Features of this design

- A ready-made core network design

External connectivity: (upstream ISPs, peers, links to other sites)

Dual-attached networks (upstream ISPs, peers, links to other sites)

Single-attached networks

1. Network within a single site. If you have multiple sites, replicate this design at each site

2. Links (switch ports) can be 10M, 100M, gigabit, or any combination

3. Whenever you run out of router ports, just plug another router (or pair) into the core

4. Core switches give you very high aggregate bandwidth e.g. 2 routers, each with two 100M interfaces = 1000M total bandwidth

5. Core switches give you very high aggregate bandwidth e.g. 2 routers, each with two 100M interfaces = 1000M total bandwidth

6. All routers are dual-attached; can withstand a failure of any single interface, cable, or core

7. Traffic is always active down both paths, so you have confidence that they are working

8. OSPF provides end-to-end view of each link

9. OSPF provides end-to-end view of each link

10. All routers are dual-attached; can withstand a failure of any single interface, cable, or core

11. When you run out of router ports, just plug another router (or pair) into the core

12. Can power down and exchange core switches one at a time, with minimal disruption to network

13. Flexibility to mix and match routers; qualities limited to part of network

14. Flexibility to mix and match routers; qualities limited to part of network

15. Observation: all packets go through no more than 2 routers to reach their destination.

16. Observation: all packets go through no more than 2 routers to reach their destination.

17. Traffic is always active down both paths, so you have confidence that they are working
External connectivity (upstream ISPs, peers, links to other sites)

Each router is dual-homed: one ethernet interface into each core. If you only have a single border router that's fine, there will be no BGP, just a static default to your upstream provider. It's a single point of failure of course. If you have multiple border/backbone routers, they will iBGP peer with each other. Your iBGP peering sessions should be between loopback interfaces on your routers. This is so that if connectivity into the core switches changes, it does not affect any iBGP sessions.

Border routers connect to your upstream providers or peers. Backbone routers connect to WAN links between your sites. As far as this design is concerned, they are the same.

neighbor x.x.x.x remote-as yyyy
neighbor x.x.x.x update-source Loopback0

The key piece to look for is non-blocking performance. The scalability depends on being able to pump more and more traffic through the switch without it losing packets.

Appropriate number and speed of ports for the types of routers you want to connect

Choose appropriate core, so that 10G is more expensive than 1G and 1G even more expensive than 100M. For ease of management use minimal bandwidth, e.g. non-defaulted 64 or 128 Kbps.

Use MD5 authentication. Disable OSPF except on necessary interfaces.

Try to keep routing within one site with minimal redistribution. This will allow you to use one BGP peering session to communicate between all of your routers. If you follow these recommendations, the router with the lowest defaultroute metric will be the "preferred" router for outgoing traffic from the access routers. Routing of outgoing traffic may not be optimal - it may hit the 'wrong' router first and be bounced to the right one - but this is typically not a problem.

Use MD5 authentication. Disable OSPF except on necessary interfaces.

Each router only should originate defaultrouter into the OSPF cloud. Never attempt to redistribute BGP into OSPF!

The key feature to look for is non-blocking performance. The scalability depends on being able to pump more and more traffic through the switch without it losing packets.

Try to keep routing within one site with minimal redistribution. This will allow you to use one BGP peering session to communicate between all of your routers. If you follow these recommendations, the router with the lowest defaultroute metric will be the "preferred" router for outgoing traffic from the access routers. Routing of outgoing traffic may not be optimal - it may hit the 'wrong' router first and be bounced to the right one - but this is typically not a problem.

Use MD5 authentication. Disable OSPF except on necessary interfaces.

Each router only should originate defaultrouter into the OSPF cloud. Never attempt to redistribute BGP into OSPF!

The key feature to look for is non-blocking performance. The scalability depends on being able to pump more and more traffic through the switch without it losing packets.

Try to keep routing within one site with minimal redistribution. This will allow you to use one BGP peering session to communicate between all of your routers. If you follow these recommendations, the router with the lowest defaultroute metric will be the "preferred" router for outgoing traffic from the access routers. Routing of outgoing traffic may not be optimal - it may hit the 'wrong' router first and be bounced to the right one - but this is typically not a problem.

Use MD5 authentication. Disable OSPF except on necessary interfaces.

Each router only should originate defaultrouter into the OSPF cloud. Never attempt to redistribute BGP into OSPF!

The key feature to look for is non-blocking performance. The scalability depends on being able to pump more and more traffic through the switch without it losing packets.

Try to keep routing within one site with minimal redistribution. This will allow you to use one BGP peering session to communicate between all of your routers. If you follow these recommendations, the router with the lowest defaultroute metric will be the "preferred" router for outgoing traffic from the access routers. Routing of outgoing traffic may not be optimal - it may hit the 'wrong' router first and be bounced to the right one - but this is typically not a problem.

Use MD5 authentication. Disable OSPF except on necessary interfaces.

Each router only should originate defaultrouter into the OSPF cloud. Never attempt to redistribute BGP into OSPF!

The key feature to look for is non-blocking performance. The scalability depends on being able to pump more and more traffic through the switch without it losing packets.

Try to keep routing within one site with minimal redistribution. This will allow you to use one BGP peering session to communicate between all of your routers. If you follow these recommendations, the router with the lowest defaultroute metric will be the "preferred" router for outgoing traffic from the access routers. Routing of outgoing traffic may not be optimal - it may hit the 'wrong' router first and be bounced to the right one - but this is typically not a problem.

