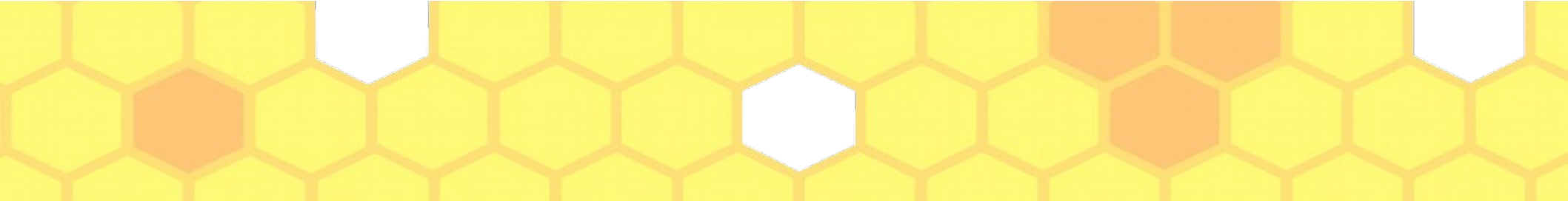




A DarkMesh



Hola Soy ReD!!

SecOpsDev

Formador, cuando me dejan

Activista tecnológico

- Soberanía tecnológica
- Defensor de la privacidad
- Cofundador de Hacklabs y M4H



