Cisco.com

DVMRP

Module 8

Module Objectives

Cisco.com

- Explain the basic concepts of DVMRP
- Identify the various DVMRP Packet types
- Explain the detailed operation of DVMRP

Module Agenda

Cisco.com

- DVMRP Overview
- DVMRP Packet Formats
- DVMRP Basic Concepts

DVMRP Overview

Cisco.com

- **Distance vector-based**
  - **Similar to RIP**
  - **Infinity = 32 hops**
  - **Subnet masks in route advertisements**
- **Routing information carried in IGMP packets**
  - **IP Protocol 2 (IGMP)**
  - **IGMP type 0x13 (DVMRP)**

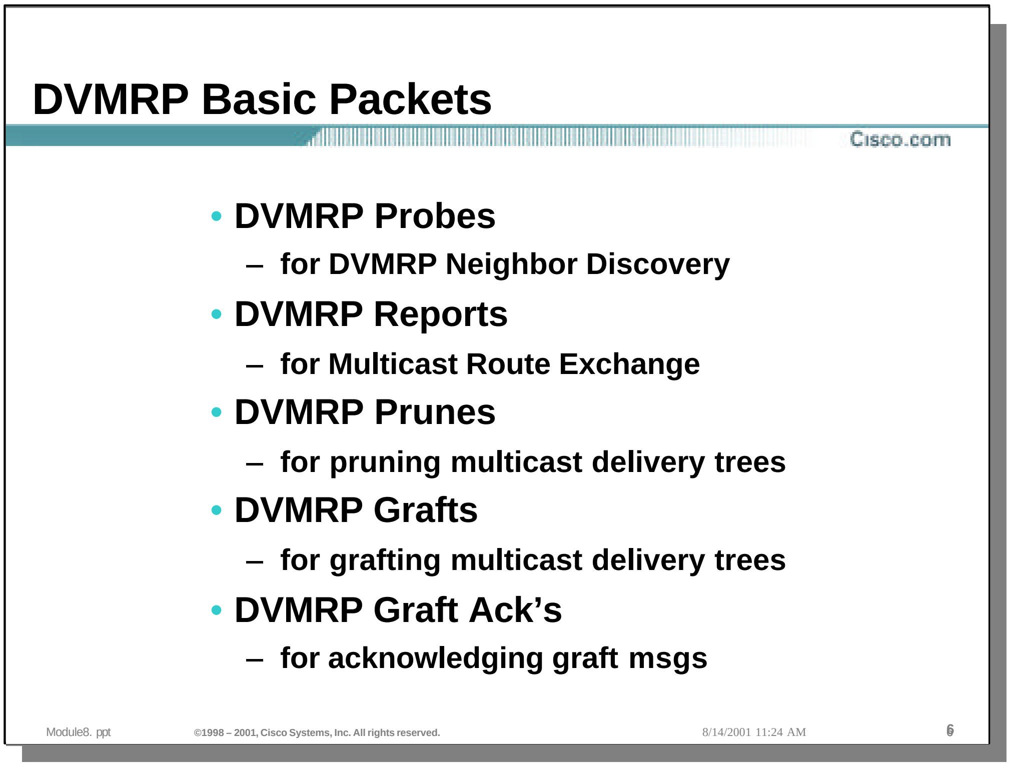
- **DVMRP Overview**
  - DVMRP is a Distance vector based protocol that is modeled after RIPv1 with the following fundamental differences:
    - Infinity = 32 (hops)
    - Subnet masks are sent in the route advertisements which make DVMRP a Classless protocol.
    - DVMRP also makes special use of Poison-Reverse advertisements which is explained in the following slides.
  - DVMRP routing information is carried inside of IGMP (IP protocol 2) packets. Therefore, if you are trying to capture a DVMRP conversation using equipment like a Network General Sniffer, you will need to capture IGMP packets and futher decode them.
    - The IGMP type code for DVMRP is 0x13.

