Instituto Politécnico de Lisboa (IPL)

Instituto Superior de Engenharia de Lisboa (ISEL)

Área Departamental de Engenharia da
Eletrónica e Telecomunicações e de Computadores(ADEETC)
LEETC, LEIC, LEIM, LEIRT, MEIC

Redes de Internet (RI) – Trabalho nº 3 (BGP)

Inverno de 2018/2019 - Data limite de entrega: Ver Moodle

Este trabalho tem como objetivo os alunos aprofundarem os seus conhecimentos sobre o protocolo BGP.

Cada uma das quatro fases do trabalho tem um peso de 10, 15, 30 e 45% respetivamente na nota final.

O trabalho prático é de execução por grupos de até 3 alunos, podendo na aula prática de realização do trabalho, ou parte, existir avaliação do grupo e/ou individual sobre a realização do mesmo e o tema que envolve.

Este trabalho, tal como os anteriores, é considerado pedagogicamente fundamental ("NORMAS DE AVALIAÇAO DE CONHECIMENTOS", Conselho Pedagógico do ISEL, ponto 2.3.1).

Os alunos devem saber utilizar convenientemente os comandos de configuração dos equipamentos, incluindo os de *show* e *debug*, para validar o seu trabalho e resolver os desafios que lhe vão aparecendo.

O docente decidirá conforme os relatórios entregues e as notas individuais se fará, e com que grupos fará, discussão final dos trabalhos.

É fornecido um ficheiro para o GNS3 como proposta de configuração base que corresponde, aproximadamente, à necessária para as três primeiras das quatro fases do trabalho a realizar. A configuração fornecida é apenas uma proposta podendo ser alterada de maneira a se atingirem os objetivos pretendidos. Devem ser confirmadas todas as configurações propostas devendo ser alteradas aquelas que apresentarem falhas ou em que exista uma melhor alternativa de configuração. Pode ser usado outro simulador que não o GNS3, o PT não inclui as capacidade suficientes, nomeadamente iBGP.

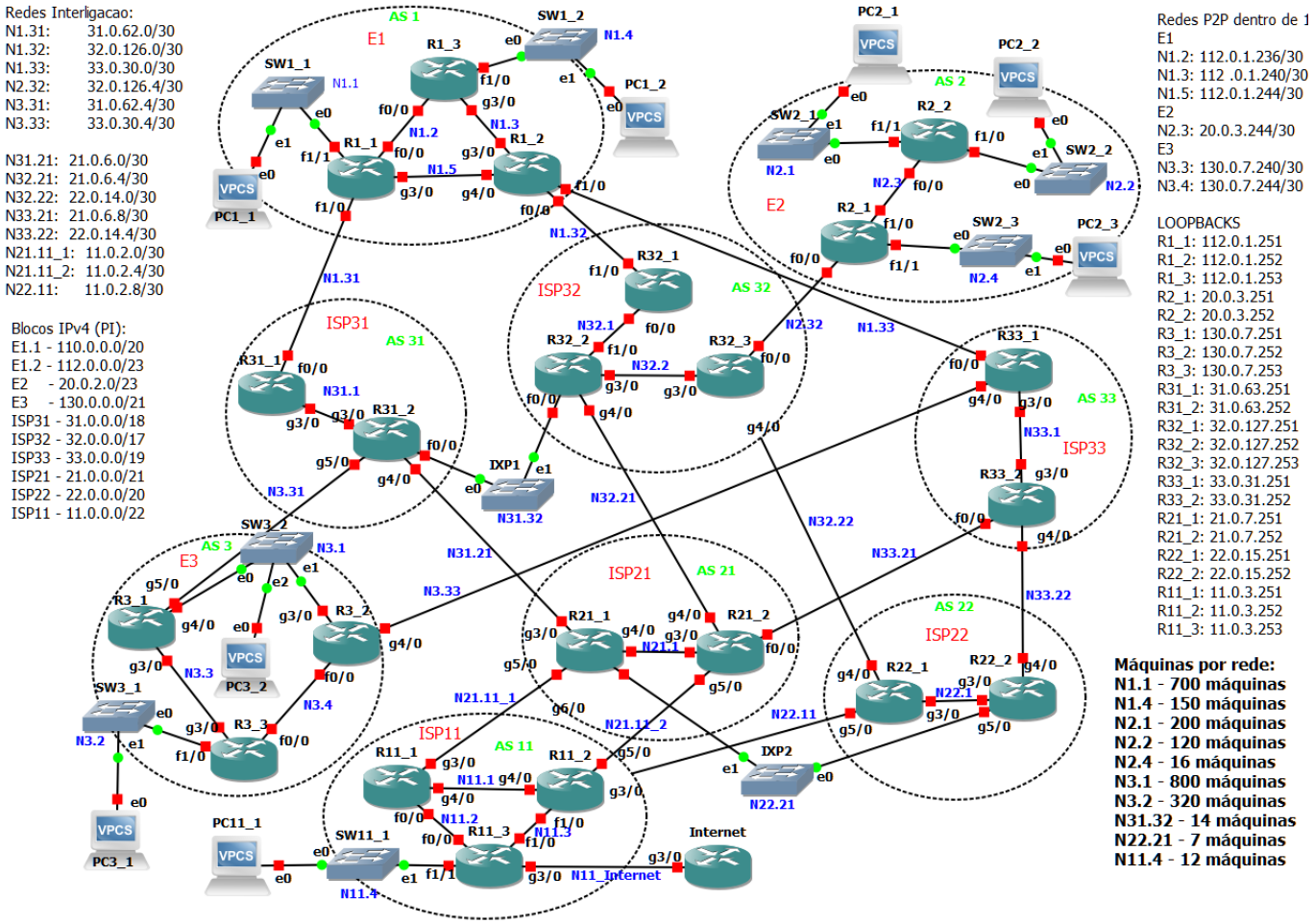
Nota: Ler TODO o enunciado antes de se começar a configurar os equipamentos! A atribuição de endereços IP (preenchimento da tabela de acordo com as especificações indicadas) deve ser realizada antes da aula prática indicada para o início do trabalho em laboratório.)

