PowerLink Bandwidth Aggregation Redundant WAN Link and VPN Fail-Over Solutions

Find your network example:

1. Basic network with PowerLink and 2 WAN lines - click here

2. Add a web server to the LAN - click here

3. Add a web, mail and pptp server to the LAN - click here

4. Duplicate web servers* on the LAN - click here

5. Basic network with PowerLink, 2 WAN lines and a Firewall - click here

6. Add Ipsec server to the Firewall - click here

7. Activate Authoritative DNS server on the PowerLink - click here

** Duplicate servers allow two or more servers (i.e. two mail servers or two web servers)

MORE

ASTROCOM

Find your network example:

8. VPN Failover using DNS - click here

ASTROCOM

Network Scenario #1

Objective: to achieve bandwidth aggregation and outbound redundancy for a simple LAN with no firewall and no internal servers hosted.

Network topology and services:

- 2 ADSL lines to 2 ISPs
- PowerLink
- Workstations in the LAN
- typical traffic: web browsing, e-mail, file transfer
- DNS, web and mail services hosted outside the LAN, at the ISP's site

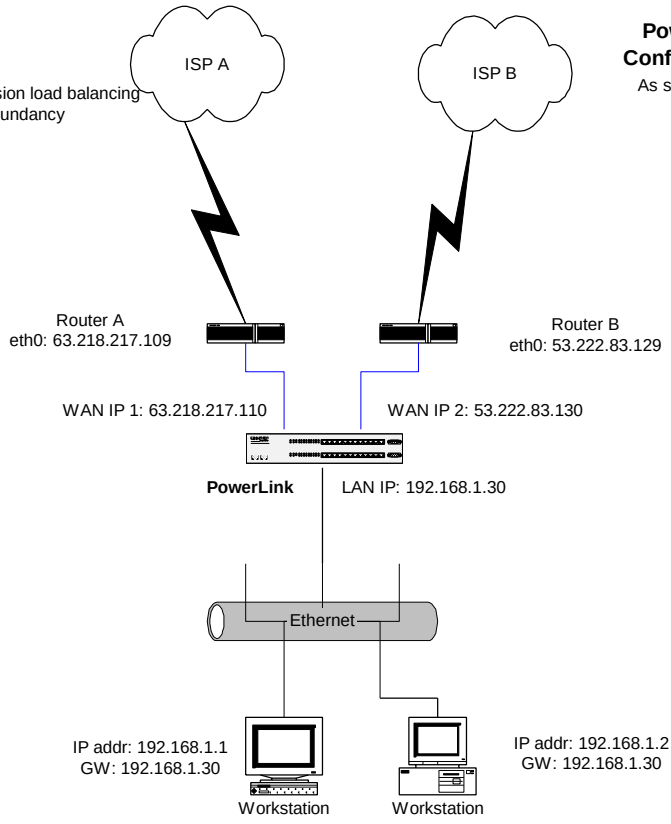
ASTROCOM

Network Scenario #1

Basic Network

Features: - Outbound Session load balancing
- Outbound Redundancy

PowerLink Configuration:
As shown



Back to index

ASTROCOM

Network Scenario #2

Objectives: to achieve bandwidth aggregation and outbound redundancy for a LAN with a web server and no firewall. Further, to increase the bandwidth available for the web server.

Network topology and services:

- 2 ADSL lines to 2 ISPs
- PowerLink
- Workstations in the LAN
- typical traffic out: web browsing, e-mail, file transfer
- typical traffic in: web access, e-mail
- DNS and mail services are hosted outside the LAN, at the ISP's site