DVMRP Overview

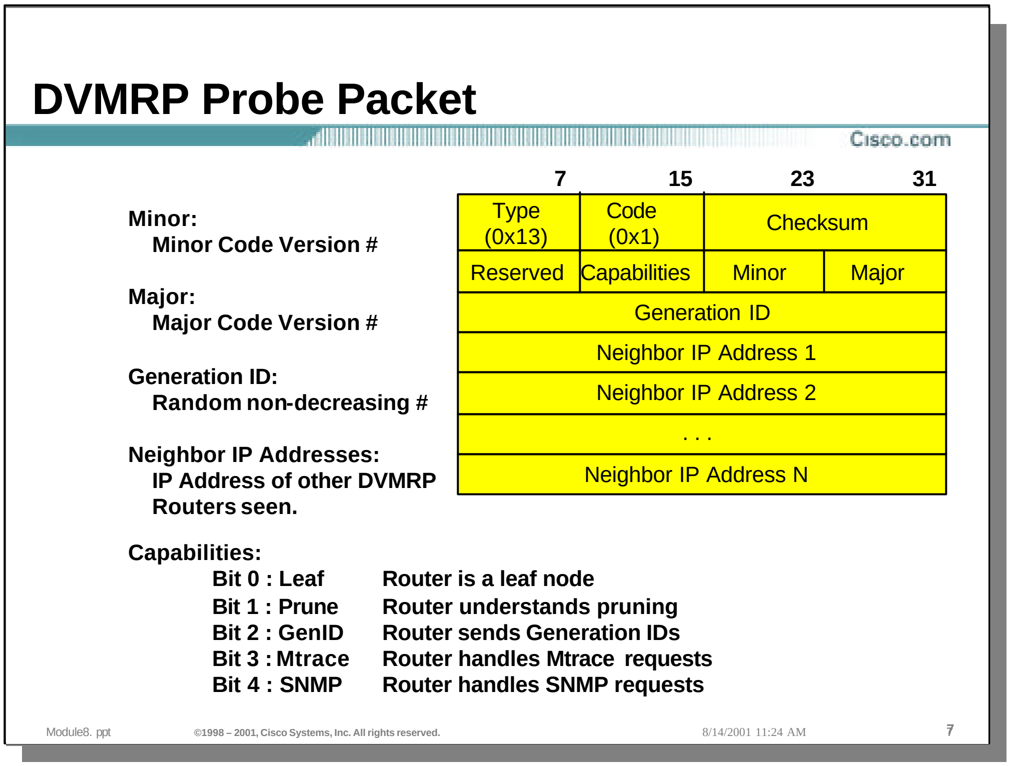
Cisco.com

- **Similar to PIM DM**
  - **Broadcast and prune operation**
  - **Uses DVMRP route table for RPF check**
- **Virtual interfaces**
  - **Physical: Ethernet, FDDI, Token Ring, etc.**
  - **Tunnels: IP-in-IP tunnels (IP Protocol 4)**
- **Current version**
  - **mrouted 3.9**
  - **Available for most UNIX environments**

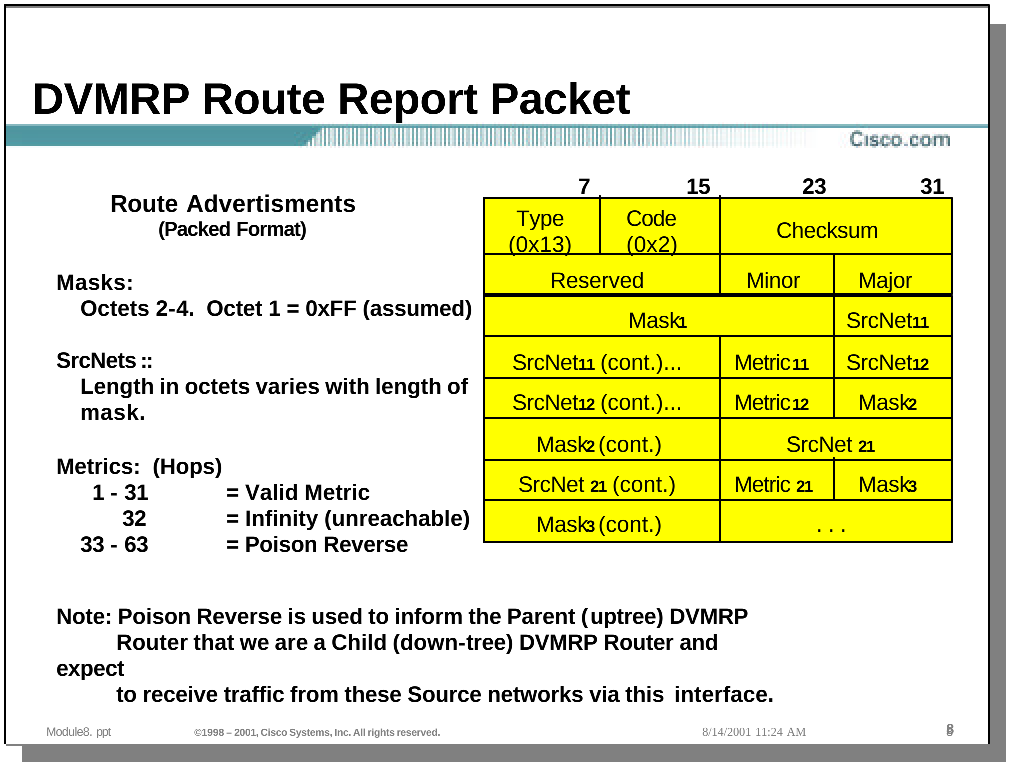
- **DVMRP Overview (cont.)**
  - In many ways, DVMRP operates like PIM Dense mode.
    - The basic “Broadcast and Prune” model is used similar to Dense mode PIM with the exception that DVMRP builds source distribution trees using DVMRP routing information.
    - Unlike PIM which uses the Unicast routing table to perform the RPF check, DVMRP uses its own DVMRP Multicast routing table which is built from periodic DVMRP route advertisements.
  - DVMRP uses the concept of “Virtual” interfaces which may be any of the following:
    - Physical: Ethernet, FDDI, Token Ring, etc. are all examples of “Physical” interfaces.
    - Tunnels: DVMRP makes extensive use of IP-in-IP Tunnels to traverse Unicast-only clouds. (IP-in-IP Tunneling is assigned IP Protocol 4).
  - Current version of DVMRP
    - In most cases, DVMRP is implemented to run on Unix workstations as “mrouted”.
    - At the time that this presentation was written, “mrouted” version 3.8 is the latest version and is available for most Unix environments. A beta version of 3.9 is also in the field and appears to be stable.