Conteúdo

Introdução

Este trabalho tem como objetivo familiarizar os alunos com o protocolo de encaminhamento BGP.

Topologia da rede a configurar



Pode usar o ficheiro para o GNS3 com a topologia acima e configurações básicas que é fornecido através do Moodle.

Aconselha-se a que use o Notepad++, ou outro editor de texto, para criar e manter as configurações de cada um dos equipamentos de maneira mais expedita.

Objetivo

Pretende-se ligar as empresas E1, E2 e E3 à Internet. Por Internet entende-se tudo o que é exterior a uma empresa e ou ISP (qualquer AS).

Para se ligarem à Internet estas empresas utilizam os serviços dos Internet Service Providers (ISP): ISP31, ISP32 e ISP33. Estes ISP, os quais são de *tier* 3, utilizam os serviços de outros ISP de *tier* superior (*tier* 2): ISP21 e 22. Por sua vez os ISP de *tier* 2 usam os serviços dos ISP de *tier* 1.

Neste trabalho apenas se representa um ISP de *tier* 1, o ISP11, para não tornar a topologia mais complexa mas, num caso real, este ISP ligar-se-ia a outros ISP do mesmo *tier* e prestaria serviços a ISPs de *tier* inferior.

Requisitos gerais

Cada empresa e cada ISP tem o seu próprio número sistema autónomo (AS *number*) (ver figura).

Cada AS possui um ou mais blocos de endereços IPv4 atribuídos por uma entidade oficial: IANA/RIR (*Regional Internet Registries*). Tenha em consideração a tabela de "**Blocos IPv4 atribuídos a cada ISP**" atribuídos às empresas e aos ISP.

Blocos IPv4 atribuídos a cada ISP:

ISP31 - 31.0.0.0/18
ISP32 - 32.0.0.0/17
ISP33 - 33.0.0.0/19
ISP21 - 21.0.0.0/21
ISP22 - 22.0.0.0/20
ISP11 - 11.0.0.0/22

Blocos IPv4 atribuídos a cada empresa:

E1.1 - 110.0.0.0/20
E1.2 - 112.0.0.0/23
E2 - 20.0.2.0/23
E3 - 130.0.0.0/21

Cada empresa quando realizou o contrato com os respetivos ISP recebeu destes um bloco /24 de endereços IPv4 públicos passando assim a possuir os blocos cedidos pelo ISP e os fornecidos pela entidade onde registou o AS.

No caso dos endereços públicos ao dispor de cada empresa não serem suficientes deverão ser usados endereços privados da gama 10.0.0.0/8. Relembre-se que endereços privados não podem circular na Internet.

Os endereços IP atribuídos às empresas podem ser usados internamente por estas como muito bem entenderem.

Qualquer máquina deve poder aceder à Internet. Deve existir, no mínimo, uma rede em cada empresa cujas máquinas devem poder ser acedidas a partir de qualquer parte na Internet.

A distribuição dos endereços IPv4 pelas redes dos diversos AS deve ter em consideração o número de máquinas previstas na respetiva tabela ("**Máquinas por rede**"). Os endereços IPv4 que sobrarem após a atribuição de endereços a cada rede devem ser guardados para uma eventual futura expansão das redes internas de cada AS.

Máquinas por rede:

N1.1 - 700 máquinas
N1.4 - 150 máquinas
N2.1 - 200 máquinas
N2.2 - 120 máquinas
N2.4 - 16 máquinas
N3.1 - 800 máquinas
N3.2 - 320 máquinas
N31.32 - 14 máquinas
N22.21 - 7 máquinas
N11.4 - 12 máquinas

Apesar das redes das empresas/sistemas autónomos terem uma dimensão considerável, neste trabalho são representada apenas por um AS com dois ou três *routers* e um ou dois PC por rede de maneira a simplificar.

Deve ser definido e configurado para cada *router* um identificador (*routerId*) cujo valor esteja incluído num dos blocos de endereços IPv4 atribuídos ao respetivo AS. Estes valores são /32. As **interfaces *Loopback* que servem para identificar os *routers* (*routerId*)** devem usar endereços no topo dos blocos de endereços IPv4 dos respetivos AS. Pode optar por outra solução. Confirme sempre se toda e qualquer atribuição de endereços é possível e se está correta.