VPNs



Herramientas no corporativas



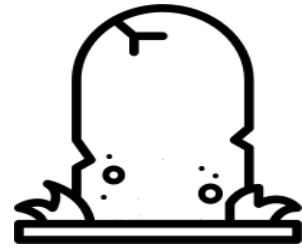
Entornos de pruebas



Mensajería instantánea



darkme.sh



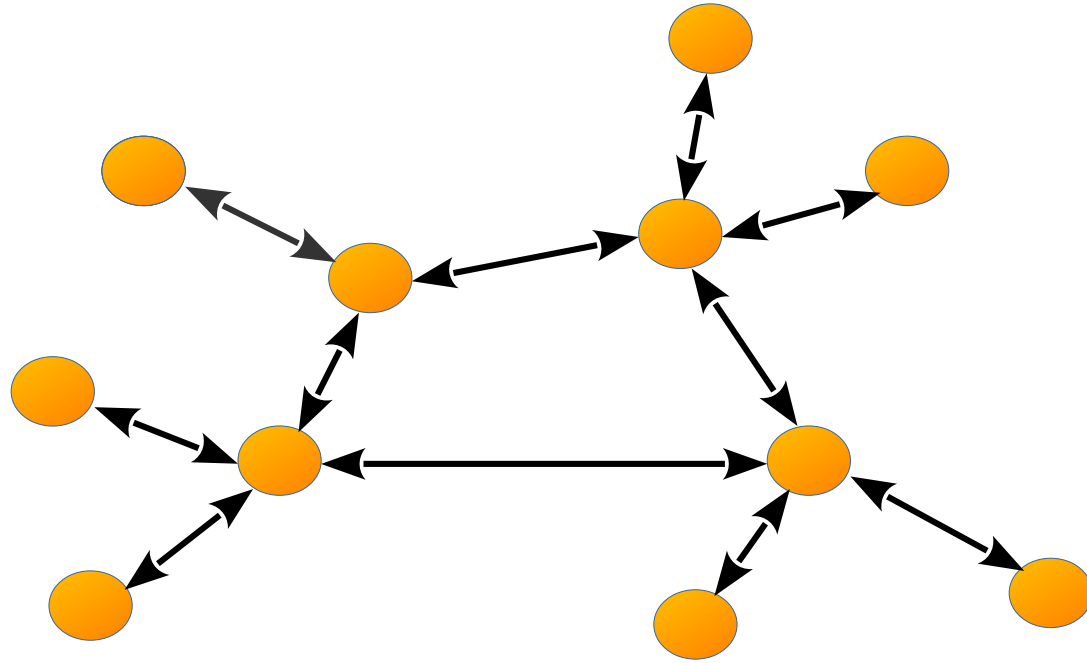
DarkMesh



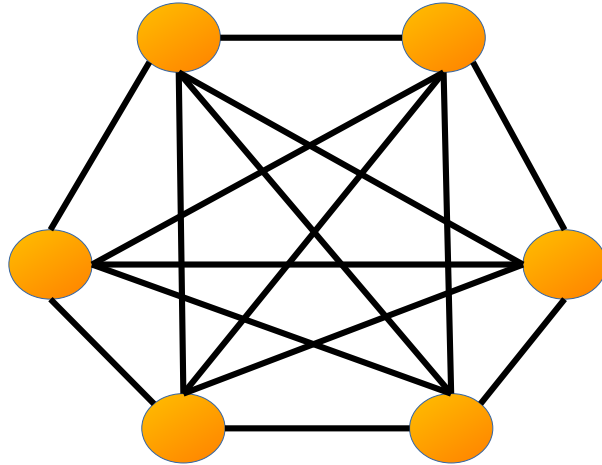
 RandomThinks



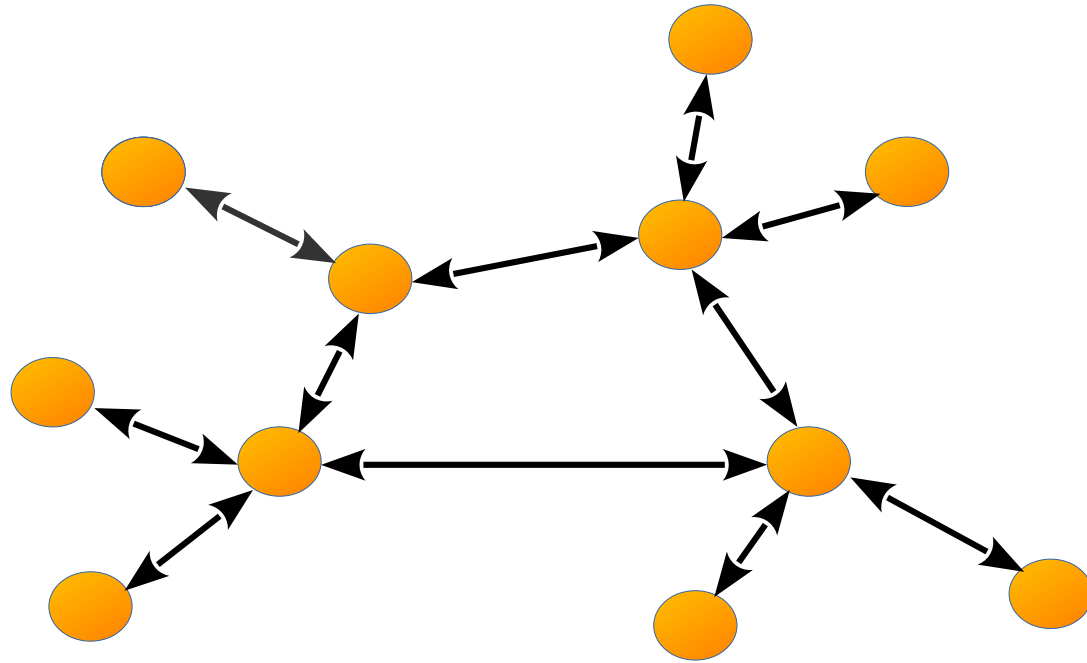
Red Mesh



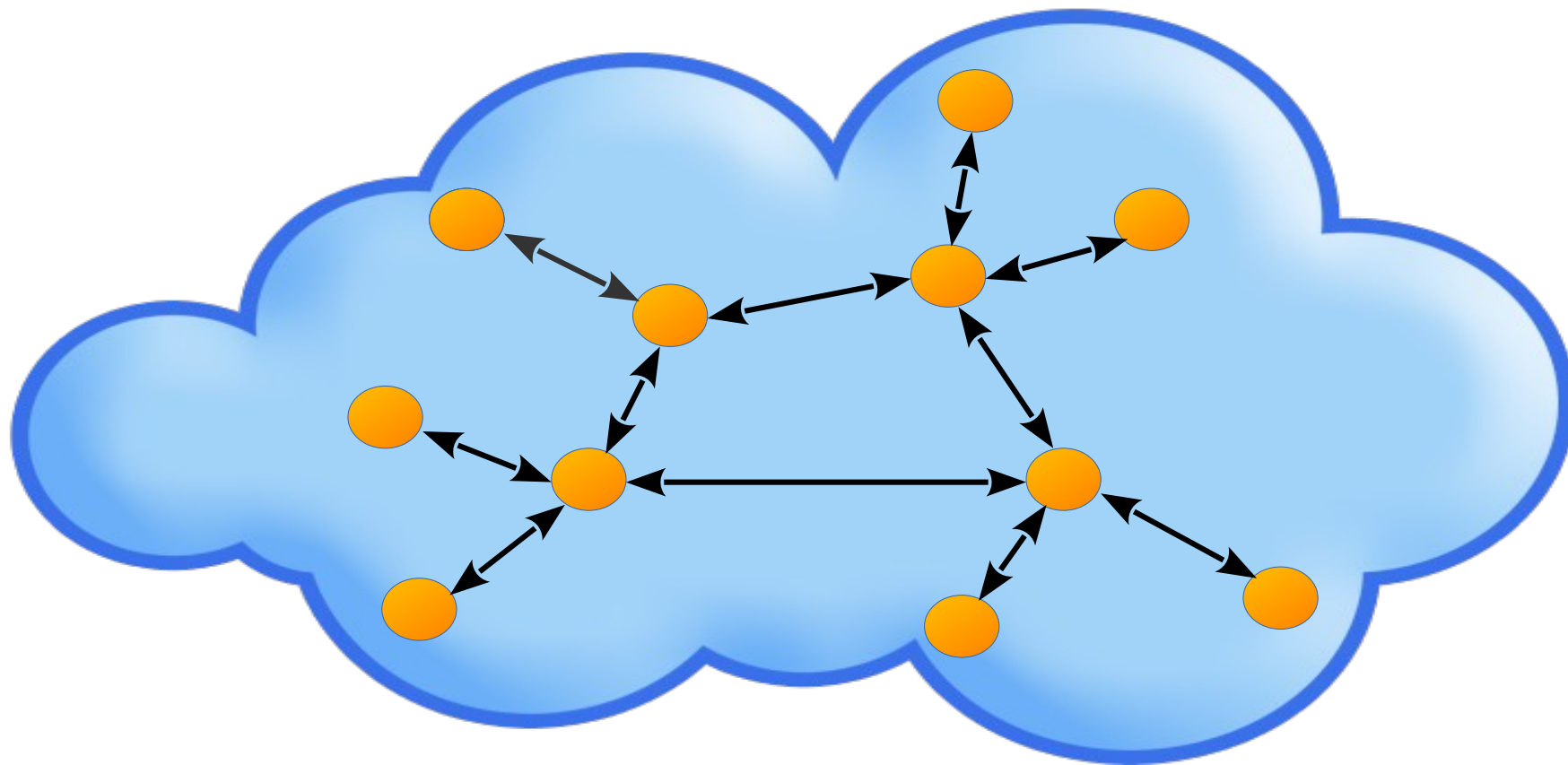
Red Mesh



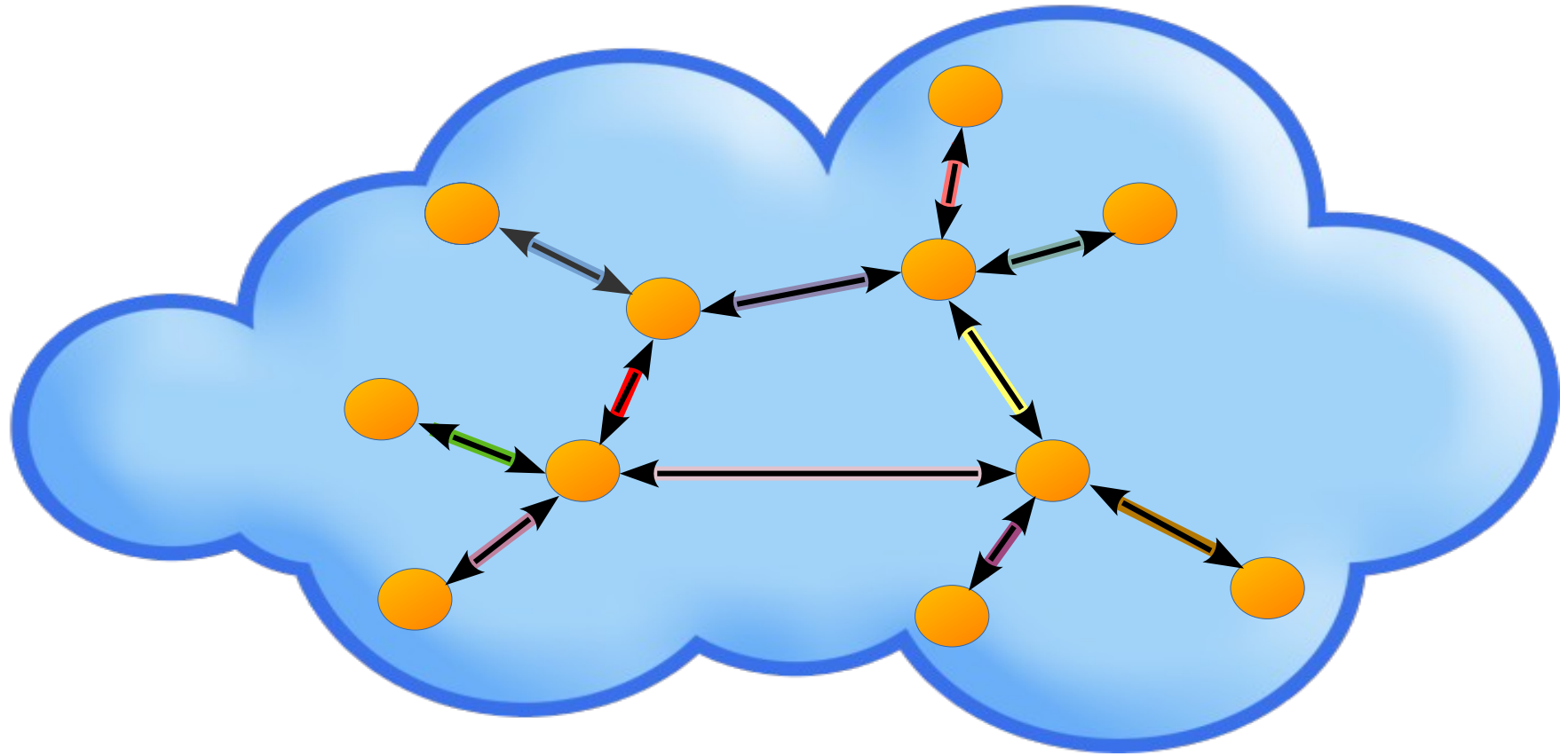
Red DarkMesh



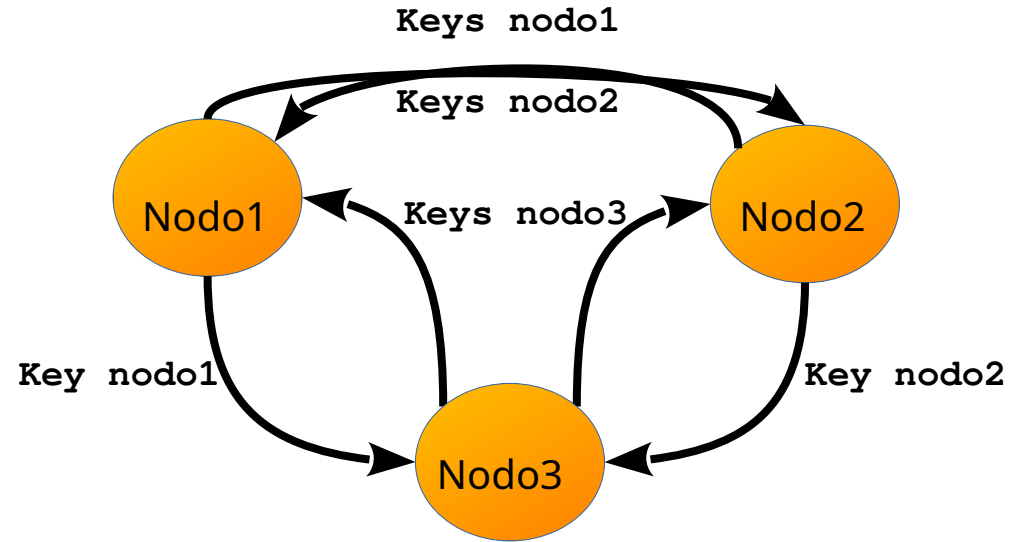
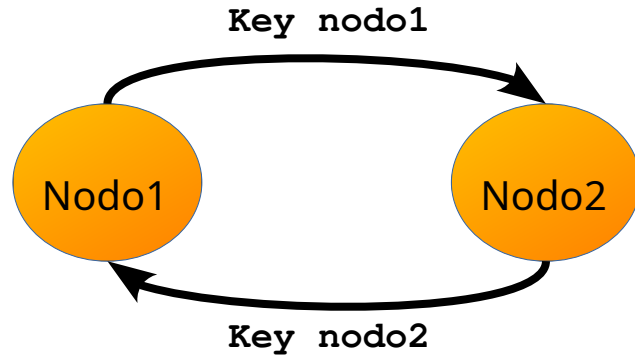
Red DarkMesh