ASTROCOM

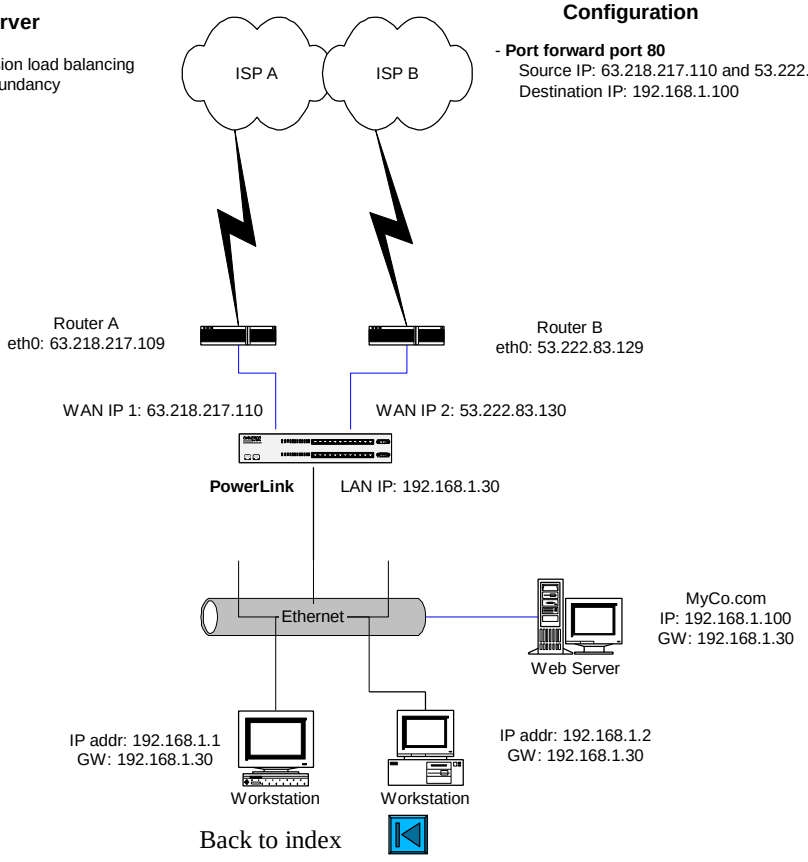
Network Scenario #2

Network with one server

Features: - Outbound Session load balancing
- Outbound Redundancy

PowerLink Configuration

- **Port forward port 80**
  Source IP: 63.218.217.110 and 53.222.83.130
  Destination IP: 192.168.1.100



Back to index

ASTROCOM

Network Scenario #3

Objectives: to achieve bandwidth aggregation and outbound redundancy for a LAN with a web server, mail server and a VPN server (using PPTP or IPSEC).

Network topology and services:

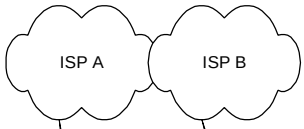
- 2 ADSL lines to 2 ISPs
- PowerLink
- Workstations in the LAN
- typical traffic out: web browsing, e-mail, file transfer
- typical traffic in: pptp, web access, e-mail, file transfer
- DNS authority outside the LAN, at the ISP's site

ASTROCOM

Network Scenario #3

Network with three servers

Features: - Outbound Session load balancing
- Outbound Redundancy



PowerLink Configuration

- **Port forward port 80**
  Source IP: 63.218.217.110 and 53.222.83.130
  Destination IP: 192.168.1.100
- **Port forward port 25**
  Source IP: 63.218.217.110 and 53.222.83.130
  Destination IP: 192.168.1.101
- **Port forward port 1723**
- **Protocol forward 47**
  Source IP: 63.218.217.110 and 53.222.83.130
  Destination IP: 192.168.1.102

Router A
eth0: 63.218.217.109

Router B
eth0: 53.222.83.129

WAN IP 1: 63.218.217.110

WAN IP 2: 53.222.83.130

PowerLink LAN IP: 192.168.1.30

Mail Server
mail.MyCo.com
IP: 192.168.1.101
GW: 192.168.1.30

PPTP Server
vpn.MyCo.com
IP: 192.168.1.102
GW: 192.168.1.30

Ethernet

Web Server
MyCo.com
IP: 192.168.1.100
GW: 192.168.1.30

IP addr: 192.168.1.1
GW: 192.168.1.30

Workstation

Workstation
IP addr: 192.168.1.2
GW: 192.168.1.30

Back to index

ASTROCOM

Network Scenario #4

Objectives: to achieve bandwidth aggregation and outbound redundancy for a LAN with 2 web servers and no firewall. Further, to increase the bandwidth available for the web servers.