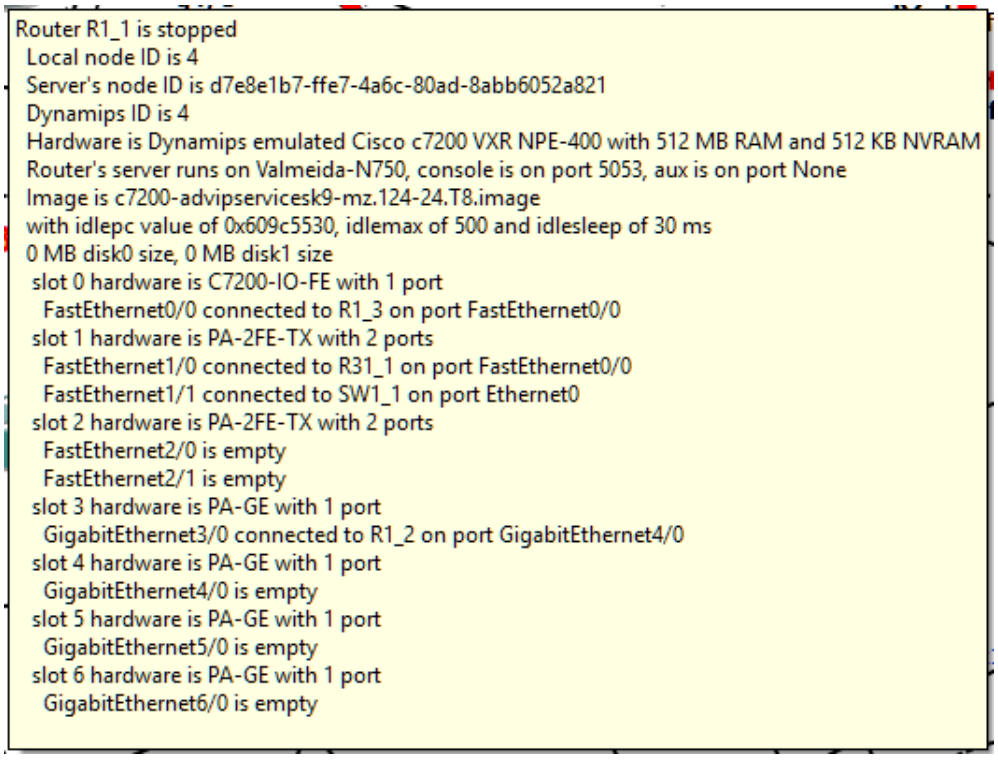
O *router* R11_3 deve incluir um conjunto de interfaces *Loopback* (4 no mínimo) que simulem endereços IPv4 públicos noutros AS remotos (resto da Internet).

O *router* designado Internet deve ser ignorado de momento.

O *Interior Gateway Protocol* (IGP) utilizado nos AS, quando necessário, é o **OSPFv2**.

O *Exterior Gateway Protocol* (EGP) utilizado é o **BGPv4**.

Configuração física dos *routers* no GNS3 (exemplo R1)



Requisitos em termos de tráfego

Foram delineados para cada empresa alguns requisitos no que respeita à comunicação com o exterior, foi também definido como os ISP se devem comportar quanto às rotas a utilizar.
É responsabilidade do aluno verificar se tudo o que é requerido é possível e a forma de configurar os *routers* de maneira a se cumprirem os vários requisitos. Para cada um dos requisitos que se seguem deve indicar textualmente no relatório o que pensa fazer para cumprir o requisito pretendido e depois indicar qual a solução em termos de configuração específica de cada um dos *routers* envolvidos, ou caso seja um requisito impossível de concretizar a respetiva justificação.

Tráfego de saída das empresas

Em todas as empresas a comunicação com as outras empresas da topologia anexa deve ser realizada via a rota BGP possível que tenha a menor métrica, exceto se esta estiver indisponível.

A empresa **E1** pretende que o tráfego IPv4 de saída na empresa se realize, preferencialmente, da seguinte forma:

- Bloco E1.1 – ISP31
- Bloco E1.2 – ISP31
- Blocos de endereços IPv4 disponibilizados pelos ISP via o ISP que o disponibilizou
- Se a ligação ao ISP 31 falhar deve ser privilegiada a ligação ao ISP33 e, se esta falhar, a ligação N32_2 ao ISP32 e, finalmente a N31_1.

A empresa **E2** apenas se liga ao ISP32.

A empresa **E3** pretende que o tráfego IPv4 de saída na empresa se realize, preferencialmente, da seguinte forma:

- Bloco E3 – ISP33
- Blocos de endereços IPv4 disponibilizados pelos ISP via o ISP que o disponibilizou

Tráfego de entrada das empresas

Preferencialmente o tráfego deve ser simétrico (as rotas de saída serem semelhantes às rotas de entrada).

Nota: Relembra-se que cada empresa apenas pode influenciar o tráfego alterando as configurações dos *routers* que lhe pertencem. O mesmo se passa com os ISP, colaboram entre si mas não inserem configurações a pedido dos concorrentes.

Outros requisitos

Os ISP não devem servir de AS de trânsito para o tráfego de outros ISP do mesmo *tier*, exceto se o tráfego pertencer a um cliente comum e não existir outra rota (falha numa ligação, por ex.)
Nenhuma empresa pretende que o respetivo AS seja de trânsito.

Alguns ISP do mesmo *tier* ligam-se entre si via **Internet Exchange Point (IXP)** para troca entre si de tráfego IPv4 com origem nos AS que servem. Pelo IXP de interligação deve apenas ser trocado tráfego com origem e destino nos respetivos ISP e/ou clientes. O IXP não deve ser usado para passar tráfego de um ISP através de outro ISP para outros operadores do mesmo *tier* ou de *tiers* mais elevados, ou seja, um ISP do mesmo nível de outro não lhe deve servir de AS de trânsito. **Os IXP representados na topologia devem permitir ligar até ao número de ISP que constam na tabela "Máquinas por rede"**.