Red DarkMesh



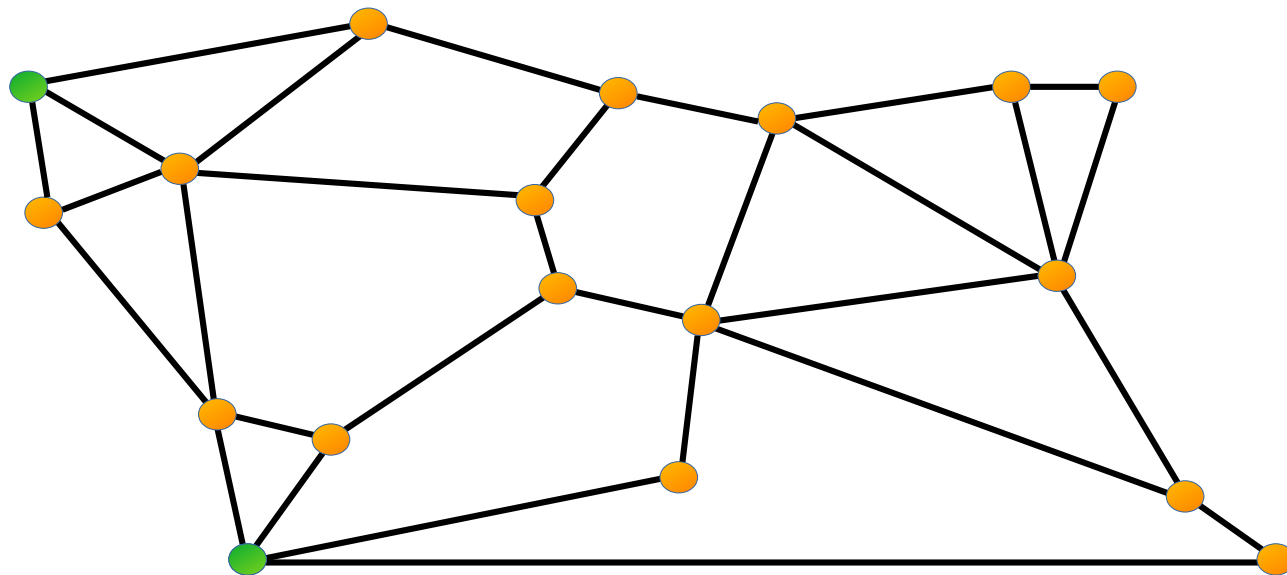
Distribución de keys



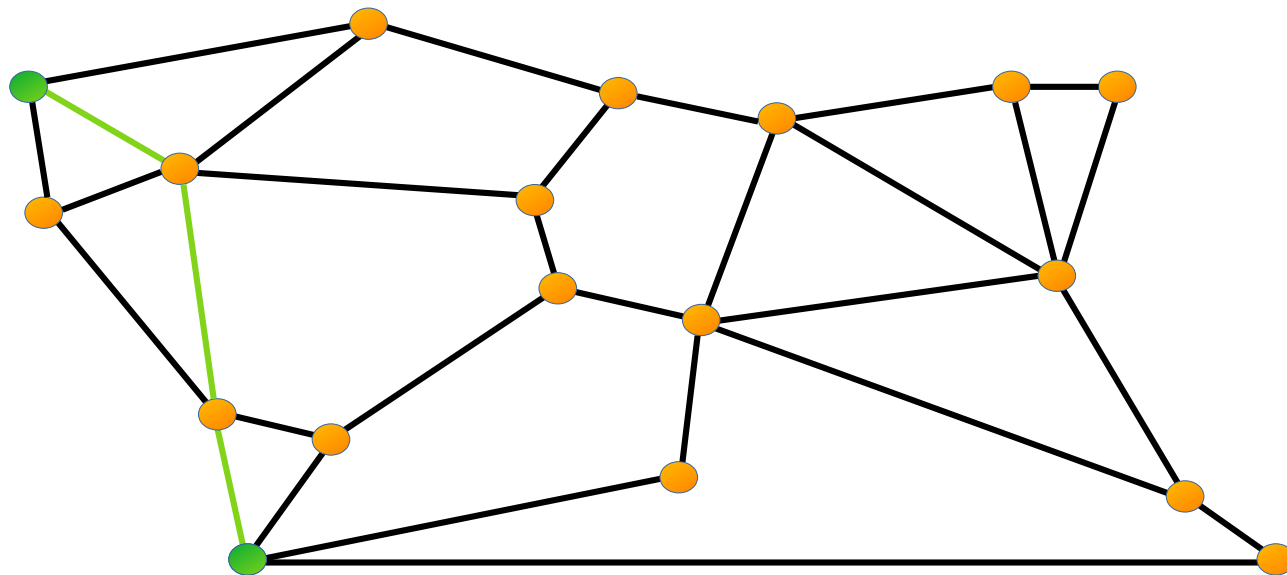
$$N * (N - 1)$$



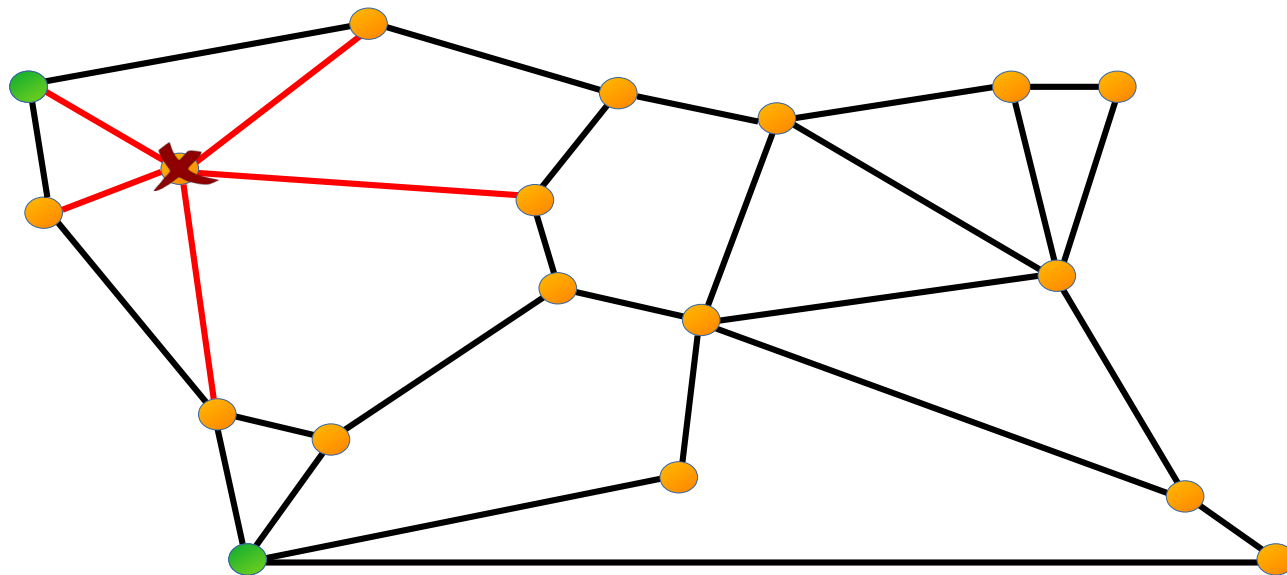
Mensajes entre nodos



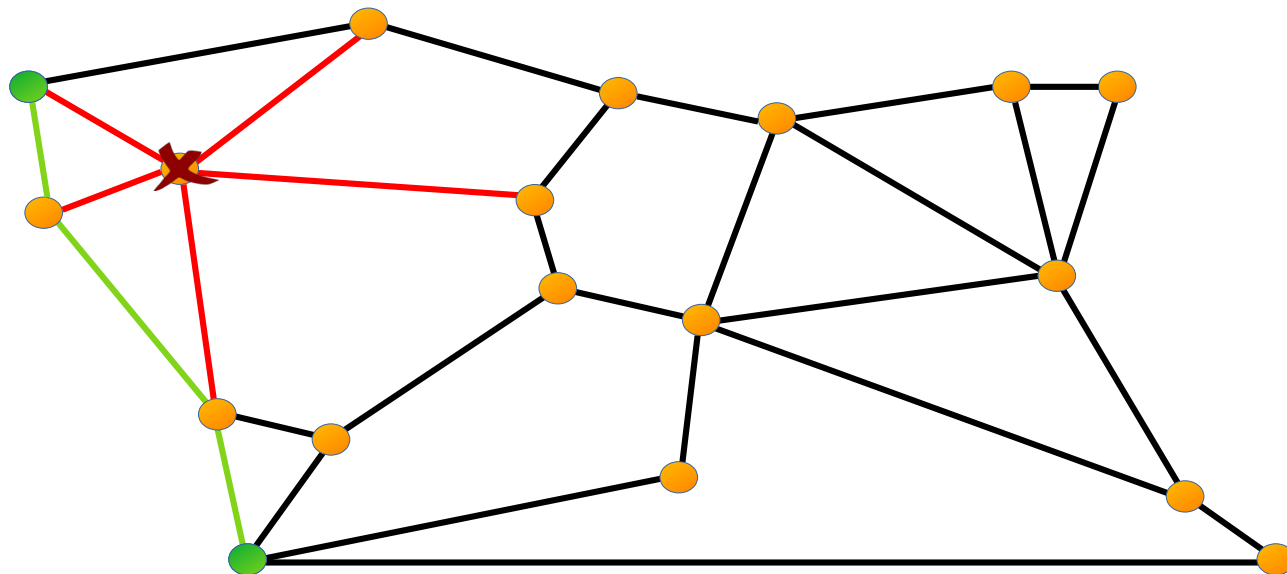
Mensajes entre nodos



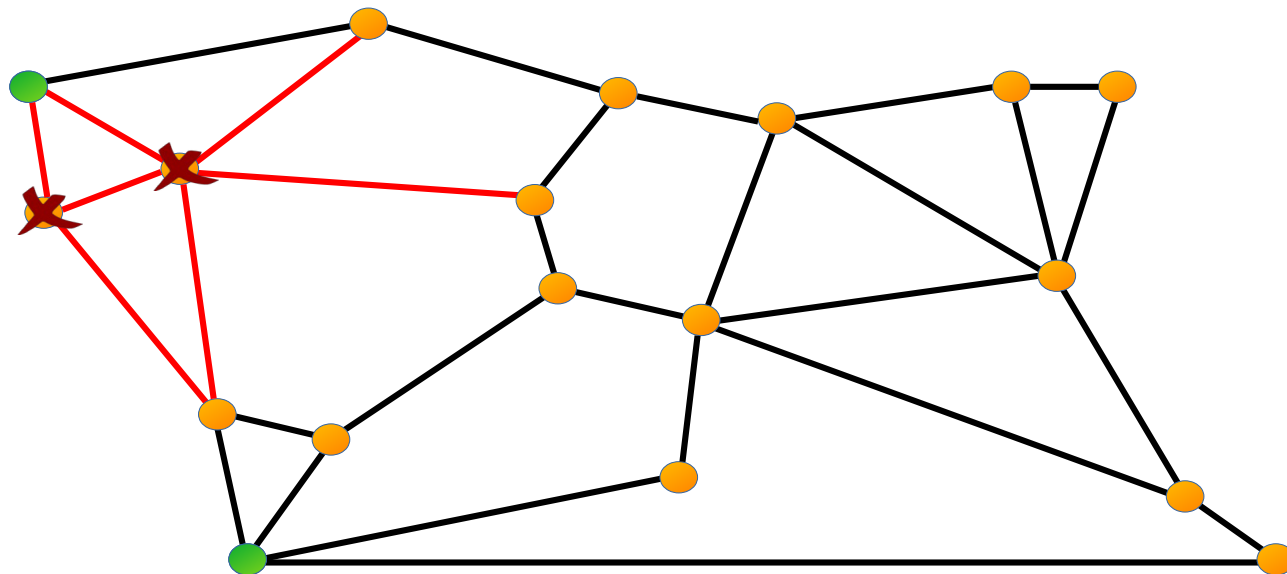
Mensajes entre nodos



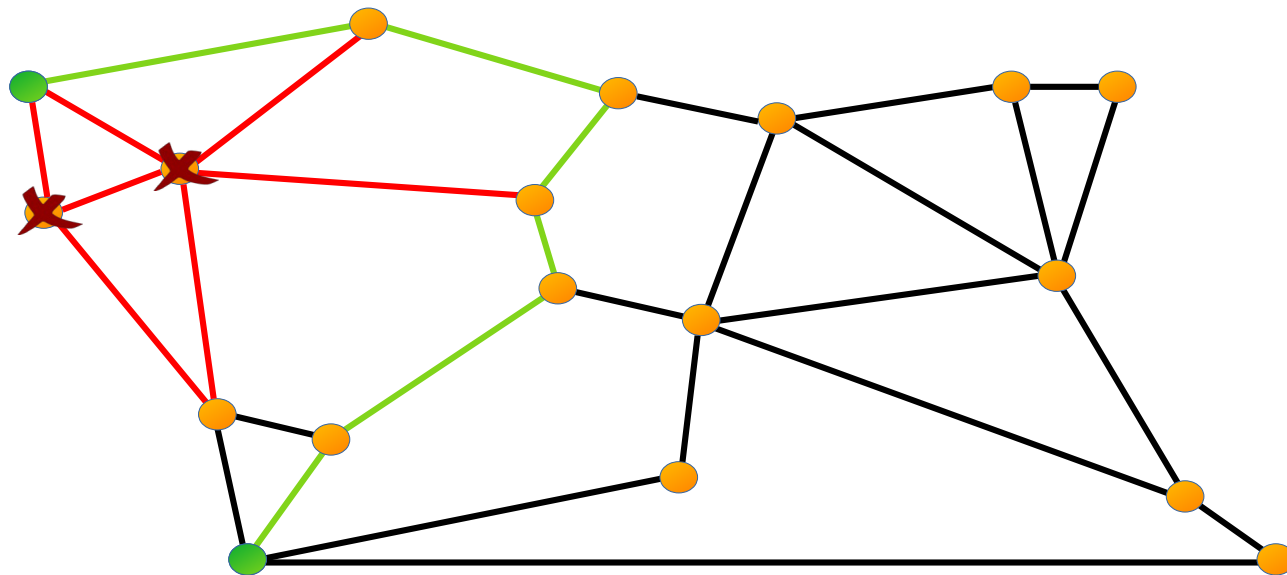
