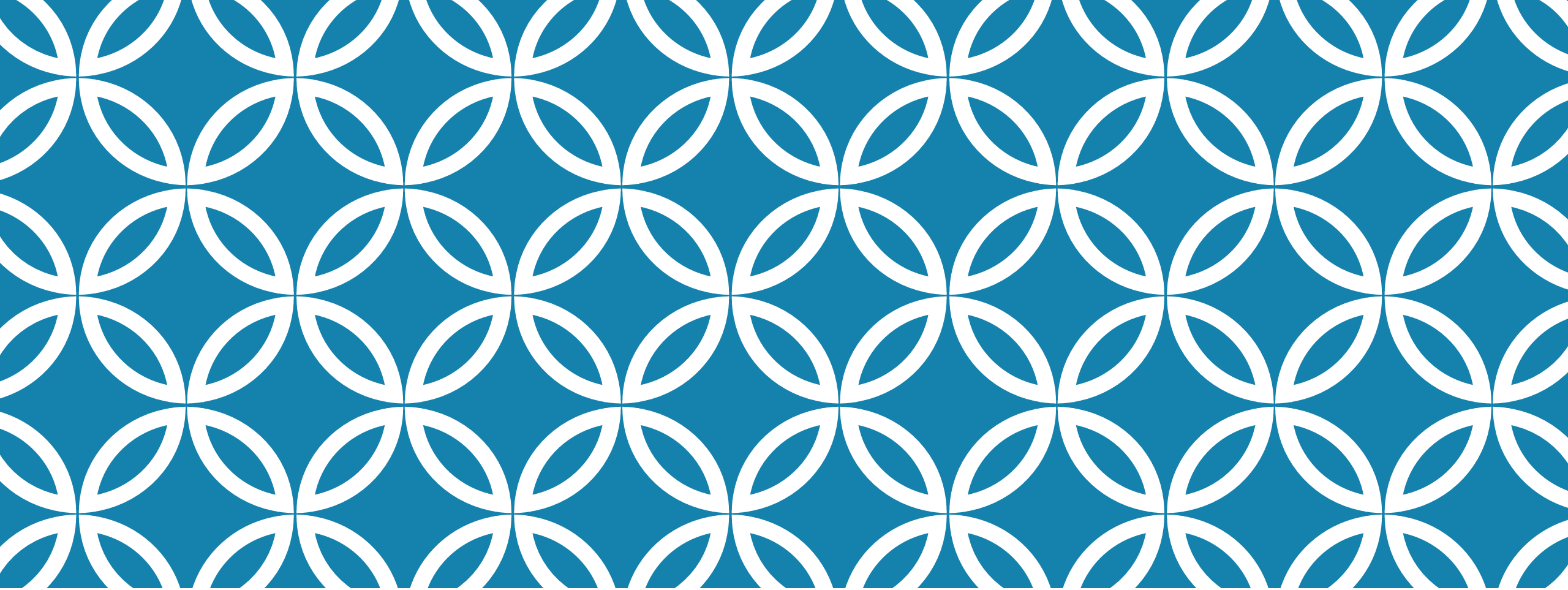


VIRTUAL PRIVATE NETWORK (VPN)

