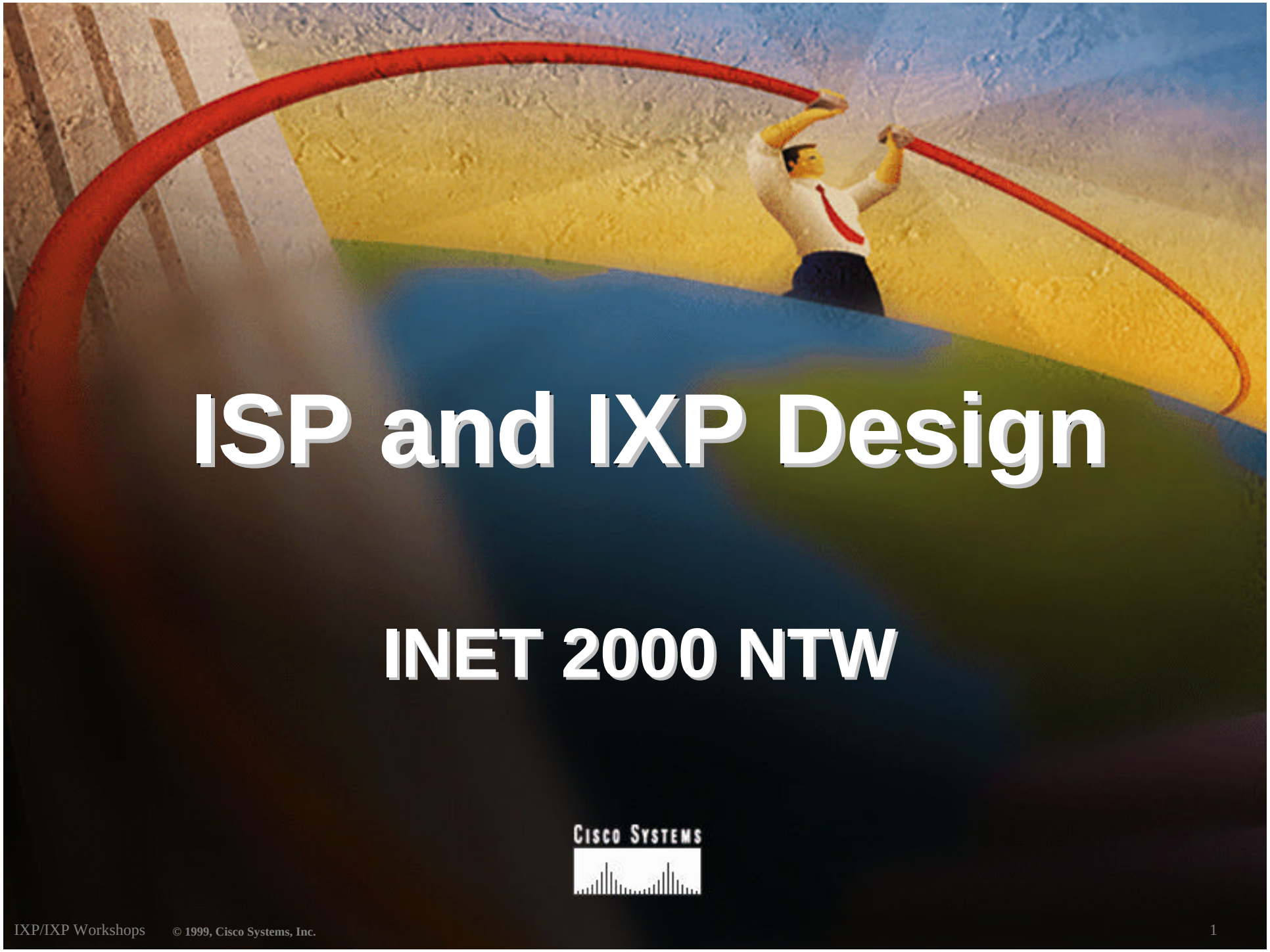


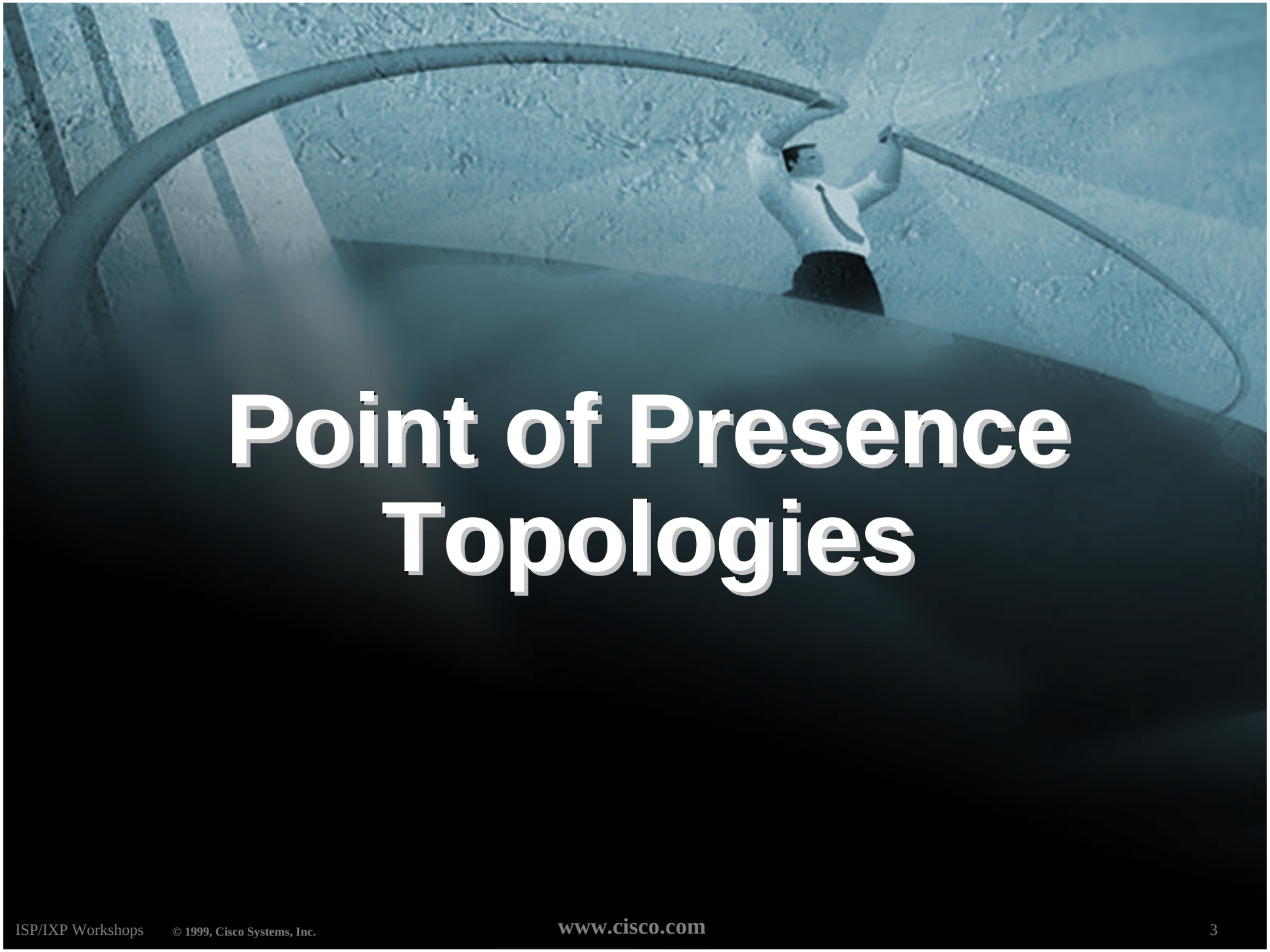
ISP and IXP Design

INET 2000 NTW

Cisco Systems

ISP Network Design

- PoP Topologies and Design
- Backbone Design
- Addressing
- Routing Protocols
- Security
- Out of Band Management



