10.40.11.254/32 is directly connected, GigabitEthernet0/0.40
79.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 79.15.82.128/30 is directly connected, Serial0/0/0
L 79.15.82.130/32 is directly connected, Serial0/0/0
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Tunnel1
L 192.168.2.2/32 is directly connected, Tunnel1
S* 0.0.0.0/0 [1/0] via 79.15.82.129

R1 Site 2:
10.0.0.0/8 is variably subnetted, 9 subnets, 5 masks
S 10.0.0.0/8 [1/0] via 192.168.1.1
C 10.10.2.0/27 is directly connected, GigabitEthernet0/0.10
L 10.10.2.30/32 is directly connected, GigabitEthernet0/0.10
C 10.20.2.0/27 is directly connected, GigabitEthernet0/0.20
L 10.20.2.30/32 is directly connected, GigabitEthernet0/0.20
C 10.30.2.0/26 is directly connected, GigabitEthernet0/0.30
L 10.30.2.62/32 is directly connected, GigabitEthernet0/0.30
C 10.40.2.0/23 is directly connected, GigabitEthernet0/0.40
L 10.40.3.253/32 is directly connected, GigabitEthernet0/0.40
148.99.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 148.99.2.0/30 is directly connected, Serial0/0/0
L 148.99.2.2/32 is directly connected, Serial0/0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, Tunnel0
L 192.168.1.2/32 is directly connected, Tunnel0
S* 0.0.0.0/0 [1/0] via 148.99.2.1

R2 Site 2:
10.0.0.0/8 is variably subnetted, 8 subnets, 4 masks
C 10.10.2.0/27 is directly connected, GigabitEthernet0/0.10
L 10.10.2.29/32 is directly connected, GigabitEthernet0/0.10
C 10.20.2.0/27 is directly connected, GigabitEthernet0/0.20
L 10.20.2.29/32 is directly connected, GigabitEthernet0/0.20
C 10.30.2.0/26 is directly connected, GigabitEthernet0/0.30
L 10.30.2.61/32 is directly connected, GigabitEthernet0/0.30
C 10.40.2.0/23 is directly connected, GigabitEthernet0/0.40
L 10.40.3.254/32 is directly connected, GigabitEthernet0/0.40
81.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 81.22.4.252/30 is directly connected, Serial0/0/0
L 81.22.4.254/32 is directly connected, Serial0/0/0
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Tunnel1
L 192.168.2.1/32 is directly connected, Tunnel1
S* 0.0.0.0/0 [1/0] via 81.22.4.253

11. Säkerhet

Sist, men inte minst, vad gäller säkerheten i, mellan, från och till våra nätverk?

I tidigare examinationer har ”Switchport security” implementerats. Det är en viktig del av säkerheten men ni behöver inte implementera det i denna inlämningsuppgift. Vill ni göra det kan ni göra det.

I övrigt så gäller följande för vilket nätverk som kan nå vilket nätverk:

- Alla noder i ”Ekonomi” skall kunna nå varandra, oberoende av vilken site de är på
- Alla noder i ”Konstruktion” skall kunna nå varandra, oberoende av vilken site de är på
- Alla noder i ”Produktion” skall kunna nå varandra, oberoende av vilken site de är på
- Alla noder i ”Konstruktion” skall kunna webbservern för ”Produktion”, oberoende av vilken site de är på
- Alla noder i ”Ekonomi” skall kunna använda tjänster på internet, oberoende av vilken site de är på
- Alla noder i ”Konstruktion” skall kunna använda tjänster på internet, oberoende av vilken site de är på
- Noderna i ”Produktion” skall inte ha någon internetaccess
- Alla noder i ”Management” skall inte ha någon begränsning på vad de kan nå

Vilka ACL:er behöver ni för att lösa detta? Glöm inte att tänka på returtrafik!
Extended access-control list

Hur implementeras ACL:er som skydd för hot mot internet?
För att implementera ACL:er för säkerhet på internet, identifierar vi de resurser som ska skyddas och skapar tydliga regler baserat på kriterier som ip adresser och portnummer.

För att förenkla momentet så behöver vi bara tänka på att tillåta webbtrafik (HTTP-protokollet) och ICMP (exempelvis ping). Detta eftersom vi bara kan använda oss av standard- och extended-ACL:er i Packet Tracer. Tyvärr finns det i Packet Tracer inte stöd för exempelvis reflexiva ACL:er vilket hade gjort det enklare att implementera en lösning för många olika protokoll.