Mensajes entre nodos



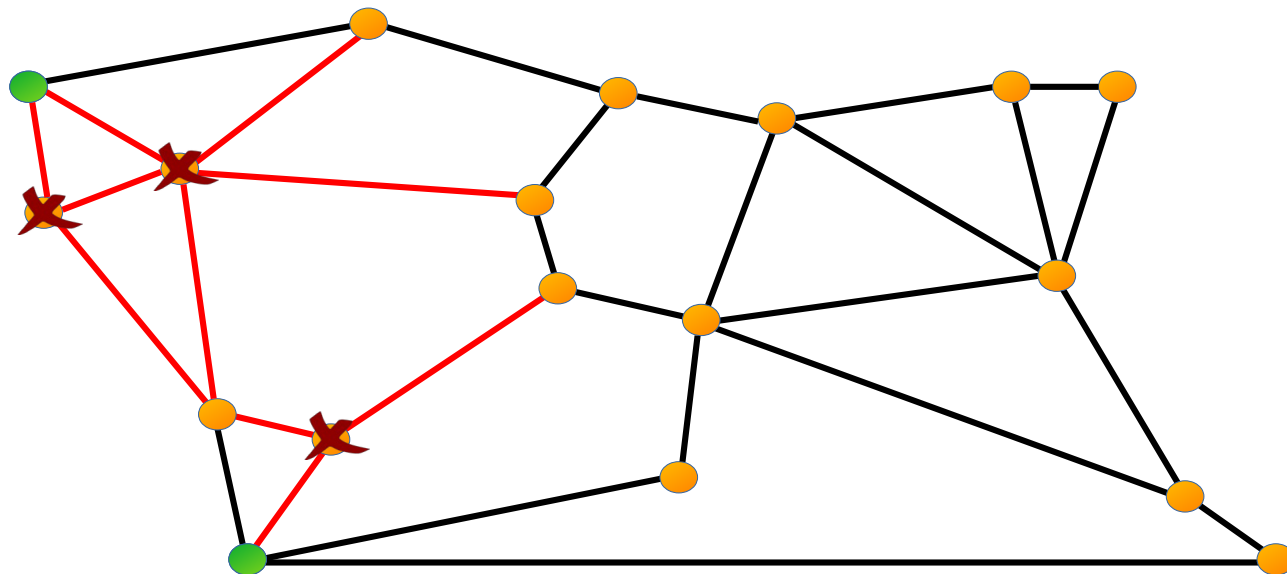
Mensajes entre nodos



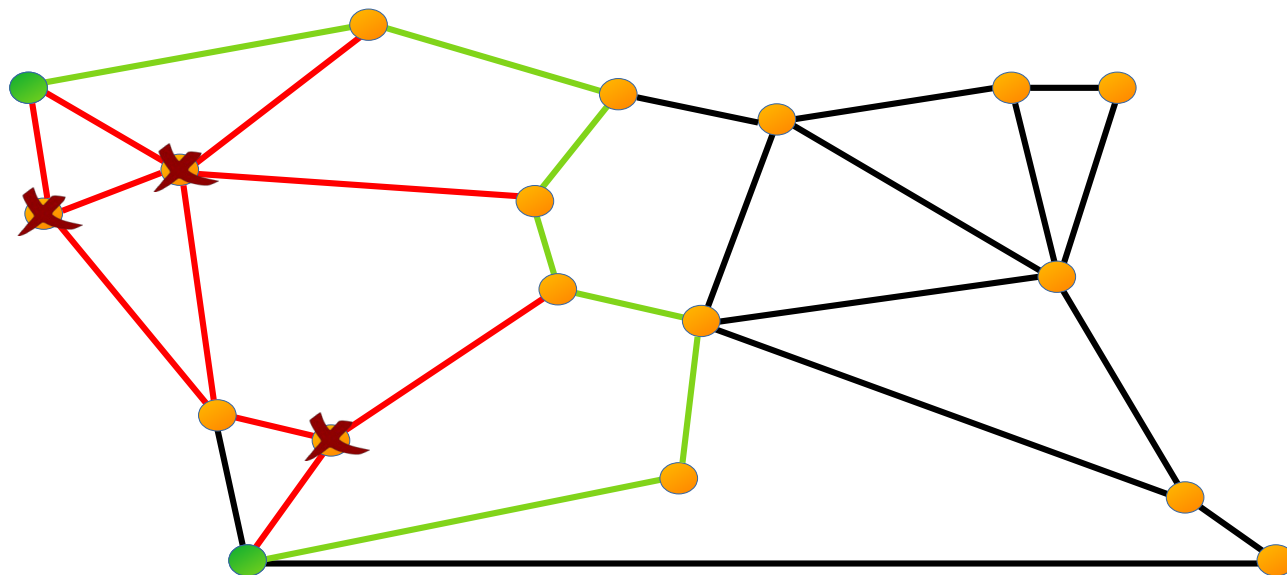
Mensajes entre nodos



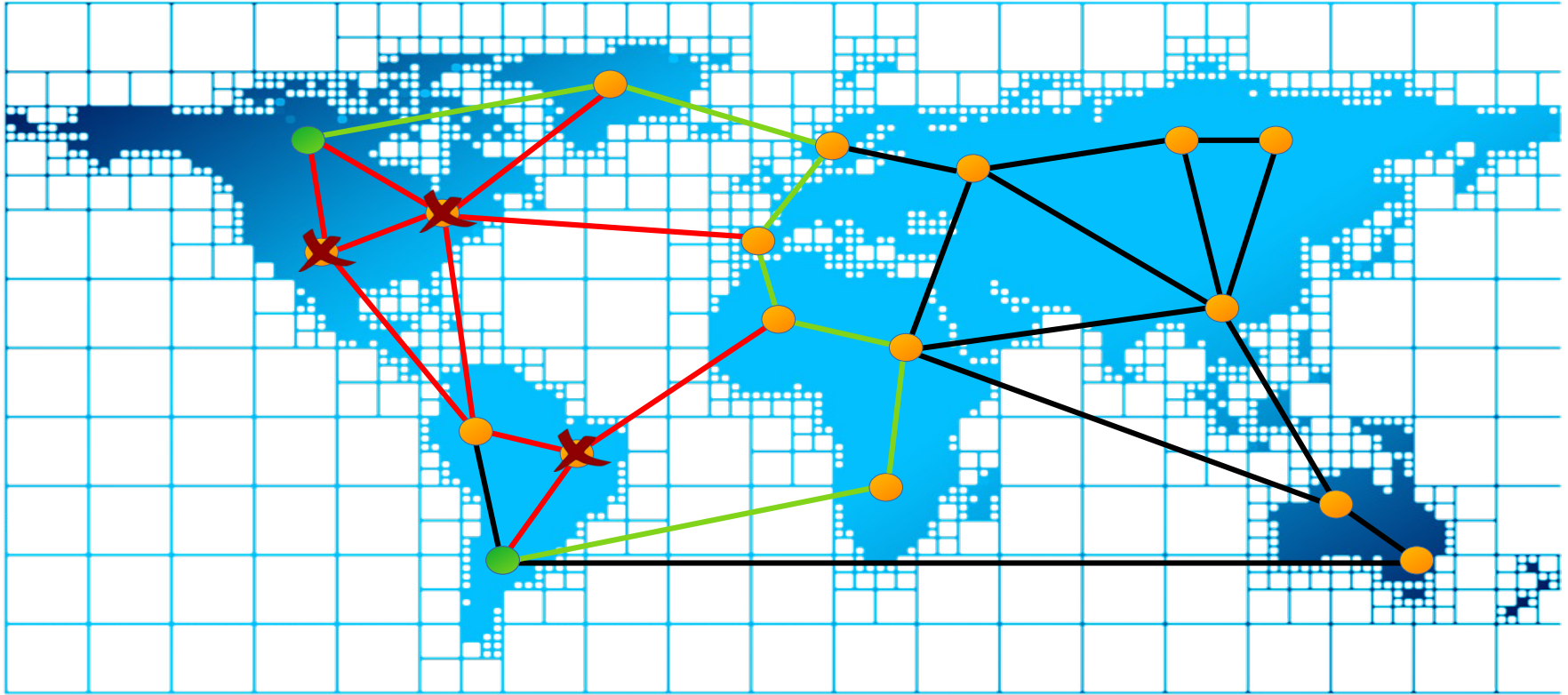
Mensajes entre nodos



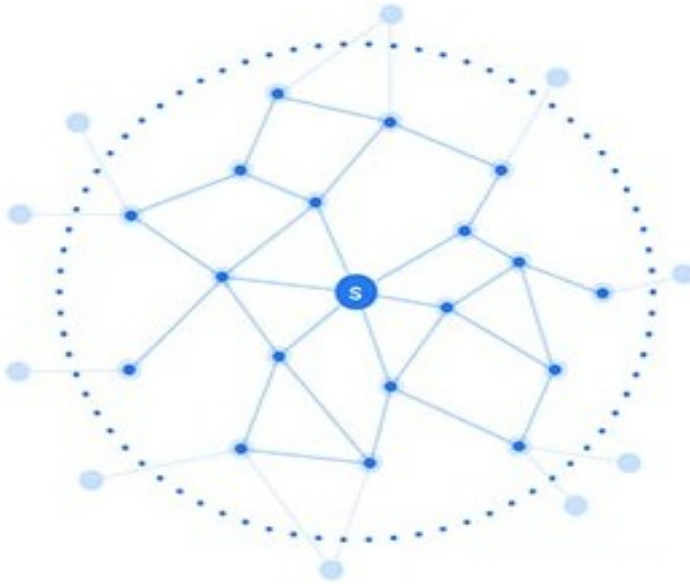
Mensajes entre nodos



Mensajes entre nodos



DarkMesh vs DarkNet



TOR

DIRECTORY AUTHORITIES

MORIA1 - 128.310.39 - RELAY AUTHORITY

TOR26 - 86.59.21.38 - RELAY AUTHORITY

DIZUM - 194.109.206.212 - RELAY AUTHORITY

TONGA - 82.94.251.203 - BRIDGE AUTHORITY

GABELMOO - 131.188.40.189 - RELAY AUTHORITY

DANNENBERG - 193.23.244.244 - RELAY AUTHORITY

URRAS - 208.83.223.34 - RELAY AUTHORITY

MAATUSKA - 171.25.193.9 - RELAY AUTHORITY

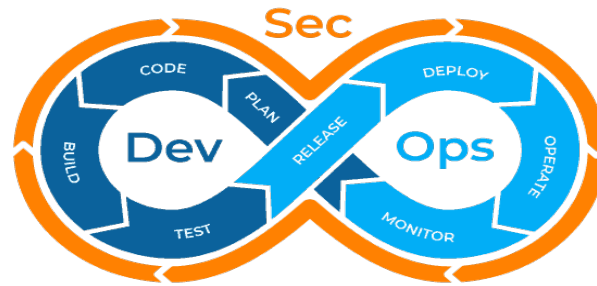
FARAVAHAR - 154.35.175.225 - RELAY AUTHORITY