Point of Presence Topologies

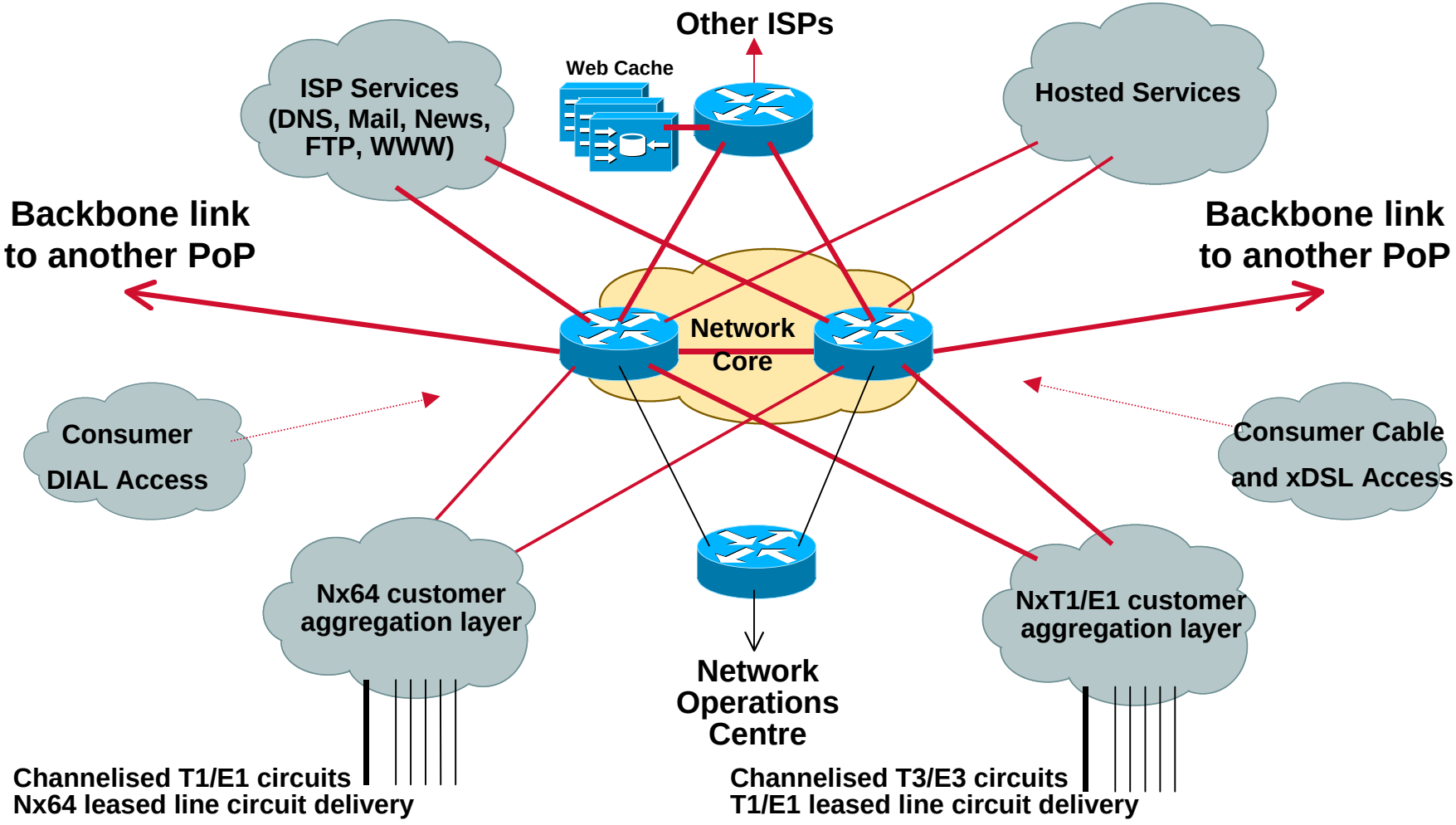
PoP Topologies

- **Core routers - high speed trunk connections**
- **Distribution routers and Access routers - high port density**
- **Border routers - connections to other providers**
- **Service routers - hosting and servers**
- **Some functions might be handled by a single router**

PoP Design

- **Modular Design**
- **Aggregation Services separated according to**
  - **connection speed**
  - **customer service**
  - **contention ratio**
  - **security considerations**

Modular PoP Design



Modular Routing Protocol Design

- **Modular IGP implementation**

  IGP "area" per module

  aggregation/summarisation into the core

- **Modular iBGP implementation**

  BGP route reflector cluster per module

  core routers are route-reflectors

  clients peer with core only

Point of Presence Design

PoP Modules

- **Low Speed customer connections**
  - **PSTN/ISDN dialup**
  - **low bandwidth needs**
  - **low revenue, large numbers**
- **Medium Speed customer connections**
  - **56/64K to sub-T1/E1 speeds**
  - **low bandwidth needs**
  - **medium revenue, medium numbers**

PoP Modules

- **High Speed customer connections**
  - **E1++ speeds**
  - **medium bandwidth needs**
  - **high revenue, low numbers**
- **Broad Band customer connections**
  - **xDSL and Cable**
  - **high bandwidth needs**
  - **low revenue, large numbers**

PoP Modules

- **PoP Core**

  Two dedicated routers

  High Speed interconnect

  Backbone Links *ONLY*

  Do not touch them!

- **Border Network**

  dedicated border router to other ISPs

  the ISP's "front" door

  transparent web caching

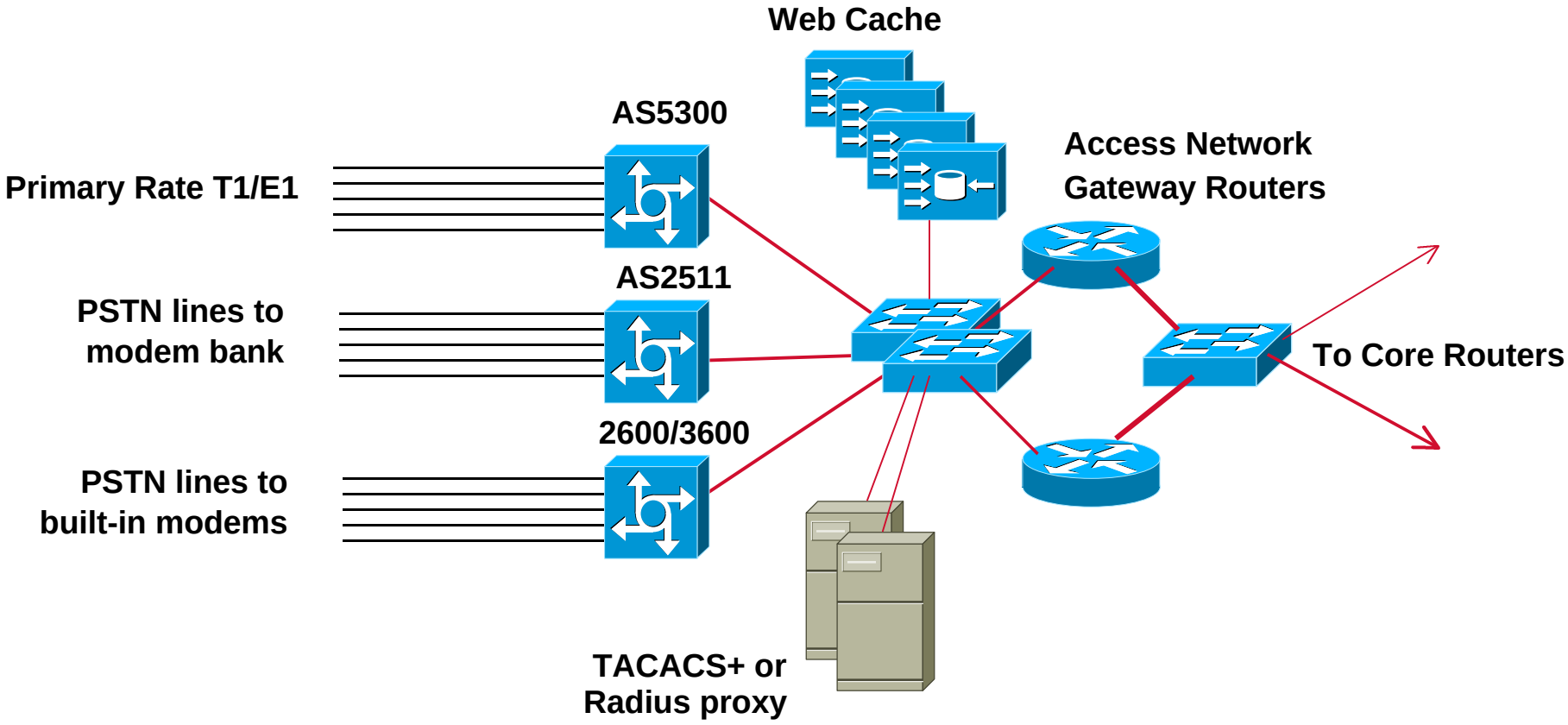
PoP Modules

- **ISP Services**
  - **DNS (cache, secondary)**
  - **News, Mail (POP3, Relay)**
  - **WWW (server, proxy, cache)**
- **Hosted Services**
  - **Virtual Web, WWW (server, proxy, cache)**
  - **Information/Content Services**
  - **Electronic Commerce**