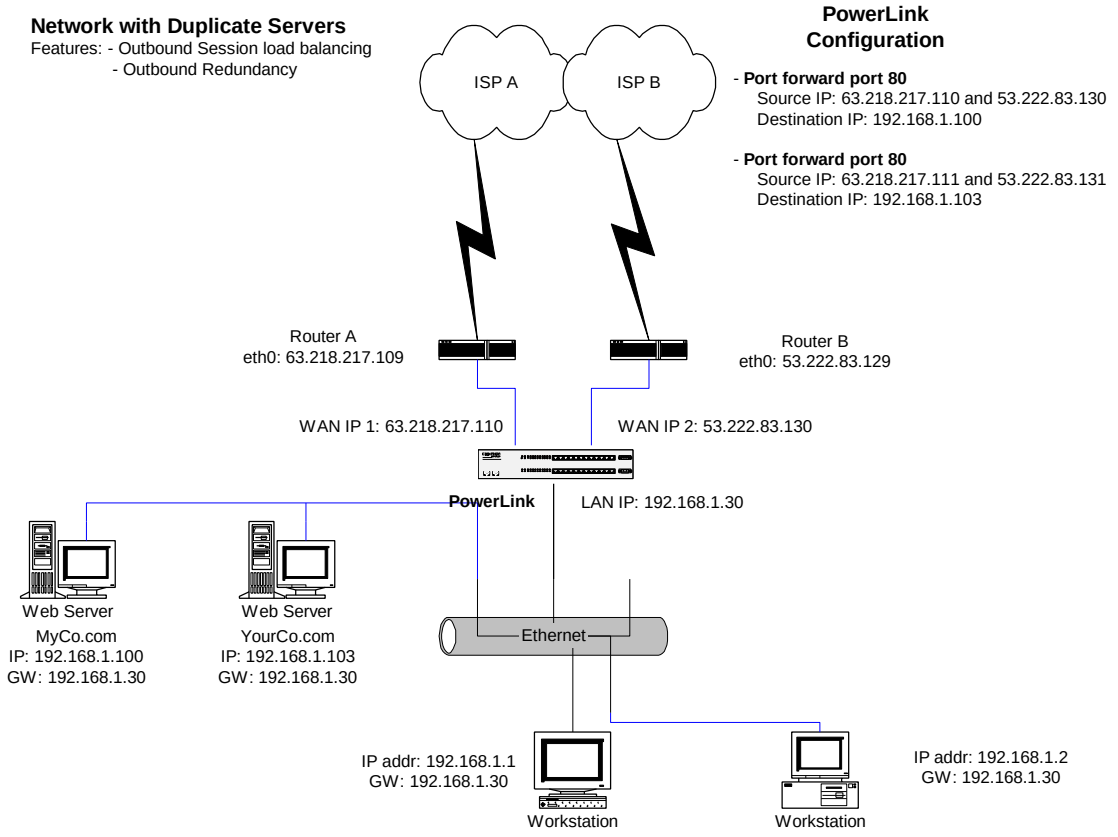
Network topology and services:

- 2 ADSL lines to 2 ISPs
- PowerLink
- Workstations in the LAN
- typical traffic out: web browsing, e-mail, file transfer
- typical traffic in: web access, e-mail
- DNS and mail services are hosted outside the LAN, at the ISP's site

ASTROCOM

Network Scenario #4

Network with Duplicate Servers
Features: - Outbound Session load balancing
- Outbound Redundancy



Back to index

ASTROCOM

Network Scenario #5

Objectives: to achieve bandwidth aggregation and outbound redundancy for a LAN with a firewall. To increase the bandwidth available for the workstations while maintaining security.