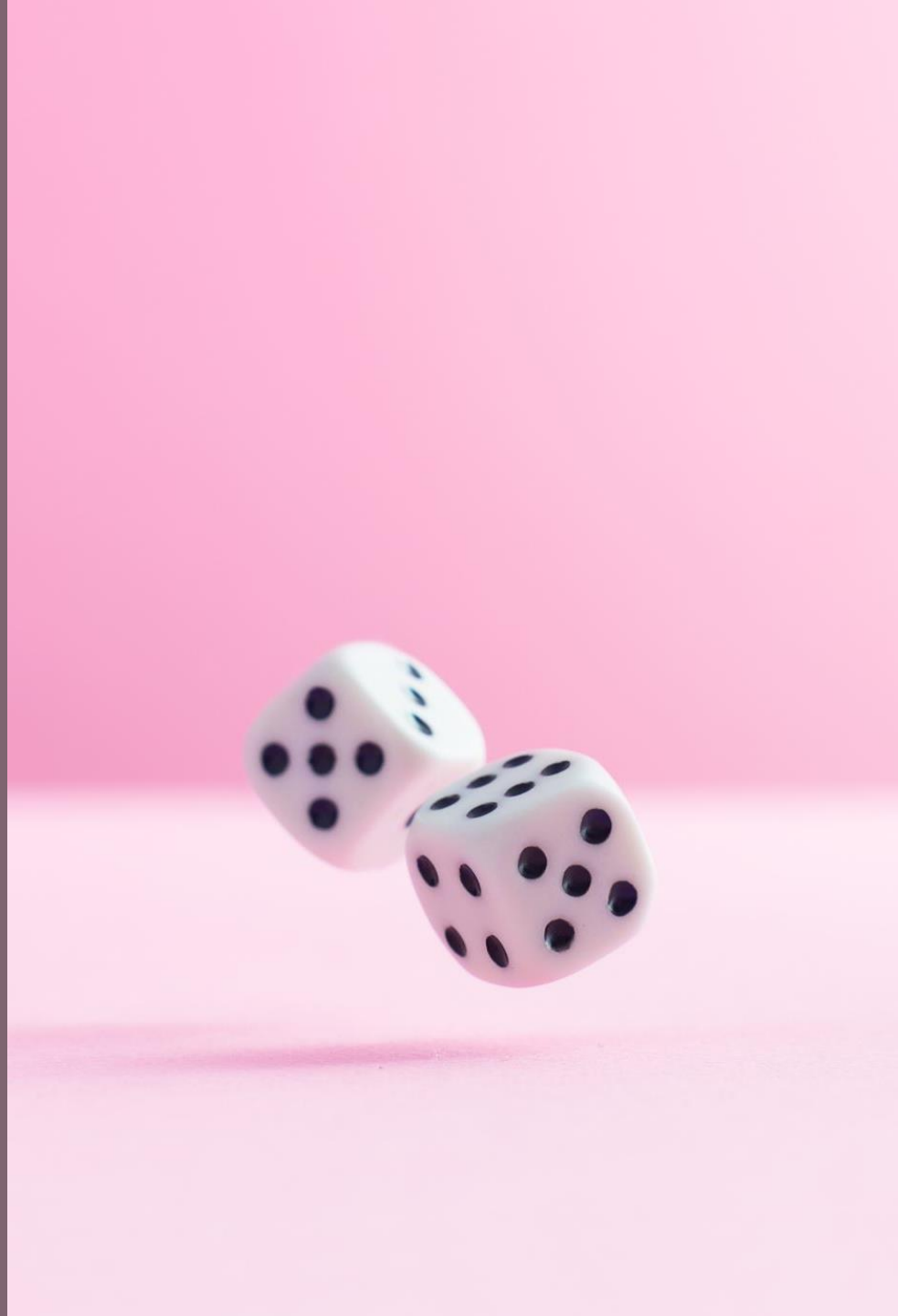
Jaringan Komputer 2

SUB CPMK :

MAMPU MEMISAHKAN JENIS-JENIS DAN FITUR MIKROTIK ROUTER DENGAN APLIKASINYA (VPN) DAN MAMPU MENJELASKAN KONSEP LOAD BALANCING MENGGUNAKAN MIKROTIK [C6,A3][MG KE 6,7]]

INDIKATOR :

Ketepatan dalam menjelaskan Cara kerja VPN dan membedakan Tipe VPN dan mampu mengkonfigurasi VPN



POKOK BAHASAN

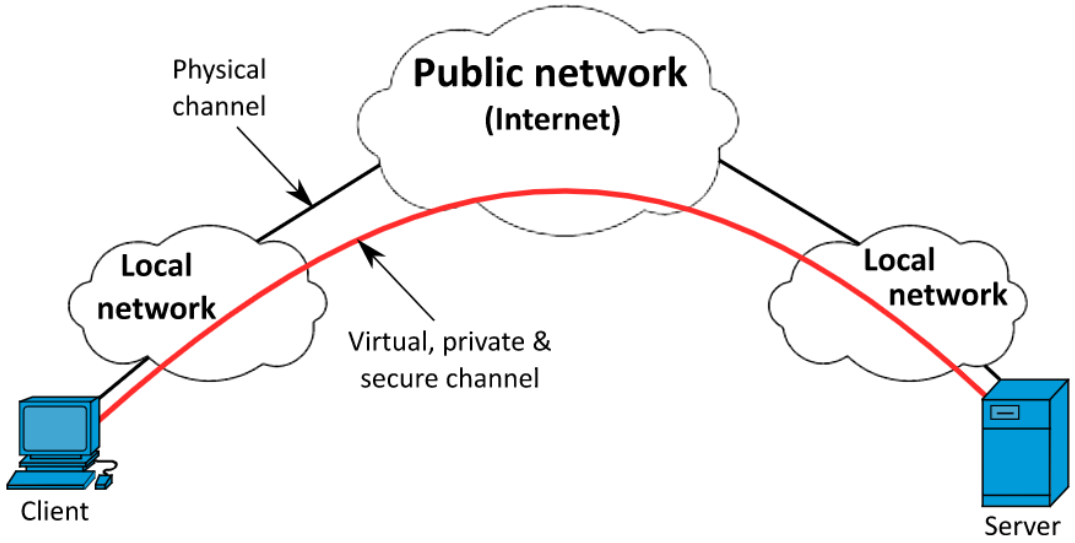
1. VPN
2. Fungsi VPN
3. Jenis VPN
4. Cara Kerja VPN

VIRTUAL PRIVATE NETWORK

Adalah suatu jaringan private yang mempergunakan sarana jaringan komunikasi publik (dalam hal ini Internet) dengan memakai tunnelling protocol dan prosedur pengamanan tertentu.

Mengapa harus “Public”?

Dengan memakai jaringan publik yang ada, dalam hal ini Internet, maka biaya pengembangan yang dikeluarkan akan jauh relatif lebih murah daripada harus membangun sebuah jaringan internasional tertutup sendiri



KENDALA

Ada resiko dengan menggunakan jaringan Public :

- kerahasiaan dan authentifikasi data yang dikirimkan

Diperlukan suatu enkripsi data sebelum dikirimkan ke jaringan public

Disisi penerima juga dilakukan pembukaan enkripsi (dekripsi) atas data yang telah diterima

Biasanya ditambah dengan kriptografi untuk menjamin keamanan data yang dikirimkan