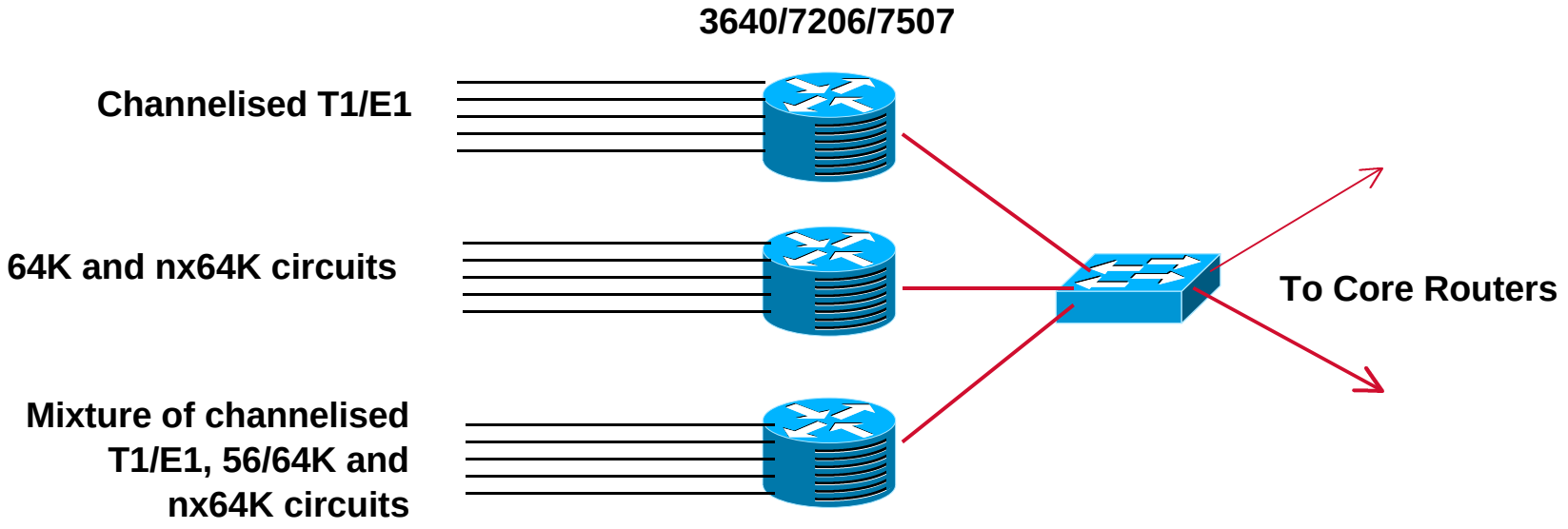
PoP Modules

- **Network Operations Centre**
  - **primary and backup locations**
  - **network monitoring**
  - **statistics and log gathering**
  - **direct but secure access**
- **Out of Band Management Network**
  - **The ISP Network “Safety Belt”**

