

MikroTik Basic Implementation in Enterprise Network

Umair Masood
Information Technology Dept
Haier Pakistan

About Me

Trainings

- Cisco Certified Network Associate (Routing & Switching)
- Cisco Certified Network Associate (Data Center)
- Cisco Certified Network Associate (Wireless)
- Cisco Certified Network Professional (Routing & Switching)
- Microsoft Certified System Administrator
- APTECH Certified Computer Professional (ACCP)
- Red Hat Certified System Administrator (RHCA)
- MTCNA (MikroTik Certified Network Associate) → In Process

Position

- Manager Network & IT Support

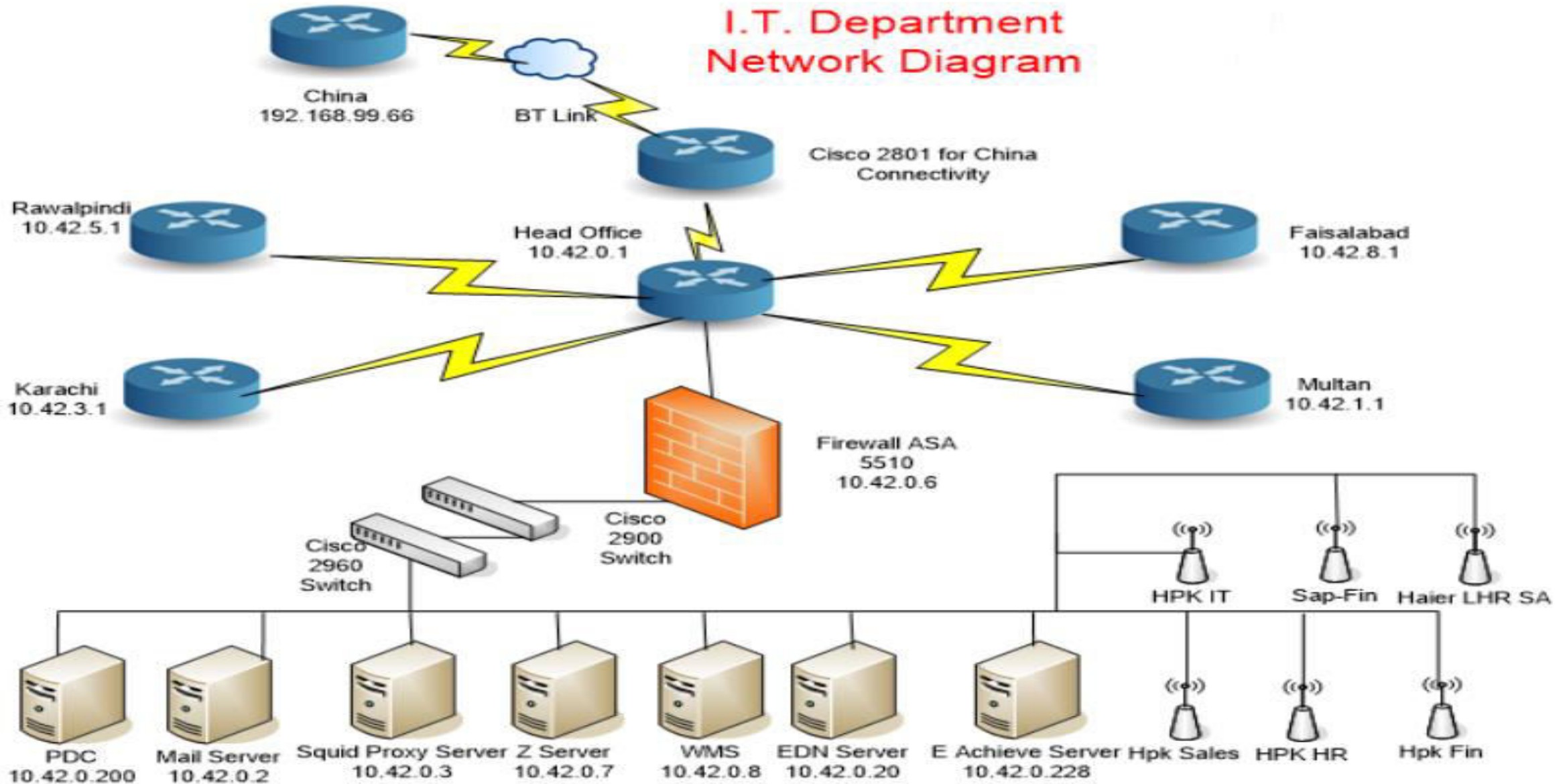
Company

- Haier Pakistan(Pvt)Ltd

Road Map

- Why MikroTik router board Implementation required in Haier Network
- DHCP Server Functionality & Mac Address Filtering
- WAN Failover Functionality
- Virtual Private Network Implementation
- Remote Access VPN Implementation
- Demilitarized Network Zone Set up & Destination Network Address Translation

Haier Network Before MikroTik



Why MikroTik router board Implementation in Haier Network

- Easy to configure and manage
- Very low cost rather than any other hardware like Cisco, Fortigate
- Intelligently handled Firewall & Failover
- Easy remote monitoring
- Very User Friendly GUI
- Support of Giga bit Ethernet Ports (i.e. GL 750 Hex)
- Site-to-Site VPN functionality in failover to support leased lines as backup
- Easy to manage configuration backup and restoration process

DHCP Server Configuration

Haier@10.42.0.7 (MikroTik) - WinBox v6.32.2 on RB3011UiAS (arm)

RouterOS WinBox

Quick Set
 Interfaces
 Bridge
 PPP
 Mesh
 IP
 MPLS
 Routing
 System
 Queues
 Files
 Log
 Radius
 Tools
 New Terminal
 Partition
 Make Supout.rtf
 Manual
 Exit

Safe Mode

Hide Passwords

IP Pool

Pools Used Addresses

Name	Addresses	Next Pool
VPN-POOL	172.18.99.1-172.18.99.254	none
default-dhcp	192.168.88.10-192.168.88.254	none

IP Pool <default-dhcp>

Name: default-dhcp
 Addresses: 0-192.168.88.254
 Next Pool: none

DHCP Server

DHCP Networks Leases

0 items

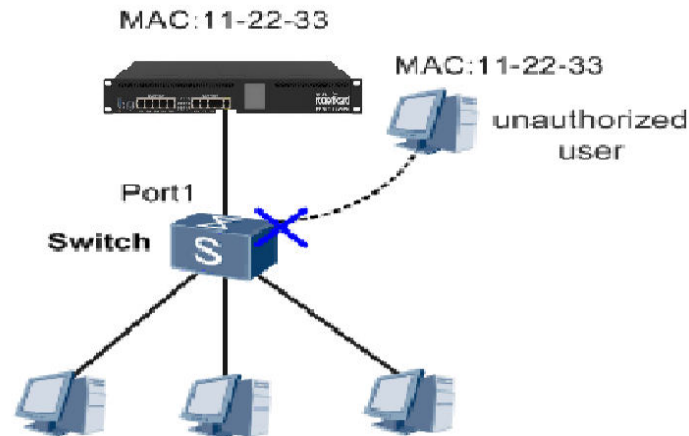
New DHCP Server

Name: Haier DHCP
 Interface: local
 Relay:
 Lease Time: 00:10:00
 Bootp Lease Time: forever
 Address Pool: default-dhcp
 Src. Address:
 Delay Threshold:
 Authoritative: after 2s delay
 Bootp Support: static
 Lease Script:
 Add ARP For Leases
 Always Broadcast
 Use RADIUS
 enabled

2 items (1 selected)

Mac Address Filtration

- Normally, a router allows any device to connect as long as it knows the appropriate passphrase
- With **MAC address filtering**
 - A router will first compare a device's **MAC address** against an approved list of **MAC addresses**
 - Then only allow a device onto the Local network if its **MAC address** has been specifically approved



MAC Address Filtering

Open your local interface → ARP → reply-only

Haier@10.42.0.7 (MikroTik) - WinBox v6.32.2 on RB3011UiAS (arm)

