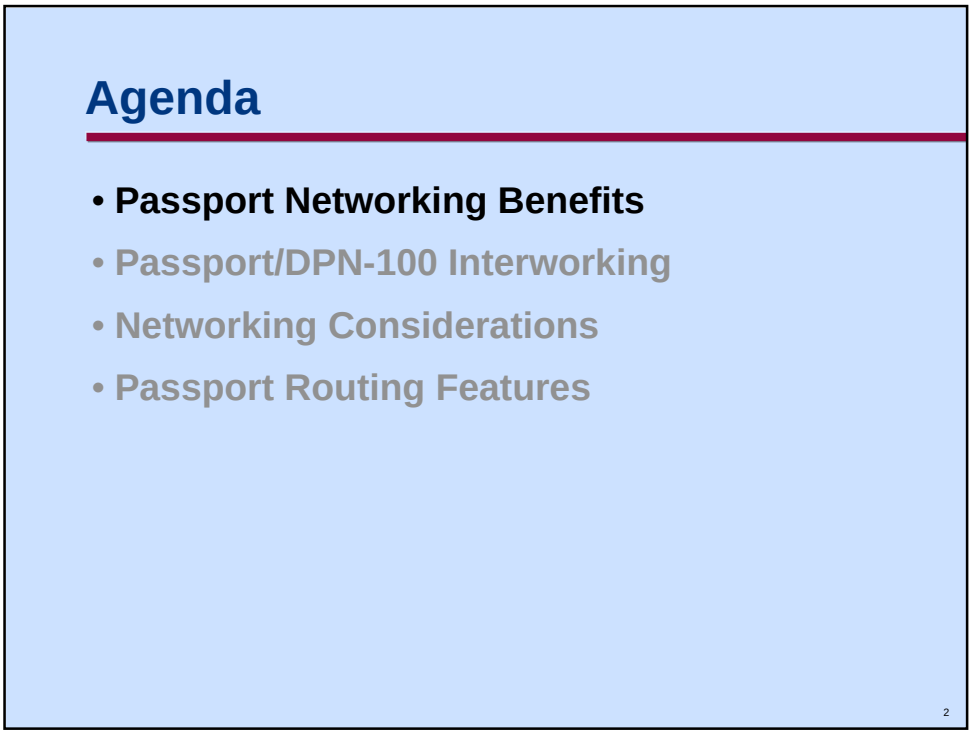
This presentation will demonstrate the ease of network growth and evolution using Magellan Passport. An overview of Passport/DPN-100 interworking will be presented, highlighting the simplicity with which Passport can be deployed as a high-speed backbone for a DPN-100 network. Engineering guidelines for efficient Passport/DPN-100 interworking and an overview of some new networking features will also be provided.

About the presenter:

Elizabeth Hache started her career in Magellan development in the late 1980s specializing in DPN-100 call routing and backup systems.

She has been involved in Passport/DPN-100 interworking since the first release of Passport. The major interworking features for which she has been responsible include the Call Server Resource Module (CSRM), Interconnecting Passport RID Subnets, and X.25/ X.75 Gateways on AMs off Passport.

As a advisor in the Passport/DPN-100 routing group, Elizabeth is involved in consulting on the design of Passport features, and providing technical expertise in the routing area to support Nortel Engineering and Global Technical Support groups. She is also involved in routing feature design for both Passport and DPN-100.



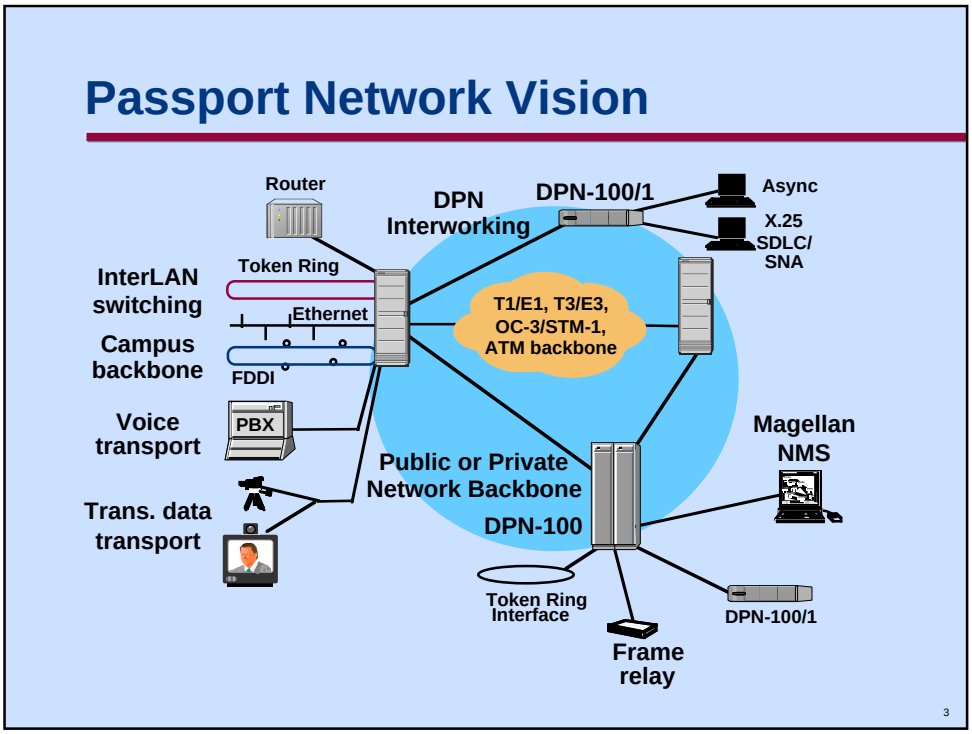
This presentation consists of four sections.

The first section “Passport Networking Benefits” highlights the value-added benefits of deploying a Passport backbone in a DPN-100 network.

The section “Passport/DPN-100 Interworking” will present a high-level view of the seamless interworking of Passport with DPN-100.

The “Networking Considerations” section will provide more technical detail regarding the interworking of Passport with DPN-100 modules, and will also provide some networking strategies for Passport/DPN-100 interworking networks.

Finally, the section “Passport Routing Features” will present an overview of the Passport connectionless routing system’s features and advantages.

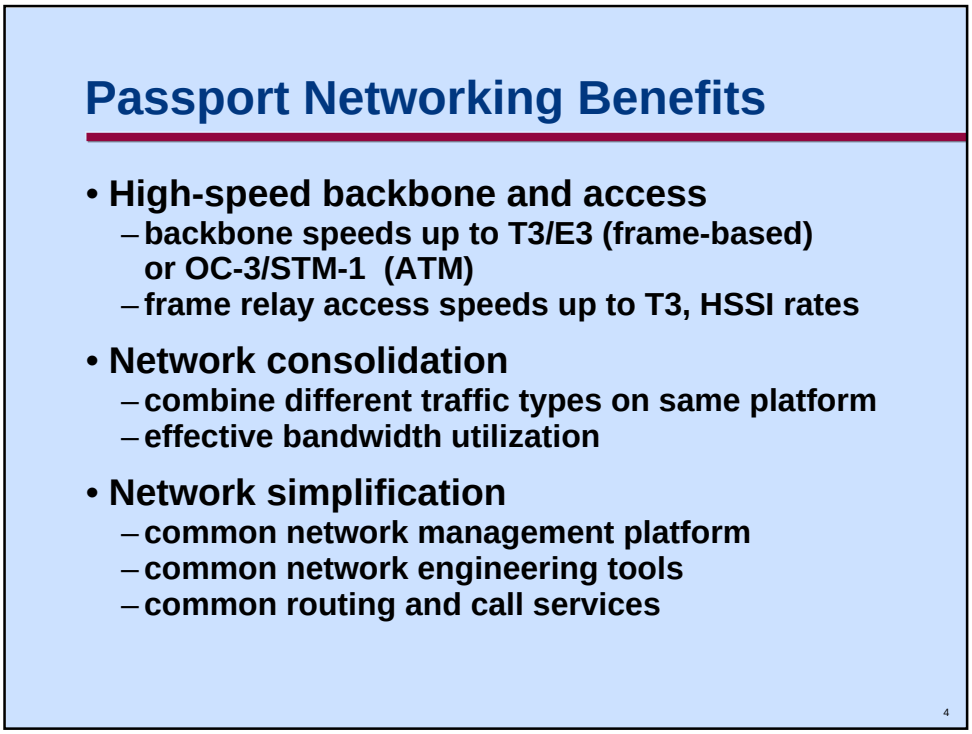


Nortel's vision is to provide a solution for service provider and enterprise networking requirements with the Magellan family of products. Passport supports the platform for many of the components of this vision.

Some of Passport's main target applications include:

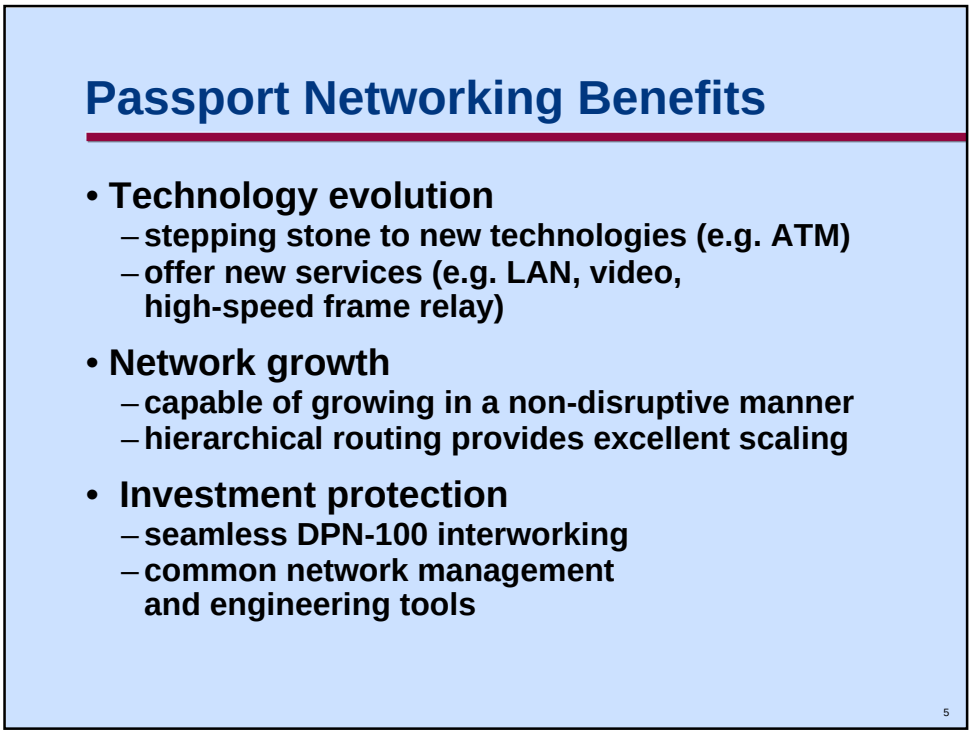
- interworking with DPN-100 to accommodate network growth of existing services and the introduction of new data services;
- expansion of the network to include LAN internetworking by providing a rich set of LAN and WAN interfaces, as well as bridge/router protocols for full multi-vendor interworking;
- bandwidth consolidation of voice, video, image and data traffic onto a single high-speed network backbone; and
- ATM-based networking.