<Kopiera dina ACL:er från Packet Tracer och klistra in här. Kopiera in för alla dina routrar. Ange även på vilka interface dem är applicerade, och i vilken riktning, in eller ut>

R1 Site 1:

ip access-list extended 100

access-list 100 permit ip 10.10.1.0 0.0.0.63 10.10.2.0 0.0.0.31
access-list 100 permit ip 10.20.1.0 0.0.0.127 10.20.2.0 0.0.0.31
access-list 100 permit ip 10.30.1.0 0.0.0.63 any
access-list 100 permit ip 10.40.10.0 0.0.1.255 10.40.2.0 0.0.1.255
access-list 100 permit ip host 10.40.10.4 10.20.2.0 0.0.0.31
access-list 100 permit ip host 10.40.10.4 10.40.2.0 0.0.1.255
access-list 100 permit ip 10.20.1.0 0.0.0.127 host 10.40.10.4
access-list 100 permit ip host 10.40.10.4 10.30.1.0 0.0.0.63
access-list 100 permit ip host 10.40.10.4 10.20.1.0 0.0.0.127
access-list 100 permit ip 10.30.2.0 0.0.0.63 any
access-list 100 permit ip any 10.30.2.0 0.0.0.63

access-list 100 permit ip 10.10.1.0 0.0.0.63 112.4.8.0 0.0.0.255
access-list 100 permit ip 10.20.1.0 0.0.0.127 112.4.8.0 0.0.0.255
access-list 100 permit icmp 10.20.1.0 0.0.0.127 host 10.20.1.1
access-list 100 permit icmp 10.10.1.0 0.0.0.63 host 10.10.1.1
access-list 100 permit icmp 10.40.10.0 0.0.1.255 host 10.40.10.1

Lägga till listorna på subinterfacen:
interface GigabitEthernet0/0.10
ip access-group 100 in

interfaces GigabitEthernet0/0.20
ip access-group 100 in

interface GigabitEthernet0/0.30
ip access-group 100 in

interface GigabitEthernet0/0.40
ip access-group 100 in

R2 Site 1:

ip access-list extended 100

access-list 100 permit ip 10.10.1.0 0.0.0.63 10.10.2.0 0.0.0.31
access-list 100 permit ip 10.20.1.0 0.0.0.127 10.20.2.0 0.0.0.31
access-list 100 permit ip 10.30.1.0 0.0.0.63 any
access-list 100 permit ip 10.40.10.0 0.0.1.255 10.40.2.0 0.0.1.255
access-list 100 permit ip host 10.40.10.4 10.20.2.0 0.0.0.31
access-list 100 permit ip host 10.40.10.4 10.40.2.0 0.0.1.255
access-list 100 permit ip 10.20.1.0 0.0.0.127 host 10.40.10.4
access-list 100 permit ip host 10.40.10.4 10.30.1.0 0.0.0.63
access-list 100 permit ip host 10.40.10.4 10.20.1.0 0.0.0.127
access-list 100 permit ip 10.30.2.0 0.0.0.63 any
access-list 100 permit ip any 10.30.2.0 0.0.0.63
access-list 100 permit ip 10.10.1.0 0.0.0.63 112.4.8.0 0.0.0.255
access-list 100 permit ip 10.20.1.0 0.0.0.127 112.4.8.0 0.0.0.255
access-list 100 permit icmp 10.20.1.0 0.0.0.127 host 10.20.1.1
iaccess-list 100 permit icmp 10.10.1.0 0.0.0.63 host 10.10.1.1
access-list 100 permit icmp 10.40.10.0 0.0.1.255 host 10.40.10.1