Assuma na configuração fornecida que **aos ASBR das empresas podem ser enviadas todas as rotas BGP** (*full routing*) e estas propagadas para os *routers* interiores OSPF (Redistribuição do BGP no OSPF) o que, na vida real, poderia não ser razoável por significar centenas de milhares de rotas e poderia significar uma sobrecarga muito elevada para alguns dos *routers* ASBR devido a terem de lidar com todas elas (a alternativa era apenas recebem a default por BGP). Em muitas situações (ver caso da empresa E2) não é necessário que os ASBR da empresa lidem com as tabelas BGP completas enveredando-se por outras soluções, o mesmo é verdade para os *routers* interiores OSPF. Esta questão é abordada nos últimos pontos deste trabalho. **Confirme se a empresa E2 necessita de um número público de AS e de blocos IPv4 públicos.** Deve procurar:

- **Simplificar as tabelas de *routing* dos *routers* ASBR da empresa:** Altere a configuração para que os *routers* ASBR da empresa não necessitem lidar com todas as rotas BGP
- **Simplificar as tabelas de *routing* dos *routers* interiores OSPF da empresa:** Altere a configuração dos ASBR da empresa para que não seja necessário injetar todas as rotas BGP nos *routers* interiores OSPF. Justifique as opções que tomar.

Nota: Tenha em atenção que as alterações a realizar nos *routers* para influenciar o tráfego de saída e de entrada no AS das empresas deverá implicar alterações apenas nos *routers* da sua empresa. As alterações nos operadores devem ser mínimas.

Simulador

A configuração básica BGP e OSPF dos *routers*, se disponibilizada para este trabalho, deverá ser adaptada ao seu simulador e à forma como o configurar. Os alunos devem estudá-la, compreendê-la, corrigi-la onde entenderem necessário (justificando as suas opções), alterá-la para atingirem os objetivos indicados e responderem às questões colocadas. Deverão complementar a configuração fornecida de maneira a conseguirem realizar a fase 4 do trabalho. Nos casos em que considere que um objetivo indicado não pode ser cumprido devido a limitações do BGP isso deverá ser justificado no relatório.

Relatório

O relatório final deve ser dividido segundo as várias fases do trabalho. Cada parte referente a uma fase deve descrever de forma concisa e precisa o que foi feito para efetuar a respetiva fase, deve ainda indicar o que foi alterado relativamente às fases anteriores, se for o caso. Devem ser evitadas sobreposições de explicações sobre o mesmo tema (por exemplo: repetir na fase 2 a explicação das opções tomadas na configuração das interfaces dos *routers*), exceto se for necessário efetuar alguma alteração em relação a fases anteriores para se poder atingir o objetivo da fase atual.

Pretende-se como resultado deste trabalho um relatório onde conste, devidamente comentadas/justificadas:

- Para cada uma das fases do trabalho pretende-se a listagem da configuração utilizada para se atingirem os objetivos indicados para a respetiva fase.
- As listagens das tabelas BGP dos ASBR da empresa E1 e E2 e do *router* (R11_3) do operador de *tier* mais elevado para cada fase (se se aplicar).
- As listagens das tabelas de encaminhamento dos ASBR da empresa E1, do R1_3 e do *router* R11_3 do operador de *tier* mais elevado (se se aplicar).
- A listagem dos LSA do *router* R1_3.
- O resultado da execução do *script* tclsh que efetua Ping a todas as redes da topologia a partir dos *routers* R1_3 e R11_3.
- As rotas (*trace route* ou o Ping estendido) entre cada um dos blocos IP da empresa e "resto do mundo", nos dois sentidos (se se aplicar).
- Respostas às questões efetuadas neste enunciado referentes a cada uma das fases do trabalho.
- Em anexo as listagens das configurações finais dos *routers*. Podendo ser utilizados os ficheiros obtidos nos simuladores como, por exemplo, no GNS3 com "file>Import/Export device configs".
- **Em anexo ao relatório o ficheiro do GNS3, tipo "Export Portable Project", sem imagens, correspondente ao trabalho efetuado (pode ser na forma de um *link* para uma "box/cloud").**

Bibliografia

Pode consultar qualquer bibliografia, no entanto para configurar o OSPF aconselha-se a bibliografia indicada nos trabalhos anteriores.

Para configurar a parte que respeita ao BGP aconselha-se a consultar a documentação disponibilizada no *link* no Thoth de RI: "CD_alunos_2017-2018", em especial nos "BGP docs". Existem lá muitos exemplos de configuração e muitos tutoriais. Dê uma vista de olhos rápida nos vários, escolha e depois conforme necessário aprofunde aqueles que precisar. Os dois "cis185" são igualmente uma boa fonte de informação:

- cis185-mod9-BGP-Part1.pdf
- cis185-mod9-BGP-Part2.pdf

O documento da Cisco "BGP tutorial" em "Cisco-BGP.pdf" é igualmente uma boa referência para começar.

Todos os outros documentos em "BGP docs" têm uma ou outra coisa interessante mas muito repetida entre eles no entanto deve "espreitá-los" e decidir por si!

A documentação do CCNA da Cisco é interessante mas não inclui o BGP.