Passport protects your initial investment and enables a smooth transition to new technologies and services.



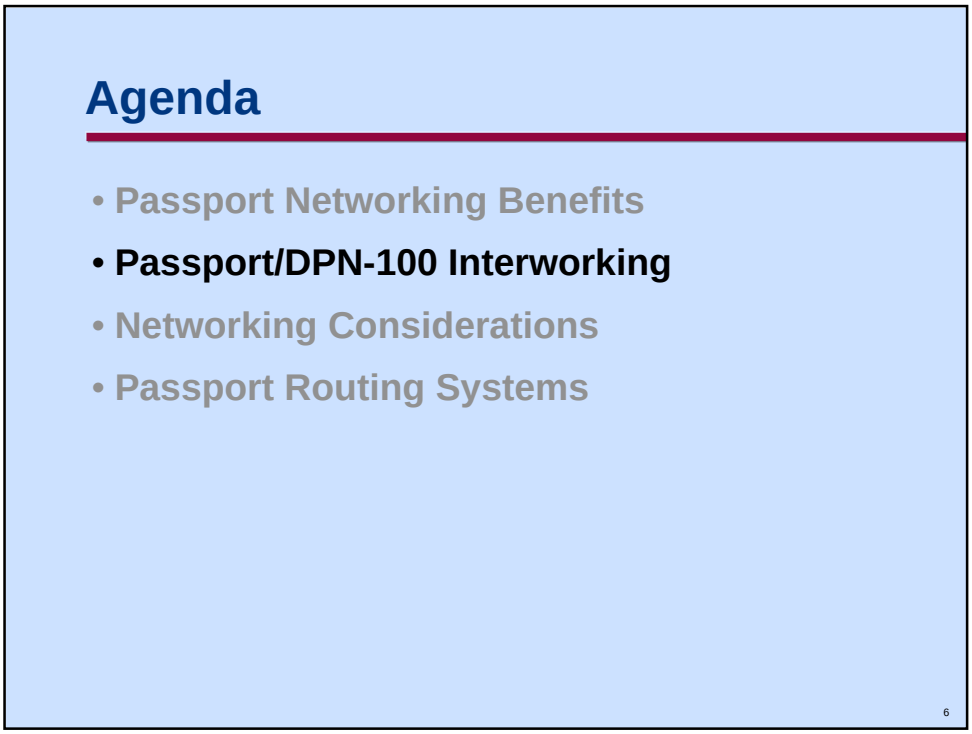
Network evolution using Passport protects current investments while enabling a smooth transition to new technologies and services. Deploying Passport as a backbone for a DPN-100 network provides the following benefits:

- **High-speed backbone and access**: Passport provides up to T3/E3 frame-based trunking capacity, and up to OC-3/STM-1 ATM trunking capability. Frame relay UNI access speeds are supported up to T3 and HSSI rates.
- **Network consolidation**: Passport effectively combines DPN-100 traffic with other multimedia applications such as voice and video, using dynamic bandwidth management. In addition to providing cost-effective bandwidth utilization, this also results in additional economic benefits such as reduced operations expense, lower capital costs, and reduced maintenance.
- **Network simplification**: Choosing Passport as a high-speed backbone for DPN-100 traffic ensures networking simplicity using a common network management platform, common routing and call services, and common network engineering tools. Growth, changes, and reconfigurations in the network are handled simply and much more quickly.

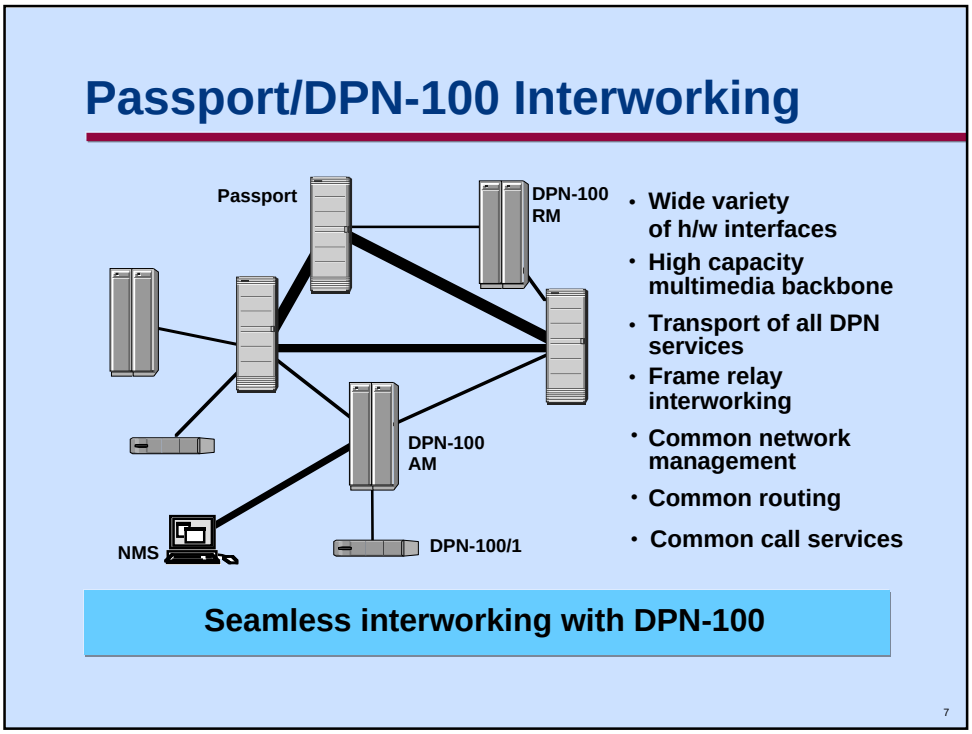


The following benefits are also derived by deploying Passport in a DPN-100 network:

- **Technology evolution:** Magellan networks can easily evolve from data packet switching, to multimedia services (such as telemedicine or Internet dial-up), to ATM broadband, while protecting your existing infrastructure investment. Passport allows DPN-100 customers to incrementally build on their initial investment.
- **Network growth:** The Passport/DPN-100 hierarchical routing system allows for networks to grow to 1000s of nodes with total ease. Network growth is accommodated in a non-disruptive manner.
- **Investment protection:** Passport operates seamlessly with DPN-100 networks using the existing DPN-100 network management platform and network engineering tools. Passport provides an orderly smooth migration to a high-speed backbone, minimizing impacts on existing network operations.



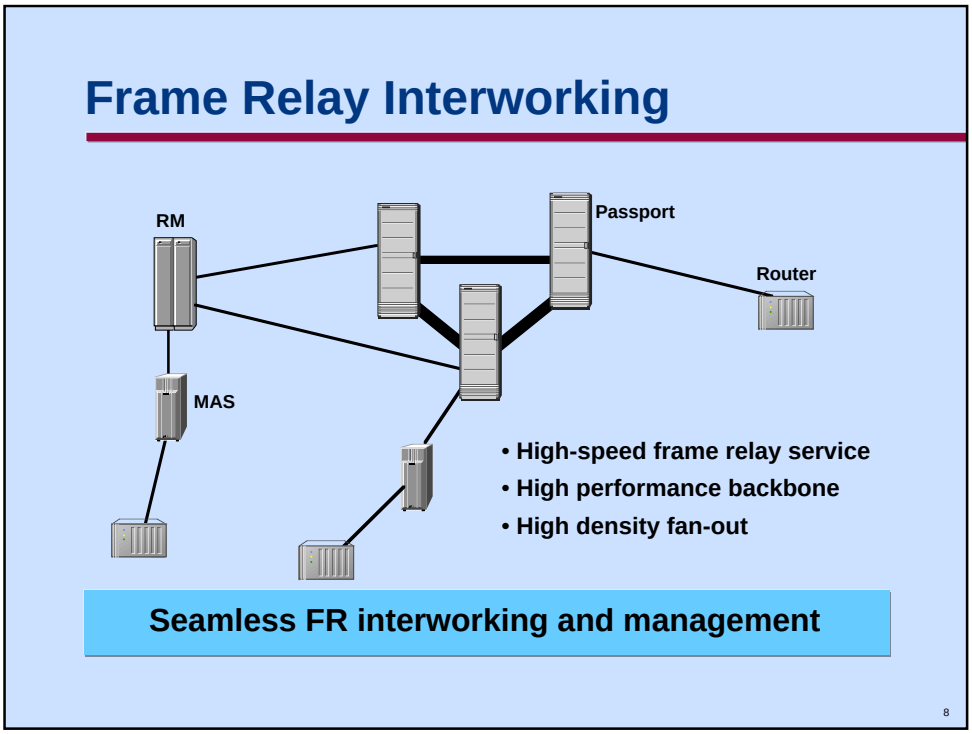
This section will present a high level view of the seamless interworking of Passport with DPN-100.



DPN-100 networks are deployed throughout the world and provide data communication services such as X.25, frame relay, SNA, bisync and asynchronous terminal support. Passport interworks with, and enhances, the DPN-100 capabilities. Passport offers a high-speed frame-based trunking capacity at up to T3 and E3 rates and ATM trunking up to OC-3/STM-1 rates, Passport also supports frame relay UNI access up to T3 and HSSI rates. Passport offers a wide variety of hardware interfaces to DPN-100 modules including V.35, V.11, T1, and E1.

Passport can transport all DPN-100 services, with support for DPN-100 network services such as call recovery, Access Module (AM) clusters, and routing Class of Services (CoS). Passport also interworks seamlessly with the DPN-100 frame relay service supporting frame relay UNI and NNI, Committed Information Rate, FECN/BECN Congestion Control and packet discard eligibility.