CARA KERJA VPN

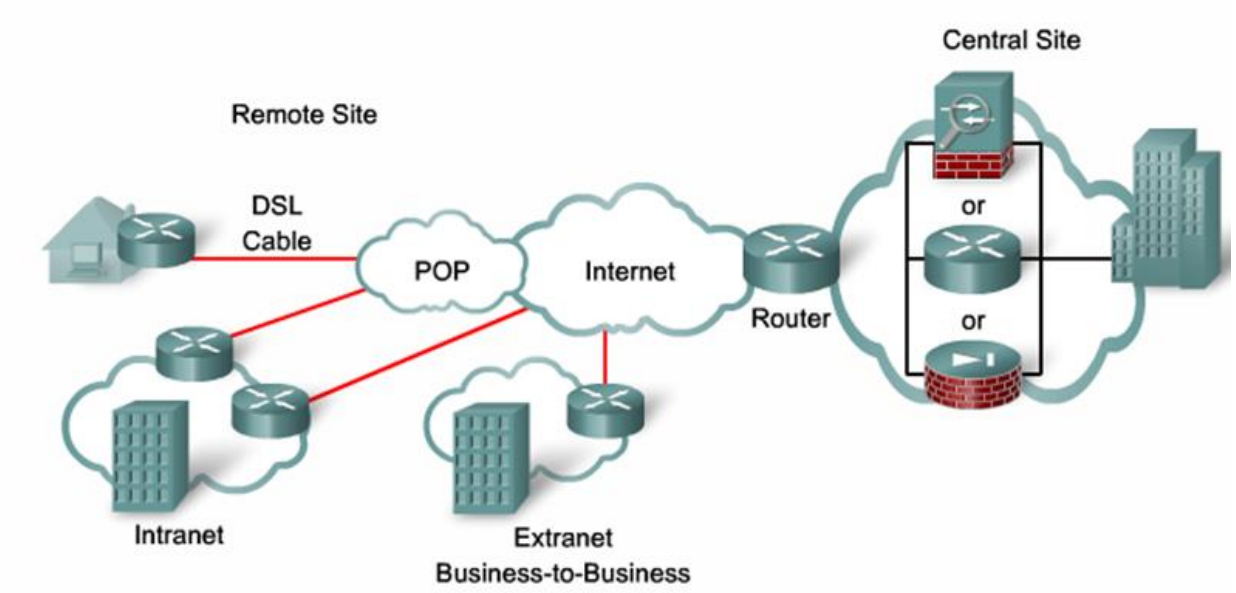
VPN membutuhkan sebuah server yang berfungsi sebagai pengubung antara PC dengan Server VPN. Dan hal ini bisa berupa komputer dengan aplikasi VPN Server atau sebuah Router.

VPN mendukung banyak protokol jaringan seperti PPTP, L2TP, IPSec dan SOCKS. Protokol-protokol inilah yang membantu jaringan VPN untuk memproses autentikasi.

VPN Klien dapat membuat sambungan dan mengidentifikasi orang-orang yang diberi jalur akses terhadap jaringan.

VPN menggunakan teknologi enkripsi yang mana akan meningkatkan fitur keamanan.

JENIS VPN



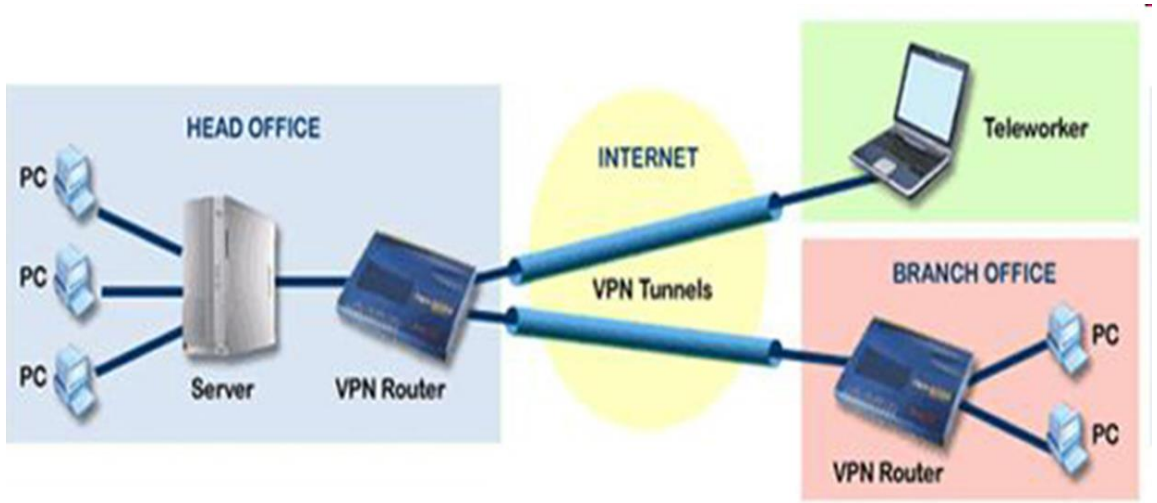
Adapun jenis jaringan VPN dapat di kelompokkan menjadi :

1. Intranet VPN
2. Extranet VPN dan
3. Remote Acces VPN

INTRANET VPN

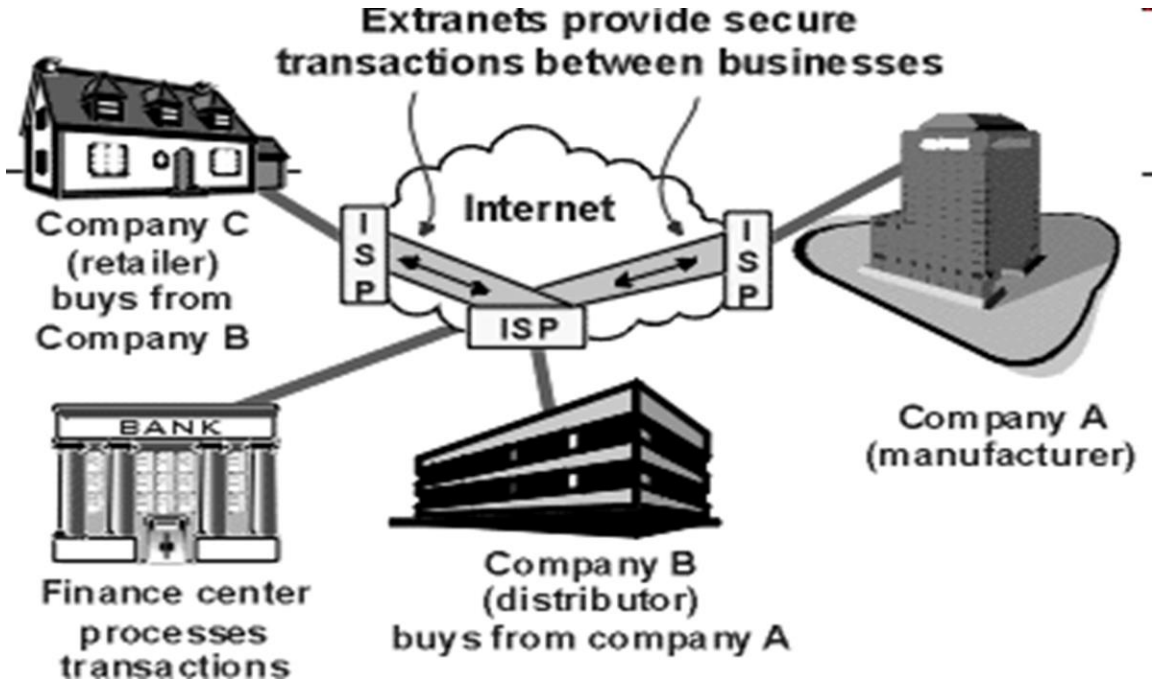
Intranet merupakan jaringan yang terhubung antara kantor pusat dengan kantor cabang yang tersebar di lokasi-lokasi yang terpisah dengan kantor pusat.