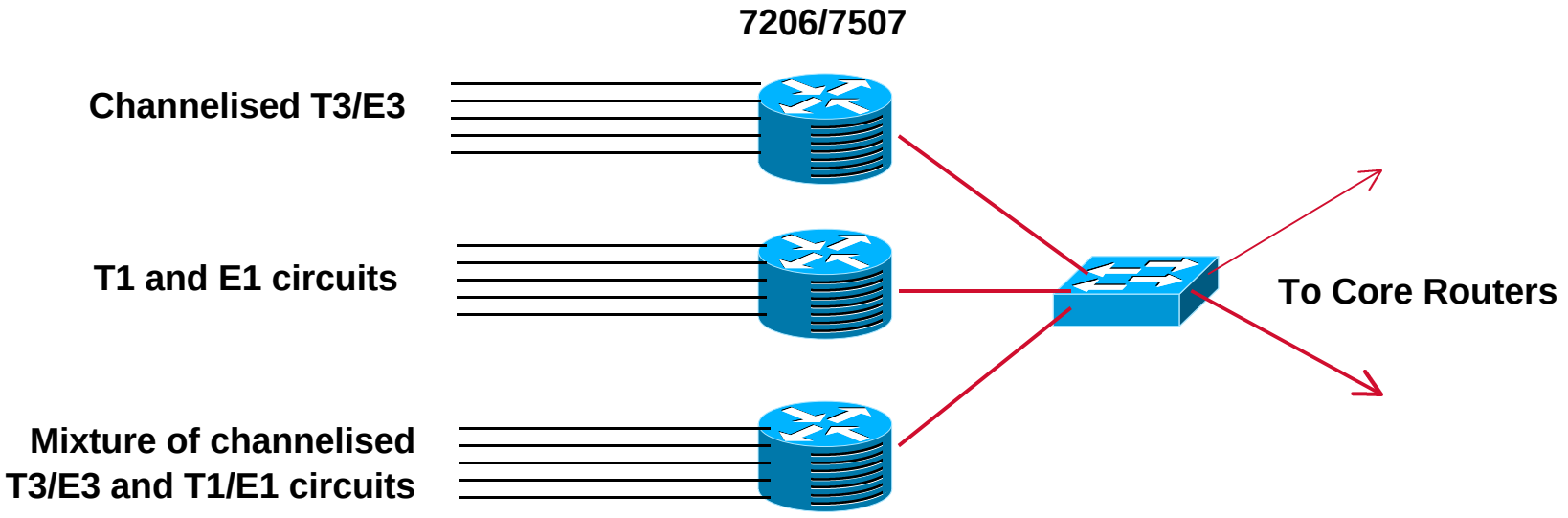
Low Speed Access Module



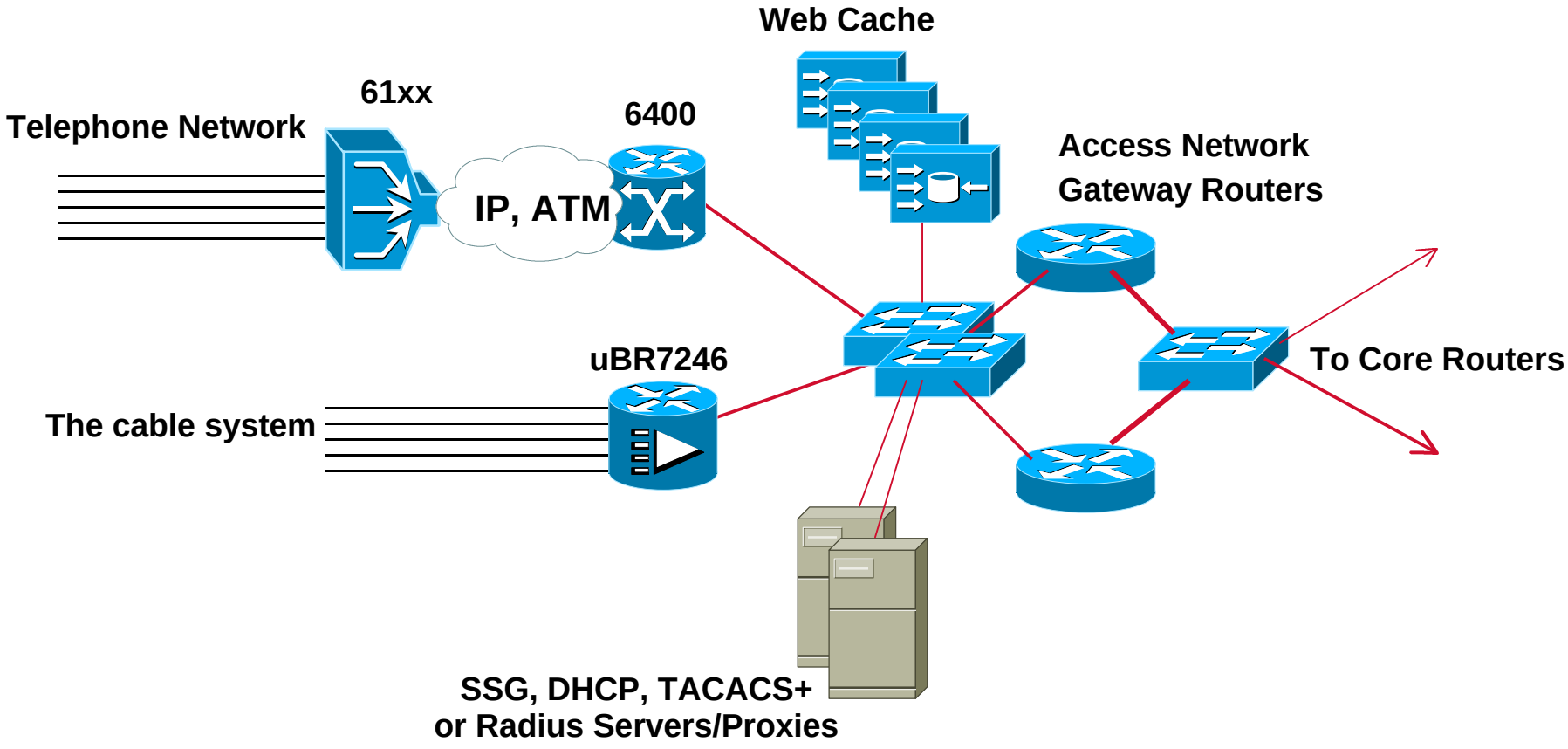
Medium Speed Access Module



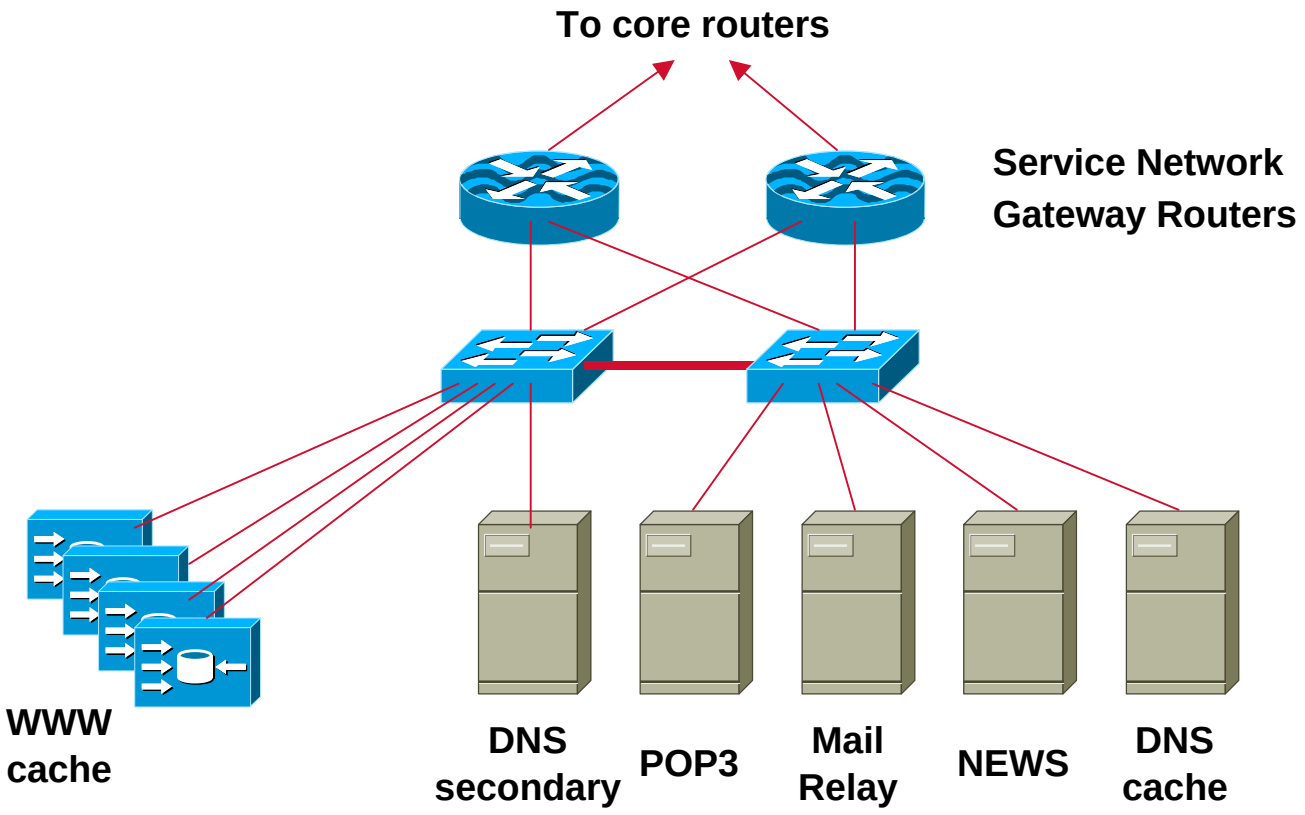
High Speed Access Module



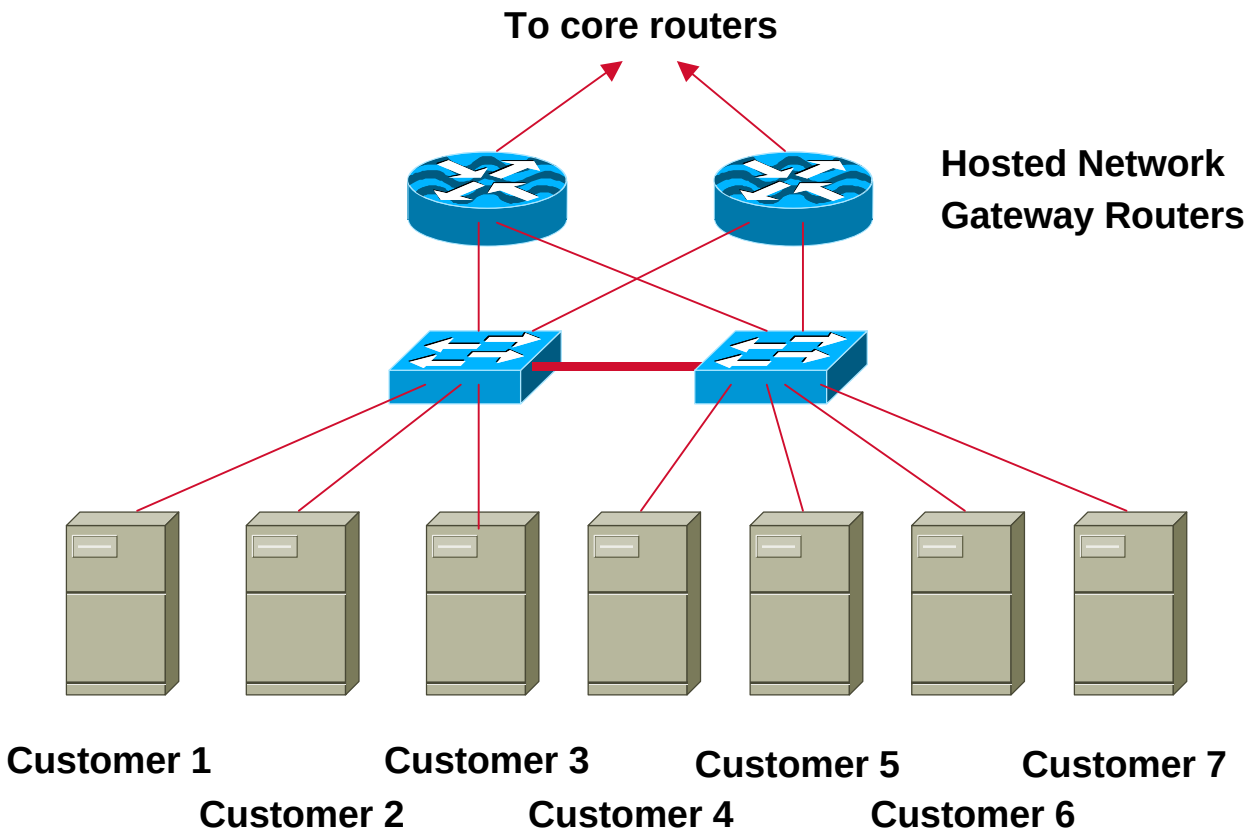
Broad Band Access Module



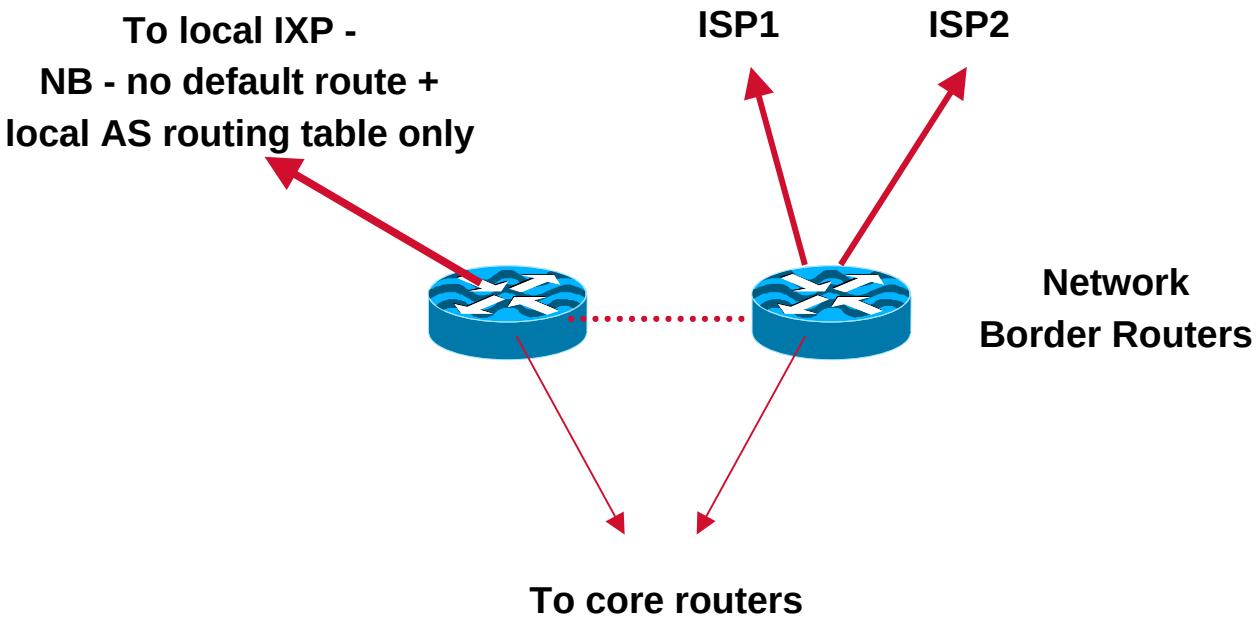
ISP Services Module



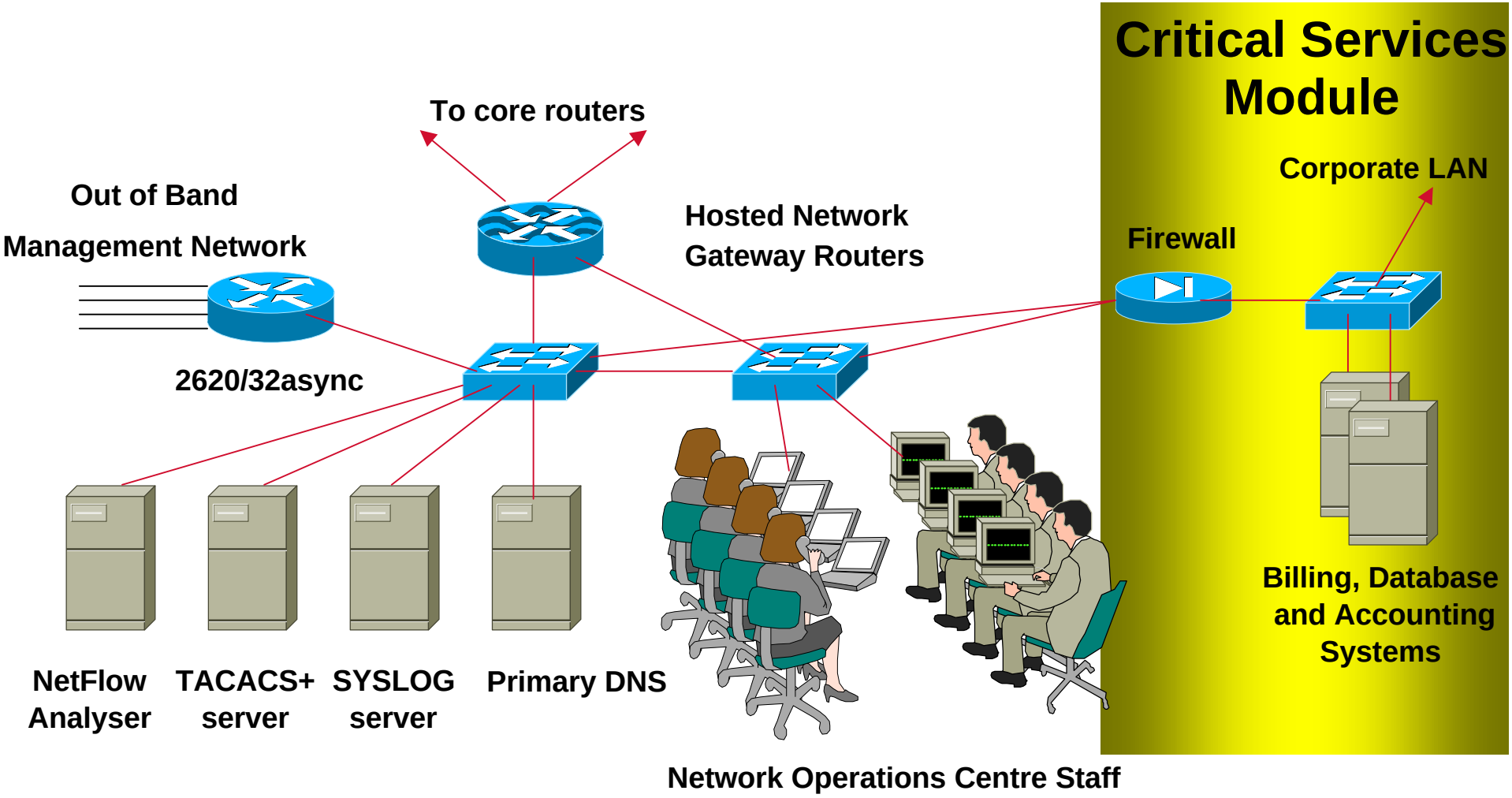
Hosted Services Module



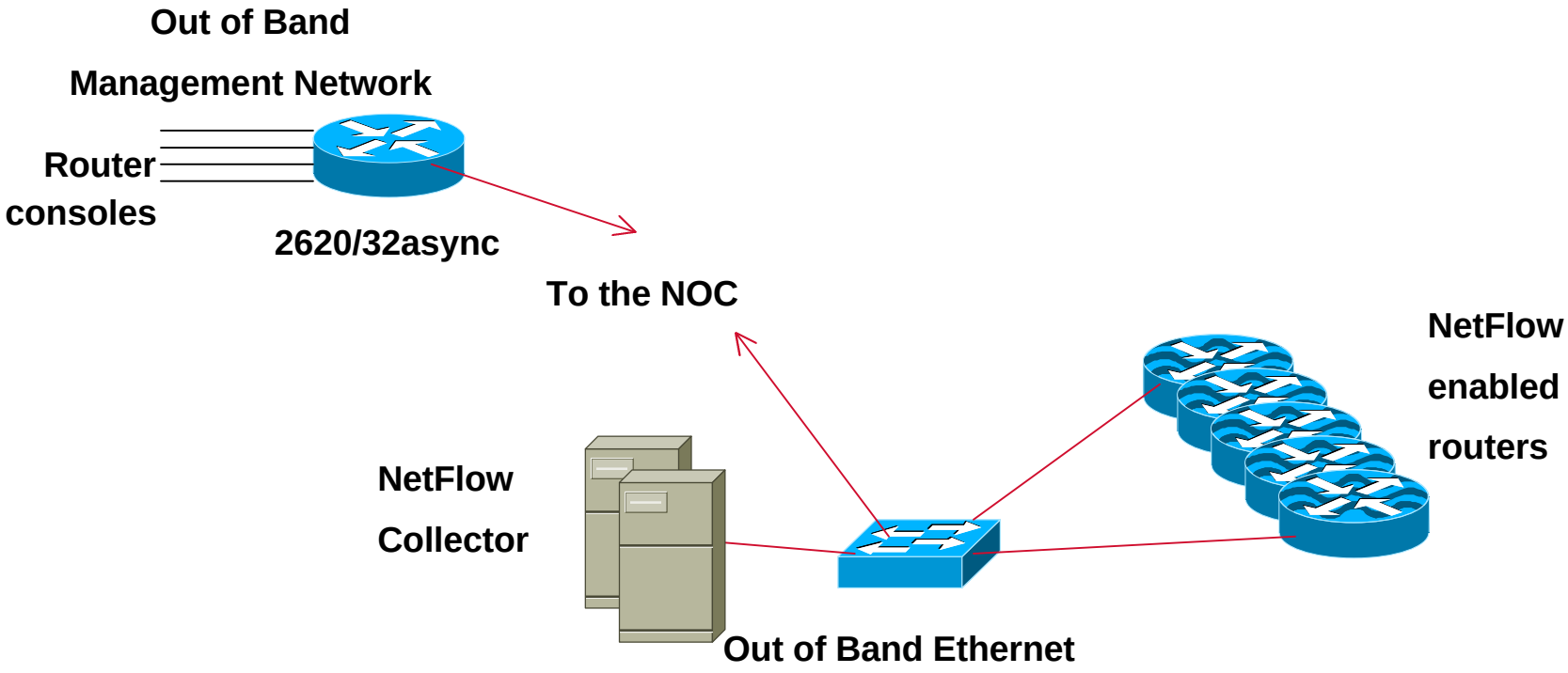
Border Module



NOC Module