Network topology and services:

- 2 ADSL lines to 2 ISPs
- PowerLink
- Workstations in the LAN
- typical traffic out: web browsing, e-mail, file transfer
- typical traffic in: e-mail and file transfer
- DNS, web and mail services are hosted outside the LAN, at the ISP's site

ASTROCOM

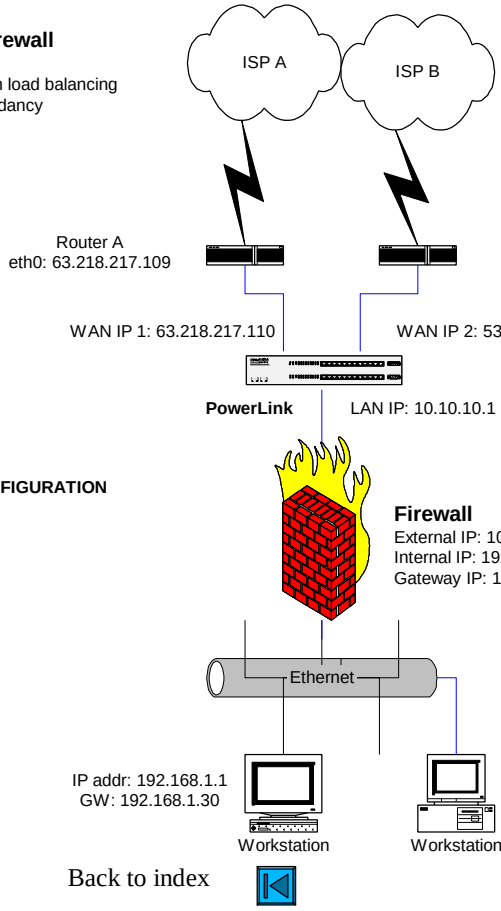
Network Scenario #5

Basic Network with Firewall

Features: - Outbound Session load balancing
- Outbound Redundancy
- LAN Security

PowerLink Configuration

As shown



FIREWALL CONFIGURATION

As shown

Back to index

Network Scenario #6

Objectives: to achieve bandwidth aggregation and outbound redundancy for a LAN with a web server. To increase the bandwidth available for the web server and assure network security with a firewall.

Network topology and services:

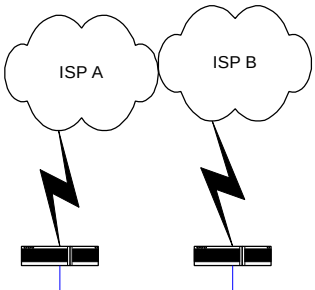
- 2 ADSL lines to 2 ISPs
- PowerLink
- Workstations in the LAN
- typical traffic out: web browsing, e-mail, file transfer
- typical traffic in: web access, e-mail
- DNS and mail services are hosted outside the LAN, at the ISP's site

ASTROCOM

Network Scenario #6

Network with Firewall and one server

Features: - Session load balancing
- Outbound Redundancy
- LAN Security



POWERLINK CONFIGURATION

- **Port forward port 80**
  Source IP: 63.218.217.110 and 53.222.83.130
  Destination IP: 10.10.10.2

Router A
eth0: 63.218.217.109

Router B
eth0: 53.222.83.129

WAN IP 1: 63.218.217.110

WAN IP 2: 53.222.83.130

PowerLink

LAN IP: 10.10.10.1

FIREWALL CONFIGURATION

Port 80 left open for incoming traffic
NAT- Source IP: 10.10.10.2
Dest IP: 192.168.1.30

Firewall
External IP: 10.10.10.2
Internal IP: 192.168.1.30
Gateway IP: 10.10.10.1

Ethernet

MyCo.com
IP: 192.168.1.100
GW: 192.168.1.30

Web Server

IP addr: 192.168.1.1
GW: 192.168.1.30

Workstation

IP addr: 192.168.1.2
GW: 192.168.1.30

Workstation

Back to index

Network Scenario #7

Objectives: to achieve bandwidth aggregation and inbound and outbound redundancy for a LAN with a web server. To increase the bandwidth available for the web server while maintaining remote clients security and DNS (inbound) redundancy.