Intranet memberikan fasilitas komunikasi dan pertukaran data serta informasi antar internal suatu perusahaan atau departemen dengan cabang yang berjauhan lokasinya.



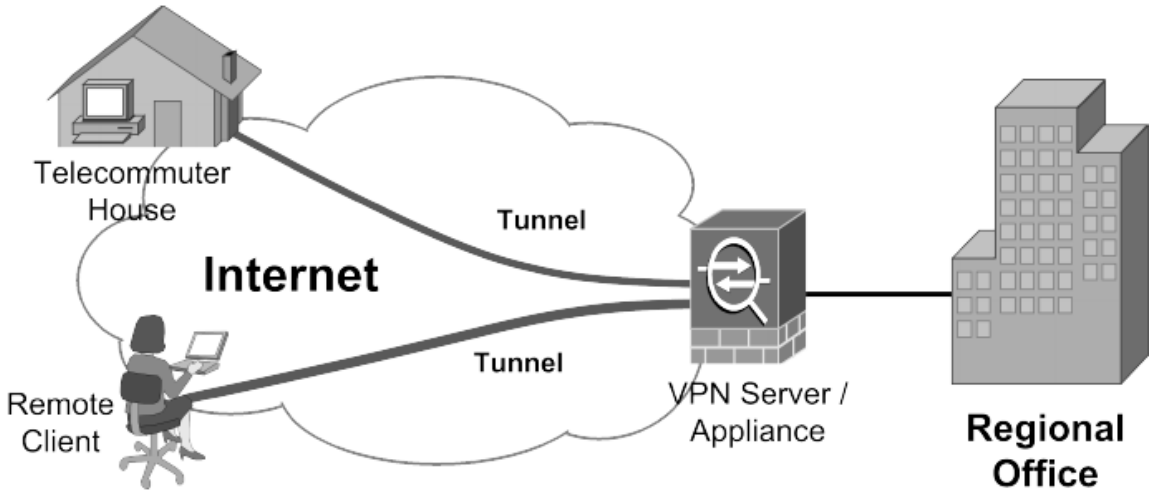
EXTRANET VPN

Jaringan koneksi intranet yang memungkinkan bagi partner bisnis suatu perusahaan untuk bisa mengakses suatu resource yang dimiliki, dengan ketentuan harus bisa melewati “Firewall” yang diberikan oleh jaringan intranet.



REMOTE ACCESS VPN

Intranet dimana setiap host yang telah dilengkapi dengan software VPN client yang akan mengirimkan paket yang telah dienkapsulasi dan dienkripsi terlebih dahulu sebelum dikirimkan melalui internet ke VPN gateway di batas jaringan network tujuan.



KELEBIHAN KEKURANGAN VPN

kelebihan

- VPN merupakan solusi efektif untuk organisasi bisnis besar dengan fasilitas jaringan khusus. Dengan VPN Maka biaya pasang jaringan akan terminimkan
- Data-data pastinya akan terjamin keamanannya

kekurangan

- Karena VPN menggunakan jaringan publik, maka tentunya kita harus lebih ekstra perhatian terhadap keamanan jaringan itu. Siapa tahu, kemudian hal-hal yang tidak diinginkan terjadi; seperti halnya penyadapan, hacking dan tindakan merugikan lainnya yang menyerang jaringan VPN kita. Hal tersebut tentunya akan berdampak besar terhadap jaringan VPN dan khususnya data-data rahasia organisasi kita.

PROTOKOL DALAM VPN

Point-to-point tunneling protocol (PPTP) :

Layer-2 forwarding (L2F) :

Layer-2 tunneling protocol (L2TP) :