LONGCLAW - 199.254.238.52 - RELAY AUTHORITY



documento vivo llamado **consenso**

Nuestra DarkMesh



Tinc

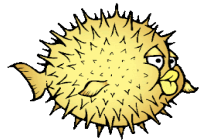
- Prerelase v1.1
- Multiplataforma
- Cifrado punto a punto (VPN)
- software libre
- Compresión usando zlib o lzo



Mac OS X



FreeBSD



OpenBSD

Configuración Tinc

/etc/tinc/tinc.conf
/etc/tinc/hosts/

/etc/tinc/netname/tinc.conf
/etc/tinc/netname/hosts/

Public/private key pairs

tinc-up

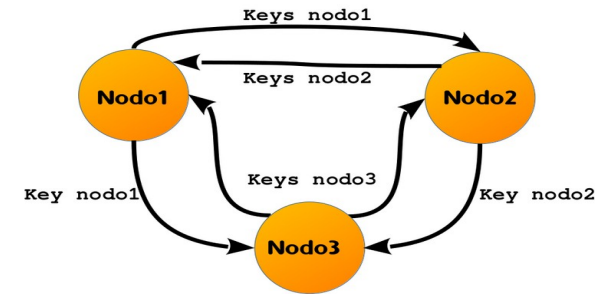
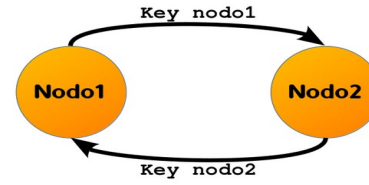
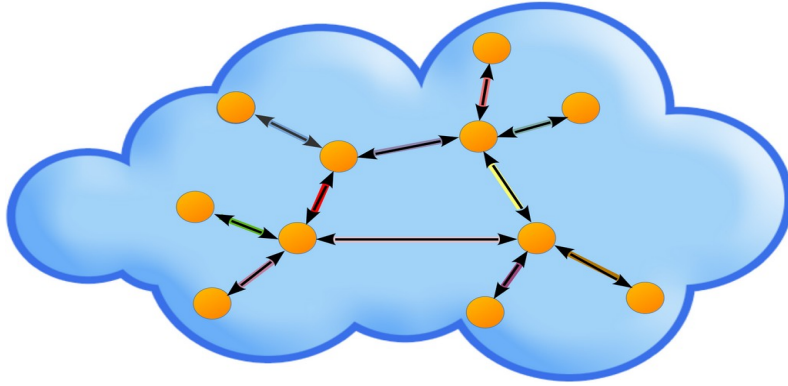
tinc-down



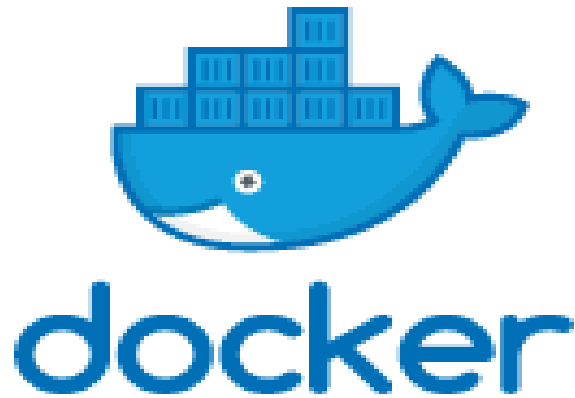
Fichero por nodo

```
Address=test.darkme.sh
Cipher=blowfish
Compression=0
Digest=sha1
IndirectData=no
Port=6669
Subnet=10.125.254.0/24
TCPonly=yes
-----BEGIN RSA PUBLIC KEY-----
MIICCAgEAx00WFIR0h3mWpgtm8ihdFnX5YAfAMLPoAl3LVn4X3CS6k3+cD+pW
/zLLPtFApd45gCjJPYC7o+ISfxiWuC2FcMO/S7YaHEFI23xttQx0lkZUqG0hZNyK
qR7m4jWQTtwA8VGWh/m6n69qEIsWdLH9S20t5LVnA9Q4/xx40ioxhjL1zfkoNFNR
I4ZM49/zFImKgDqY5/fWXfo6FHVKURJmKMmy7xpW2LYRe8VtOl8rJP+AyKJR+mec
UgDwQ+S4GASBHvvyTjDCtWK5abUde00Apd7ctah8hD+7IGbyfJLLZvr0JiEepUch
f36RcaT55yQcuhkxC+ocL0kfOuHUyDVxIsAhxxhAlpR7AzfY306i0JeL03vWbSaJ
AHXFANqF6D0yPytxbUdn8AWvqT1uQaS6tYE0Agx/qRg9tuQbKZe6hjLg4s4jQUVc
InN60IeKj2SlVL/rJPwb8tu6gWBsEjafj8/hKECFj2Pi2oR+VxLwv17XqR3uuTHF
NxqZYWAlK5+fWYJAZFH5aC6qW6KJKZYvyVN8pzQj8n+ulpB/cTuRWFNxLYWA5BAL
X505rwLx6t3+BENhx334fXk2rMYdqOp5C0mVLuBaF4a9W9us8+B4EVSvgcENSQN
uP+R5UI69/YUTqt5X3HVt4rrWrW47uMslX8wc8psqhhxldv6Roc0YjUCAwEAAQ==
-----END RSA PUBLIC KEY-----
Ed25519PublicKey = N9hzigqMfmpK9YDxM+bRpwrPm3KfLWKaYEC/UTcwunD
```