Network topology and services:

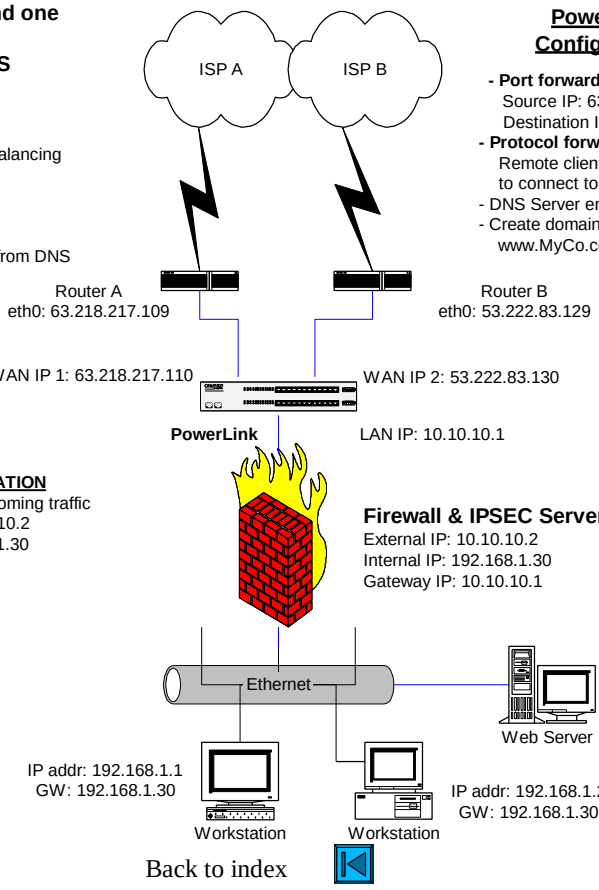
- 2 ADSL lines to 2 ISPs
- PowerLink configured as DNS authoritative server
- Workstations in the LAN
- typical traffic out: web browsing, e-mail, file transfer
- typical traffic in: web access, e-mail and file transfer
- mail services are hosted outside the LAN, at the ISP's site

ASTROCOM

Network Scenario #7

Network with IPsec Firewall and one LAN server
PowerLink is Authoritative DNS Server

Features:
- Outbound & Inbound Session load balancing
- Outbound & Inbound Redundancy
- LAN Security
- VPN access of LAN
- Automatic failover of VPN tunnels
- Instant removal of faulty WAN lines from DNS advertisement



Firewall & IPSEC Server
External IP: 10.10.10.2
Internal IP: 192.168.1.30
Gateway IP: 10.10.10.1

MyCo.com
IP: 192.168.1.100
GW: 192.168.1.30

PowerLink Configuration

- **Port forward port 80 & 500**
  Source IP: 63.218.217.110 and 53.222.83.130
  Destination IP: 10.10.10.2
- **Protocol forward protocol 50**
  Remote clients use 63.218.217.110 or 53.222.83.130 to connect to the VPN server
- DNS Server enabled
- Create domain MyCo.com
  www.MyCo.com = 63.218.217.110 & 53.222.83.130

FIREWALL CONFIGURATION
Port 80 left open for incoming traffic
NAT- Source IP: 10.10.10.2
Dest IP: 192.168.1.30