Links úteis

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-3se/3850/irg-xe-3se-3850-book/irg-prefix-filter.html

http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13754-26.html

http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfbgp.html#wp1000934

Fases do trabalho

Fase 1 – Endereçamento e interfaces

Configuração básica de todos os equipamentos da topologia de maneira a que todos os equipamentos consigam "pingar" os vizinhos:

Utilize um editor de texto tipo Notepad++ para criar todas as suas configurações dos *routers* e ir copiando depois as mesmas para os *routers*. Para tal não se esqueça de ir colocando também no ficheiro os comando para subir e descer de contexto nos *routers* (ex: configure terminal, exit, end, etc.). Não se esqueça de ir salvando (*copy run start*) as configurações dos *routers* para memória não volátil (NVRAM) destes.

Q1.1: A empresa E2 necessita de um número público de AS e de blocos IPv4 públicos.
Q1.2: Pretende-se o menor desperdício de endereços IPv4. Verifique se, face aos blocos de endereços IPv4 atribuídos, os endereços das redes e os RouterId poderiam ser atribuídos como consta na tabela abaixo (os IP no exemplo abaixo podem ser diferentes dos atribuídos na configuração no GNS3 proposta).

Endereços das redes de interligação entre os AS

Assuma que ao atribuir os endereços IPv4 as interfaces exteriores dos ASBR das empresas irão receber um endereço do bloco do ISP ao qual se ligam. No caso dos ASBR dos ISP as suas interfaces de ligação às empresas ou ao ISP de *tier* menor recebem um endereço do bloco do ISP de *tier* superior, as interfaces das ligações aos ISP de *tier* superior recebem endereços do seu bloco. Na ligação ao *router* Internet decida o endereço IPv4 a utilizar!

RouterID

Deve ser definido e configurado para cada *router* um identificador (*routerId*) cujo valor esteja incluído num dos blocos de endereços IPv4 atribuídos ao respetivo AS. Estes valores são /32. As **interfaces *Loopback* que servem para identificar os *routers* (*routerId*)** devem usar endereços no topo dos blocos de endereços IPv4 dos respetivos AS. Pode optar por outra solução. Confirme sempre se toda e qualquer atribuição de endereços é possível e se está correta.

Simular endereços IPv4 do "resto do mundo"

O *router* R11_3 deve incluir um conjunto de interfaces *Loopback* (4 no mínimo) que simulem endereços IPv4 públicos noutros AS remotos (resto da Internet).

Distribuição de endereços IPv4

Blocos de endereços atribuídos às várias entidades deste trabalho:

Blocos IPv4 atribuídos a cada ISP:

ISP31 - 31.0.0.0/18
ISP32 - 32.0.0.0/17
ISP33 - 33.0.0.0/19
ISP21 - 21.0.0.0/21
ISP22 - 22.0.0.0/20
ISP11 - 11.0.0.0/22

Blocos IPv4 atribuídos a cada empresa:

E1.1 - 110.0.0.0/20
E1.2 - 112.0.0.0/23
E2 - 20.0.2.0/23
E3 - 130.0.0.0/21

Cada empresa recebeu um bloco de **256 endereços IPv4 públicos disponibilizados por cada um dos seus ISP (Preencher antes da aula prática)**

Endereços IPv4 de rede				
Nome	**Endereço rede**	**Máscara**	**End. de *broadcast***	**Nº de máquinas**
N1.1				700
N1.2				2
N1.3				2
N1.4				150
N1.5				2
N2.1				200
N2.2				120
N2.3				2
N2.4				16
N3.1				800
N3.2				320
N3.3				2
N3.4				2
N31.1				2
N32.1				2
N32.2				2
N33.1				2
N21.1				2
N22.1				2
N11.1				2
N11.2				2
N11.3				2
N11.4				12
N1.31				2
N1.32				2
N1.33				2
N2.32				2
N3.31				2
N31.32				14
N3.33				2
N31.21				2
N32.21				2
N32.22				2
N33.21				2
N33.22				2
N21.11_1				2
N21.11_2				2
N22.11				2
N22.21				7
N11_Internet				2
Lo0.R11_3				2
Lo1.R11_3				2
Lo2.R11_3				2
Lo3.R11_3				2

RouterId				
Nome	**Endereço rede**	**Máscara**	**End. de *broadcast***	**Nº de máquinas**
R1_1				
R1_2				
R1_3				
R2_1				
R2_2				
R3_1				
R3_2				
R3_3				
R31_1				
R31_2				
R32_1				
R32_2				
R32_3				
R33_1				
R33_2				
R21_1				
R21_2				
R22_1				
R22_2				
R11_1				
R11_2				
R11_3				
R_Internet				

Q1.3: As interfaces *lo0* que podem servir para atribuir uma identificação aos *routers* poderiam ter qualquer valor como endereço IP? No R11_3 também é o *lo0* que é usado para RouterId?
Utilize os comandos como os que se seguem como sugestão para **configurar as interfaces** dos *routers* da empresa:

!Router R1_1
hostname R1_1
!
!Configure as interfaces de *loopback* que irão servir para identificar os *routers* também no BGP
interface Loopback0
ip address <end> <mask>
---
interface Fa0/0
ip address <end> <mask>
no shutdown
…
!Router R1_2
hostname R1_2
…
!Router R1_3
hostname R1_3
…

Q1.4: Justifica-se a alteração dos routerId tipo 1.1.1.1, 2.2.2.2, 3.3.3.3, … para os usados na configuração dos *routers* da topologia e que têm a ver com os blocos de endereços IP utilizados?