Complejo de escalar



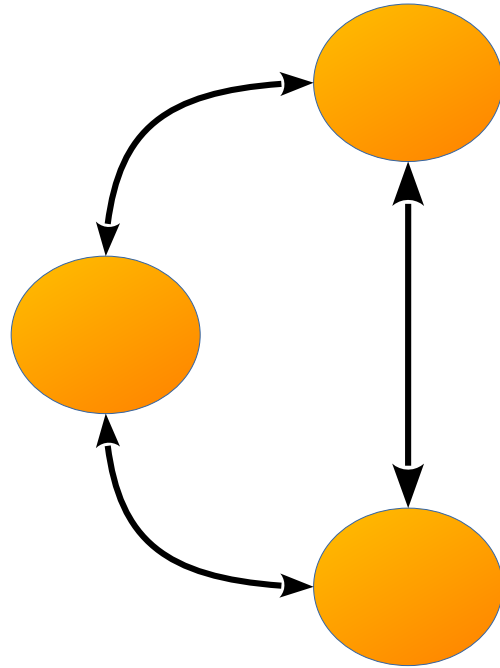
Como hacerlo funcionar



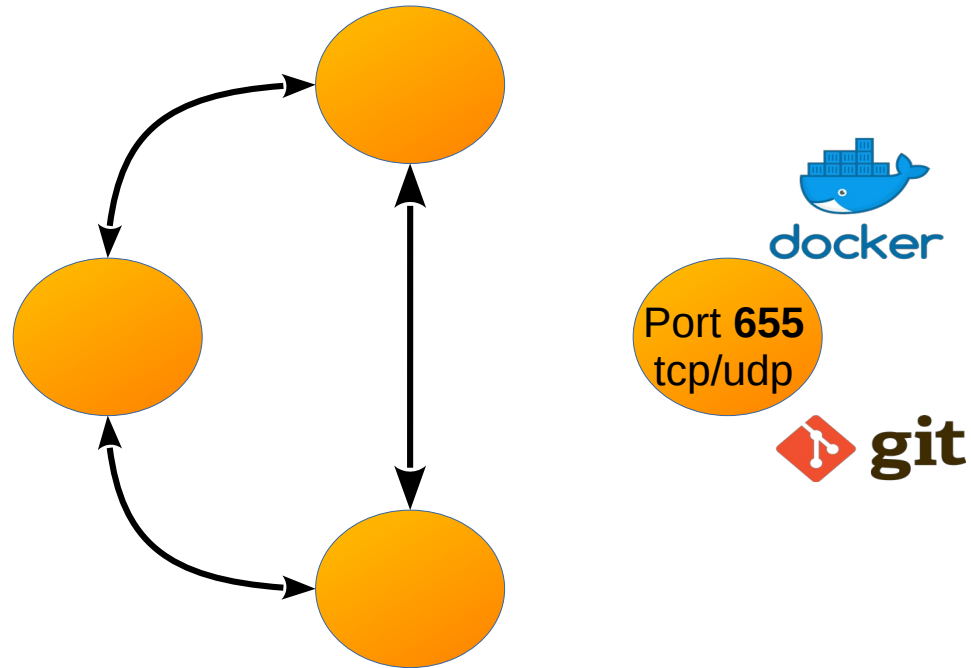
git



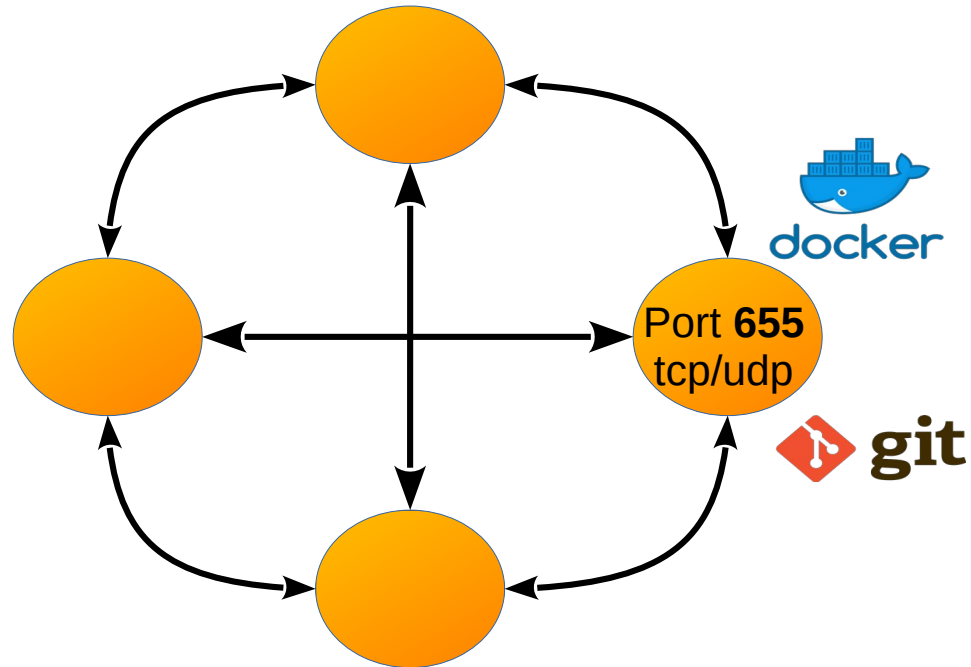
¿Cómo nos conectamos?



¿Cómo nos conectamos?

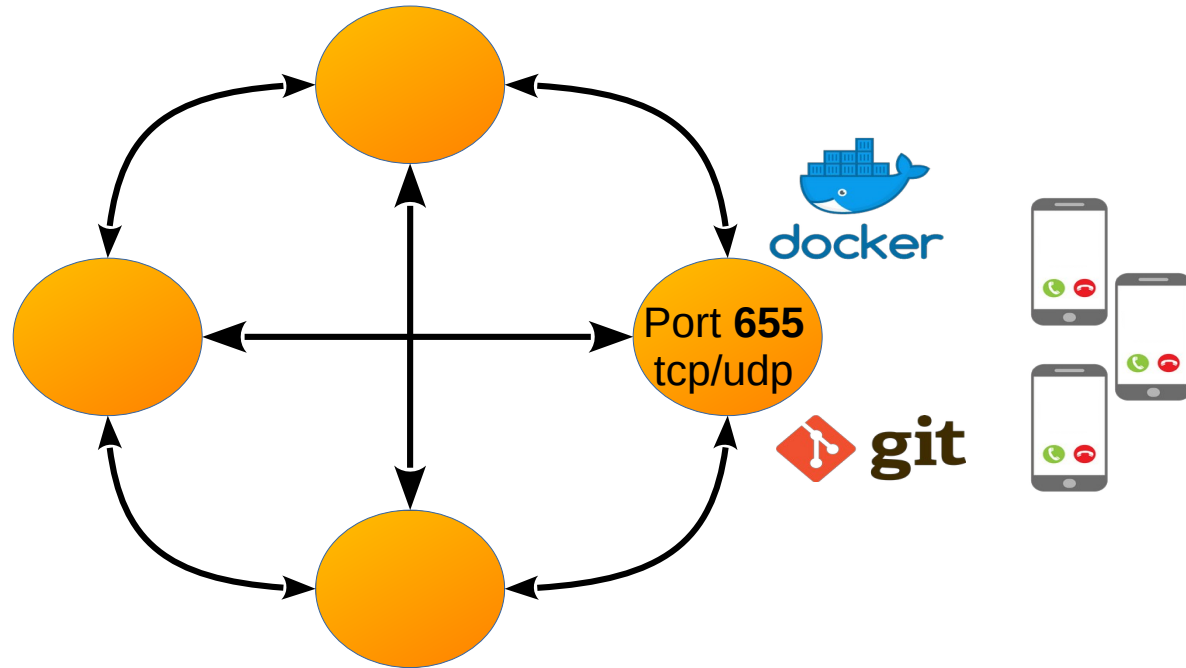


¿Cómo nos conectamos?



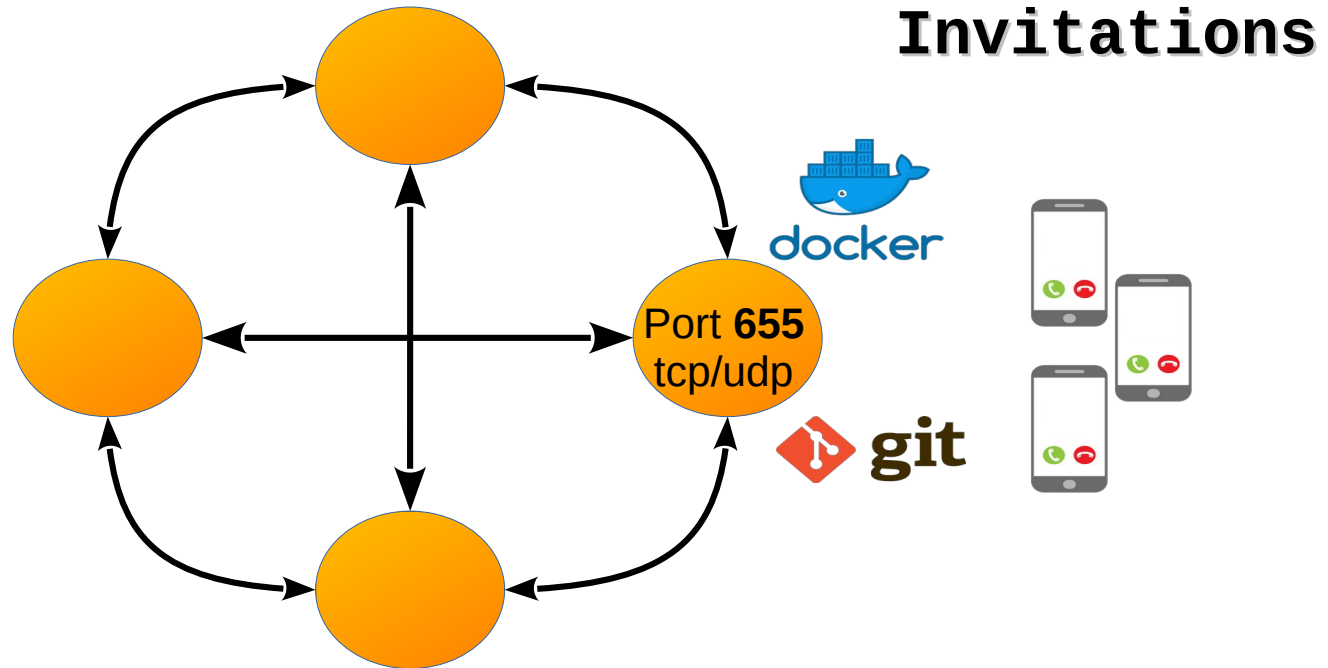
¿Cómo nos conectamos?