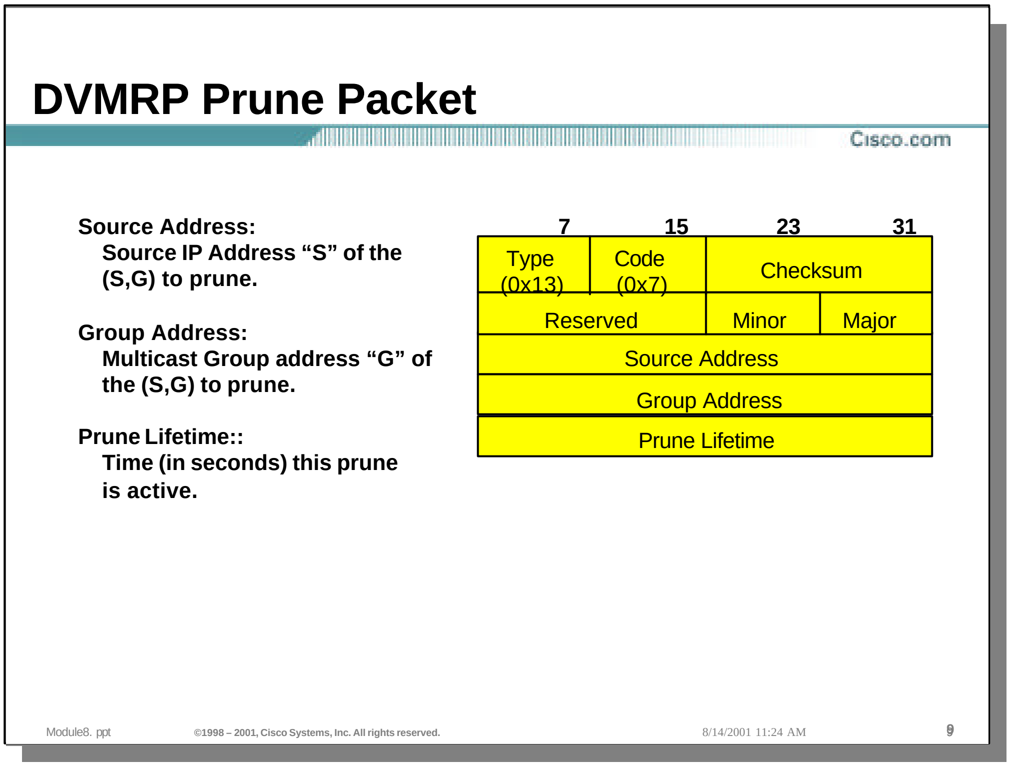
- **DVMRP Basic Packets**
  - Again, DVMRP rides inside of the IGMP protocol, (Type = 0x13). The following different DVMRP packets are differentiated via the Code field of the IGMP packet.
  - DVMRP Probes
    - Used to discover other DVMRP Neighbors on a Network
  - DVMRP Reports
    - Used to exchange DVMRP Source routing information. These packets are used to build the DVMRP Multicast Routing table which, in turn, is used to build Source Trees and also perform RPF checks on incoming multicast packets
  - DVMRP Prunes
    - These function similar to PIM Prunes and prune the multicast delivery tree(s).
  - DVMRP Grafts
    - These function similar to PIM Grafts and graft a branch back onto the multicast delivery tree.
  - DVMRP Graft-Acks
    - These function similar to PIM Grafts-Ack in that they are used to acknowledge DVMRP Graft messages.