Teste a configuração das interfaces utilizando o Ping entre as interfaces ligadas diretamente entre si. Também deve usar comandos como o *sh ip route* ou o *sh int.*

Configure os PC das empresas. Não se esqueça de configurar também em cada um dos PC o endereço IP do respetivo *gateway*. Caso não se lembre dos comandos o "?" faz "milagres", quer nos PC, quer nos *routers*.

No fim desta fase deve ser possível realizar "Ping" entre todos os equipamentos ligados diretamente entre si nas várias redes dos AS das empresas. Utilize o tclsh para realizar *Pings* com um único comando.

Fase 2 - OSPF

Utilize os comandos que se seguem como sugestão para a **configuração do OSPF monoárea, nos AS em que for necessário, nos *routers* da topologia**. Assuma que todos os *routers* das empresas se encontram na área de *backbone*. No OSPF devem ser incluídos todas as redes da empresa e também aquelas a que os respetivos AS se ligam diretamente. Tenha em atenção que as mensagens do protocolo OSPF a correr nos AS não devem ser enviadas para fora dos respetivos AS nem para as interfaces de *loopback,* devendo para isso serem configuradas como interfaces passivas.

Se necessário configure o IGP nas redes internas dos operadores.
Configure o OSPF nos *router* da empresa:

!Router R1_1
router ospf n
network <rede N1_1> area 0
network <rede N1_2> area 0
…
!Router R1_2
router ospf n
…
!Router R1_3
router ospf n
…

Utilize os comandos como o *sh ip route* e/ou o *sh ip ospf database* para verificar se o OSPF está bem configurado e se aparecem todas as redes da empresa na tabela de *routing.*
Teste a configuração do OSPF utilizando o Ping entre os vários *routers* dos mesmos AS.

Q2.1: Porque devem as redes de ligação entre os AS serem incluídas no OSPF?

Q2.2: Porquê o *passive-interface* nas interfaces exteriores dos ASBR?

Q2.3: As redes de ligação do AS das empresas aos ISP constam nas tabelas de *routing* de todos os *routers* das empresas?

Q2.4: As interfaces *loopback* devem aparecer nas tabelas de *routing*?

Q2.5 Confirme que do PC1_1 consegue realizar Ping a todos os equipamentos/interfaces da empresa.
Q2.6: No caso da atual topologia é necessário configurar um IGP como o OSPF noutros AS que não o da Empresa?

Fase 3 – BGP básico

Nota: Leia o "Anexo" antes de começar a realizar esta fase.

Utilize os comandos que se seguem como sugestão para **configurar o BGP nos *routers*** (numa primeira configuração pretende-se colocar o BGP a funcionar da forma mais simples possível e sem qualquer filtros ou uso de atributos e sem ter em consideração as restrições de tráfego anunciadas, estas serão tratadas posteriormente):

Configure o iBGP no *router* R1_1:

```
router bgp 1
neighbor <endereço IPv4> remote-as 1
neighbor <endereço IPv4> update-source lo0
…
```

Q3.1: Para que serve o comando ***neighbor < endereço IPv4> update-source lo0***?

Configure o iBGP no R1_2:

```
router bgp 1
neighbor <endereço IPv4> remote-as 1
neighbor <endereço IPv4> update-source lo0
…
```

Q3.2: Verifique se o R1_1 e o R1_2 se tornaram vizinhos BGP usando o comando: ***show ip bgp neighbors***

Q3.3: Como é que os *routers* R1_1 e R1_2 sabem que a ligação entre eles é iBGP e não eBGP?

Configure o eBGP no *router* R1_1:

```
ip route <redeX> <mask> null0
router bgp 1
neighbor <endereço IPv4 A> remote-as 31          ! Duas ligações
neighbor <endereço IPv4 B> remote-as 32
network <redeX>
…
```

Configure o eBGP no *router* R1_2:

```
ip route <redeY> <mask> null0
router bgp 1
neighbor <endereço IPv4 C> remote-as 32
neighbor <endereço IPv4 D> remote-as 33
network <redeY>
…
```

Q3.4: Para que serve os comandos do tipo ***ip route <redeY> <mask> null0*** e qual o objetivo da sua utilização?

Q3.5: Qual a razão do comando "update-source loopback 0" ser usado em iBGP e não o ser em eBGP (complemente de pergunta anterior sobre o mesmo tema)?

Configure os restantes *routers* para iBGP. Teste.

Configure os restantes *routers* para eBGP. Teste.

Configure no R11_3 a simulação da ligação para o "resto do mundo". Nesta fase usando interfaces de *loopback* (Lo1 a Lo4) e, no final, usando uma ligação *cloud* (ver "Afinações finais").

Salve as configurações efetuadas na memória não volátil (NVRAM) dos *routers*: ***copy run start***

Utilize o comando ***show ip bgp neighbors*** para verificar se todos os *routers* reconhecem os seus vizinhos.

Utilize o ***show ip bgp summary*** para verificar quantos atributos de caminhos BGP estão a ser usados e que memória ocupam.

Após usar ***clear ip bgp ****** para reiniciar as tabelas do BGP e esperar um pouco para que convirjam, verifique se tem acesso de todas as redes para todas as outras, nomeadamente para as redes entre o PC1_1, o PC2_2 e o PC11_1. Justifique.