Use MD5 authentication. Disable OSPF except on necessary interfaces.

Each router only should originate defaultrouter into the OSPF cloud. Never attempt to redistribute BGP into OSPF!

The key feature to look for is non-blocking performance. The scalability depends on being able to pump more and more traffic through the switch without it losing packets.

Try to keep routing within one site with minimal redistribution. This will allow you to use one BGP peering session to communicate between all of your routers. If you follow these recommendations, the router with the lowest defaultroute metric will be the "preferred" router for outgoing traffic from the access routers. Routing of outgoing traffic may not be optimal - it may hit the 'wrong' router first and be bounced to the right one - but this is typically not a problem.

Use MD5 authentication. Disable OSPF except on necessary interfaces.

Each router only should originate defaultrouter into the OSPF cloud. Never attempt to redistribute BGP into OSPF!

The key feature to look for is non-blocking performance. The scalability depends on being able to pump more and more traffic through the switch without it losing packets.

Try to keep routing within one site with minimal redistribution. This will allow you to use one BGP peering session to communicate between all of your routers. If you follow these recommendations, the router with the lowest defaultroute metric will be the "preferred" router for outgoing traffic from the access routers. Routing of outgoing traffic may not be optimal - it may hit the 'wrong' router first and be bounced to the right one - but this is typically not a problem.

Use MD5 authentication. Disable OSPF except on necessary interfaces.

Each router only should originate defaultrouter into the OSPF cloud. Never attempt to redistribute BGP into OSPF!

The key feature to look for is non-blocking performance. The scalability depends on being able to pump more and more traffic through the switch without it losing packets.

Try to keep routing within one site with minimal redistribution. This will allow you to use one BGP peering session to communicate between all of your routers. If you follow these recommendations, the router with the lowest defaultroute metric will be the "preferred" router for outgoing traffic from the access routers. Routing of outgoing traffic may not be optimal - it may hit the 'wrong' router first and be bounced to the right one - but this is typically not a problem.

Use MD5 authentication. Disable OSPF except on necessary interfaces.

Each router only should originate defaultrouter into the OSPF cloud. Never attempt to redistribute BGP into OSPF!
Dual-attached networks

Single-attached networks

In theory, you could connect them directly into the core switches, if they have two ethernet ports, and if you trust their OSPF implementation, and if you're sure they won't flapping routes (e.g., announce a separate /32 for each dial-in user!). Safer to connect them downstream of access routers, with default routes/HSRP. Use static routes on the access routers to point to their dial-in IP pool. These routers will then redistribute static to the other routers, giving you more control and less reliance on possibly unreliable OSPF implementations.

Two routers, using HSRP/VRRP or equivalent
Use for essential services such as mail and dial-in servers.
Note that the two routers will still have to connect to a common switch, which can be a single.

Single-ended networks

Dial-in servers (NAS)

If you need high availability, you could connect them directly into the core switches. However, this will reduce your control and increase your reliance on possibly unreliable OSPF implementations.

Enough ports, including 2 ethernet ports to link into core. A 5-port ethernet router will only give you 3 ports usable for networks, since the other 2 are for linking into the core.

Robust OSPF implementation with equal-cost multipath support.

Redundant PSUs and fans are nice, especially for single-ended networks.

On large Cisco switches, you can use a Cisco Express Forwarding (CEF) implementation.

Enough performance to handle the full load of traffic on the core.

Choice of router

Connecting dial-in servers (NAS)

These routers will then announce a single /72 for each dial in

Robust OSPF implementation with equal-cost multipath support.

On large Ciscos: remember to enable Cisco Express Forwarding (ip cef [distributed]).

Redundant PSUs and fans are nice, especially for single-ended networks.
The last thing you want is flapping /32 routes throughout your network whenever customers dial in or hang up. They will kill your routers. It might work now, but you will have severe problems in the future. Supporting it will become very expensive.

1. Make sure that all static IP addresses are within the same netblock(s).
2. Make sure your existing static IP users all hit ONE NAS. You may have to set up a separate telephone number (hunt group) and get them to use this number.
3. Static route this netblock to this NAS.
4. Don’t allow static IP roaming between POPs.

DON’T SELL ANY MORE STATIC IP ACCOUNTS!

In many cases, what they really want is SMTP mail delivery. There are other ways of providing this. Set up a mail server which can ‘kick’ out mail via SMTP to their dynamic IP address. It can be triggered by dialling in (Tools you can use include fetchmail and serialmail). It can be triggered by dialling in your radius server, or ETRN. You may have to set up a separate telephone number (hunt group) and get them to use this number.

If there is a functional disadvantage to using static IP, customers will be more creative in finding alternative solutions. Usually this is for NT Exchange servers, and there is now a module available which can be used on Exchange to generate some scripting code. If your mail server is NT, launching the Exchange module triggers some scripting code.

If you can write scripts (fetchmail and serialmail), it can be triggered by dialling in your radius server, or ETRN. Usually this is for NT Exchange servers, and there is now a module available which can be used on Exchange to generate some scripting code.

Do your customers really need static IP anyway?

Suppose it will become very expensive.

If it might work now, then you will have severe problems in the future. Customers dial in or hang up, they will call your support!

The last thing you want is having to fix route dissection on your network whenever necessary.

IT DOESN’T SCALE

Do you provide a static IP dial-in service?