Back to index

ASTROCOM

Network Scenario #8

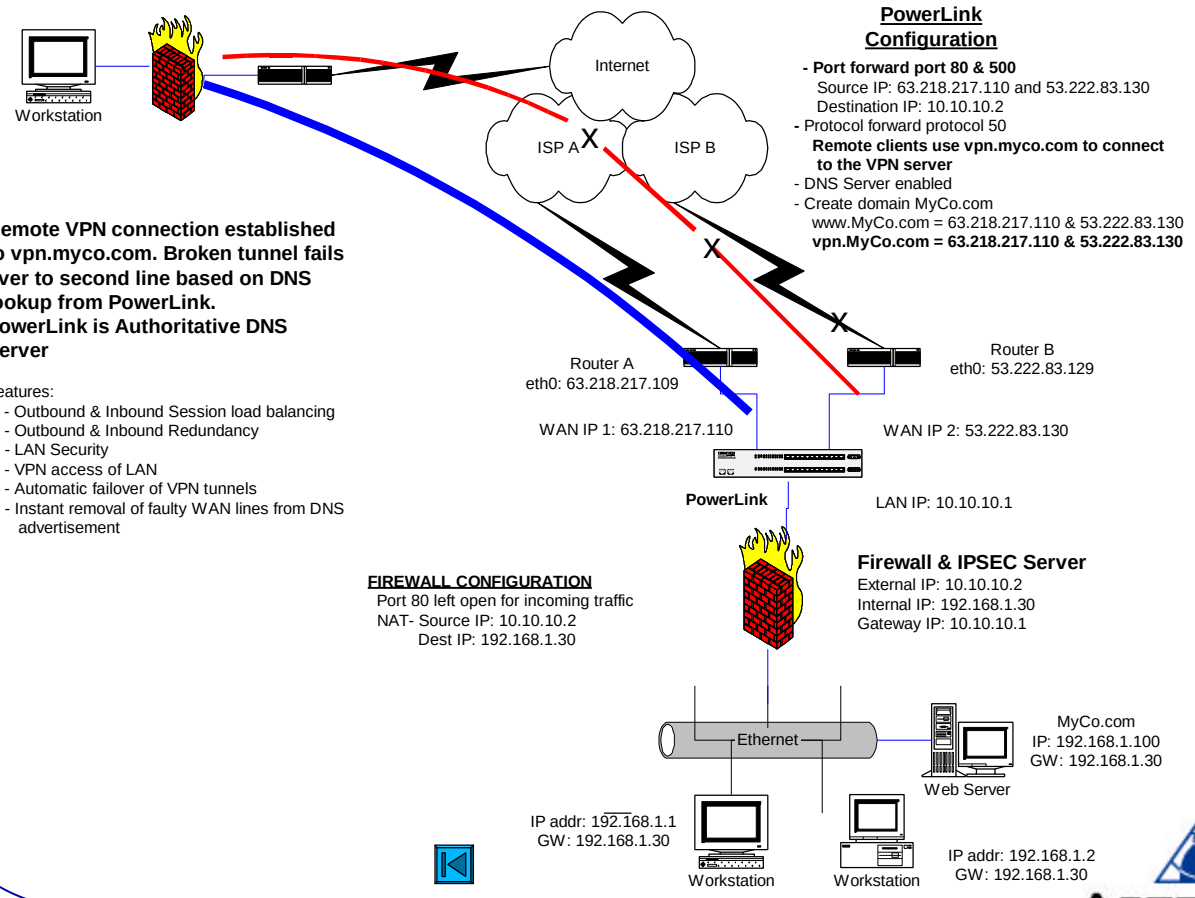
Objectives: to achieve automatic failover of VPN tunnels.

Network topology and services:

- 2 ADSL lines to 2 ISPs
- PowerLink configured as DNS authoritative server
- Workstations in the LAN
- VPN clients establishing connection based on vpn.myco.com

ASTROCOM

Network Scenario #8



PowerLink Configuration

- **Port forward port 80 & 500**
  Source IP: 63.218.217.110 and 53.222.83.130
  Destination IP: 10.10.10.2
- Protocol forward protocol 50
  Remote clients use vpn.myco.com to connect to the VPN server
- DNS Server enabled
- Create domain MyCo.com
  www.MyCo.com = 63.218.217.110 & 53.222.83.130
  vpn.MyCo.com = 63.218.217.110 & 53.222.83.130

Remote VPN connection established to vpn.myco.com. Broken tunnel fails over to second line based on DNS lookup from PowerLink. PowerLink is Authoritative DNS Server

Features:
- Outbound & Inbound Session load balancing
- Outbound & Inbound Redundancy
- LAN Security
- VPN access of LAN
- Automatic failover of VPN tunnels
- Instant removal of faulty WAN lines from DNS advertisement

FIREWALL CONFIGURATION
Port 80 left open for incoming traffic
NAT- Source IP: 10.10.10.2
Dest IP: 192.168.1.30

Firewall & IPSEC Server
External IP: 10.10.10.2
Internal IP: 192.168.1.30
Gateway IP: 10.10.10.1

ASTROCOM