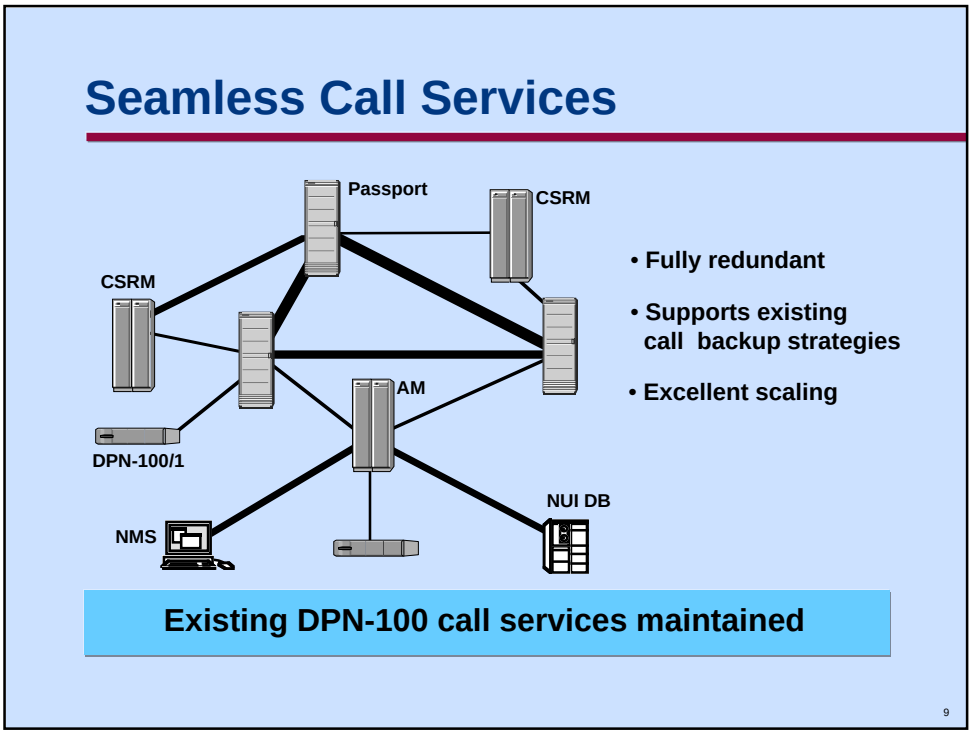
Finally, Passport makes use of existing DPN-100 call services. Resource Module (RM)-based call servers also serve the Passport backbone when configured on a specially provisioned RM designated to support Passport call services.



Passport and DPN-100 frame relay services are fully standards-compliant with seamless interworking and management across the product line. Passport's high-speed interfaces support frame relay user-to-network interface access at speeds up to T3 and HSSI rates, as well as trunk speeds up to and including OC-3/STM-1 via ATM trunking.

Passport provides excellent fanout per cabinet supporting more than 2,500 DS0s/channels per 19 inch cabinet. This results in a highly competitive price per user-to-network (UNI) and high density for a given floor space.

Passport and DPN-100 frame relay can use common network management tools. Alternatively, Passport can also use an open platform for network management, interfacing with OSI standards and the de-facto standard SNMP.



Passport uses existing DPN-100 call services through a Resource Module which is provisioned to provide the call services functions to the Passport/DPN-100 Network. In order to identify that it supports this functionality, the RM is designated as the Call Server Resource Module (CSRM).

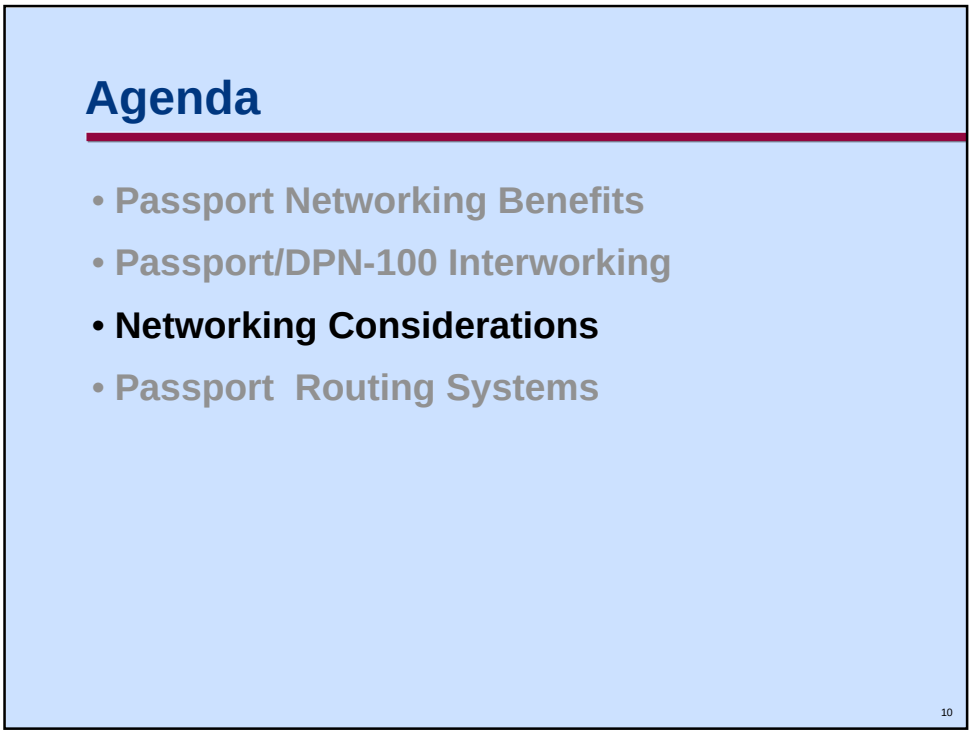
Call services provided on the CSRM include:

- Source and Destination Call Routing;
- Gateway Source and Destination Call Routing; and
- Access to Call Redirection and NUI (and Call) Translation.

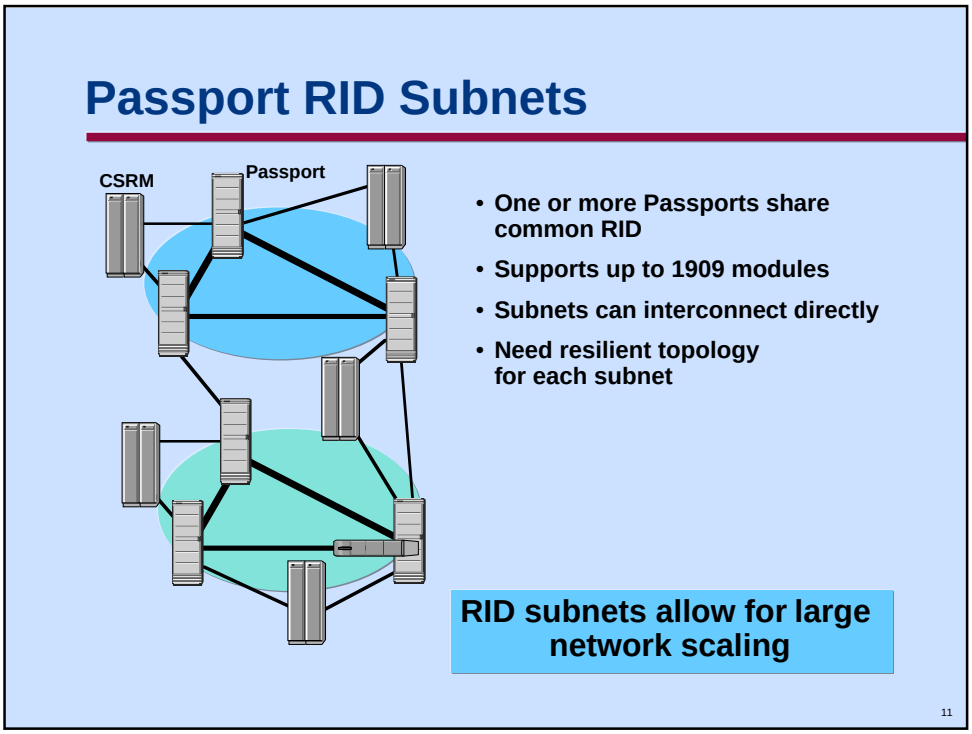
If desired, other call services can be optionally deployed on the CSRM. Note however, that these servers can be deployed anywhere in the network. These call services include:

- NUI Translation;
- Call Redirection server;
- Hunt Group server;
- Dial-Out Routing server;
- Broadcast server; and
- Mnemonic Call server.

Since Passport uses existing DPN-100 call services, no special data reconfiguration (e.g. DNA redirection, hunt group DNAs) is required for AMs when they are migrated to Passport as long as routing connectivity to the correct server is maintained.



The “Networking Considerations” section will provide more technical detail regarding the interworking of Passport with DPN-100 modules, and will also provide some networking strategies for Passport/DPN-100 interworking networks.

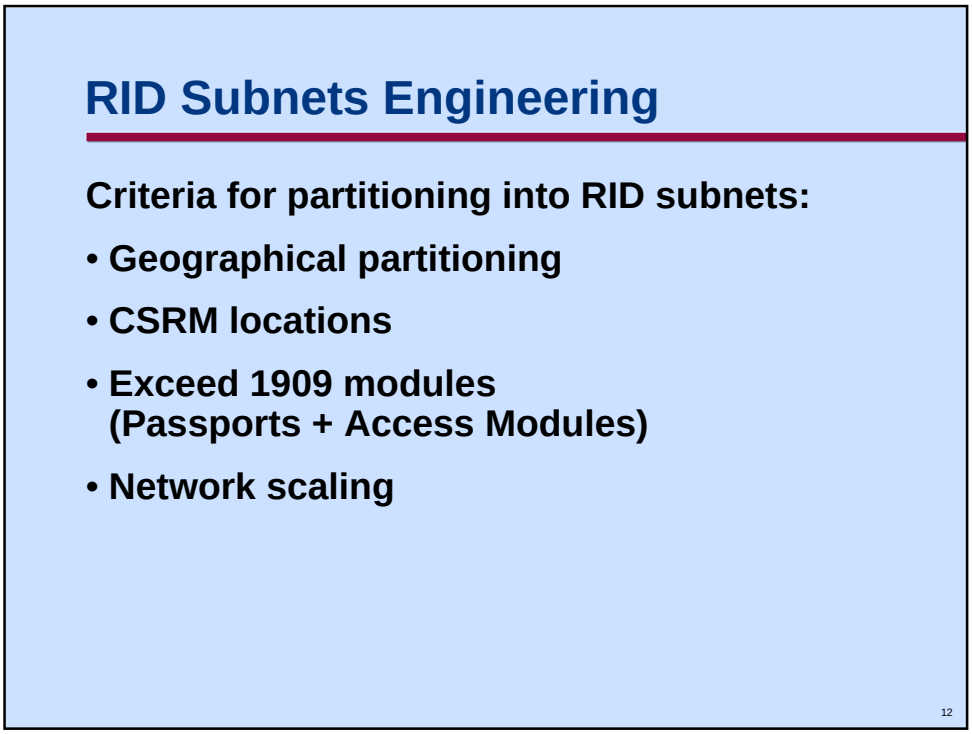


Passports are grouped into RID subnets allowing for more efficient use of RID allocation. Grouping Passport switches into RID subnets extends the number of backbone nodes in a network well beyond the DPN-100 RM backbone size.