Out of Band Network



Backbone Network Design

Backbone Design

- Routed Backbone
- Switched Backbone
- Leased point-to-point circuits

  nx64K, T1/E1, T3/E3, OC3, OC12,...
- ATM/Frame Relay service from telco

  T3, OC3, OC12,… delivery

  easily upgradeable bandwidth (CIR)

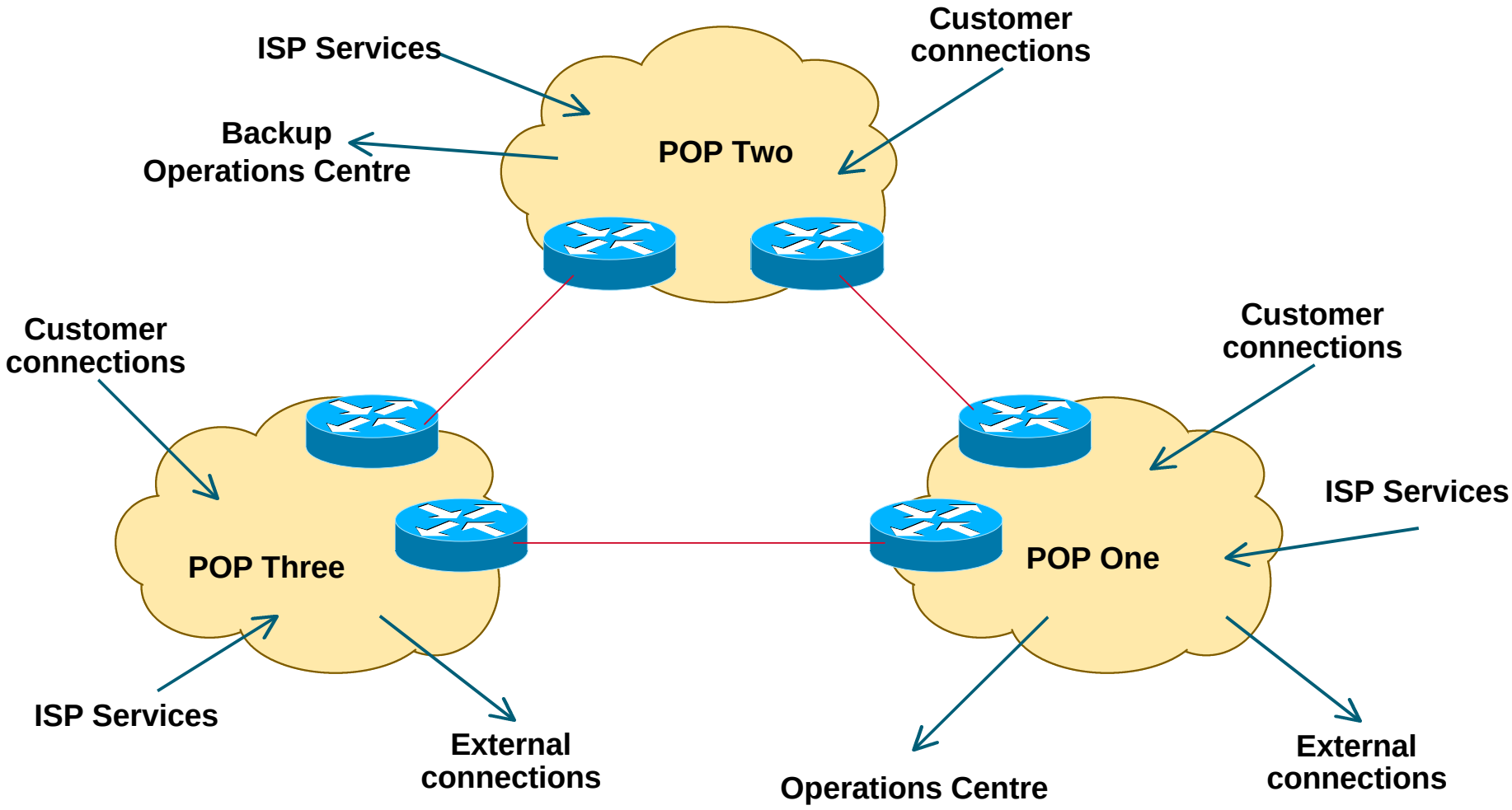
Distributed Network Design

- PoP design “standardised”

  operational scalability and simplicity

- ISP essential services distributed around backbone