Móviles



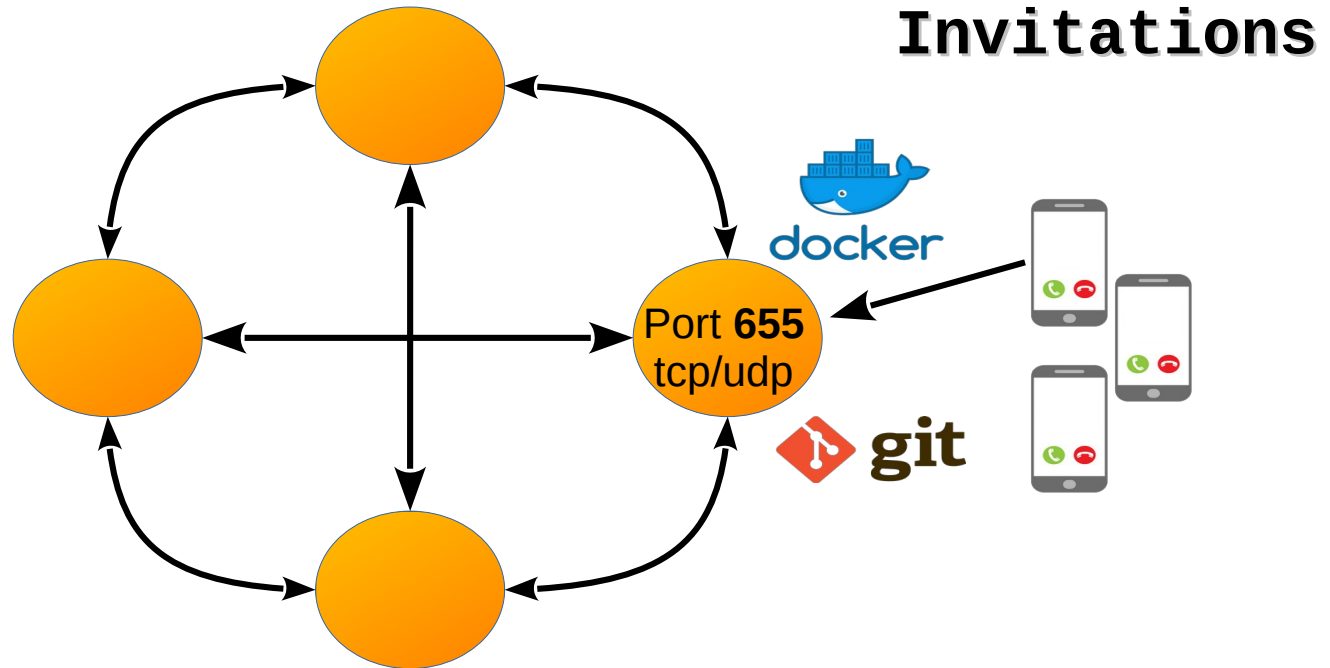
¿Cómo nos conectamos?

Móviles



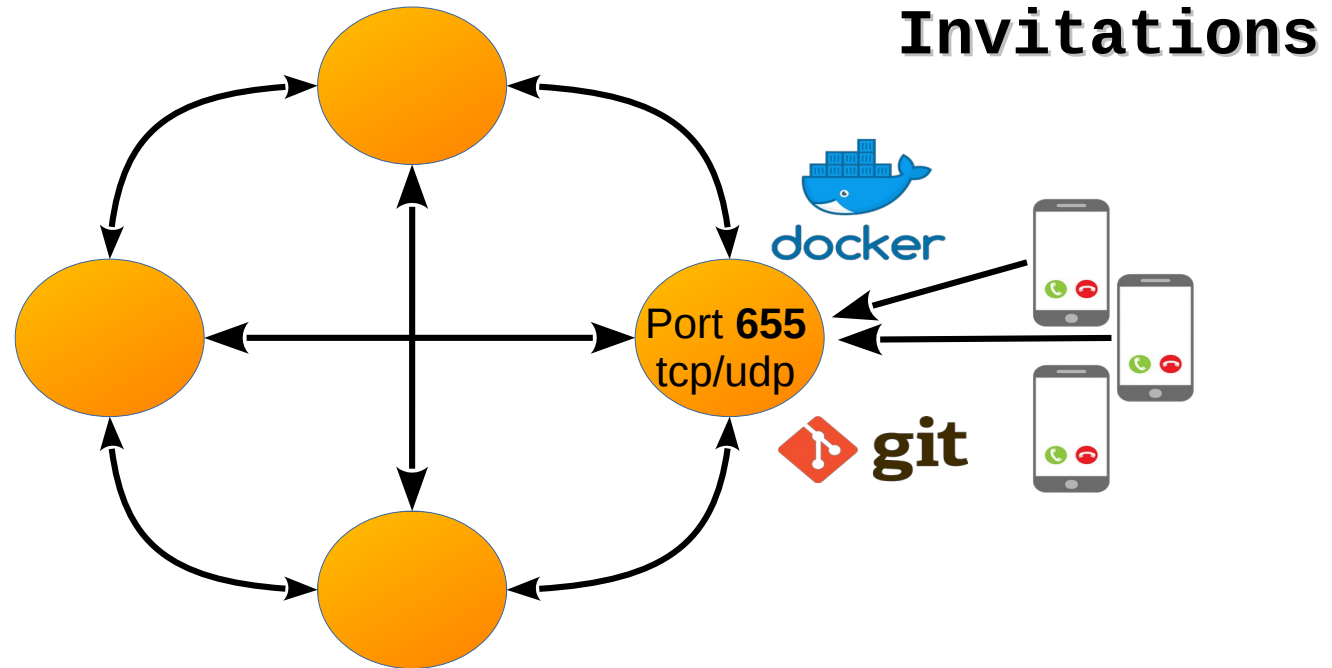
¿Cómo nos conectamos?

Móviles



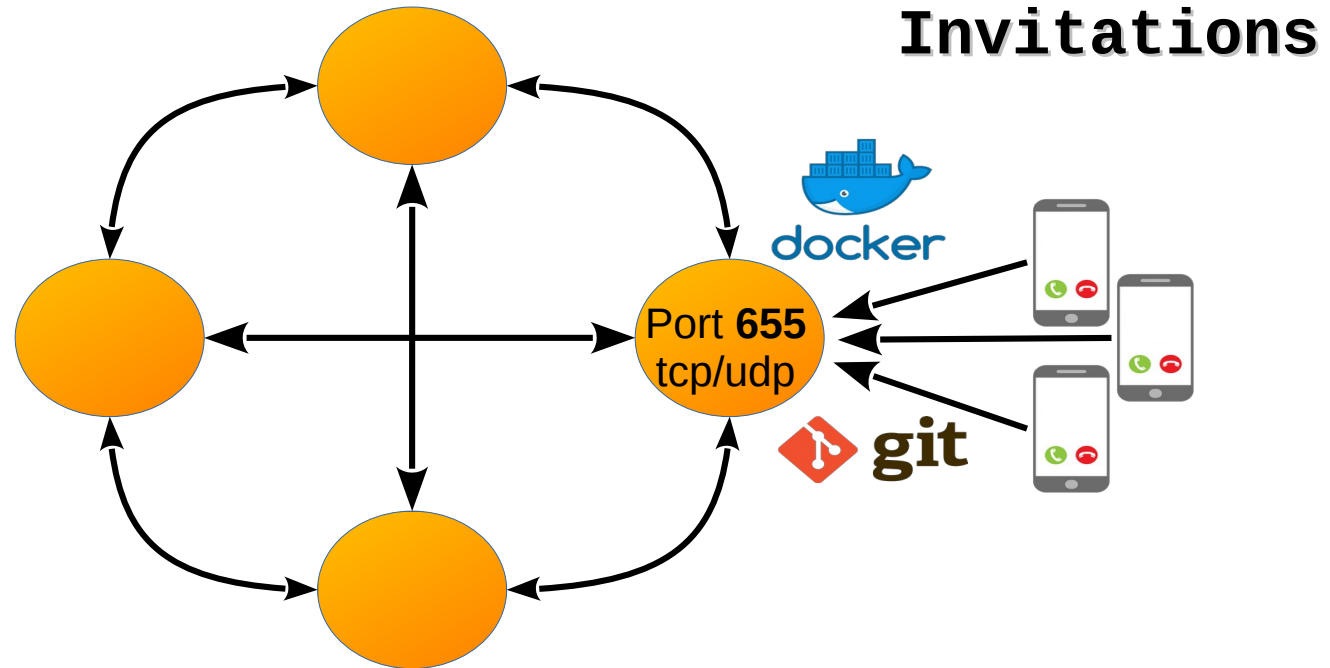
¿Cómo nos conectamos?

Móviles



¿Cómo nos conectamos?

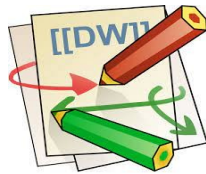
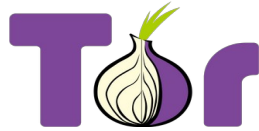
Móviles



Próximos pasos



#irc



Tinc en embebidos



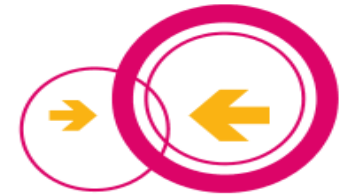
Otras DarkMesh



NYC MESH



ChaosVPN



freifunk.net

!!Gracias!!
¿Preguntas?



Me podéis contactar



XMPP



@ReD.1984

red@jabber.ccc.de

red@nosoloaulas.com