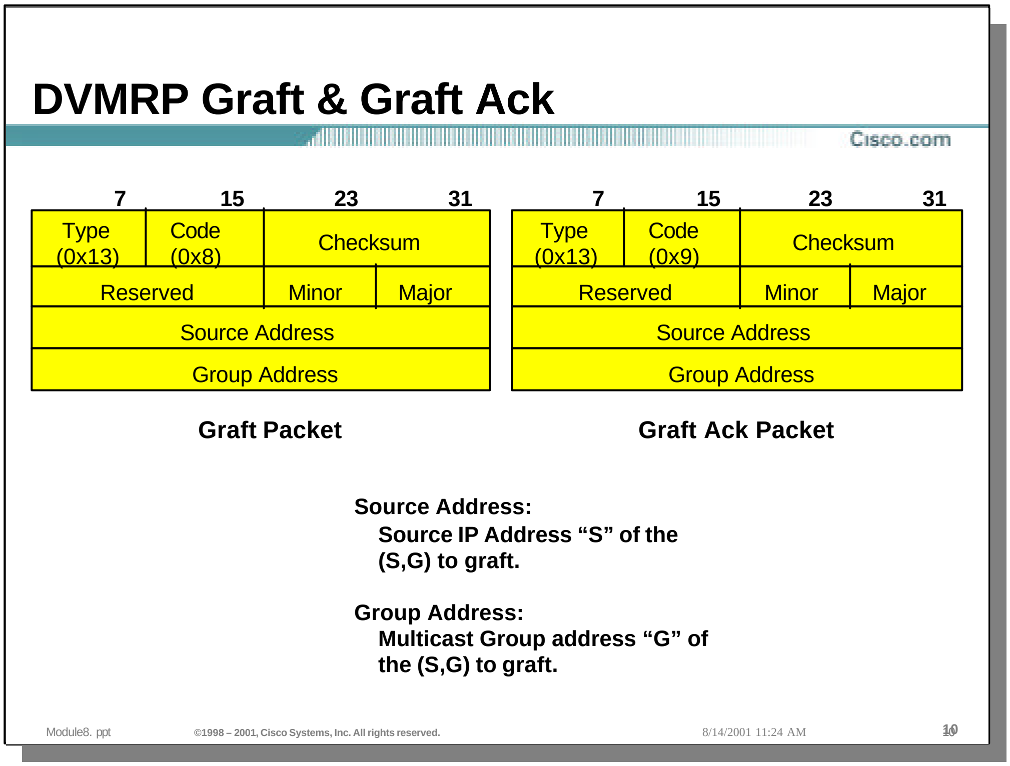
- **DVMRP Probe Packet**
  - Capabilities:
    - Bit 0 : Leaf — Router is a leaf node
    - Bit 1 : Prune — Router understands pruning
    - Bit 2 : GenID — Router sends Generation IDs
    - Bit 3 : Mtrace — Router handles Mtrace requests
    - Bit 4 : SNMP — Router handles SNMP requests
  - Minor:
    - Minor Code Version #
  - Major:
    - Major Code Version #
  - Generation ID:
    - Random non-decreasing number that permits other DVMRP neighbors to detect when detect when this router has rebooted.
  - Neighbor IP Addresses:
    - IP Address of other DVMRP Routers seen by this router. When a receiving DVMRP router sees its IP address in the list, it knows that a 2-way neighbor adjacency has been established.



- **DVMRP Report Packet**
  - Masks:
    - Octets 2-4. Octet 1 = 0xFF (assumed)
  - SrcNets:
    - Length in octets varies with length of mask.
  - Metrics: (Hops)
    - 1 - 31 = Valid Metric
    - 32 = Infinity (unreachable)
    - 33 - 63 = Poison Reverse
  - Poison Reverse metrics have a special function in DVMRP. When a DVMRP router receives a DVMRP Route Advertisement with a Poison Reverse from one of it's DVMRP Neighbors, it indicates that the neighbor is a Child DVMRP Router (I.e. down-tree) which expect to receive multicast traffic from the advertised Source network(s) from this (parent) DVMRP router.



- **DVMRP Prune Packet**
  - Source Address:
    - – Source IP Address “S” of the (S,G) to prune.
  - Group Address:
    - – Multicast Group address “G” of the (S,G) to prune.
  - Prune Lifetime::
    - – Time (in seconds) this prune is active.



- **DVMRP Graft & Graft-Ack Packets**
  - Source Address:
    - – Source IP Address “S” of the (S,G) to graft.
  - Group Address:
    - – Multicast Group address “G” of the (S,G) to graft.

DVMRP Debug Packets

Cisco.com

- **DVMRP Ask-Neighbors2**
  - **request for list of DVMRP Neighbors**
    - **(used by mrinfo)**
- **DVMRP Neighbors2**
  - **response to above**
    - **(used by mrinfo)**

- **DVMRP Debug Packets**
  - DVMRP defines some special “Debug” packets that are used by special Multicast troubleshooting applications such as “mrinfo”. These “debug” packets are as follows:

  - DVMRP Ask-Neighbors
    - Used to request a list of all known Multicast neighbor routers. (This form of the packet is obsolete and has been replaced by the “Ask-Neighbors2” packet.)
  - DVMRP Neighbors
    - Used to respond to the above “Ask-Neighbors” request. (This form of the packet is obsolete and has been replaced by the “Neighbors2” packet.)
  - DVMRP Ask-Neighbors2
    - This is the newer format of the “Ask-Neighbors” packet.
  - DVMRP Neighbors2
    - This is the newer format of the “Neighbors” packet.