Safe Mode

Hide Passwords

RouterOS WinBox

Quick Set
Interfaces
Bridge
PPP
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
Partition
Make Supout.rif
Manual
Exit

IP Pool

Pools Used Addresses

Interface <local>

Interface

General Ethernet Status Traffic

Name: local

Type: Ethernet

MTU: 1500

L2 MTU: 1598

Max L2 MTU: 8156

MAC Address: E4:8D:8C:03:F0:45

ARP: reply-only

OK
Cancel
Apply
Disable
Comment
Torch
Cable Test
Blink
Reset MAC Address

enabled running slave link ok

27 items (1 selected)

2 items

	Tx Packet (p/s)	Rx Packet (p/s)
0 bps	0	0
11.9 kbps	21	17
0 bps	0	0
0 bps	1	0
544 bps	0	1
26.7 kbps	27	30
19.4 kbps	32	31
0 bps	0	0
0 bps	0	0
0 bps	0	0
0 bps	0	0
320 bps	1	1
0 bps	0	0
8.8 kbps	6	6
0 bps	0	0
0 bps	0	0
0 bps	0	0
347.4 kbps	510	411
50.7 kbps	54	67
0 bps	0	0
0 bps	0	0
0 bps	0	0
0 bps	0	0
0 bps	0	0
0 bps	0	0
245.3 kbps	325	249
0 bps	0	0

In IP→ARP

Put your users/Lan Ip address here and User's Mac Address with interface local

Haier@10.42.0.7 (MikroTik) - WinBox v6.32.2 on RB3011UiAS (arm)

RouterOS WinBox

Safe Mode

Hide Passwords

Find

ARP List

	IP Address	MAC Address	Interface
D	10.42.0.1	00:23:5E:CA:16:F1	bridge-local
D	10.42.0.2	00:06:5B:87:DC:86	bridge-local
D	10.42.0.8	E4:1F:13:31:05:D4	bridge-local
D	10.42.0.19	00:1C:C4:DA:C1:F2	bridge-local
D	10.42.0.20	E4:1F:13:B8:63:A6	bridge-local
D	10.42.0.24	80:EE:73:7D:3B:32	bridge-local
D	10.42.0.32	08:ED:B9:73:AE:93	bridge-local
D	10.42.0.39	50:68:0A:21:3E:72	bridge-local
D	10.42.0.49	60:6C:66:16:41:DF	bridge-local
D	10.42.0.57	00:22:B0:E1:29:52	bridge-local
D	10.42.0.64	20:16:D8:59:76:87	bridge-local
D	10.42.0.74	A8:A7:95:30:BC:67	bridge-local
D	10.42.0.95	A4:2B:B0:BE:98:88	bridge-local
D	10.42.0.103	34:23:87:E0:32:AD	bridge-local
D	10.42.0.113	00:88:22:00:01:50	bridge-local
D	10.42.0.210	00:15:00:0A:A9:FD	bridge-local
D	10.42.0.214	9C:D2:1E:96:0E:69	bridge-local
D	10.42.0.241	E0:2A:82:5E:08:BD	bridge-local
D	202.142.170.73	18:8B:9D:D7:F1:04	bridge-local

New ARP

IP Address: 10.42.0.24

MAC Address: 80:EE:73:7D:3B:32

Interface: local

Published

enabled published

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Make Static
Ping
MAC Ping
Telnet
MAC Telnet
Torch

19 items

Difference with Cisco IP SLA Failover Monitoring

The image displays a network simulation in GNS3 and a terminal window in SuperPuTTY. The network diagram shows a 'Main' network with routers R1 (192.168.20.2) and R2 (192.168.30.2) connected to a switch SW1 (192.168.40.1). A 'Branch' network has router R3 (192.168.20.1) connected to switch SW2. R3 is connected to R1 via a 'Primary Link' (f0/0 to f0/0) and to R2 via a 'Secondary Link' (f0/1 to f0/0). The terminal window shows the configuration of IP SLA 1 on R3, including ICMP echo and reachability tracking, and the execution of the 'sh track' command showing the SLA is up.

```
Unsaved project* — GNS3
File Edit View Control Device Annotate Tools Help
[Icons]
[Router] [Switch] [Console] [Terminal] [Network] [Tools]
[Router] [Switch] [Console] [Terminal] [Network] [Tools]

192.168.20.1
f0/0
192.168.20.2
f0/0
192.168.30.1
f0/1
192.168.30.2
f0/0
192.168.40.1
f0/1
192.168.40.2
f0/1

Primary Link
Secondary Link

Main
Branch

R3
SW2

R1
R2
SW1

Console
GNS3 management console. Running GNS3 version 1.1 on Windows (64-bit).
Copyright (c) 2006-2014 GNS3 Technologies.
=>

SuperPuTTY - R3
File View Tools Help
R1 R2 R3
R3#
R3#
*Mar 21 14:15:51.291: %OIR-6-INSCARD: Card inserted in slot 1, Interfaces ad
R3#
*Mar 21 14:15:54.979: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEt
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ip sla 1
R3(config-ip-sla)#icmp-ech
R3(config-ip-sla)#icmp-echo 192.168.20.2 source-int
R3(config-ip-sla)#icmp-echo 192.168.20.2 source-interface f0/0
R3(config-ip-sla-echo)#freq
R3(config-ip-sla-echo)#frequency 10
R3(config-ip-sla-echo)#timeou
R3(config-ip-sla-echo)#timeout 6000
R3(config-ip-sla-echo)#exit
R3(config)#ip sla sched
R3(config)#ip sla schedule 1 start
R3(config)#ip sla schedule 1 start-time now life forev
R3(config)#ip sla schedule 1 start-time now life forever
R3(config)#trac
R3(config)#track 10 ip sla 1
R3(config-track)#exit
R3(config)#track 10 ip sla 1 reac
R3(config)#track 10 ip sla 1 reachability
R3(config-track)#exit
R3(config)#exit
R3#sh trac
R3#sh track
*Mar 21 14:40:55.727: %SYS-5-CONFIG_I: Configured from console by console
R3#sh track
Track 10
  IP SLA 1 reachability
  Reachability is Up
    1 change, last change 00:00:53
  Latest operation return code: OK
  Latest RTT (milliseconds) 68
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ip route
```

WAN Failover Functionality with few clicks as compared to Cisco

Haier@10.42.0.7 (MikroTik) - WinBox v6.32.2 on RB3011UiAS (arm)

Safe Mode Hide Passwords

Quick Set

- Interfaces
- Bridge
- PPP
- Mesh
- IP
- MPLS
- Routing
- System
- Queues
- Files
- Log
- Radius
- Tools
- New Terminal
- Partition
- Make Supout.rif
- Manual
- Exit

Gateway	Distance	Routing Mark	Pref. Source
202.142.170.73 reachable bridge-local	1		
122.129.79.254 unreachable	2		
10.10.0.1 unreachable	1		
bridge-local reachable	0		10.42.0.7
l2tp-out 1 reachable	0		10.42.0.7
10.42.0.1 reachable bridge-local	1		
10.42.0.1 reachable bridge-local	1		
10.42.40.1 unreachable	1		10.42.0.7
10.44.0.1 reachable <l2tp-khi_warehouse>	1		
<l2tp-khi_warehouse> reachable	0		10.42.0.7
<l2tp-rawalpindi> reachable	1		
<l2tp-rawalpindi> reachable	0		10.42.0.7
10.44.80.1 reachable <l2tp-multan>	1		
<l2tp-multan> reachable	0		10.42.0.7
<l2tp-multan?> reachable	0		10.42.0.7

Route <0.0.0.0/0>

General Attributes

Dst. Address: 0.0.0.0/0

Gateway: 122.129.79.254 unreachable

Check Gateway: ping

Type: unicast

Distance: 2

Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:

OK
Cancel
Apply
Disable
Comment
Copy
Remove

Route <0.0.0.0/0>

General Attributes

Dst. Address: 0.0.0.0/0

Gateway: 202.142.170.73 reachable bridge-local

Check Gateway: ping

Type: unicast

Distance: 1

Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:

OK
Cancel
Apply
Disable
Comment
Copy
Remove

RouterOS WinBox

Virtual Private Network

- Virtual Private Network is a type of private network that uses public networks, such as Internet, instead of leased lines to communicate
- Two connections – one is made to the Internet and the second is made to the VPN
- Datagrams – contains data, destination and source information
- Firewalls – VPNs allow authorized users to pass through the firewalls
- Protocols – protocols create the VPN tunnels

Protocols Used in VPN

- PPTP -- Point-to-Point Tunneling Protocol
- L2TP -- Layer 2 Tunneling Protocol
- IPsec -- Internet Protocol Security

Virtual Private Network Types

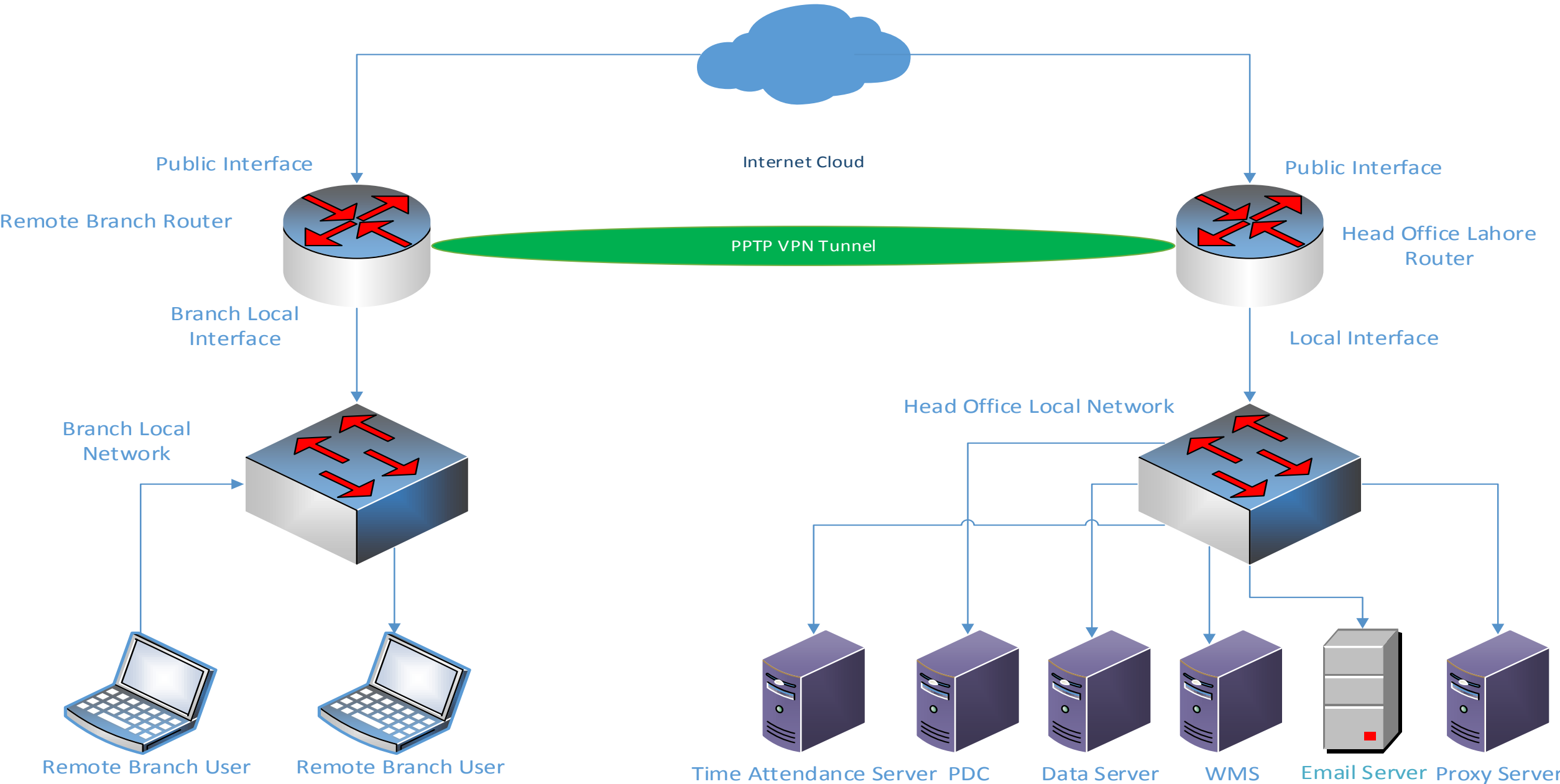
- **Site-Site VPN**

- Router-router VPN
- Required for two geographic locations.
- Works over Internet
- Connect two different LANs

- **Remote Access VPN**

- Works over internet
- Connects remote users from anywhere with Office Intranet
- Dialup set up required to connect

Site-Site VPN Diagram



Site-Site VPN Configuration for Head Office routerboard

```
/ interface l2tp-server server
set enabled=yes max-mtu=1460 max-mru=1460 \
authentication=pap,chap,mschap1,mschap2 default-profile=default-encryption
```

```
/ ppp secret
add name="user1" service=l2tp caller-id="" password="P@ssw0rd" \
profile=default-encryption local-address=192.168.3.254 \
remote-address=10.0.1.254 routes="" limit-bytes-in=0 limit-bytes-out=0 \
comment="" disabled=no
```

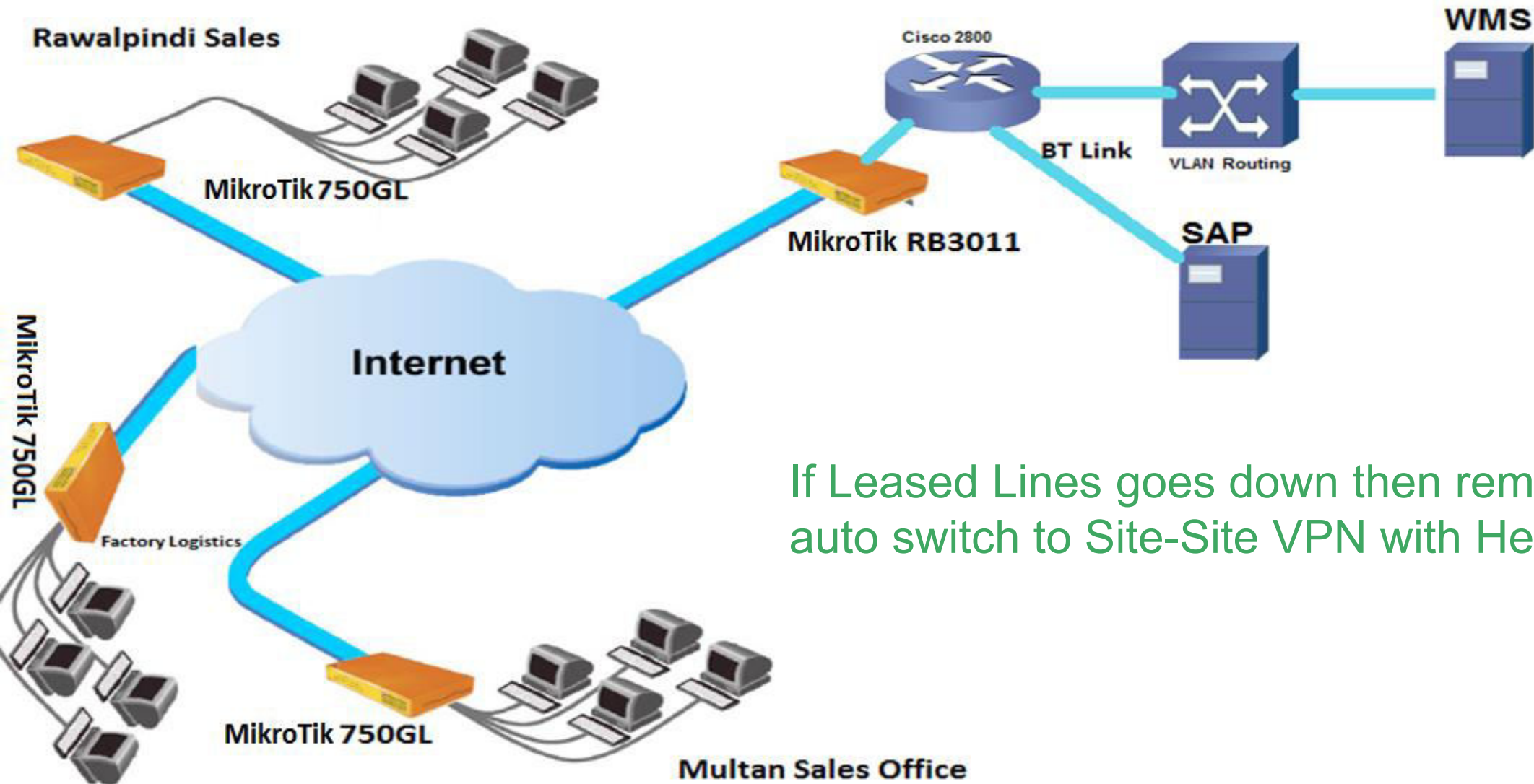
```
/ ip route
add dst-address=10.0.1.0/24 gateway=10.0.1.254 scope=255 target-scope=10 \
comment="" disabled=no
```