Passport RID subnets can be directly interconnected using all Passport trunk types. DPN traffic views the trunk between separate Passport RID subnets as an **internal gateway**, all other traffic types (e.g. voice, LAN) simply perceive the connection as a trunk. The DPN-100 routing systems on Passport do not propagate MID information across internal gateways, thereby reducing the amount of routing traffic propagated between RID subnets, and allowing for MID re-use across RID subnets.

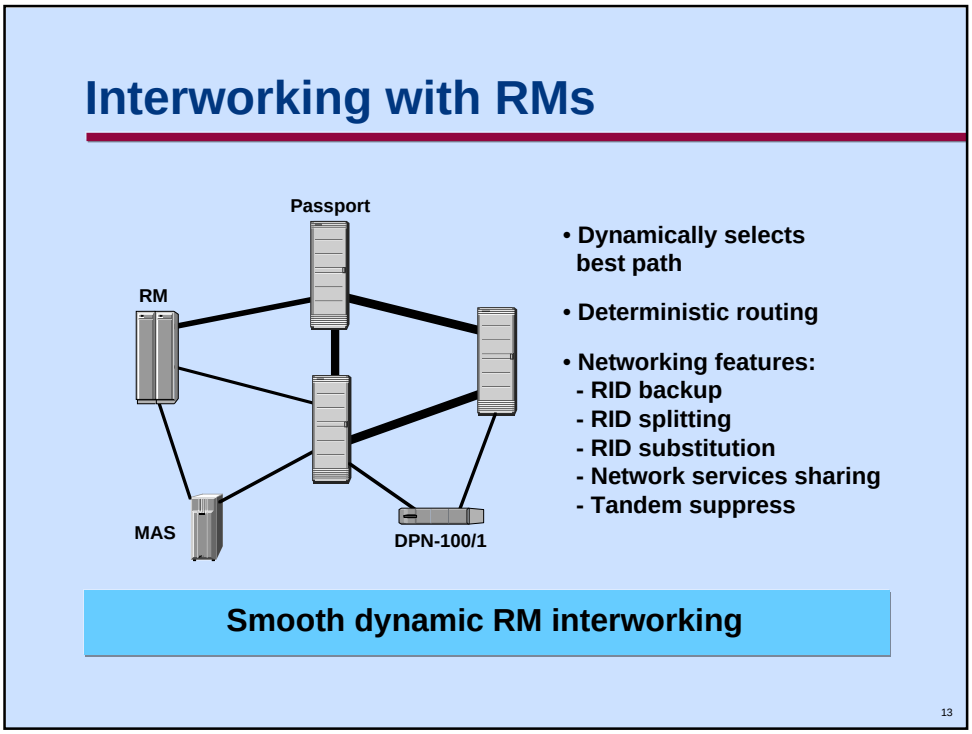
Passport RID subnets dynamically determine their internal gateways to other RID subnets, no special configuration is required. Upon establishing connectivity to another RID subnet, Passport dynamically learns network RID topology information and distributes it across the RID subnet. This assimilation and distribution of information enables Passports within the RID subnet to determine their best paths to other RID subnets or RMs in the network.

RID subnets must be well-connected in order to ensure that a single failure will not sever the RID subnet, since this would result in inconsistent routing.



Passport RID subnets allow DPN-100 networks to easily grow to thousands of nodes. Each RID subnet is a separate routing zone, enabling re-use of MID addressing space within each RID subnet. Reasons for partitioning a Passport/DPN-100 interworking network into more than one RID subnet include:

- **Geographical partitioning**: A global network may consider partitioning into RID subnets to prevent the propagation of routing information about subnet MIDs across transatlantic links, and to simplify MID re-use across different network regions.
- **CSRM locations**: CSRM location may determine RID subnet partitioning for large global networks to ensure that CSRMs are spread across the network in order to be closely located to the source of calls.
- **Exceed 1909 modules**: A Passport RID subnet can support up to 1909 MIDs, including Passport and access modules (note that the term **access module** refers to AMs as well as DPN-100/1, MAP, and Magellan Access Switch (MAS) modules).
- **Network scaling**: The large network scaling feature available in Passport Release 3.3 provides for smooth network scaling to over 1,000 backbone nodes through the use of RID subnets.

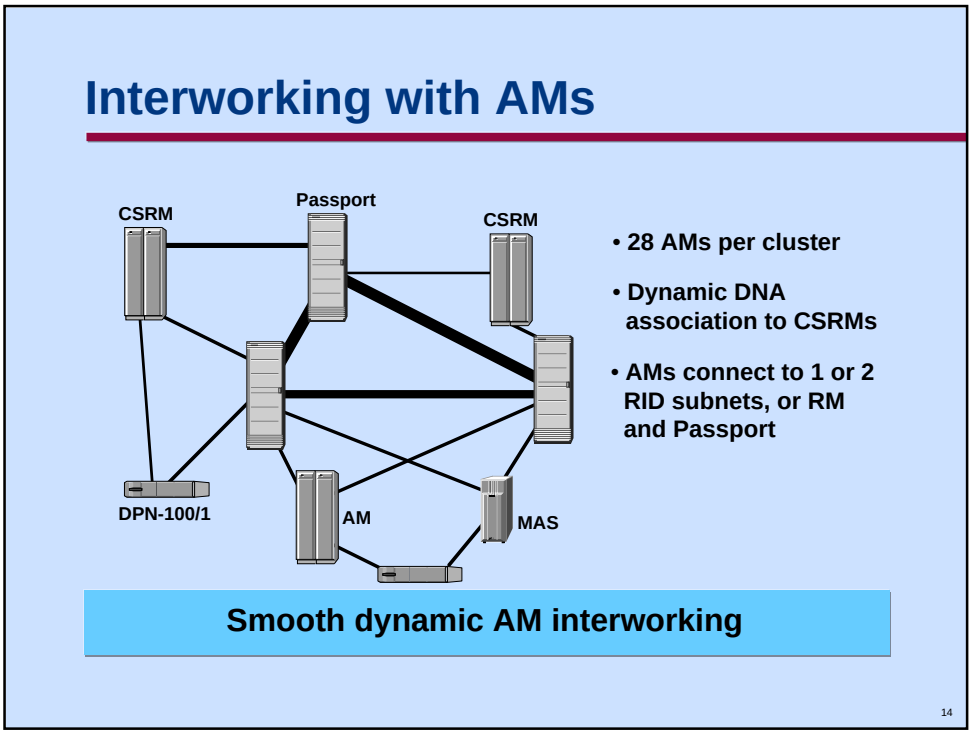


RMs connect to Passport using UTP trunks. RMs do not differentiate between trunks to Passports versus trunks to other RMs. No special provisioning is required to connect an RM trunk to Passport.

The self-learning properties and plug-and-play philosophies of the DPN-100 routing system are maintained across the Passport backbone. RMs learn network RID topology information upon establishing connectivity to the Passport RID subnet. Similarly, the Passport RID subnet learns the RM's RID topology information as well.

RMs select the best path into the RID subnet and to RIDs beyond. When equal cost paths into the RID subnet exist, deterministic routing is used to determine the primary path. Using deterministic routing enables network engineering tools to accurately predict traffic flows.

DPN-100 networking features continue to be supported between RMs and Passport RID subnets. An RM supports **RID backup** to a Passport RID subnet (and vice versa if desired). An RM can be **RID split** to a Passport RID subnet in order to support AM migration. A RID subnet can also be RID split, however, it is unlikely that a RID subnet would be RID split to an RM. **RID substitution** is supported for access modules which are dual connected to both an RM and a Passport RID subnet. **Network Services Sharing (NSS)** is supported between the RM can be **tandem suppressed** to prevent Passport backbone traffic from tandeming through it.

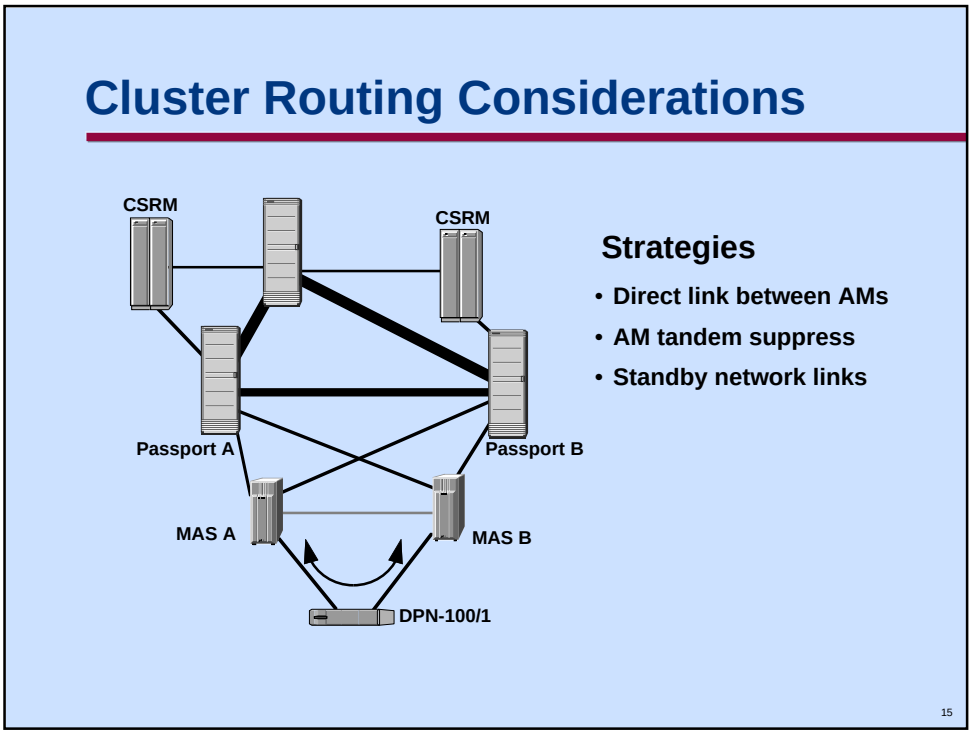


DPN-100 plug and play philosophy is also maintained for Passport/AM interworking. Note that the term AMs includes DPN-100/1, MAP and Magellan Access Switch modules as well as concentrator AMs. No special configuration is required for AM network links in order to establish connectivity to Passport.