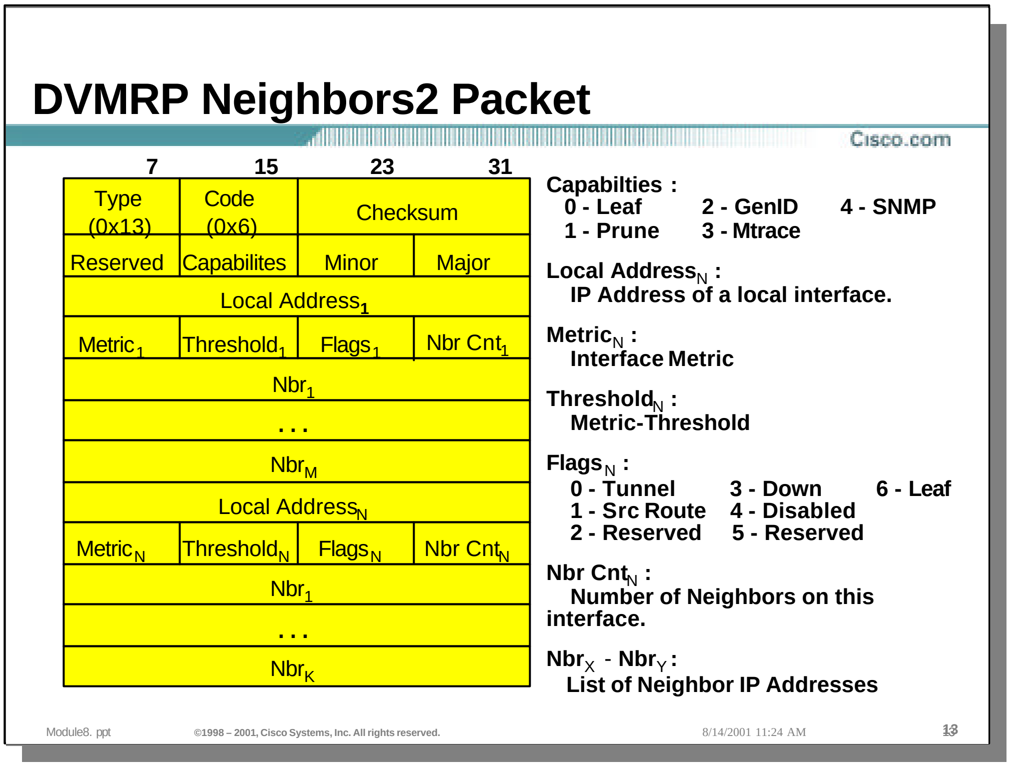
DVMRP Ask-Neighbors2 Packet

Cisco.com

7	15	23	31
Type (0x13)	Code (0x5)	Checksum	
Reserved		Minor	Major

The *Ask-Neighbors2* packet is a unicast request packet directed at a DVMRP router requesting the destination router to respond with a unicast *Neighbors2* message back to the sender.

- **DVMRP Ask-Neighbors2 Packet**
  - The Ask-Neighbors2 packet is a unicast request packet directed at a DVMRP router requesting the destination router to respond with a unicast Neighbors2 message back to the sender.

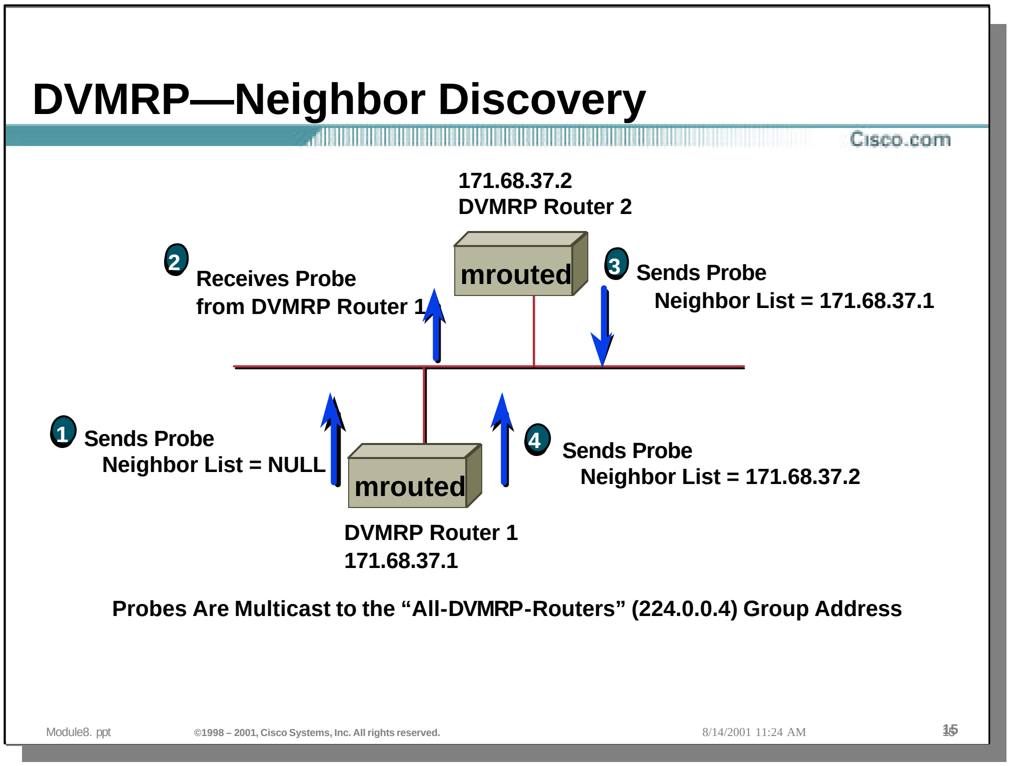


- **DVMRP Neighbors2 Packet**
  - Capabilties :
    - 0 - Leaf 2 - GenID 4 - SNMP
    - 1 - Prune 3 - Mtrace
  - Local AddressN :
    - IP Address of a local interface.
  - MetricN :
    - Interface Metric
  - ThresholdN :
    - Metric-Threshold
  - FlagsN :
    - 0 - Tunnel 3 - Down 6 - Leaf
    - 1 - Src Route 4 - Disabled
    - 2 - Reserved 5 - Reserved
  - Nbr CntN :
    - Number of Neighbors on this interface.
  - NbrX - NbrY :
    - List of Neighbor IP Addresses