Site-Site VPN Remote branch configuration

```
/interface l2tp-client
add add-default-route=no allow=pap, chap, mschap1, mschap2 comment="" \
connect-to=80.80.80.110 disabled=no max-mru=1460 max-mtu=1460 \
mrru=disabled name="l2tp-out1" password="P@ssw0rd" \
profile=default-encryption user="user1"
```

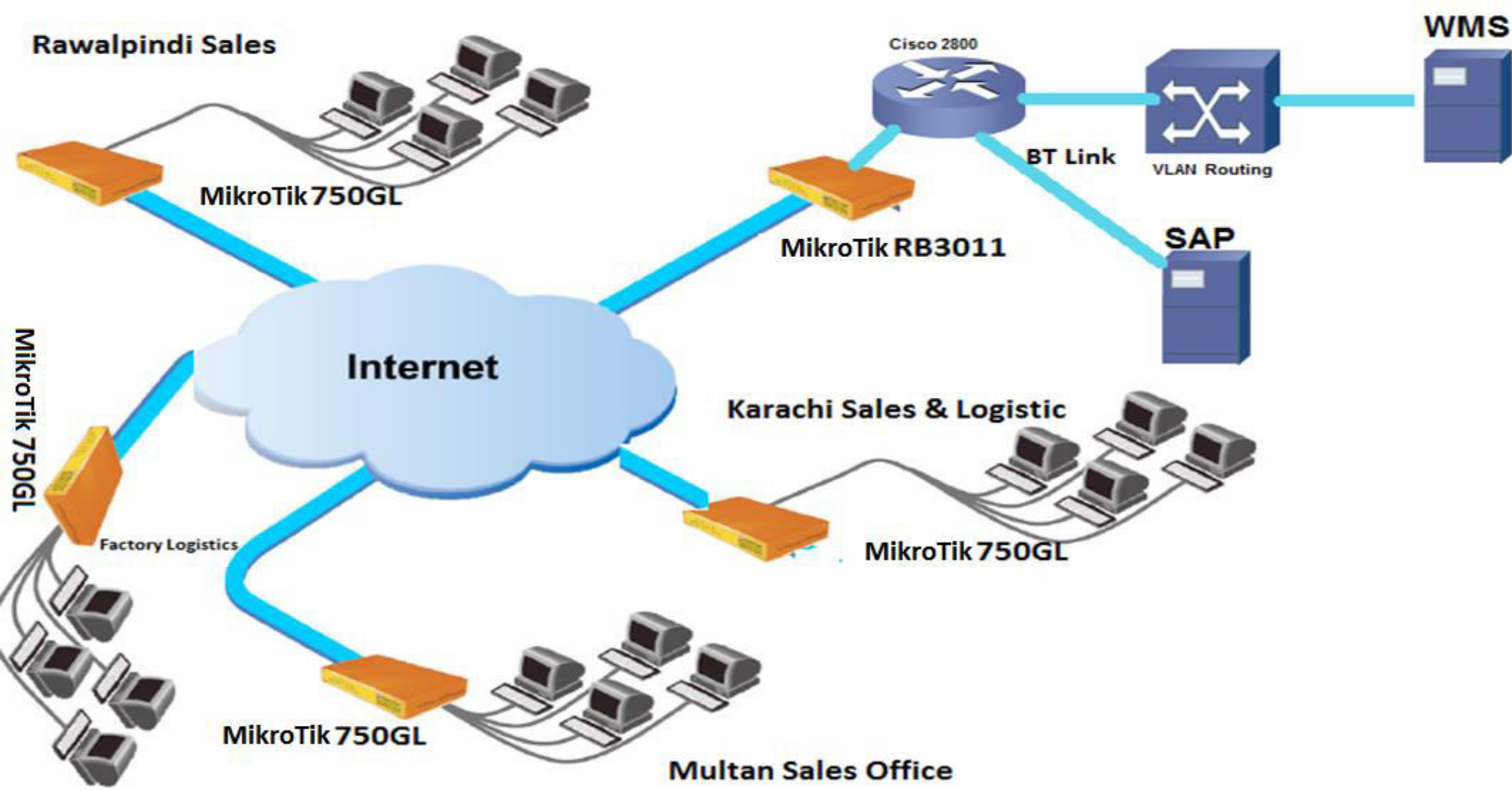
```
/ip route
add comment="" disabled=no distance=1 dst-address=192.168.2.0/23 \
gateway=192.168.3.254 scope=255 target-scope=10
```

Site-Site VPN at Public Network



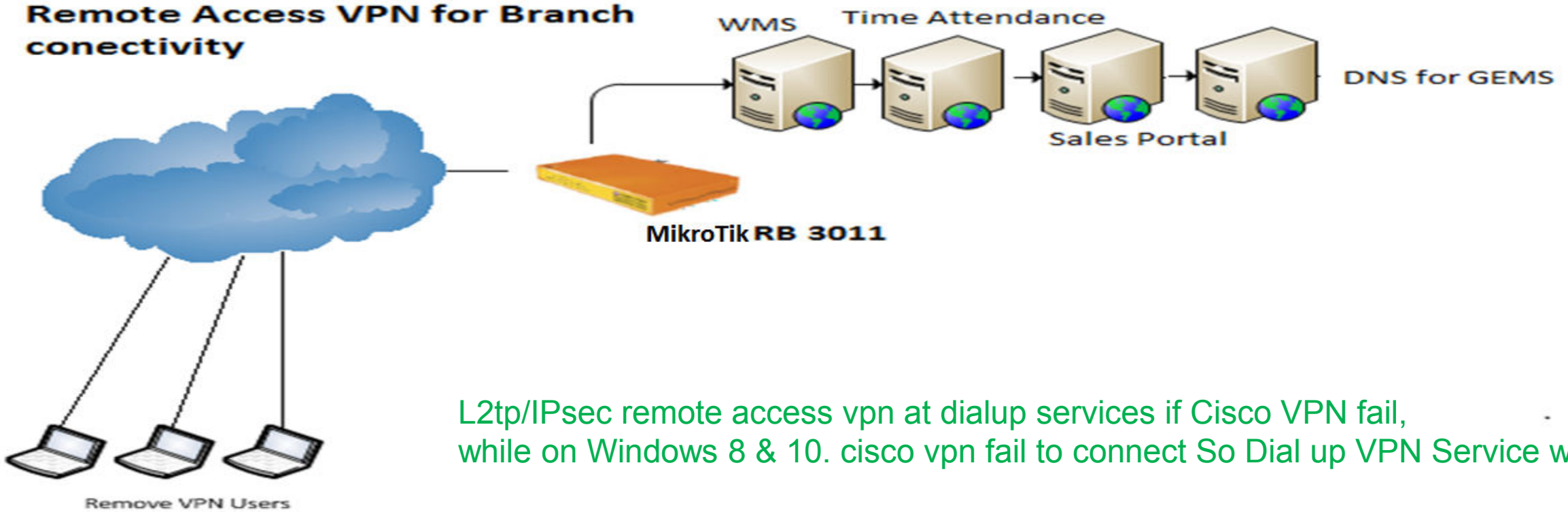
If Leased Lines goes down then remote sites auto switch to Site-Site VPN with Head Office