- NOC and “backup” NOC
- Redundant backbone links

Distributed Network Design



Backbone Links

- **ATM/Frame Relay**

  now less popular due to overhead, extra equipment, and shared with other customers of the telco

- **Leased Line**

  more popular with backbone providers

  IP over Optics and MPLS coming into the mainstream

Long Distance Backbone Links

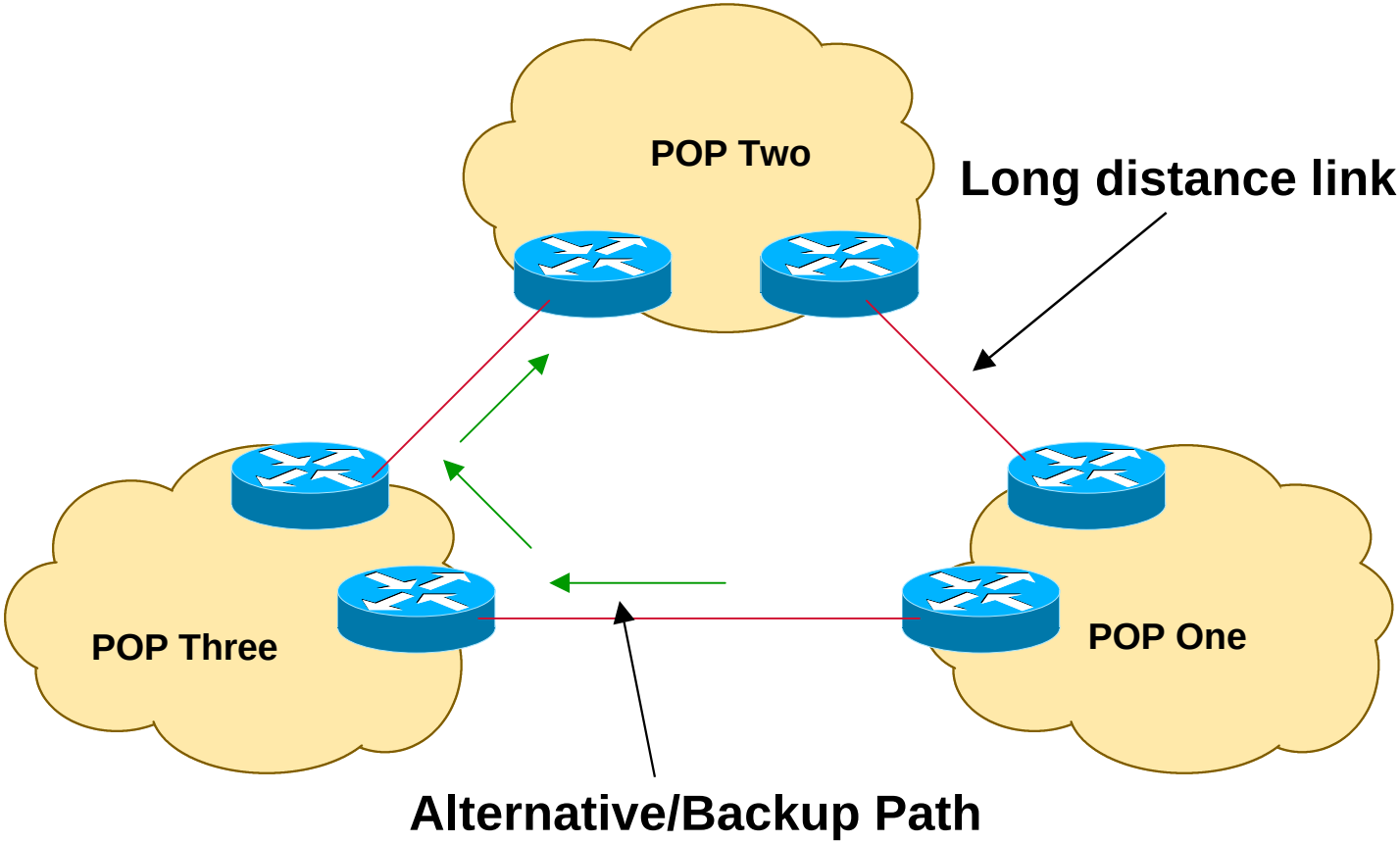
- Tend to cost more
- Plan for the future (at least two years ahead) but stay in budget