DVMRP—Basic Concepts

Cisco.com

- **Neighbor discovery**
- **Route exchange**
- **Source trees**
- **Multicast forwarding**
- **Pruning**
- **Grafting**
- **Tunnels**

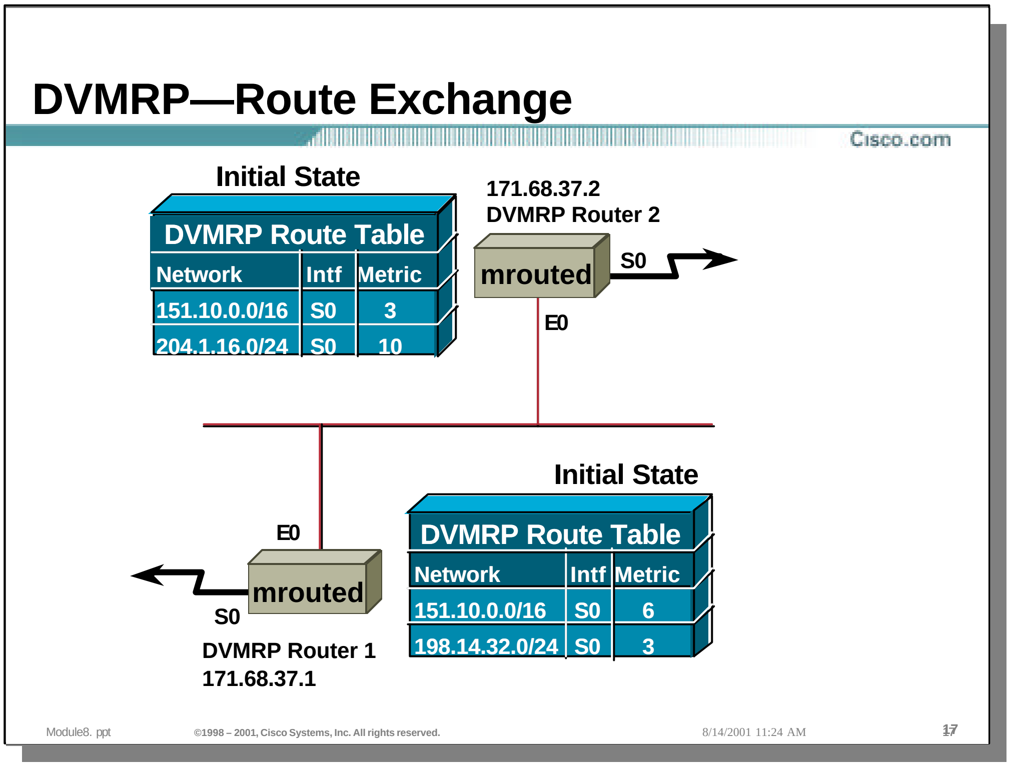


- **DVMRP Neighbor Discovery**
  1) DVMRP "Router 1" multicasts a "DVMRP Probe" packet (to "All-DVMRP-Routers", 224.0.0.4) with an empty Neighbor List.
  2) DVMRP "Router 2" receives this packet and adds "Router 1" to its internal list of DVMRP Neighbors.
  3) DVMRP "Router 2" now multicasts it's own "DVMRP Probe" and includes "Router 1" in the packet's Neighbor List.
  4) DVMRP "Router 1" receives the packet and adds "Router 2" to its internal list of DVMRP Neighbors and responds with a "DVMRP Probe" that has "Router 2" in the packet's Neighbor List.