MikroTik Implemented Network Map



Network Diagram of Remote Access VPN at L2tp/IPsec

Remote Access VPN for Branch connectivity



L2tp/IPsec remote access vpn at dialup services if Cisco VPN fail, while on Windows 8 & 10. cisco vpn fail to connect So Dial up VPN Service works well

7 Steps to configure VPN with L2TP/IPsec

- Create IP Pool/VPN Pool
- Create profile for Remote Access VPN
- Create User credentials for Remote VPN Users
- Tunnel Encryption through IPsec
- IPsec Peers and Proposals
- Firewall settings for Outside access
- Adding Routes for VPN-User Traffic

Create IP Pool/VPN Pool

Haier@10.42.0.7 (MikroTik) - WinBox v6.32.2 on RB3011UiAS (arm)

Safe Mode

Quick Set

Interfaces

Bridge

PPP

Mesh

IP

MPLS

Routing

System

Queues

Files

Log

Radius

Tools

New Terminal

Partition

Make Supout .rif

Manual

Exit

IP Pool

Pools

Used Addresses



Name	Addresses	Next Pool
VPN-POOL	172.18.99.1-172.18.99.254	none
default-dhcp	192.168.88.10-192.168.88.254	none

IP Pool <VPN-POOL>

Name: VPN-POOL

Addresses: 172.18.99.1-172.18.99.254

Next Pool: none

OK

Cancel

Apply

Copy

Remove



Name	Local Address	Remote Address	Bridge	Rate Limit...	Only One
VPN-Profile	10.42.0.7	VPN-POOL			default
default					default
default-encr...	10.42.0.7	unknown			default

PPP Profile <VPN-Profile>

General Protocols Limits Queue

Name: VPN-Profile

Local Address: 10.42.0.7

Remote Address: VPN-POOL

Bridge:

Bridge Port Priority:

Bridge Path Cost:

Incoming Filter:

Outgoing Filter:

Address List:

DNS Server: 202.141.224.34
202.141.229.34

WINS Server:

- Change TCP MSS
 default no yes

OK
Cancel
Apply
Comment
Copy
Remove

Create User credentials for Remote VPN Users

Haier@10.42.0.7 (MikroTik) - WinBox v6.32.2 on RB3011UiAS (arm)

Safe Mode

Hide Passwords

RouterOS WinBox

Quick Set

Interfaces

Bridge

PPP

Mesh

IP

MPLS

Routing

System

Queues

Files

Log

Radius

Tools

New Terminal

Partition

Make Supout.rtf

Manual

Exit

PPP Authentication & Accounting

Name	Password	Service	Caller ID	Profile	Local Address	Remote Address	Last Logged Out
ihelum	*****	l2tp		VPN-Profile	10.42.0.7		May/27/2016 10:33:47
kamran	*****	l2tp		VPN-Profile	10.42.0.7		Jun/08/2016 09:19:18
kamranservice=l2tp call...	*****	any		default-encr...	10.42.0.7	10.90.0.1	
karachi2	*****	l2tp		VPN-Profile	10.42.0.7		Jun/13/2016 12:02:11
karachicsd2	*****	l2tp					Jun/08/2016 12:55:50
khi_warehouse	*****	l2tp					Jun/12/2016 22:50:39
multan	*****	l2tp					Mar/14/2016 13:42:34
multan2	*****	l2tp					Jun/13/2016 15:55:14
multanwh	*****	l2tp					Jun/13/2016 17:14:14
multanwh1	*****	l2tp					
nadeemmnt	*****	l2tp					Apr/12/2016 16:00:24
peshawarlog	*****	l2tp					May/24/2016 18:34:10
peshawarsales	*****	l2tp					May/07/2016 01:00:10
peshawarwh	*****	l2tp					Jun/13/2016 13:15:27
qtalog	*****	l2tp					Jun/08/2016 07:25:12
rawalpindi	*****	l2tp					Jun/13/2016 13:00:57
rawalpindisale	*****	l2tp					
sahiwallog	*****	l2tp					Jun/11/2016 13:51:01
sahiwalsale2	*****	l2tp					May/07/2016 03:15:02
sahiwalsale4	*****	l2tp					Jun/13/2016 16:04:58
sahiwalsales	*****	l2tp					Jun/13/2016 16:54:38
sahiwalsales3	*****	l2tp					Jun/09/2016 11:34:40
sahiwalwh	*****	l2tp					
sargodha	*****	l2tp					Jun/13/2016 10:37:47
sargodhasale	*****	l2tp					May/03/2016 05:10:13
sgdsale	*****	l2tp					Jun/13/2016 15:06:17
sgdsales	*****	l2tp					
sgdwh	*****	l2tp					
sialkot	*****	l2tp					Apr/28/2016 11:49:18
sialkotcsd	*****	l2tp		VPN-Profile	10.42.0.7		
sialkotcsd1	*****	l2tp		VPN-Profile	10.42.0.7		Apr/25/2016 16:55:12
sialkotsale	*****	l2tp		VPN-Profile	10.42.0.7		
sialkotwh	*****	l2tp		VPN-Profile	10.42.0.7		Jun/09/2016 08:45:34
sukkur	*****	l2tp		VPN-Profile	10.42.0.7		Feb/24/2016 16:32:31
sukkursale	*****	l2tp		VPN-Profile	10.42.0.7		Jun/13/2016 16:42:06
tariq	*****	l2tp		VPN-Profile	10.42.0.7		May/01/2016 10:06:19
umair	*****	l2tp		VPN-Profile	10.42.0.7		Jun/13/2016 14:23:36

55 items (1 selected)

PPP Secret <umair>

Name:

Password:

Service:

Caller ID:

Profile:

Local Address:

Remote Address:

Routes:

Limit Bytes In:

Limit Bytes Out:

Last Logged Out:

enabled

OK Cancel Apply Disable Comment Copy Remove

Tunnel Encryption through IPsec

The screenshot displays the Mikrotik WinBox interface for configuring IPsec. The left sidebar shows the navigation menu with 'IPsec' selected, indicated by a white arrow. The main window shows the 'IPsec Peer' configuration dialog for the peer address 0.0.0.0/0. The configuration includes the following details:

- Address:** 0.0.0.0/0
- Port:** 500
- Local Address:** ::
- Auth. Method:** pre shared key
- Secret:** [masked]
- Policy Template Group:** default
- Exchange Mode:** main l2tp
- Send Initial Contact:**
- NAT Traversal:**
- My ID:** auto
- Proposal Check:** obey
- Hash Algorithm:** sha1
- Encryption Algorithm:**
 - des
 - 3des
 - aes-128
 - aes-192
 - aes-256
 - blowfish
 - camellia-128
 - camellia-192
 - camellia-256
- Mode Configuration:** [dropdown]
- DH Group:** modp1024
- Generate Policy:** port override
- Lifetime:** 1d 00:00:00

The status bar at the bottom indicates '1 item (1 selected)' and 'enabled'.

IPsec Peers and Proposals

Haier@10.42.0.7 (MikroTik) - WinBox v6.32.2 on RB3011UiAS (arm)

RouterOS WinBox

Safe Mode

Hide Passwords

IPsec

Policies Groups Peers Remote Peers Mode Configs Proposals Installed SAs Keys Users

Address	Port	Propos...	Hash Al...	Encrypt...
0.0.0.0/0	500	obey	sha1	3des a...