Passport supports an AM cluster size of 28 AMs. AMs learn the RIDs of the RID subnet CSRMs upon connecting to a Passport module in the subnet. AMs will dynamically associate their DNAs to the CSRMs upon learning the RIDs.

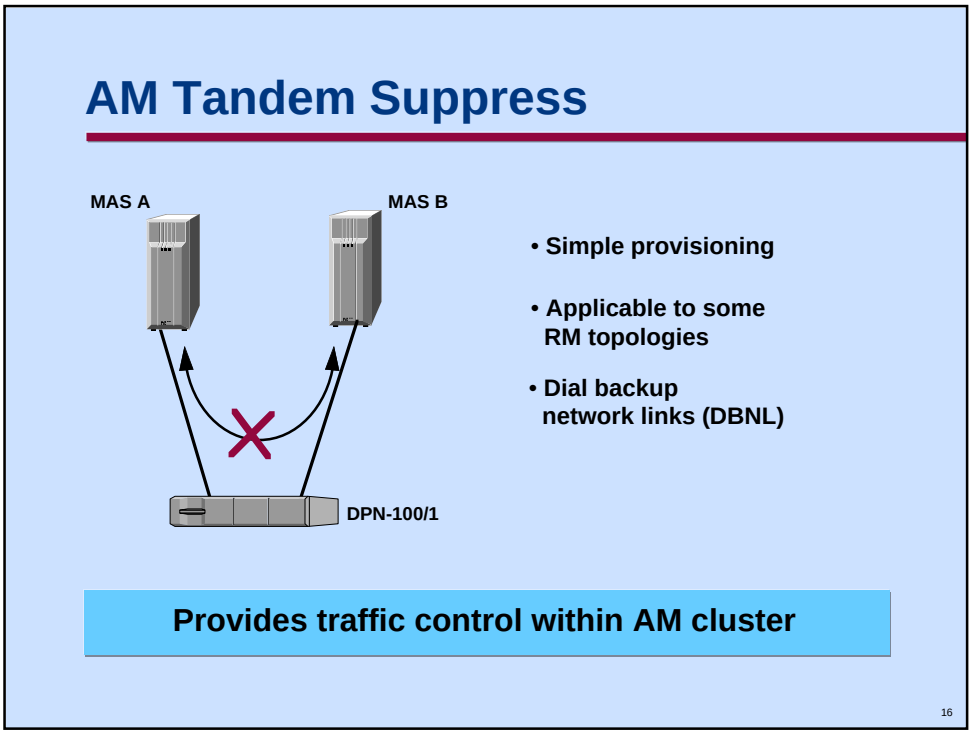
A variety of interworking topologies are supported for AM clusters. AMs can connect to two Passports in the same RID subnet, or in two different RID subnets. As well, an AM can connect to a RID subnet and an RM simultaneously, however, no more than two connections should be established up to the network level.

Easy AM migration procedures allow for operational simplicity when migrating AMs to a Passport backbone. These steps will be presented in later slides.



When AM clusters are connected to a Passport backbone, routing behaviour differs from RM-based cluster routing. Any traffic between modules within a cluster will choose an intra-cluster route rather than route traffic via the Passport. In the example depicted in this slide, traffic between the two first level Magellan Access Switch (MAS) modules (i.e. MAS A and MAS B in the diagram), will tandem via the second level DPN-100/1 rather than routing via either Passport A or Passport B.

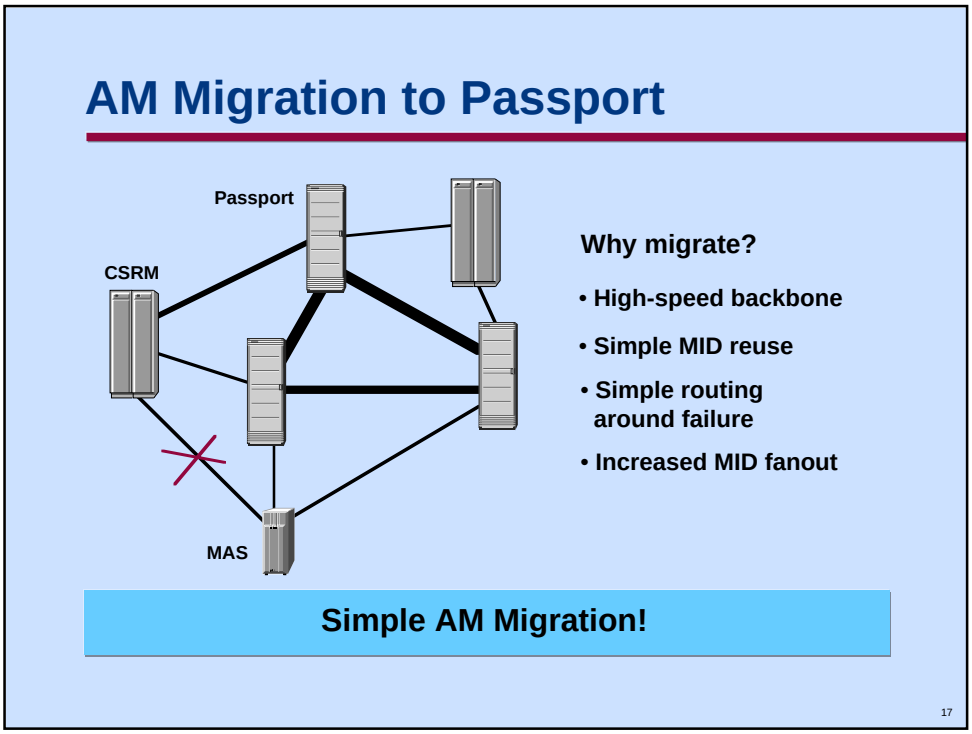
If the community of interest (COI) within the cluster results in intra-cluster routing, several strategies exist to prevent tandeming traffic via modules which are lower in the cluster hierarchy. In particular, if cost-effective, a link can be established between the two first level modules. If this strategy is not feasible, the new **AM Tandem Suppress** feature prevents traffic from tandeming through modules in the cluster under certain topologies. Finally, other cluster topologies lend themselves to strategies using **Standby Network Links**.



The AM tandem suppress feature gives the network operator increased control over intra-cluster routing behaviour by preventing intra-cluster traffic from tandeming through selected AMs. AM tandem suppress is a non-critical provisionable module service data option. It can be used to control AM cluster traffic flows in the following ways:

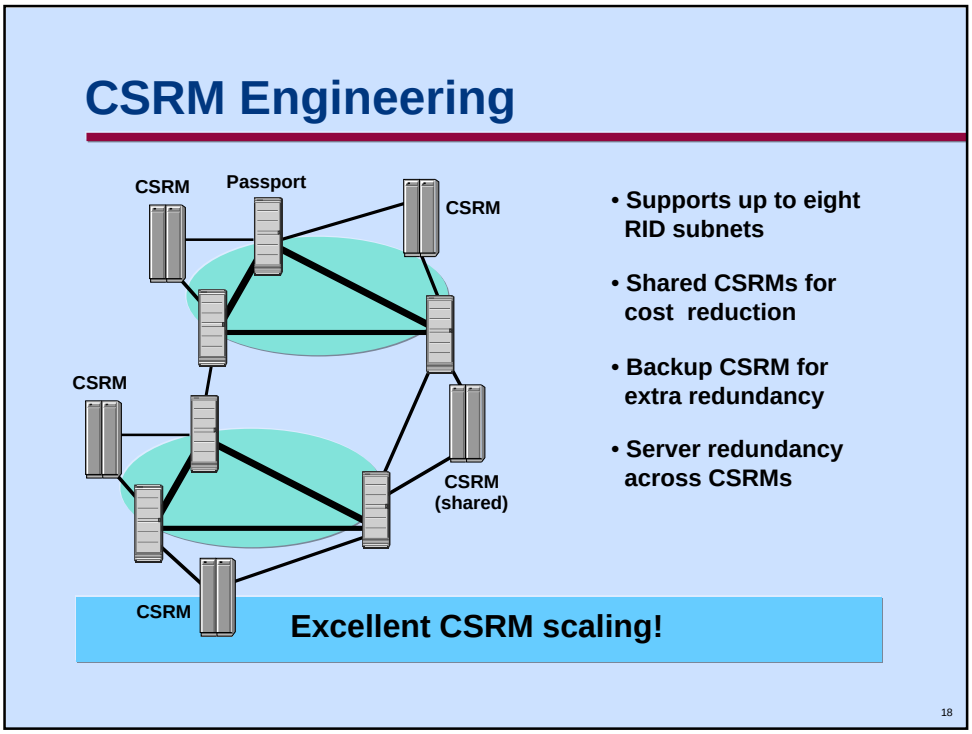
- Prevent traffic from tandeming via AMs with insufficient CPU or link capacity, or via customer premise equipment (CPE)
- Route intra-cluster traffic via a Passport RID subnet
- Prevent traffic from tandeming through a singly-linked AM when both dial backup network link, and the primary link are active simultaneously
- Route intra-cluster traffic via cluster RMs in topologies where first level AMs are singly connected to separate RMs (not a recommended topology, but may be deployed for cost-effective connectivity)

AM tandem suppress is not applicable for all topologies. In some cases, standby network links can be used to alter traffic flow. In all cases, it is necessary to ensure that all modules in the cluster maintain network connectivity during single link failures.