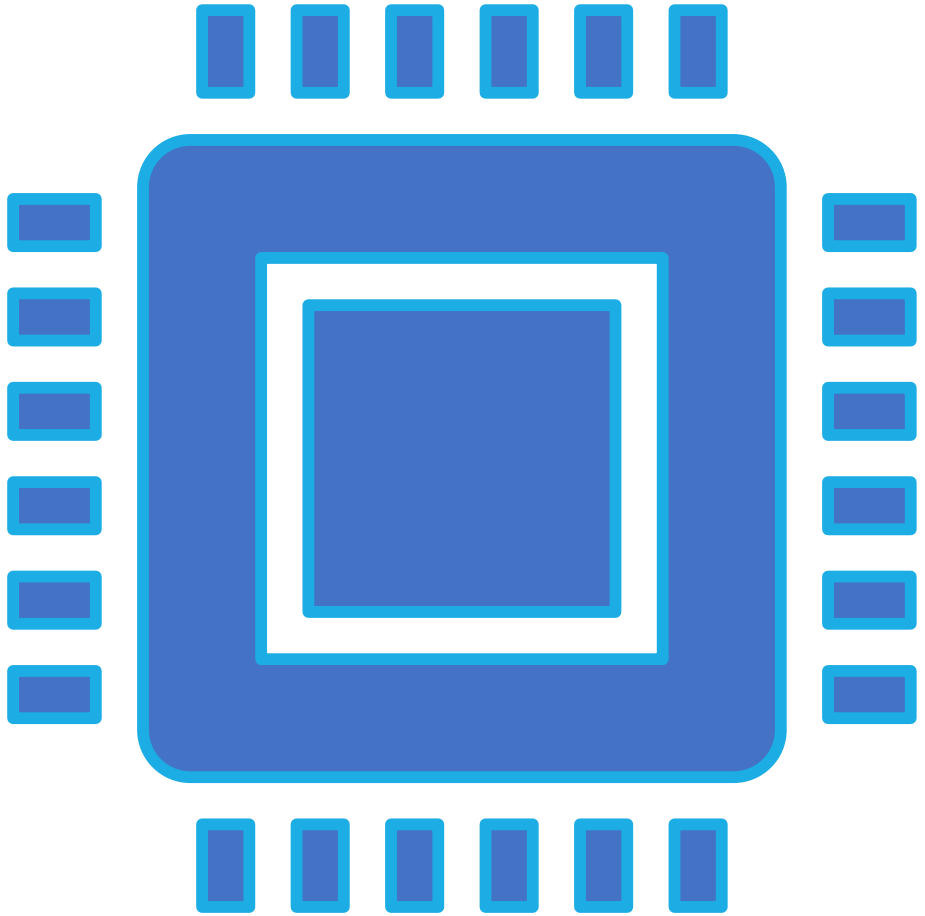
IP security protocol (IPSec)

POINT-TO-POINT TUNNELING PROTOCOL (PPTP)

Point-to-Point Tunneling Protocol, dikembangkan oleh konsorsium yang didirikan oleh Microsoft untuk membuat VPN melalui jaringan dial-up, dan dengan demikian telah lama menjadi protokol standar untuk VPN internal diperusahaan-perusahaan. Ini adalah protokol VPN standar, dan bergantung pada berbagai metode otentikasi untuk memberikan keamanan (MS-CHAP v2 adalah yang paling umum). Tersedia sebagai standar VPN pada hampir semua platform dan perangkat, dan dengan demikian menjadi mudah untuk mengatur tanpa perlu menginstal perangkat lunak tambahan, itu tetap menjadi pilihan populer baik untuk bisnis dan penyedia VPN.

LAYER-2 FORWARDING (L2F)

L2F adalah singkatan dari Layer 2 Forwarding, adalah protokol tunneling media-independen yang dikembangkan oleh Cisco Systems. Protokol Layer 2 Forwarding (L2F) terowongan data-link layer frame dalam protokol seperti Point-to-Point Protocol (PPP) atau Serial Line Internet Protocol (SLIP), sehingga memungkinkan untuk membuat jaringan pribadi virtual (VPN) melalui publik jaringan seperti Internet.



LAYER-2 TUNNELING PROTOCOL (L2TP)

Layer 2 Tunneling Protocol (L2TP) adalah standar IETF dikembangkan untuk menggantikan PPTP. Ini adalah hasil dari penggabungan teknologi dari Microsoft PPTP dengan Layer 2 Forwarding (L2F) protokol tunneling Cisco. Selain jaringan IP, L2TP mendukung tunneling melalui berbagai jenis jaringan point-to-point termasuk Frame Relay, X.25, dan ATM.

IP SECURITY PROTOCOL (IPSEC)

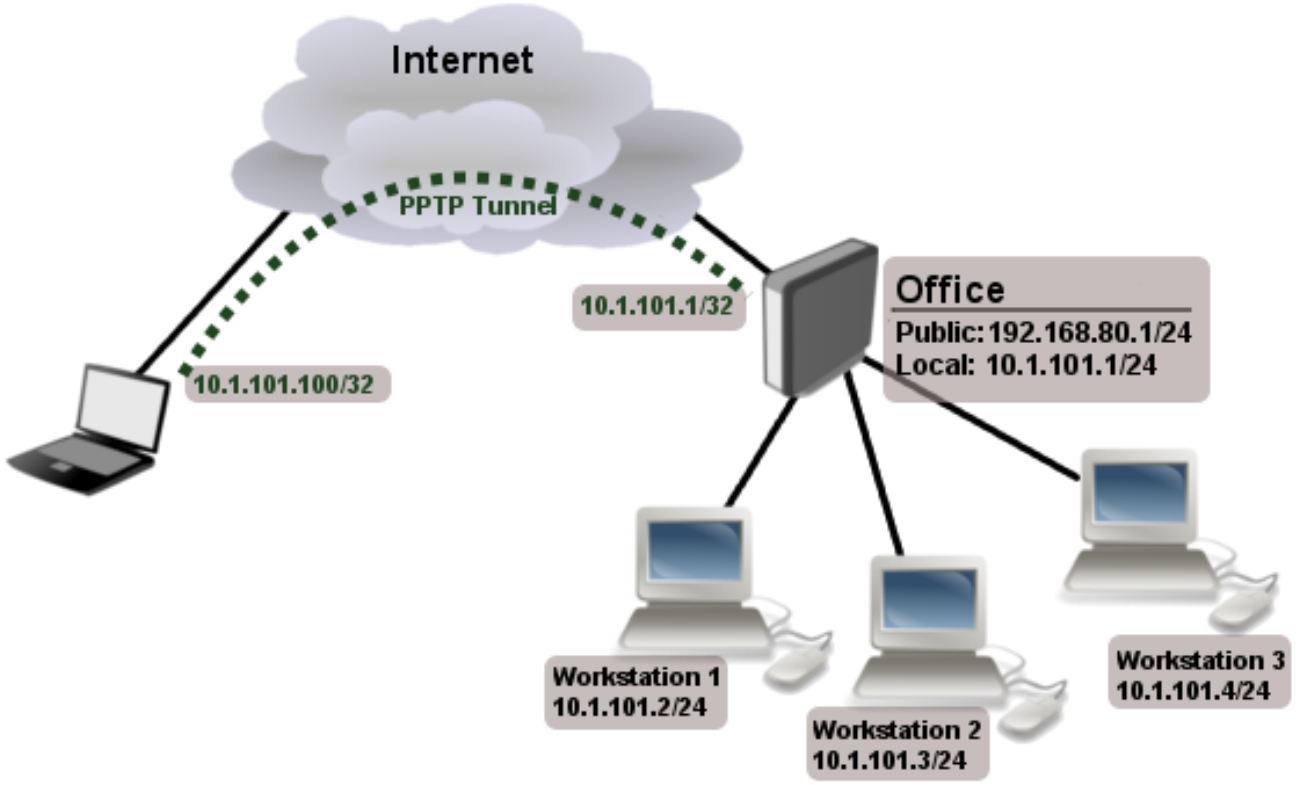
Pengembagan antara L2TP dengan IPSec yang menghasilkan protocol baru L2TP/IPSec, adalah kolaborasi antara Microsfot dan Cisco system untuk menyempurnaka protocol L2TP tunneling protocol ini.