1 item (1 selected)

IPsec Proposal <default>

Name: default

Auth. Algorithms

- md5
- sha1
- sha256
- sha512
- null

Encr. Algorithms

- null
- 3des
- aes-192 cbc
- aes-128 cbc
- aes-256 cbc
- aes-192 gcm
- aes-128 gcm
- aes-256 gcm
- des
- aes-128 cbc
- aes-256 cbc
- aes-128 ctr
- aes-256 ctr
- aes-192 gcm
- aes-256 gcm
- twofish
- camellia-128
- camellia-192
- camellia-256
- aes-128 ctr
- aes-256 ctr

Lifetime: 00:30:00

PFS Group: modp1024

IPsec Peer <0.0.0.0/0>

Address: 0.0.0.0/0

Port: 500

Local Address: ::

Auth. Method: pre shared key

Passive

Secret: *****

Policy Template Group: default

Exchange Mode: main I2tp

Send Initial Contact

NAT Traversal

My ID: auto

Proposal Check: obey

Hash Algorithm: sha1

Encryption Algorithm

- des
- 3des
- aes-128
- aes-192
- aes-256
- blowfish
- camellia-128
- camellia-192
- camellia-256

Mode Configuration:

DH Group: modp1024

Generate Policy: port override

Lifetime: 1d 00:00:00

Lifeytes:

Firewall settings for Outside access

Haier@10.42.0.7 (MikroTik) - WinBox v6.32.2 on RB3011UiAS (arm)

RouterOS WinBox

Safe Mode

Hide Passwords

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

Reset Counters Reset All Counters

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port
0	acc...	input	172.18.99.0/24	10.42.0.7		

1 item (1 selected)

Firewall Rule <172.18.99.0/24->10.42.0.7>

General Advanced Extra Action Statistics

Chain:

Src. Address: 172.18.99.0/24

Dst. Address: 10.42.0.7

Protocol: udp

Src. Port:

Dst. Port: 500, 1701, 450

Any. Port:

P2P:

In. Interface: *mitinet1*

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Adding Routes for VPN-User Traffic and VPN Done

Haier@10.42.0.7 (MikroTik) - WinBox v6.32.2 on RB3011UiAS (arm)

RouterOS WinBox

Safe Mode

Hide Passwords

Route <172.18.99.0/24>

General | Attributes

Dest. Address: 172.18.99.0/24

Gateway: local

Check Gateway: ping

Type: unicast

Distance: 1

Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:

enabled active static

OK
Cancel
Apply
Disable
Comment
Copy
Remove

Dialup connection for VPN User

Change your networking settings



Set up a new connection or network

Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.



Connect to a network

Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.



Choose homegroup and sharing options

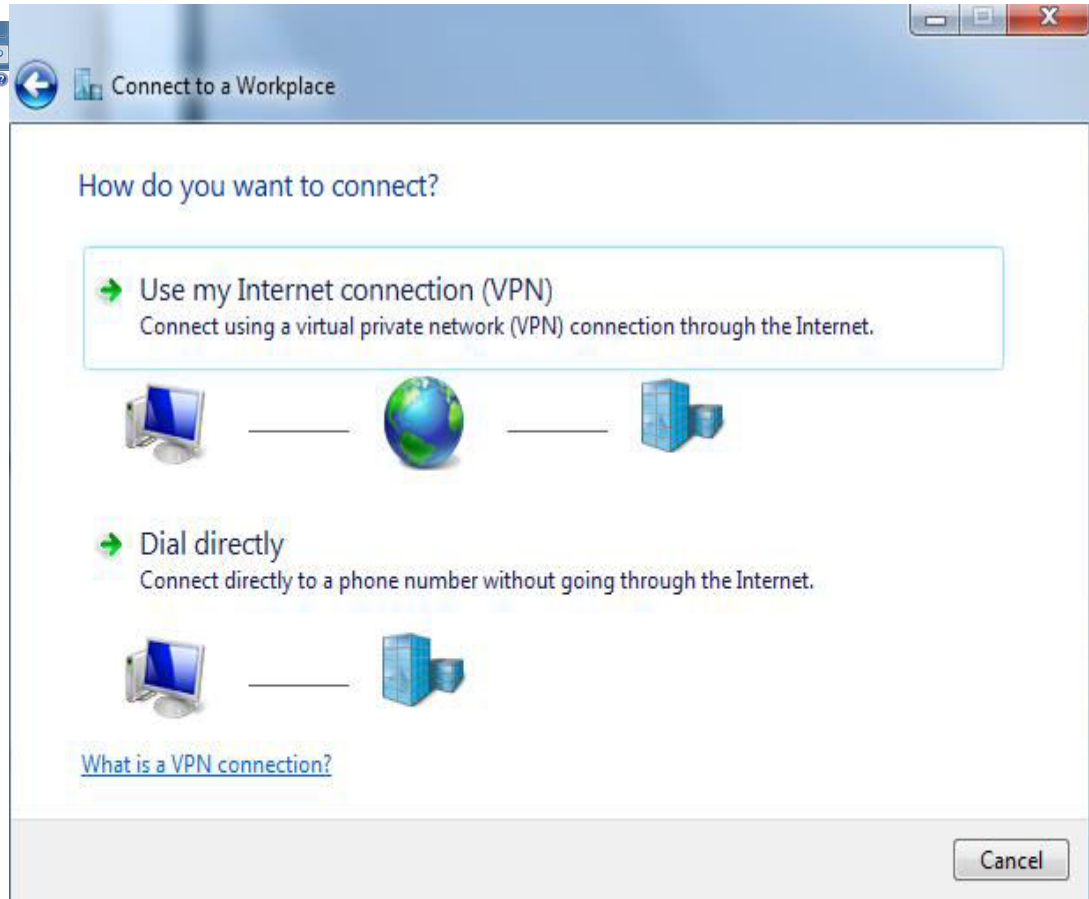
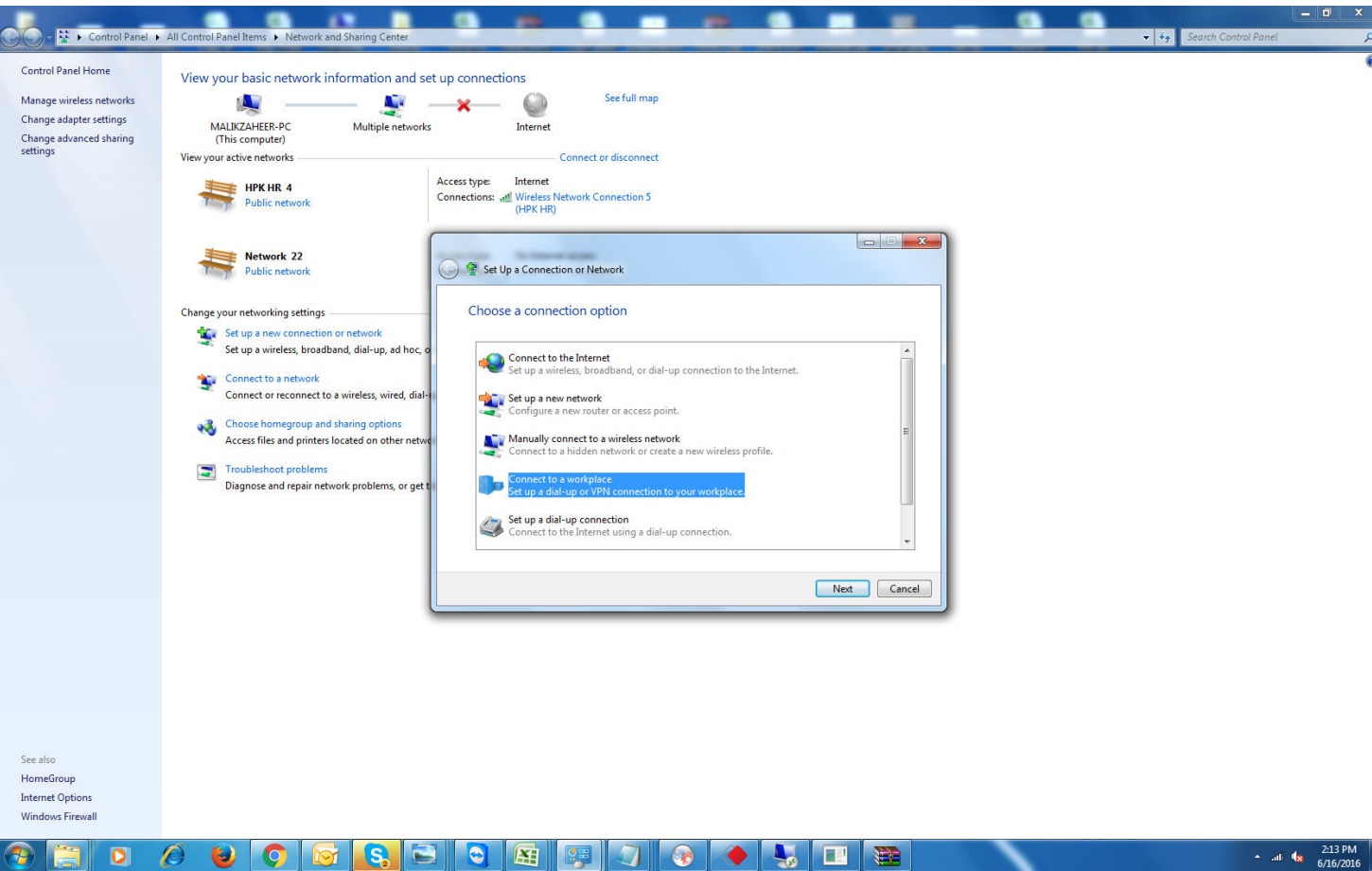
Access files and printers located on other network computers, or change sharing settings.