interface GigabitEthernet0/0.10
ip access-group 100 in

interface GigabitEthernet0/0.20
ip access-group 100 in

interface GigabitEthernet0/0.30
ip access-group 100 in

interface GigabitEthernet0/0.40
ip access-group 100 in

R1 Site 2:

```
ip access-list extended 100
access-list 100 permit ip 10.10.2.0 0.0.0.31 10.10.1.0 0.0.0.63
access-list 100 permit ip 10.20.2.0 0.0.0.31 10.20.1.0 0.0.0.127
access-list 100 permit ip 10.30.2.0 0.0.0.63 any
access-list 100 permit ip 10.20.2.0 0.0.0.31 10.40.10.0 0.0.1.255
access-list 100 permit ip 10.40.2.0 0.0.1.255 10.40.10.0 0.0.1.255
access-list 100 permit ip 10.20.2.0 0.0.0.31 112.4.8.0 0.0.0.255
access-list 100 permit ip 10.10.2.0 0.0.0.31 112.4.8.0 0.0.0.255
permit icmp 10.10.2.0 0.0.0.31 host 10.10.2.1
permit icmp 10.20.2.0 0.0.0.31 host 10.20.2.1
permit icmp 10.40.2.0 0.0.1.255 host 10.40.2.1


interface GigabitEthernet0/0.10
ip access-group 100 in

interface GigabitEthernet0/0.20
ip access-group 100 in

interface GigabitEthernet0/0.30
ip access-group 100 in

interface GigabitEthernet0/0.40
ip access-group 100 in
```

R2 Site 2:

```
ip access-list extended 100

access-list 100 permit ip 10.10.2.0 0.0.0.31 10.10.1.0 0.0.0.63
access-list 100 permit ip 10.20.2.0 0.0.0.31 10.20.1.0 0.0.0.127
access-list 100 permit ip 10.30.2.0 0.0.0.63 any
access-list 100 permit ip 10.40.2.0 0.0.1.255 10.40.10.0 0.0.1.255
access-list 100 permit ip 10.20.2.0 0.0.0.31 112.4.8.0 0.0.0.255
access-list 100 permit ip 10.10.2.0 0.0.0.31 112.4.8.0 0.0.0.255
access-list 100 permit ip 10.20.2.0 0.0.0.31 host 10.40.10.4

permit icmp 10.10.2.0 0.0.0.31 host 10.10.2.1
permit icmp 10.20.2.0 0.0.0.31 host 10.20.2.1
permit icmp 10.40.2.0 0.0.1.255 host 10.40.2.1

interface GigabitEthernet0/0.10
ip access-group 100 in

interface GigabitEthernet0/0.20
ip access-group 100 in

interface GigabitEthernet0/0.30
```

ip access-group 100 in

interface GigabitEthernet0/0.40
ip access-group 100 in

12. Övrigt

Om något är otydligt, eller vi har missat att ge någon vital information, använd i första hand kursens diskussionsforum för inlämningsuppgiften för att ställa din fråga, annars ta upp det på labbpassen.

13. NAT

R1 Site 1:

access-list 1 permit 10.10.1.0 0.0.0.63
access-list 1 permit 10.20.1.0 0.0.0.127
access-list 1 permit 10.30.1.0 0.0.0.63

ip nat inside source list 1 interface Serial0/0/0 overload

interface s0/0/0
ip nat outside

interface GigabitEthernet0/0.10
ip nat inside

interface GigabitEthernet0/0.20
ip nat inside

interface GigabitEthernet0/0.30
ip nat inside

interface GigabitEthernet0/0.40
ip nat inside

R2 Site 1

access-list 1 permit 10.10.1.0 0.0.0.31
access-list 1 permit 10.20.1.0 0.0.0.31
access-list 1 permit 10.30.1.0 0.0.0.63

ip nat inside source list 1 interface Serial0/0/0 overload

interface s0/0/0
ip nat outside

interface GigabitEthernet0/0.10
ip nat inside

interface GigabitEthernet0/0.20
ip nat inside

interface GigabitEthernet0/0.30
ip nat inside

interface GigabitEthernet0/0.40
ip nat inside

R1 Site 2:

access-list 1 permit 10.10.2.0 0.0.0.31
access-list 1 permit 10.20.2.0 0.0.0.31
access-list 1 permit 10.30.2.0 0.0.0.63

ip nat inside source list 1 interface Serial0/0/0 overload

interface s0/0/0
ip nat outside

interface GigabitEthernet0/0.10
ip nat inside

interface GigabitEthernet0/0.20
ip nat inside

interface GigabitEthernet0/0.30
ip nat inside

interface GigabitEthernet0/0.40
ip nat inside

R2 Site 2:

access-list 1 permit 10.10.2.0 0.0.0.31
access-list 1 permit 10.20.2.0 0.0.0.31
access-list 1 permit 10.30.2.0 0.0.0.63

ip nat inside source list 1 interface Serial0/0/0 overload

interface s0/0/0
ip nat outside

interface GigabitEthernet0/0.10
ip nat inside

interface GigabitEthernet0/0.20
ip nat inside

interface GigabitEthernet0/0.30
ip nat inside

```
interface GigabitEthernet0/0.40
ip nat inside
```