APLIKASI VPN PADA MIKROTIK

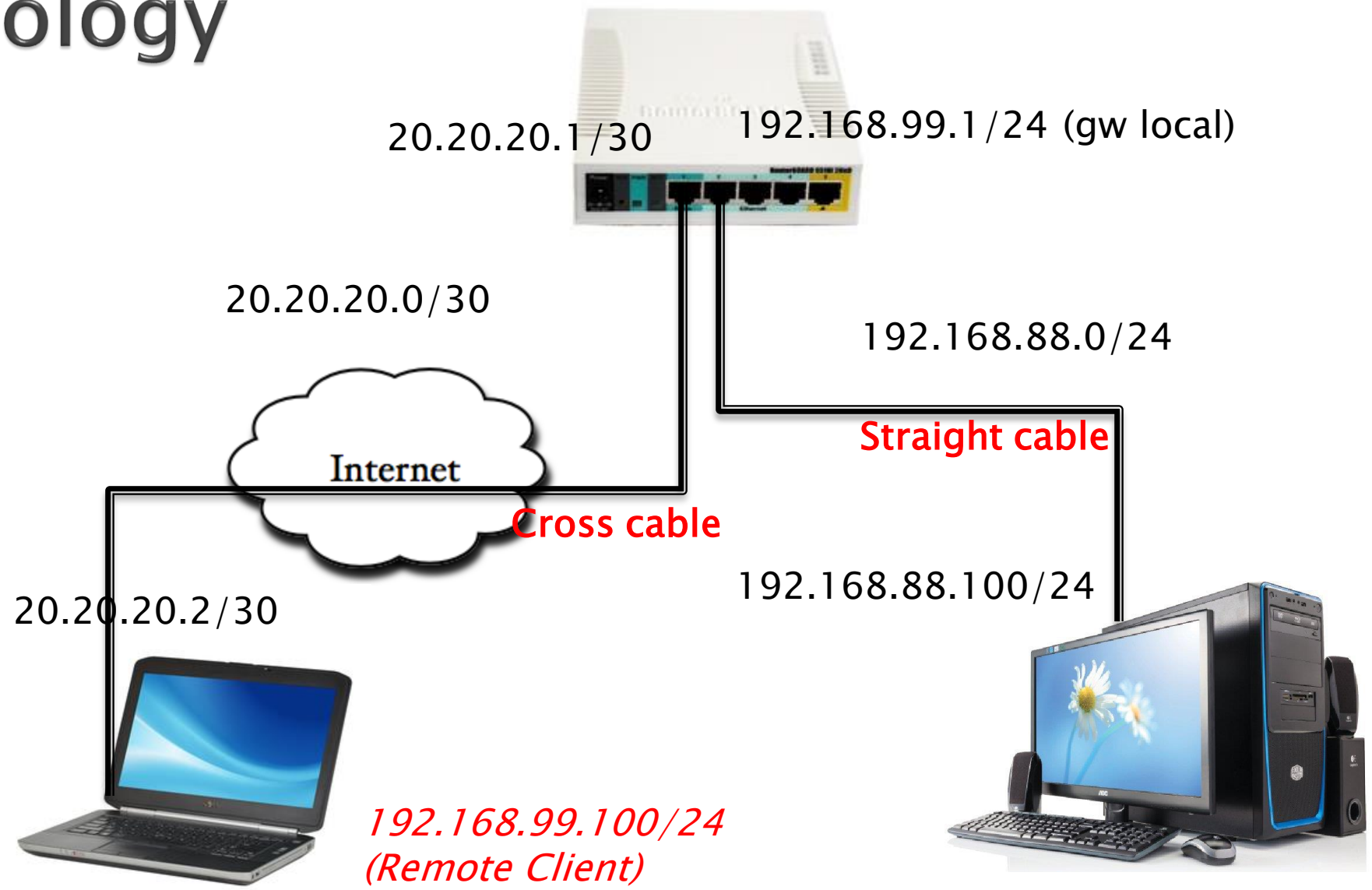
VPN REMOTE OFFICE

OFFICE TO OFFICE CONNECTION

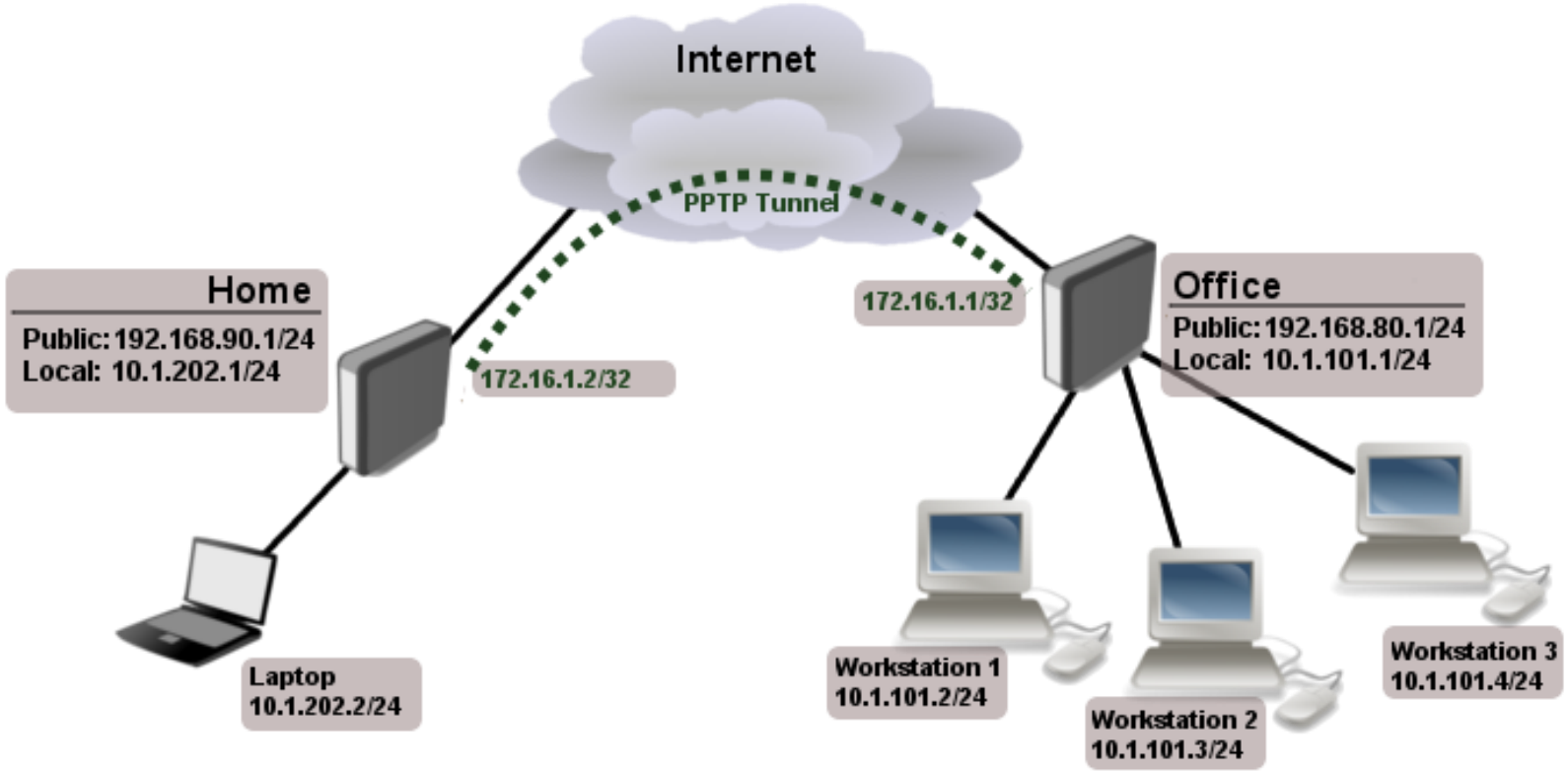
VPN Remote Office



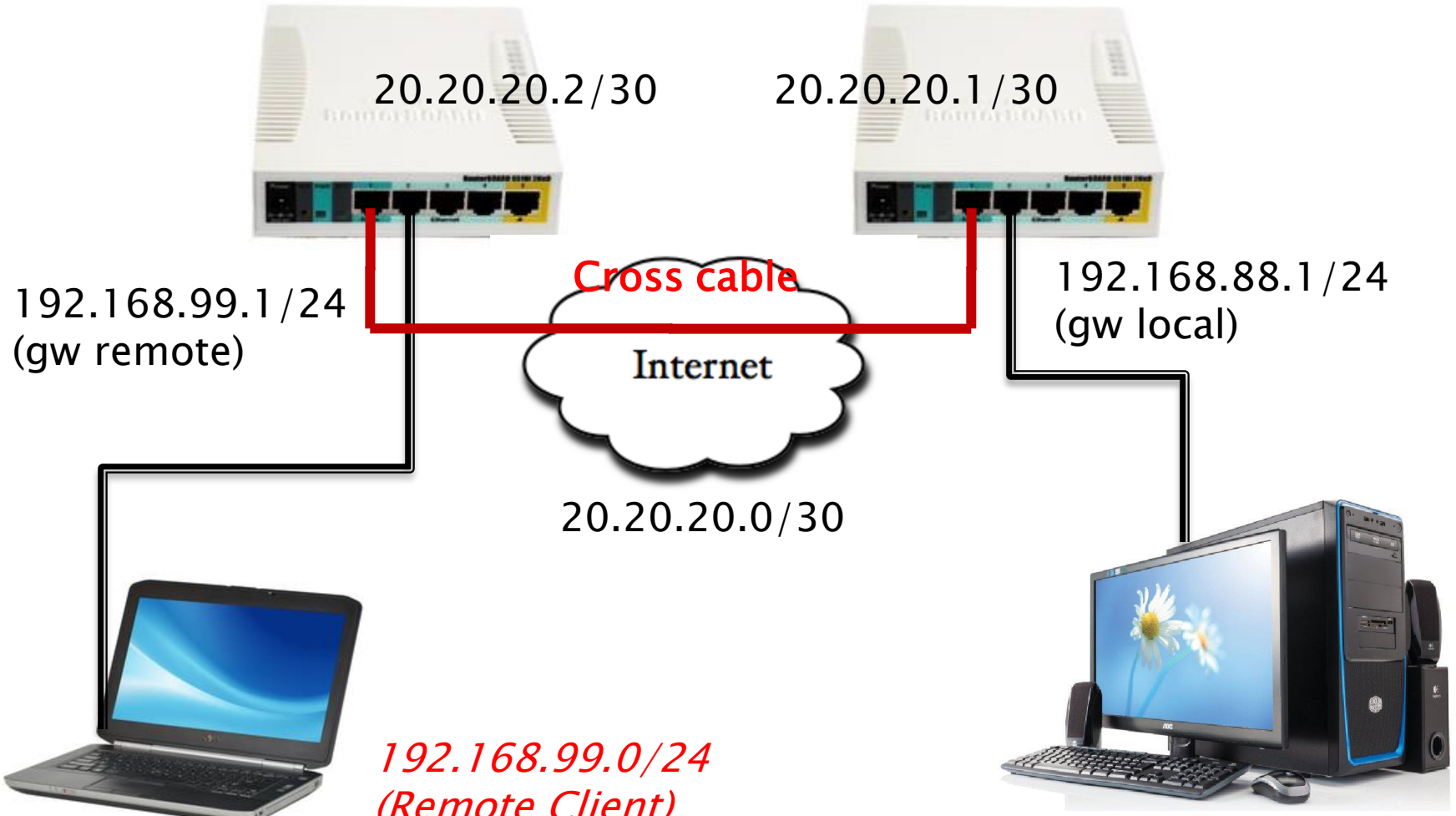
Topology