Troubleshoot problems

Diagnose and repair network problems, or get troubleshooting information.

Dialup Connection



Putting VPN Server Address

Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: [Example:Contoso.com or 157.54.0.1 or 3ffe:1234::1111]

Destination name: VPN Connection 2

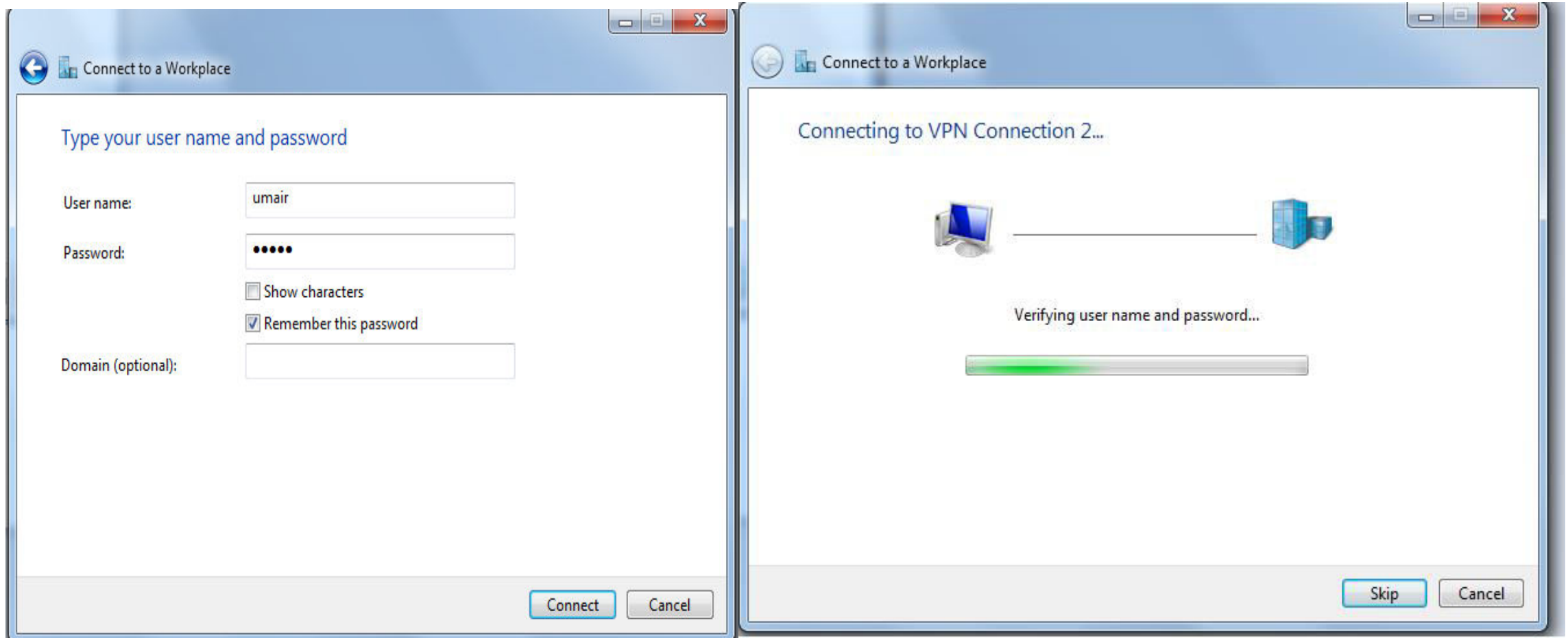
Use a smart card

Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

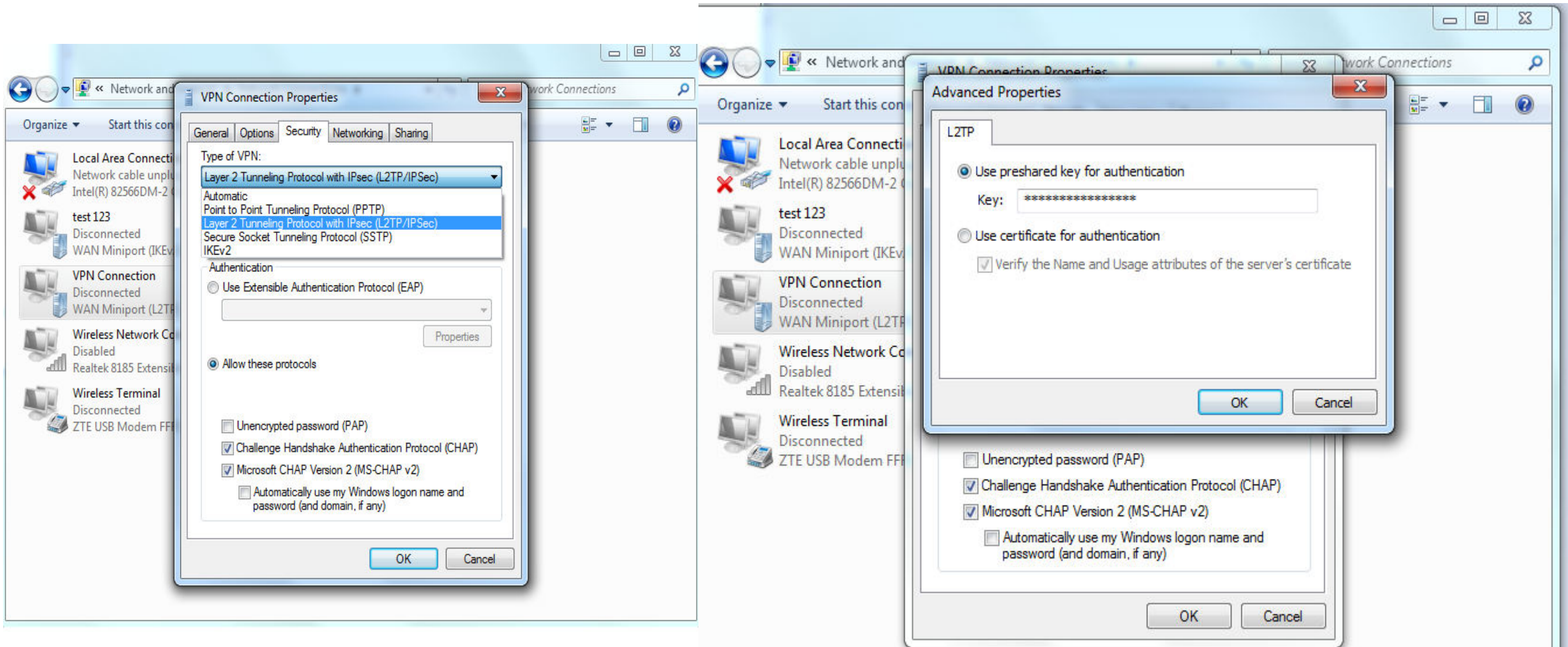
Don't connect now, just set it up so I can connect later