When migrating AMs to a Passport backbone, all existing addressing can be preserved. No DNA renumbering is required. As AMs are migrated to the Passport backbone, RMs can be removed from the backbone, freeing up RID addressing space. RMs can be re-deployed as AMs, thereby preserving original investments. AMs can also remain connected to RMs and still interwork seamlessly to AMs off Passport, however, migrating AMs to Passport provides the following benefits:

- High-speed backbone supports higher speed access from connected AMs
- When deploying large numbers of access modules, routing zone considerations are greatly simplified
- Failure of an AM link to a Passport backbone does not require VCs to go into recovery. Traffic will simply be routed along the alternate path across the RID subnet (if one exists)
- One Passport can support the full 1909 MID space

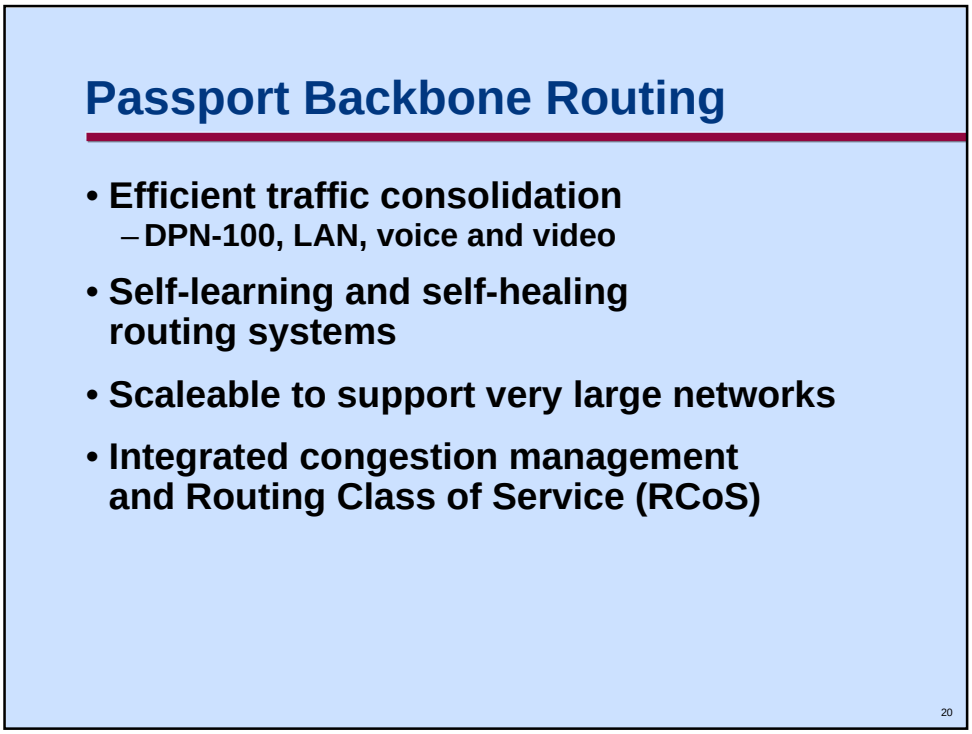


A Call Server Resource Module (CSRM) can be configured to support up to eight RID subnets subject to engineering considerations. A CSRM that is provisioned to serve more than one RID subnet is referred to as a “shared CSRM”. The call servers on the CSRMs have excellent scaling properties, supporting the sharing of CSRMs as a cost-effective networking strategy.

Although a RID subnet selects two active CSRMs, additional CSRMs can be configured to serve the RID subnet as backup CSRMs. The two CSRMs with the lowest RID values are selected as the active CSRMs. Under failure of one of the active CSRMs, a backup CSRM becomes active and all DNAs are immediately associated to this CSRM. When the CSRM with the lower RID becomes available once again, it will take over as an active CSRM. A cost-effective engineering option combines engineering a third CSRM, which is assigned a high RID value, as a shared CSRM with other RID subnets which also behaves as a backup CSRM.

The CSRM call servers provide excellent scaling ability. Up to eight of each type of server can be configured on the CSRM, with calls round-robin loadshared across all PEs supporting a server. The CSRM backplane throughput is equivalent to the frame relay backplane throughput at roughly 5900 data packets per second. Finally, efficient storage of DNAs in the Destination Call Router along with progressive server PE engineering to accommodate DCR table growth can support 50,000 or more DNAs in the DCR table depending on numbering plan allocation schemes. A new product improvement also allows the provisioned SCR table size to exceed 10,000 full length DNAs.

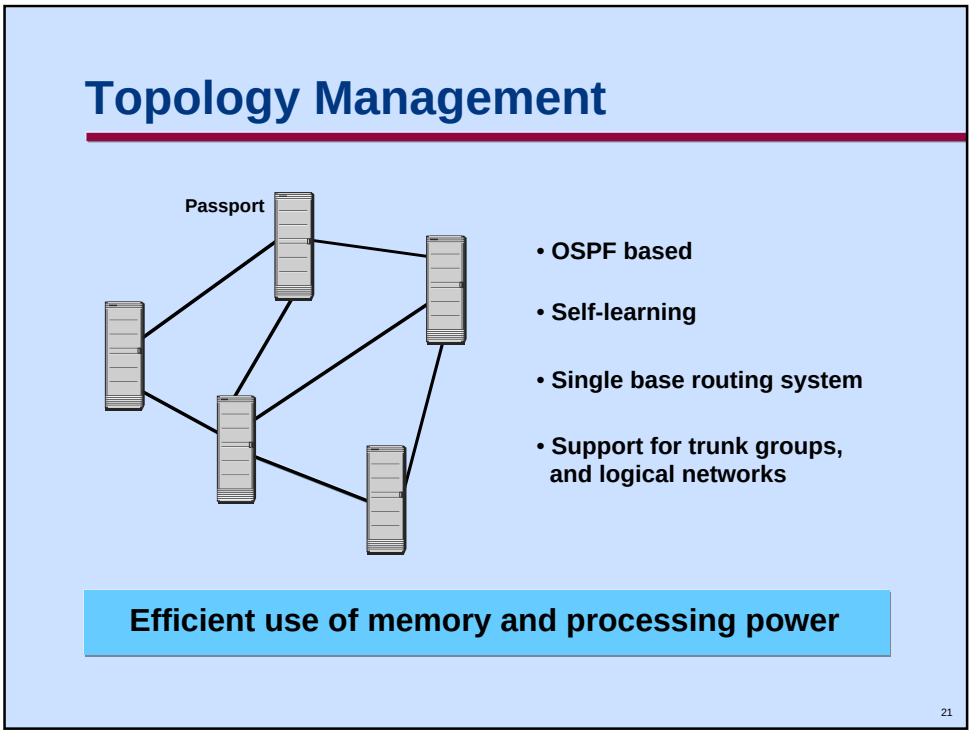
The section “Passport Routing Features” will present an overview of the Passport connectionless routing system’s features and advantages.



Passport offers the best advantages of both switching and routing, providing connection-oriented switching for applications that are delay-sensitive, like voice and video, as well as address-based routing to support LAN internetworking and existing DPN-100 networks. This enables Passport to consolidate multiple networks and applications into a single network infrastructure.

Passport has a fully distributed Open Shortest Path First (OSPF) based routing system. Passport base routing is self-learning with respect to topology, eliminating the administrative task of defining routing tables.

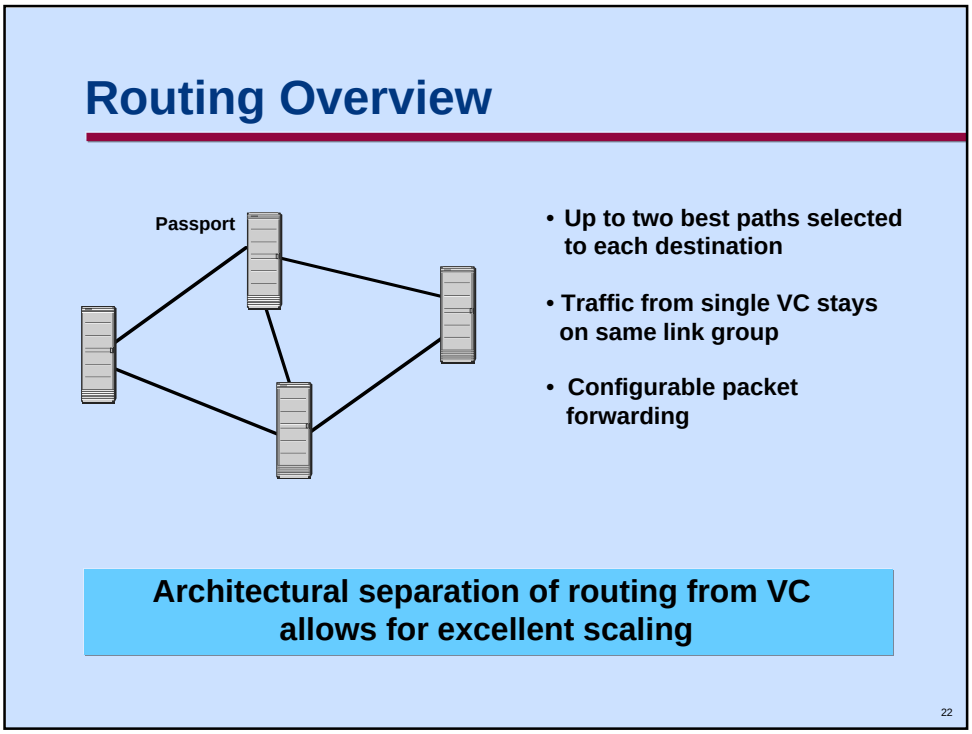
Automatic instant rerouting of traffic is initiated in failure and congestion situations. The overflow routing feature diverts traffic surges by sending frames across an overflow route during peak traffic conditions. This feature is initiated based on frame priority and congestion levels.



Passport switches use an Open Shortest Path First (OSPF) based link state routing protocol to exchange topology information, and to create the network-wide view of the topology. Passport switches automatically learn the network topology upon establishing connectivity to the network. The Passport topology system provides multipath support for up to two equal cost routes to each destination.

Passport's single base routing system provides network topology information to upper level connectionless and connection-oriented routing systems providing efficient overall routing CPU and memory allocation allowing for excellent network scaling. Passport base routing supports both delay and throughput Class of Services.

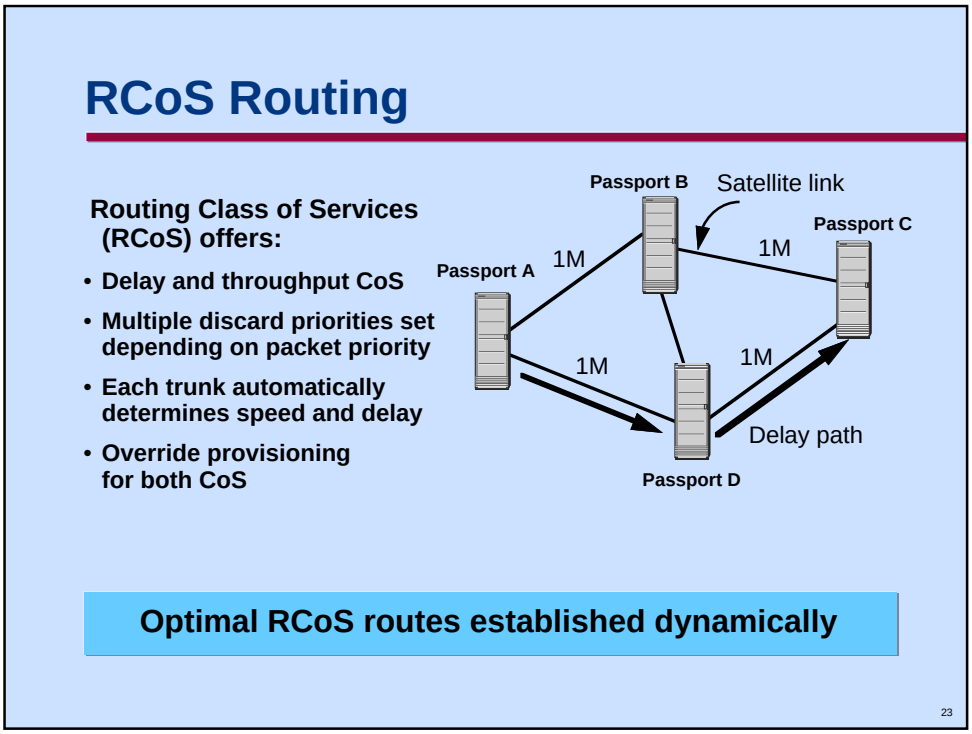
Passport extends OSPF to support logical networks for InterLAN switching, link attributes for PORS, and aggregate bandwidth information to support trunk groups.