Utilize o comando ***show ip bgp*** para verificar a tabela BGP dos *routers*. Confirme as rotas com o comando ***sh ip route***.

Q3.6: As rotas que aparecem nas tabelas do BGP são as mesmas que aparecem nas tabelas de *routing*?

No fim desta fase todas as redes devem aparecer em todas as tabelas de *routing* de todos os *routers* (sumarizadas?).
Sugestão: Utilize um *script* tclsh nos *routers* para ajudar a automatizar o teste com múltiplos Ping entre os vários equipamentos. Para isso basta usar o *script* abaixo com os endereços IP e máscaras das interfaces que pretenda testar e fazer *copy and paste* para a linha de comandos do *router* que pretenda que seja a origem dos Ping:

```
tclsh
foreach address {
<end1> >
<end2> >
…
} { ping $address
}
```

Altere a configuração fornecida para que sejam utilizadas as redes indicadas na figura, Lo1 a Lo4 no *router* R11_3, como as redes do "resto do mundo". Altere o que for necessário para que as redes que simulam o "resto do mundo", simulada por *loopbacks* no R11_3, apareçam em todas as tabelas de *routing*.

Utilize nos *routers* o Ping estendido para determinar o caminho que os pacotes seguem na ida e na vinda entre a empresa e o "resto do mundo" (simulado pela interface loopback0 no *router* do ISP_Tier1):

```
ping
Protocol [ip]:
Target IP address: <end IP destino>
Repeat count [5]: 2
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: <end IP origem>
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: record
Number of hops [ 9 ]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
```

Q3.7: Verifique qual é a rota entre o *router* R31_1 e o *router* R32_1. Desative a ligação via IXP e verifique se a rota se altera. Justifique.

Q3.8: Verifique se o BGP passou a anunciar todas as suas ligações entre os AS (**show ip bgp**).

Q3.9: Verifique a tabela BGP do *router* R1_2 (**show ip bgp**). Será necessário incluir comandos como os seguintes no R1_1 e no R1_2?

```
!R1
router bgp m
neighbor <vizinho_eBGP> next-hop-self

!R2
router bgp n
neighbor <vizinho_eBGP>  next-hop-self
```

Q3.10: Introduza os comandos **next-hop-self** nos *routers* R1_1 e R1_2 e verifique a diferença em termos de tabelas de *routing* e de BGP em relação às obtidas antes. Justifique as diferenças provocadas pelos comandos **next-hop-self** referidos anteriormente. Remova-os se não forem necessários.

Q3.11: O *router* R1_3 possui alguma rota para o "resto do mundo"? Que comandos nos *routers* R1_1, R1_2, R_33 e R11_3 contribuíram para isso?

Q3.12: Se se fizer *shutdown* à interface do *router* R31_2 para o IXP1 as rotas para o "resto do mundo" nos *routers* R1_1, R1_2 e R1_3 são alteradas? **Nota:** Tenha em atenção o tempo de convergência da rede.

Fase 4 – Manipulação dos atributos do BGP

Os comandos a utilizar nesta fase são, essencialmente, as seguintes:

- *Prefix-list* (*filter prefixes*)
- *Filter-list* (*filter ASes*)
- *Route-maps* e *communities*

Configurar os *routers* de maneira a atingir os objetivo de controlo de tráfego indicado nos requisitos.

Nota: Tenha em atenção que os *routers* em que tem "autorização" para configurar os atributos são os da "sua" empresa. Os *routers* dos ISP deverão ser tão pouco alterados quanto possível dado que, numa situação real, nunca os poderia alterar.

1. Configurar os atributos no BGP nos *routers* de maneira a que o tráfego esteja de acordo com os objetivos referidos anteriormente.
2. Realize testes cada vez que implementar um "filtro", **um a um**. Após configurar cada um dos filtros, teste para verificar se o filtro é eficaz e cumpre o objetivo desejado. Só depois é que deve avançar para a configuração do próximo filtro. Não caia na asneira de configurar todos os "filtros" e só testar no fim.

Q4.1: Indique quais as alterações nas tabelas BGP (**show ip bgp**) dos *routers* da empresa, comparando-as com as obtidas antes e justifique as alterações detetadas.

Q4.2: Como é que o Ping estendido executado no R1_2 consegue determinar o caminho que os pacotes IP seguem na ida e na vinda até ao R11_3?

Q4.3: Após forçar os *routers* a atualizarem as tabelas BGP (clear ip bgp * soft) verifique usando o *show ip bgp* se houve alterações nas tabelas BGP e, se sim, quais.

Q4.4: Se a rede/ligação N1.32 ficasse desativada quais seriam as consequências em termos de tráfego de entrada e de saída nas empresas? Teste no GNS3 a sua teoria.

Realize um *trace route* para todos as redes a partir da rede da empresa, pode usar um *script* TCL.

Q4.5: Existe mais do que uma rota entre os mesmos destinos? Se sim, o BGP faz "*load share*" entre eles?

Utilize o Ping estendido para confirmar se os percursos de ida e de volta para cada um dos AS das empresas para o "resto do mundo" são idênticos (simetria).

"Afinações finais" (opcional)

A ligação ao "resto do mundo" poderá ser simulada nas fases anteriores do trabalho por interfaces de *loopback* criadas no *router* R11_3. Para o resultado do trabalho ser mais realista deverá passar a ser simulada por uma ligação *cloud* em que o R11_3 irá adquirir o endereço IPv4 da interface ligada à *cloud* via DHCP. Podem manter as interfaces de *loopback* como "faz de conta" de redes exteriores à topologia do trabalho. Se necessário as configurações de todos os *routers* deverão ser alteradas para refletirem esta evolução.