Next Cancel

Dialup User Credentials

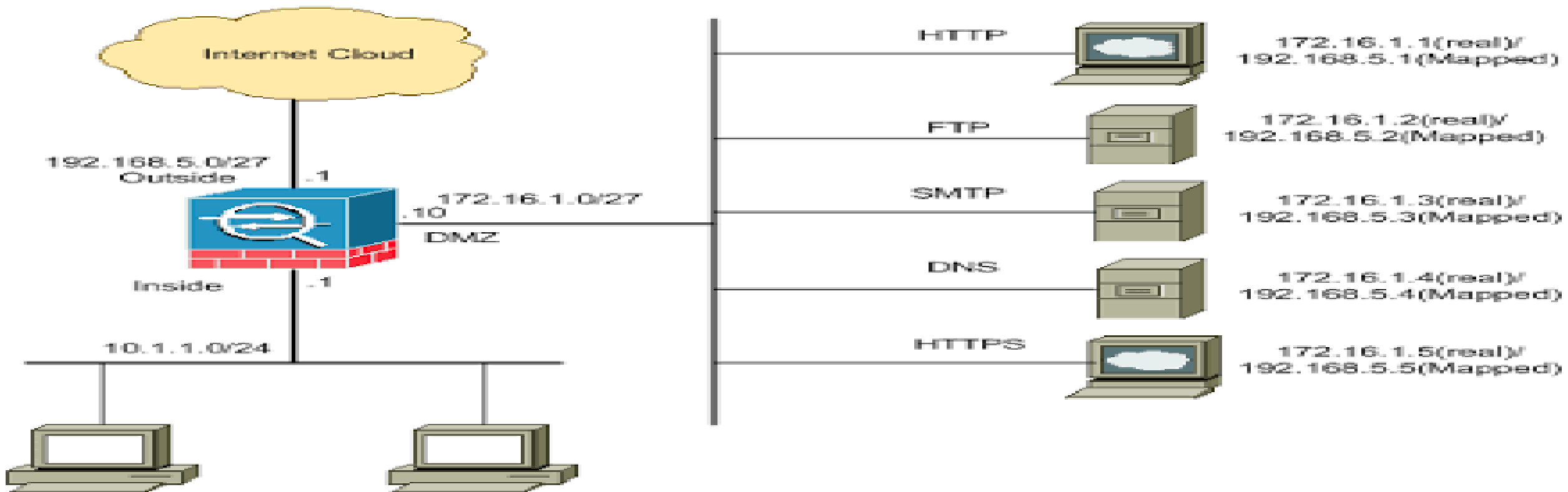


Setting IPsec preshared Key



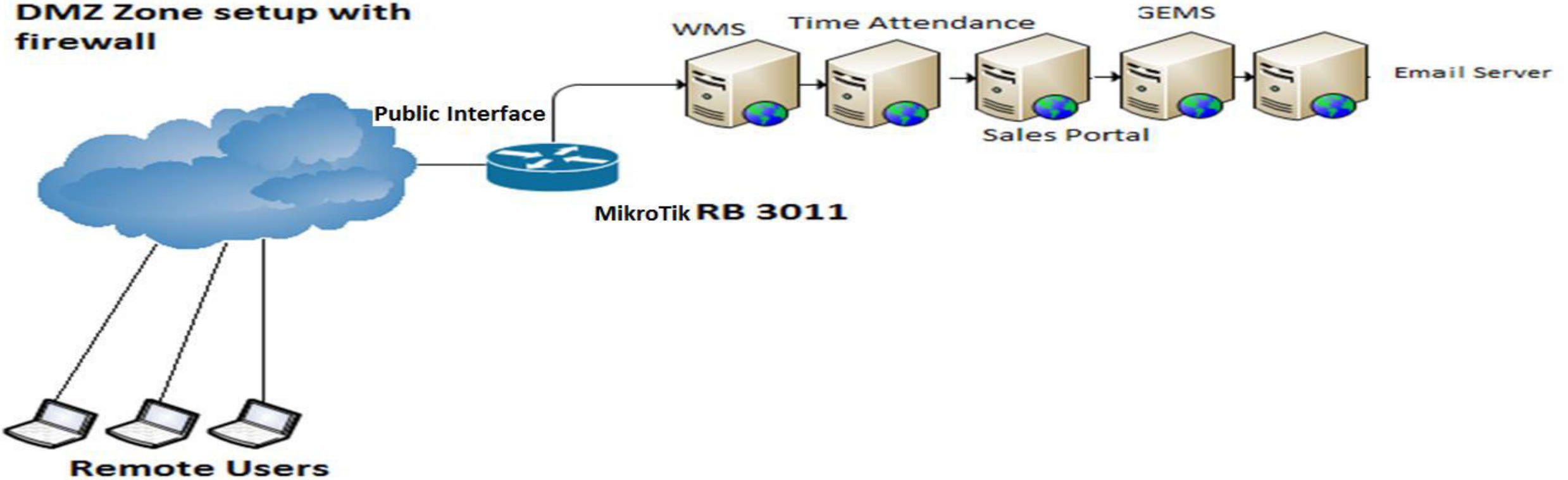
DMZ Network Zone

- Demilitarized zone (DMZ) is a host or network segment located in a "neutral zone" between the Internet and an organization's intranet (private network). It prevents outside users from gaining direct access to an organization's internal network while not exposing a web, email or DNS server directly to the Internet.



DMZ Zone firewall setup Network Diagram

DMZ Zone setup with firewall



DMZ Network Setup LAB

Haier@10.42.0.7 (MikroTik) - WinBox v6.32.2 on RB3011UiAS (arm)

RouterOS WinBox

Safe Mode

Hide Passwords

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

Reset Counters Reset All Counters

NAT Rule < [redacted]

General Advanced Extra Action Statistics

Chain: dstnat

Src. Address: [redacted]

Dst. Address: [redacted]

Protocol: 6 (tcp)

Src. Port: [redacted]

Dst. Port: 91

Any. Port: [redacted]

In. Interface: [redacted]

Out. Interface: [redacted]

Packet Mark: [redacted]

Connection Mark: [redacted]

Routing Mark: [redacted]

Routing Table: [redacted]

Connection Type: [redacted]

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

#	def	Packets
0		20 520
1		6
2		0
3		45
4		54
5		0

6 items (

Dst-Nat for Local Server and DMZ Setup done

Haier@10.42.0.7 (MikroTik) - WinBox v6.32.2 on RB3011UiAS (arm)

RouterOS WinBox interface showing Firewall NAT Rule configuration and statistics.

Firewall NAT Rule Configuration:

- General tab selected
- Action: dst-nat
- Log:
- Log Prefix: [empty]
- To Addresses: 10.42.0.20
- To Ports: 91

Statistics Table:

Packets	Count
21 119	6
	0
	49
	57
	0

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters.

Time Attendance System through DMZ setup done

Human Capital Management Software
TIMETRAX™
www.TimeTrax.com.pk

Sign in

Username
[Redacted]

Password
[Redacted]

Login

[Can't access your account?](#)

Serving over 500 satisfied clients with this robust Human Resource Management system across Pakistan in 27 cities and deployed in 17 countries across the globe; including UAE, South Africa, Korea & Brazil, with embedded payroll logic for various industries, TimeTrax is the ultimate software solution for Integrated Attendance, Payroll, Leave & Travel Management. We are proudly assisting companies in building transparency into employee productivity for the last 14 years.

Questions and Answers



Contact Details

Umair Masood

Manager Network & IT Support

Haier Pakistan(Pvt)Ltd

8th Floor, Mega Tower, Main Boulevard Gulberg-II

Lahore

Email: umair.masood@haier.com.pk , umairmian@gmail.com

Cell Phone: +923142437094 , +923347137377

facebook: <https://www.facebook.com/umair.masood7>