  Unplanned “emergency” upgrades can be disruptive without redundancy

- Allow sufficient capacity on alternative paths for failure situations

  sufficient can be 20% to 50%

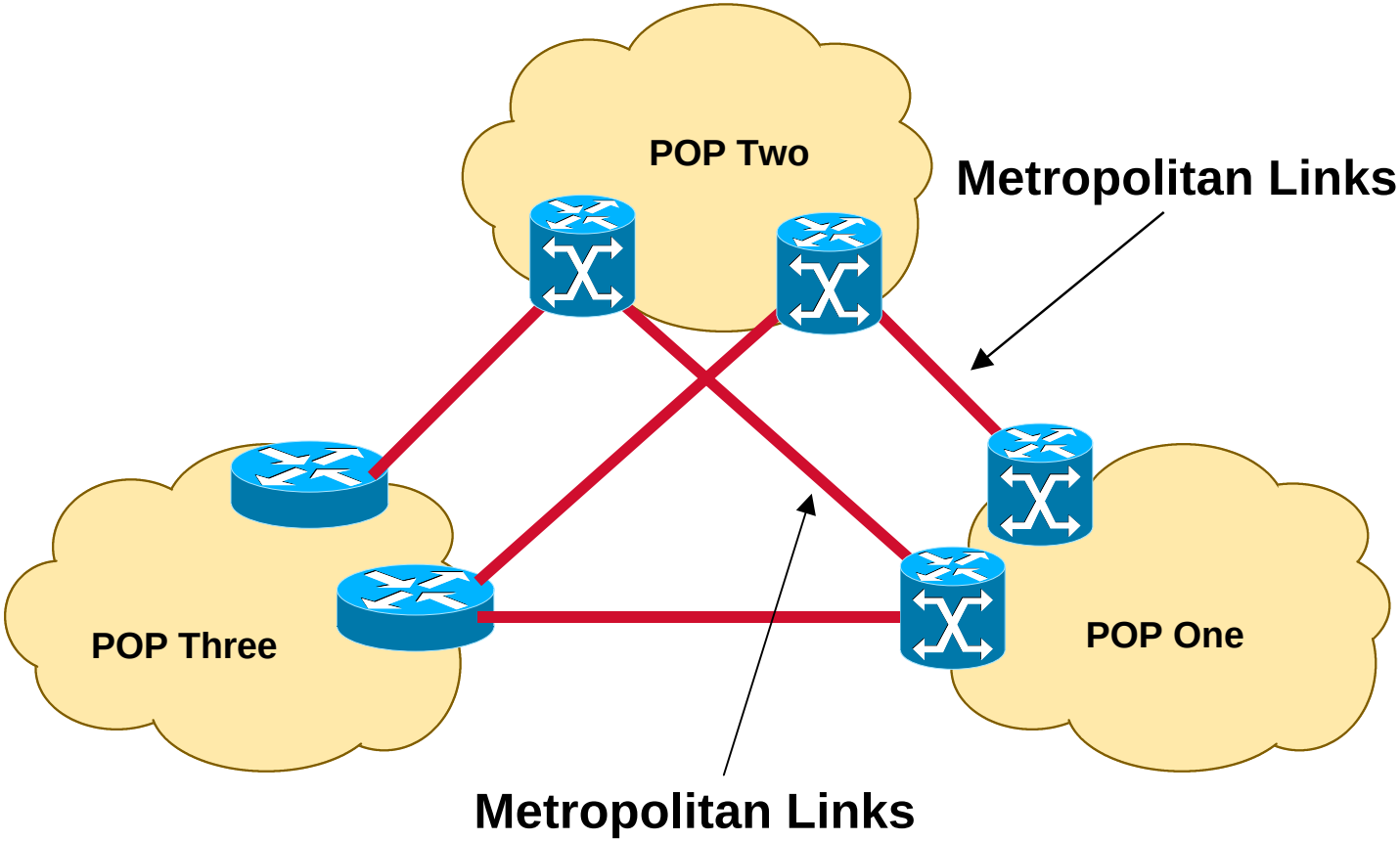
Long Distance Links



Metropolitan Area Backbone Links

- **Tend to be cheaper**
  - **Circuit concentration**
  - **Choose from multiple suppliers**
- **Think big**
  - **More redundancy**
  - **Less impact of upgrades**
  - **Less impact of failures**

Metropolitan Area Backbone Links - Example



Traditional Point to Point Links

Routing Protocols

Routing Protocols

- **IGP - Interior Gateway Protocol**

  carries infrastructure addresses, point-to-point links

  examples are OSPF, ISIS, EIGRP...

- **EGP - Exterior Gateway Protocol**

  carries customer prefixes and Internet routes

  current EGP is BGP version 4

- **No link between IGP and EGP**

Why Do We Need an IGP?

- **ISP backbone scaling**
  - **Hierarchy**
  - **Modular infrastructure construction**
  - **Limiting scope of failure**
  - **Healing of infrastructure faults using dynamic routing with fast convergence**

Why Do We Need an EGP?

- **Scaling to large network**
  - **Hierarchy**
  - **Limit scope of failure**
- **Policy**
  - **Control reachability to prefixes**
  - **Merge separate organizations**
  - **Connect multiple IGPs**

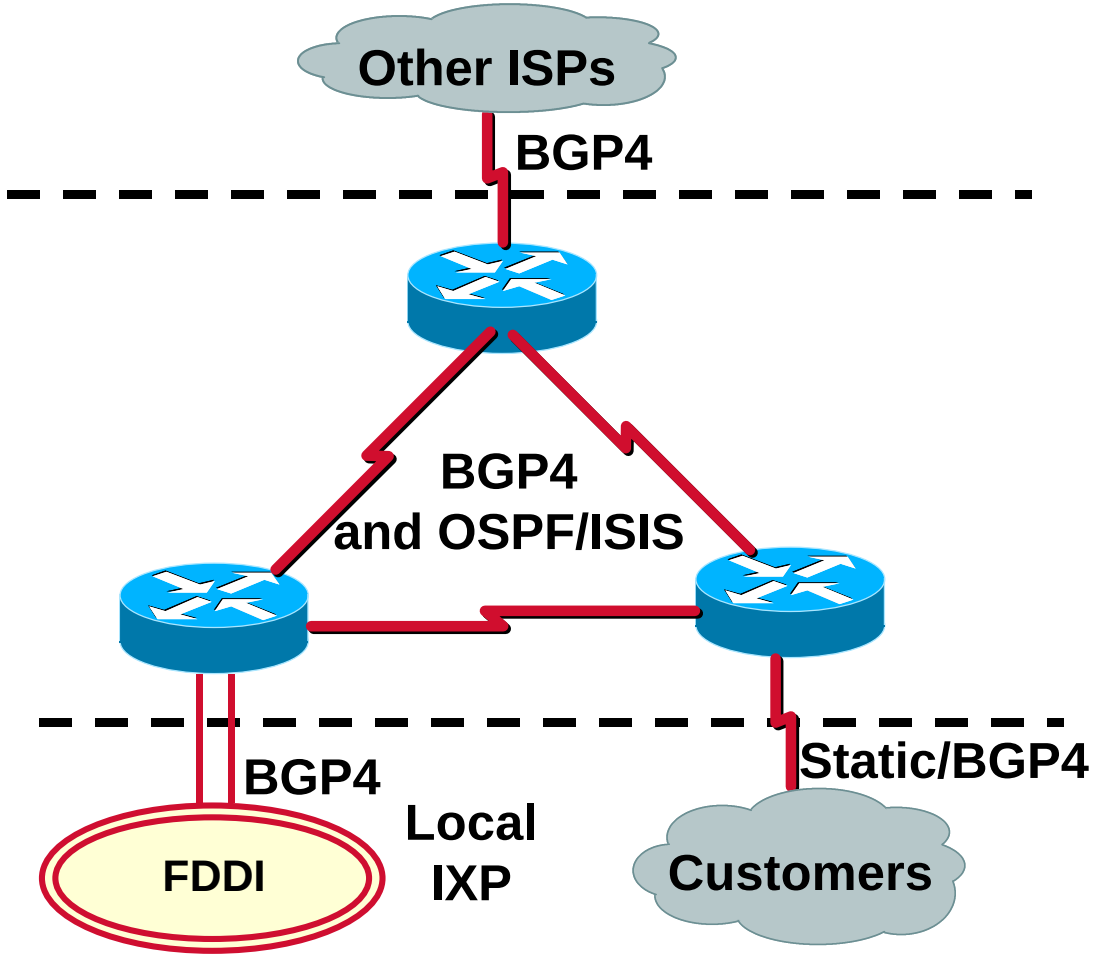
Interior versus Exterior Routing Protocols