Passport connectionless routing provides architectural separation of routing from the virtual circuit (VC), allowing for excellent scaling. Network performance, recovery and response to failure are not impacted by the number of VCs (DLCIs) carried over a trunk. Connectionless routing rapidly responds and re-adapts to changes in network topology.

Connectionless routing supports both the delay and throughput Routing Class of Service (RCoS). Up to two best paths are selected for each destination for each RCoS. Path selection is done in a deterministic manner, enabling network engineering tools to predict traffic flows. Traffic from a VC will always travel across the same link groups in its path across the network unless congestion is encountered. Ordered delivery or loadsharing can be selected for delivery of traffic across link groups.

Passport's connectionless routing system is fully distributed and scaleable. Large networks are supported using hierarchical addressing and routing. Connectionless routing is self-learning, allowing networks to grow with ease since no route provisioning is required as the network grows.

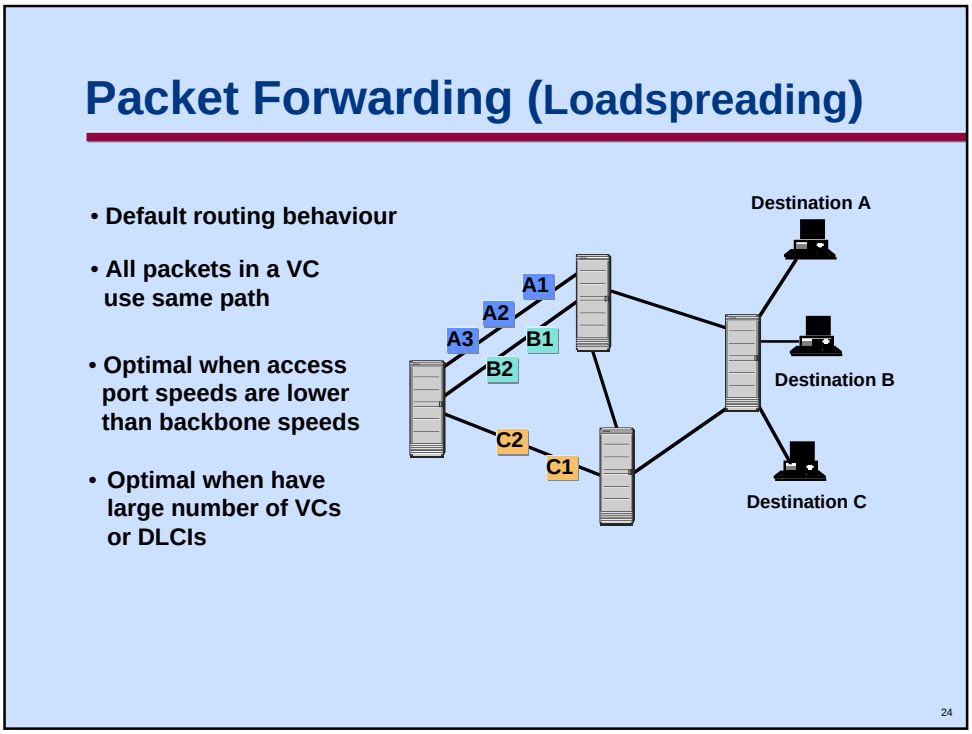


Passport supports both emission priority and discard priority traffic classes. Emission priority allows the user to choose between either Delay or Throughput Classes of Service (COS). The Delay and Throughput CoS is integrated within routing at the network level, and at the access link.

The trunks depicted in the example diagram all have equal bandwidth, however, the trunk between Passport B and Passport C is a satellite trunk. As a result, delay traffic from Passport A to Passport C will choose the path via Passport D in order to avoid the high delay incurred on the satellite link. Throughput traffic however, will be spread across both paths from Passport A to Passport C since they are of equal cost for the throughput COS.

Discard priority establishes the sensitivity to packet loss or discardability of a traffic stream. For example, calls are assigned the lowest discard priority in order to ensure that call packets are discarded first under network congestion. This prevents new calls from being established when congestion is encountered along the call's path.

Passport trunks automatically determine the bandwidth and delay of the link, relaying the information to the routing system in order to determine metric information for link groups. Override provisioning is available for both CoS providing more control over network traffic flows.

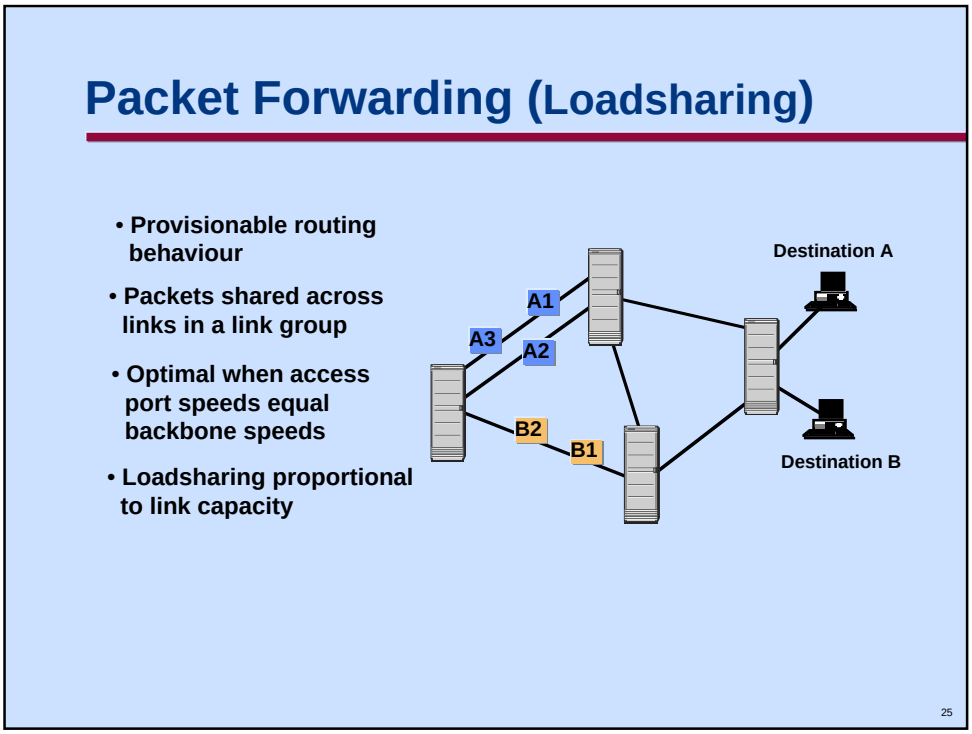


Loadspreading is the default routing behaviour within the Passport backbone. All packets from a single VC are guaranteed ordered delivery to the destination. This ensures efficient processing at the VC end points.

Loadspreading is done across links in a link group, and across link groups (when equal cost paths to the destination exist). In the example diagram, all packets for VC A will sequentially follow each other in an ordered manner across the same link in the link group. The same applies to all packets for VC B. If equal cost paths to the destination exist, then traffic will also be spread across link groups as indicated by VC C in the diagram. Passport will deterministically select up to 2 equal cost multipath link groups to each destination.

Under congestion of a link in the link group, both normal and high reliability traffic will be overflowed onto other non-congested links in the group.

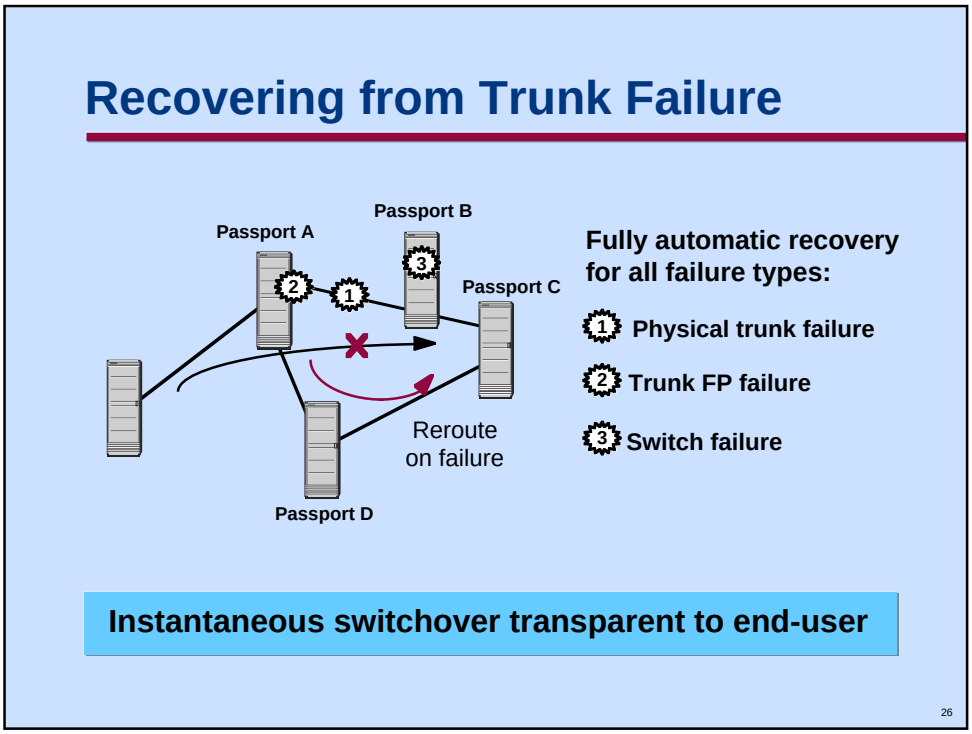
Loadspreading is optimal when many VCs are defined using access speeds which are less than the backbone trunk speeds. This results in even statistical spreading of traffic across all links in a group.