Se precisar de usar um servidor de DNS pode usar o que se encontra no endereço IPv4: 8.8.8.8 (pertence a quem?).

Dever-se-ia usar NAT no R11_3 para garantir que de todos os endereços IPv4 se pode aceder a qualquer sítio na Internet (mas estes não podem todos ser acedidos a partir do exterior por iniciativa exterior). **QA.1:** Porquê? No entanto a imagem IOS dos *routers* que é disponibilizada não suporta NAT pelo que, para ser realizado, implicaria a utilização de outra imagem (IOS) no mesmo ou noutro modelo de *router*.

QA.2: Qual a razão de ser sugerido a utilização de NAT no R11_3?

Nota: Tenha em atenção que a sua topologia não troca mensagens OSPF ou BGP com o "resto do mundo" dado os endereços usados não serem "faz de conta" e pertencerem a outras entidades noutros AS reais!

Anexo - Dicas para simplificar o trabalho

- Caso necessite limpar a configuração toda de um *router* pode usar: "*delete nvram:startup-config*". Depois de executar o comando poderá executar um *reload* mas … no GNS3 o *router* "morre". Deverá realizar *stop* e *start* do *router* e ele arrancará com uma configuração limpa.
- *Avoid to loose time when you write the wrong command*:

  Router(config)# no ip domain-lookup

- Os *routers* que servem os IXP devem ter na sua tabela de *routing*:

  - As suas rotas
  - Rotas mais específicas para todos os seus pares no IXP
  - Um agregado para todas as rotas no seu IXP
  - Um agregado para todas as rotas noutros IXP

- *Each AS will advertise the CIDR block assigned to them via BGP*:

  router bgp n

  no synchronization
  no auto-summary
  bgp log-neighbor-changes
  network <net> mask <mask>
  !
  ip route <net> <mask> null0 250

  Don't forget the static route to Null0*. This ensures that the prefix has an entry in the routing table, and therefore will appear in the BGP table. Also, don't forget to disable synchronization and auto-summarisation – these are also mandatory requirements for ISP routers connecting to the Internet. Note that the distance of 250 applied to the static router will ensure that routing protocols announcing this exact prefix will override the static (if this is required/desired).*
- *Firstly, agree on what IP addresses should be used for the point to point links between the ASes. Put the /30 networks used for the DMZ links into OSPF (network statement and passive interface). Then configure eBGP between the router pairs, for example:*

  router bgp n
  neighbor <ip_addr> remote-as 200
  !neighbor <ip_addr> description eBGP with RouterXX
  neighbor <ip_addr> soft-reconfiguration in

  Use the BGP show commands to ensure that you are receiving prefixes from your neighbouring AS. Don't forget the soft-reconfiguration command – this again is mandatory on all eBGP peerings.

- Sugestão para evitar que alguns erros de configuração noutros AS afetem o AS da empresa (**RFC 1918**):

```
router bgp <AS_number>
  network <ip_addr> mask <mask>
  neighbor <ip_addr> remote-as <AS_number>
  neighbor <ip_addr> prefix-list in-filter in
  !
  ip prefix-list in-filter deny 0.0.0.0/0                  ! Block default
  ip prefix-list in-filter deny 0.0.0.0/8 le 32
  ip prefix-list in-filter deny 10.0.0.0/8 le 32
  ip prefix-list in-filter deny 127.0.0.0/8 le 32
  ip prefix-list in-filter deny 169.254.0.0/16 le 32
  ip prefix-list in-filter deny 172.16.0.0/12 le 32
  ip prefix-list in-filter deny 192.0.2.0/24 le 32
  ip prefix-list in-filter deny 192.168.0.0/16 le 32
  ip prefix-list in-filter deny 221.10.0.0/19 le 32        ! Block local prefix
  ip prefix-list in-filter deny 224.0.0.0/3 le 32          ! Block multicast
  ip prefix-list in-filter deny 0.0.0.0/0 ge 25            ! Block prefixes >/24
  ip prefix-list in-filter permit 0.0.0.0/0 le 32
```

- *Three BASIC Principles:*

  prefix-lists to filter prefixes
  filter-lists to filter ASNs
  route-maps to apply policy

- *Finally, whenever you are configuring BGP, you will notice that changes you make to an existing configuration may not appear immediately.*
  To force BGP to clear its table and reset BGP sessions, use the clear ip bgp command. The easiest way to enter this command is as follows:
  Router#clear ip bgp *
  Router#clear ip bgp <ip_addr>
  Use this command with CAUTION, better yet, not at all, in a production network. From the net…
- *The Cisco IOS offers an optional command called **no synchronization**. This command enables BGP to override the synchronization requirement, allowing the router to advertise routes learned via IBGP irrespective of an existence of an IGP route.*
- Reconfiguração após alterações:
  router bgp 100
  neighbor 1.1.1.1 remote-as 101
  neighbor 1.1.1.1 route-map infilter in
  neighbor 1.1.1.1 **soft-reconfiguration inbound**
  ! Outbound does not need to be configured !
  Then when we change the policy, we issue an exec command
  clear ip bgp 1.1.1.1 **soft [in | out]**
- *Clear ip bgp x.x.x.x in tells peer to resend full BGP announcement*