- **Interior**
  - automatic neighbour discovery
  - generally trust your IGP routers
  - prefixes go to all IGP routers
  - binds routers in one AS together
- **Exterior**
  - specifically configured peers
  - connecting with outside networks
  - set administrative boundaries
  - binds AS's together

Interior versus Exterior Routing Protocols

- **Interior**
  - **Carries ISP infrastructure addresses only**
  - **ISPs aim to keep the IGP small for efficiency and scalability**
- **Exterior**
  - **Carries customer prefixes**
  - **Carries Internet prefixes**
  - **EGPs are independent of ISP network topology**

Hierarchy of Routing Protocols



Security

- ISP Infrastructure security
- ISP Network security
- Security is not optional!
- ISPs need to:

  protect themselves

  help protect their customers from the Internet

  protect the Internet from their customers

ISP Infrastructure Security

- **router security**

  usernames, passwords, vty filters, TACACS+

- **server security**

  usernames, passwords, TCP wrappers, filters

- **premises security**

  locks, secure access, environment control

- **staff responsibility**

- **RFC2196 (Site Security Handbook)**

ISP Network Security

- **Denial of Service Attacks**

  eg: “smurfing”

- **Effective filtering**

  network borders

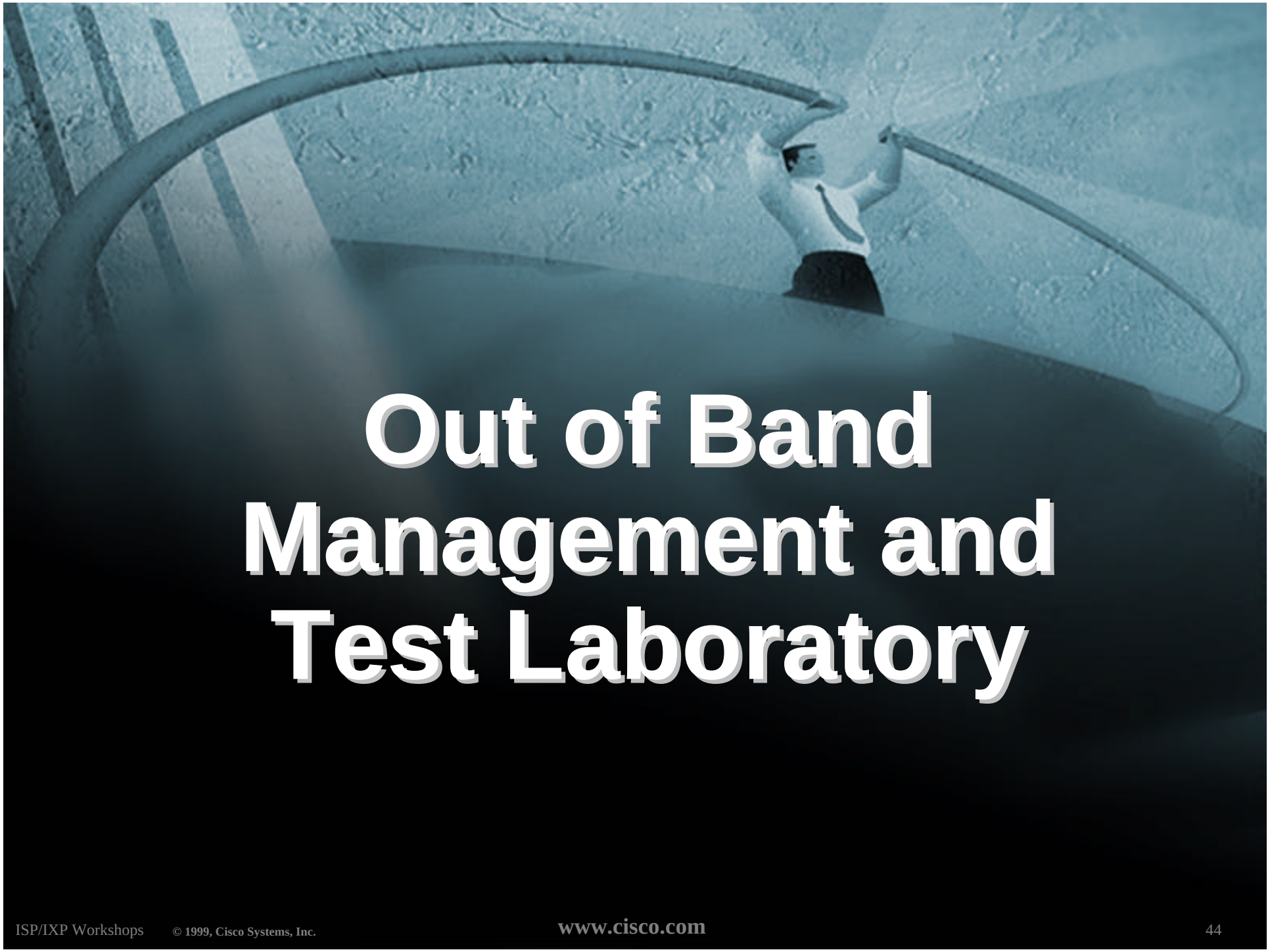
  customer connections

  network operation centre

  ISP internal network

Ingress & Egress Route Filtering

Your customers should not be sending *any* IP packets out to the Internet with a source address other then the address you have allocated to them!



Out of Band Management and Test Laboratory

Other Design Considerations

- **Out of Band Management**

  how to get to equipment when “the network is down”

- **Test Laboratory**

  how to test new services and features

  how to debug network problems

Out of Band Management

- Not optional!
- Allows access to network equipment in times of failure
- Ensures quality of service to customers
  - minimises downtime
  - minimises repair time
  - eases diagnostics and debugging

Out of Band Management

- **OoB Example - Access server:**

  modem attached to allow NOC dial in

  console ports of all network equipment connected to serial ports

  LAN and/or WAN link connects to network core, or via separate management link to NOC

- **Full remote control access under all circumstances**

Out of Band Management

- **OoB Example - Statistics gathering:**

  Routers are NetFlow and syslog enabled

  Management data is congestion/failure sensitive

  Ensures management data integrity in case of failure

- **Full remote information under all circumstances**

Test Laboratory

- Looks like a typical PoP
- Used to trial new services or new software under realistic conditions
- Allows discovery of potential problems before they are introduced to the network
- Every major ISP in the US and Europe has a test lab

Test Laboratory

- Some ISPs dedicate equipment to the lab
- Other ISPs “purchase ahead” so that today’s lab equipment becomes tomorrow’s PoP equipment
- Other ISPs use lab equipment for “hot spares” in the event of hardware failure

ISP Design Summary

- **KEEP IT SIMPLE !**
- **Simple is elegant is scalable**
- **Use Redundancy, Security, and Technology to make life easier for yourself**
- **Above all, ensure quality of service for your customers**