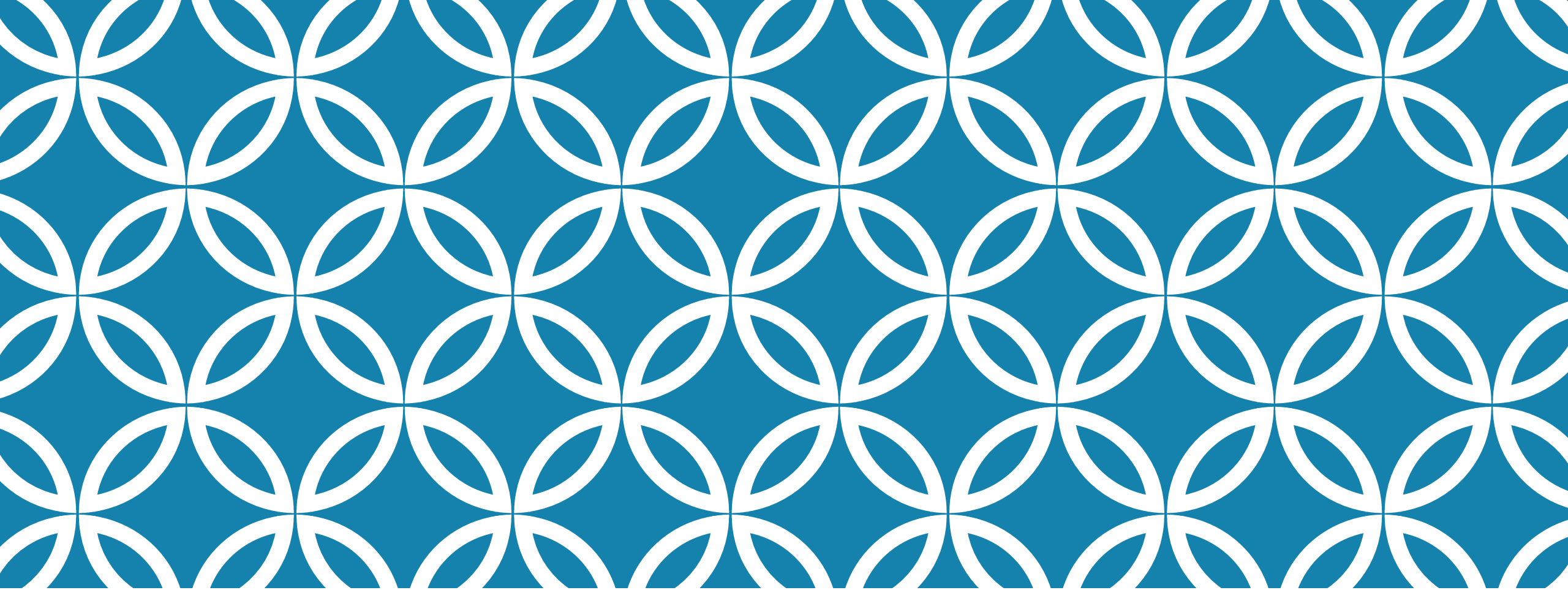

20.20.20.1/30
192.168.99.1/24 (gw local)
20.20.20.0/30
192.168.88.0/24
Straight cable
Internet
Cross cable
192.168.88.100/24
20.20.20.2/30
192.168.99.100/24
(Remote Client)

Office to Office Connection



Topology


20.20.20.2/30
20.20.20.1/30
192.168.99.1/24
(gw remote)
Cross cable
Internet
192.168.88.1/24
(gw local)
20.20.20.0/30
192.168.99.0/24
(Remote Client)
192.168.88.0/24 (net local)



TERIMA KASIH