Loadsharing is a provisionable packet forwarding behaviour. Packets from a single VC source are shared across links within a link group. Note that traffic from one VC will not be loadshared across link groups under normal routing conditions. Traffic originating from different VCs and destined to the same destination (e.g. VC A and VC B in the diagram), are spread across link groups if equal cost multipaths exist to the destination. Loadsharing uses the same mechanism as loadspreading to distribute traffic across link groups.

In the diagram, packets for VC A are distributed across all links in the link group. Loadsharing efficiently distributes traffic across all links in a group, ensuring that no link in the group will be congested while others may be under-utilized.

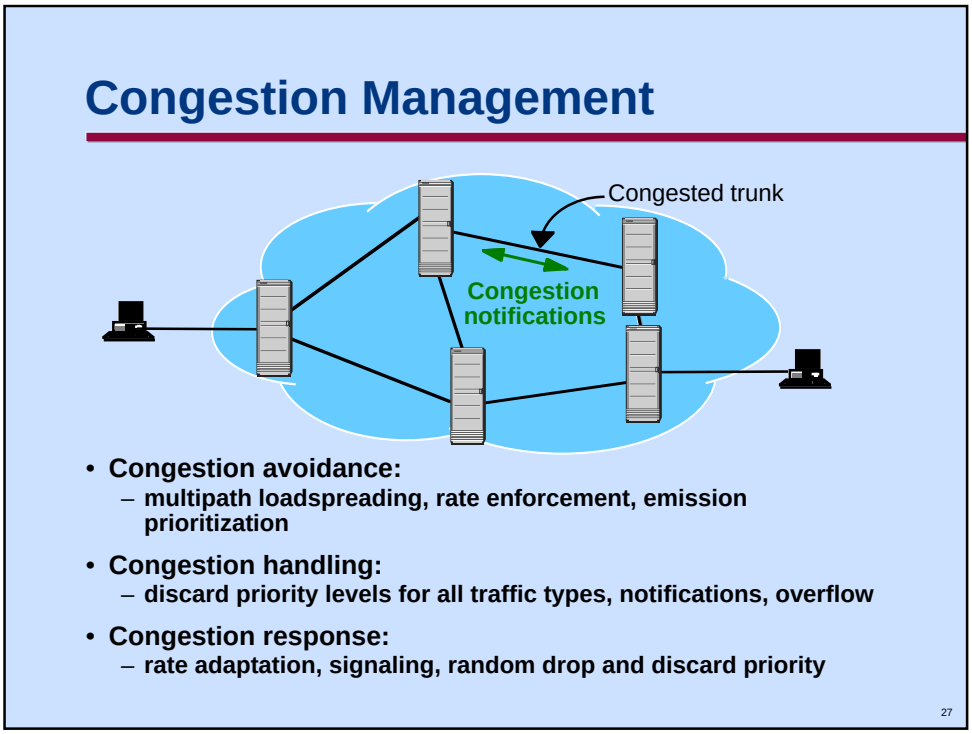
Loadsharing works well when access port speeds equal the backbone speeds. Loadsharing proportionally shares traffic across links in a link group based on link capacity. Since packets from a VC are sent via different links across a link group, minor disordering can occur, however, ordered delivery to the access service is guaranteed by the destination VC.



Passport automatically reroutes traffic under failure conditions regardless of failure type. The link state base routing system provides excellent network convergence, allowing the routing system to rapidly adapt to the failure.

Traffic is rerouted around the failure if an alternate path exists to the destination. Upon recovery, traffic will once again return to the primary path. The traffic switchover under failure and recovery is instantaneous, making the failure completely transparent to end users. In the example diagram, all the traffic between Passport A and Passport B destined to Passport C will be rerouted via Passport D during the failure. When the system recovers, traffic will once again traverse the path between Passport A and Passport B.

In the case of a **physical trunk failure,** the failure is detected by the trunking system on the FP who then propagates the information to the routing system. A **trunk FP failure** is detected directly by the routing system upon learning of the FP failure. Finally, a **switch failure** is detected by the trunks on all connected neighbours similar to a physical trunk failure. In all cases, the OSPF-based routing system allows for rapid convergence since all network nodes can autonomously re-compute network paths upon learning the updated view.

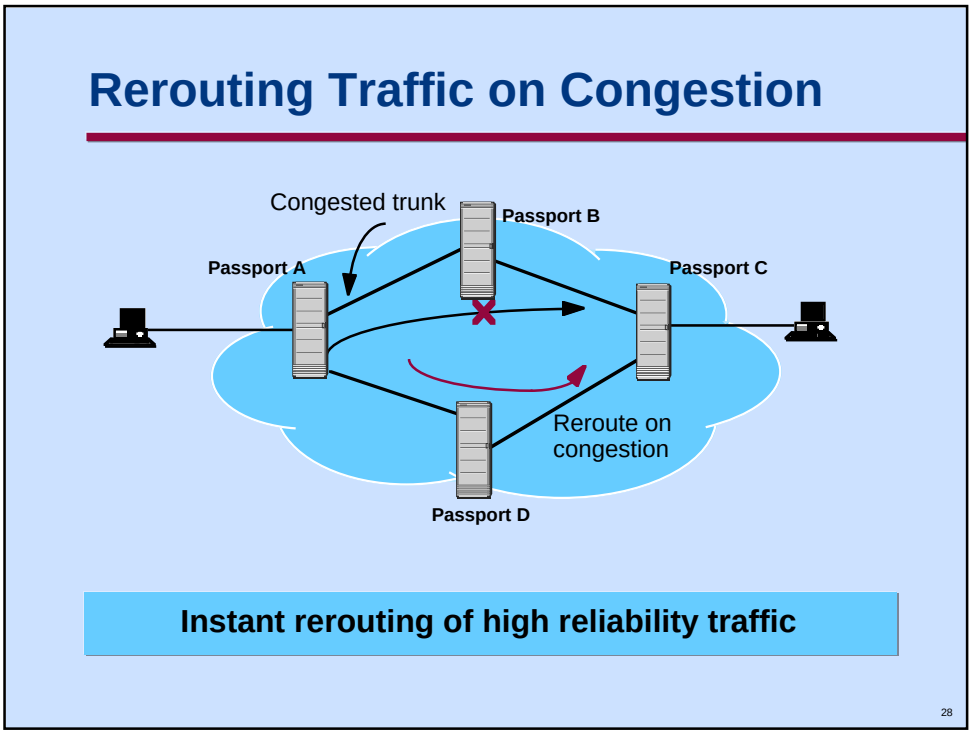


The Passport backbone also includes sophisticated congestion management capabilities. Since there are multiple traffic types on the network, there are a range of congestion response mechanisms available. All these mechanisms are coordinated into a network-wide congestion management capability.

How Passport deals with congestion:

Passport has mechanisms to prevent/react efficiently to congestion:

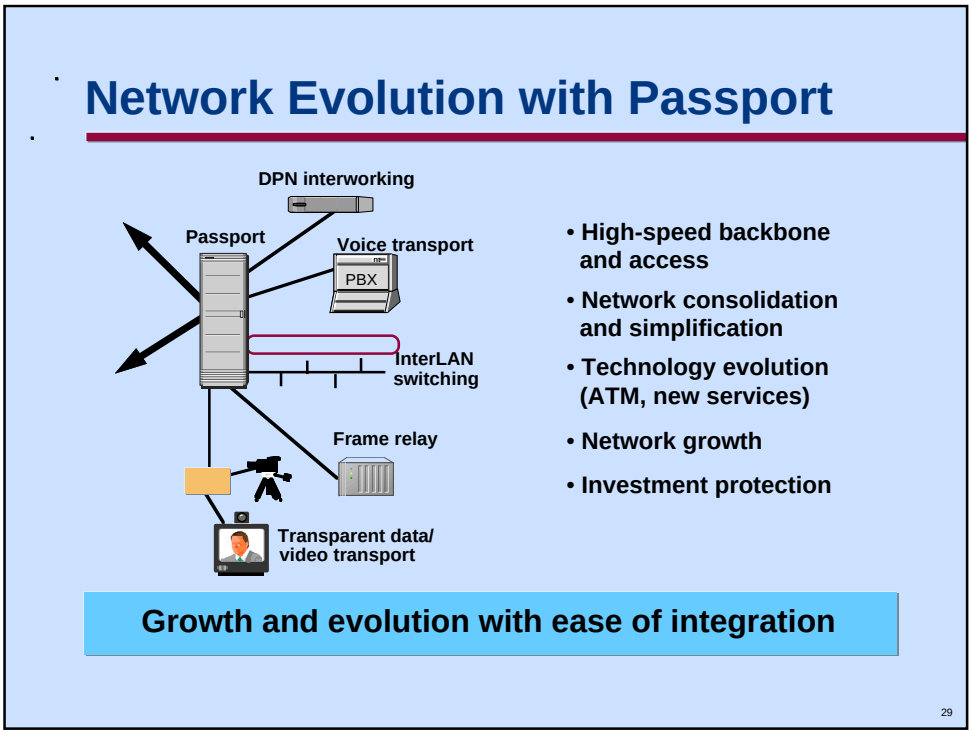
- Forward and Backward Congestion Indications (FCI/BCI) to allow higher layers to react appropriately
- Rate enforcement and rate adaptation by the access service to decrease demand on network resource and abate congestion
- Intelligent packet discards based on packet's importance (discard priority)



The overflow routing feature allows loadsharing of high reliability traffic onto other link groups in order to divert traffic surges by sending frames across an overflow route during peak traffic conditions. Overflow only occurs when an equal cost link group to the destination exists for the Class of Service. Overflow routing provides the ability to redirect frames to their destination rather than discarding them.

In the example diagram, high reliability traffic at Passport A destined to Passport C will be overflow routed via Passport D upon encountering the congested trunk between Passport A and Passport B.

Statistical information on all congestion control events is captured by the Magellan management system on a virtual circuit (VC) or trunk basis to allow Quality of Service verification. It also enables planning and performance tuning of network engineering tools.



Magellan Passport provides a smooth network evolution for DPN-100 networks, while preserving original DPN-100 investments. Interworking with Passport extends current DPN-100 networking capabilities to support evolution of traditional data environments. Passport's simplicity of architecture ensures smooth migration to future technologies and guarantees investment protection.

Passport's ability to combine different traffic types provides many cost-effective savings benefits. Network consolidation and simplification is achieved via the operational efficiencies derived from a single backbone platform as well as the integration/ interworking of products in the Magellan family. This results in reduced equipment, operations, and administration costs.

Passport's excellent scaling ability guarantees ease of network growth to very large network sizes with over 1,000 backbone nodes.

Other Related Sessions:

- DPN-100 Update
- Passport Update
- Magellan Access Solutions
- Passport/DPN-100 Interworking whiteboard clinic
- Inform '96 Demonstration Center