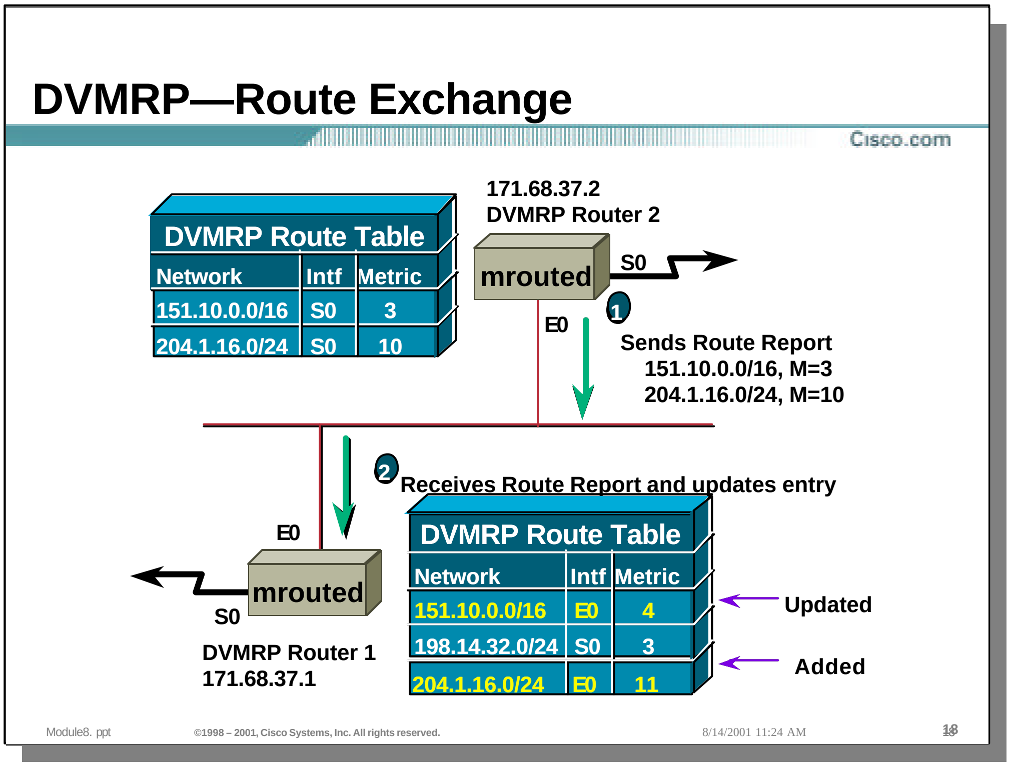
DVMRP—Basic Concepts

Cisco.com

- Neighbor discovery
- Route exchange
- Source trees
- Multicast forwarding
- Pruning
- Grafting
- Tunnels



- **DVMRP Route Exchange**
  - Initial State - Note the following:
    - Both “Router 1” and “Router 2” have DVMRP Route Table entries for network 151.10.0.0/16 albeit with different metrics.

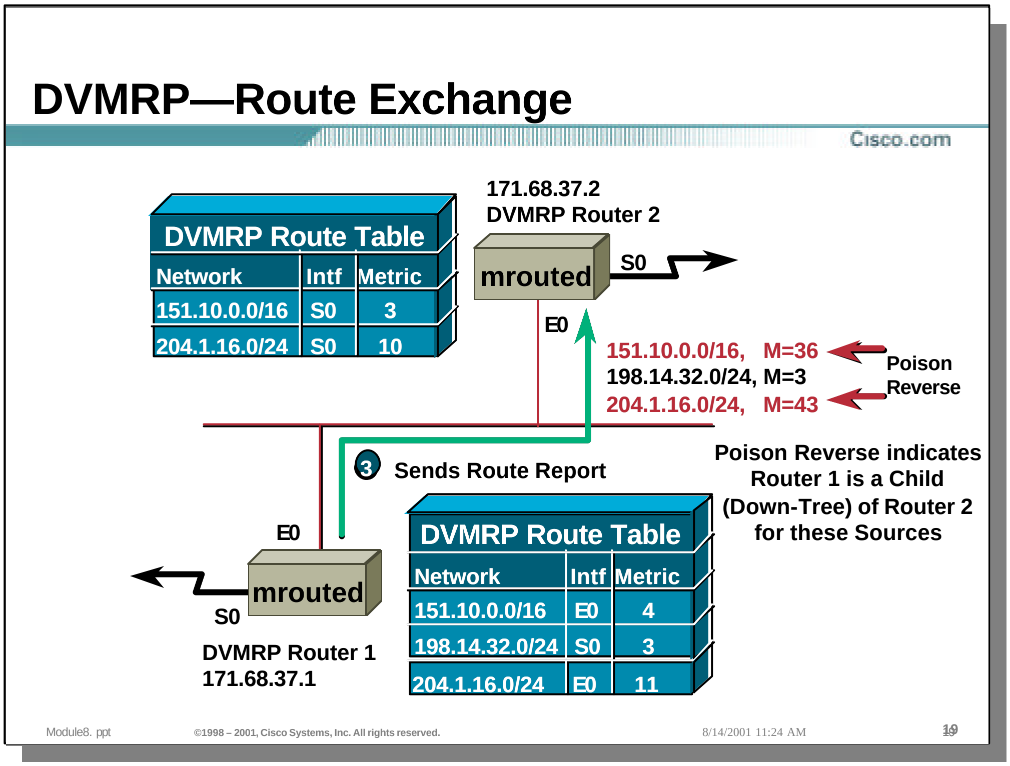


- **DVMRP Route Exchange (cont.)**

  After the two routers are connect via the Ethernet as shown above, the following transactions take place:

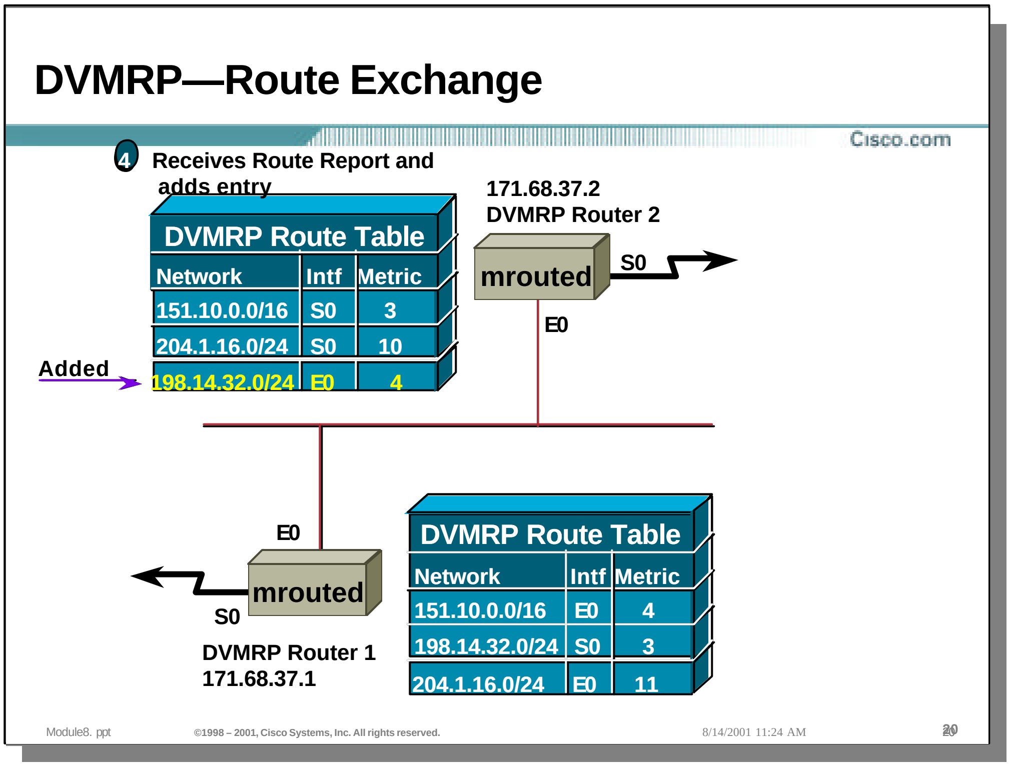
  1) "Router 2" sends a *"DVMRP Route Report"* containing the following two routes from its DVMRP Route Table:
     - 151.10.0.0/16, Metric = 3
     - 204.1.16.0/24, Metric = 10

  2)"Router 1" receives the *"DVMRP Route Report"* increments the received metrics by 1 and performs the following:
     - Updates its entry for 151.10.0.0/16 to point to "Router 2" since the metric of 4 is better than its old metric.
     - Adds and entry for 204.1.16.0/24 pointing to "Router 2".



- **DVMRP Route Exchange (cont.)**

3) "Router 1" sends its own *"DVMRP Route Report"* containing its routes to "Router 2". However, since "Router 2" has a better metric for networks 151.10.0.0/16 and 204.1.16.0/24, it Poison Reverses these two routes by adding 32 to the metric.

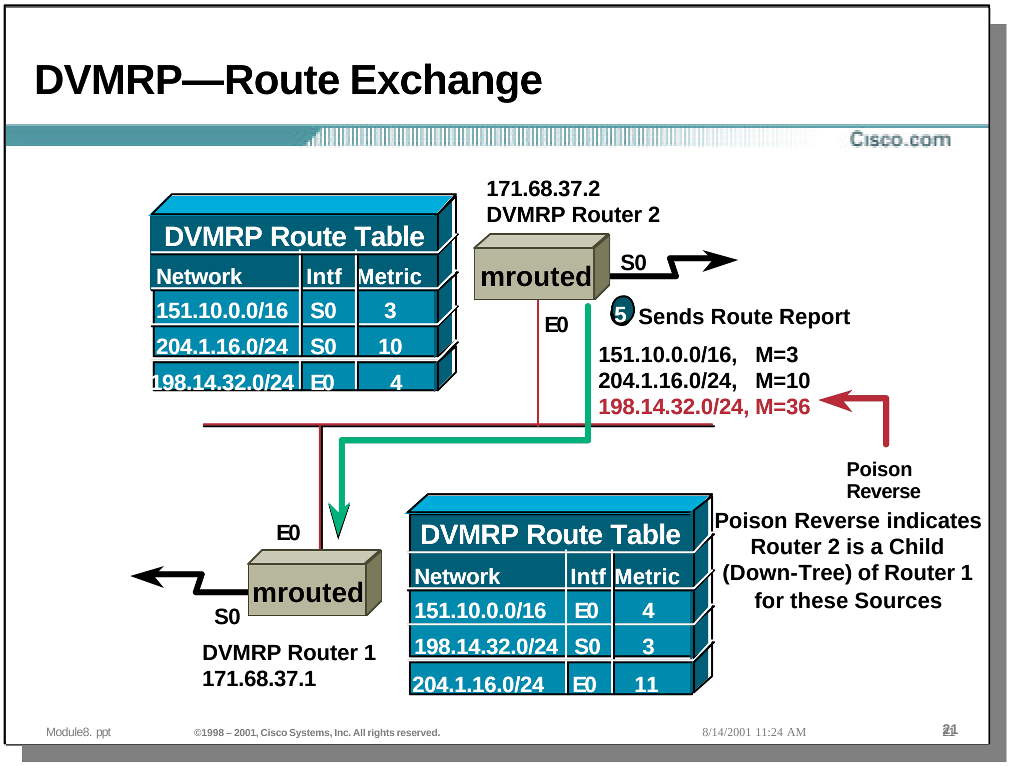


- **DVMRP Route Exchange (cont.)**

4)"Router 2" receives the *"DVMRP Route Report"* from "Router 1" and performs the following steps:

– Adds network 198.14.32.0/24 to its DVMRP Route table (after incrementing the received metric by 1).

– Notes the fact that it received "Poison Reverse" advertisements for networks 151.10.0.0/16 and 204.1.16.0/24 from "Router 1". This indicates that "Router 1" expects to receive multicast traffic for sources in these networks from "Router 2" (I.e "Router 1" is a Child of "Router 2" for these networks).



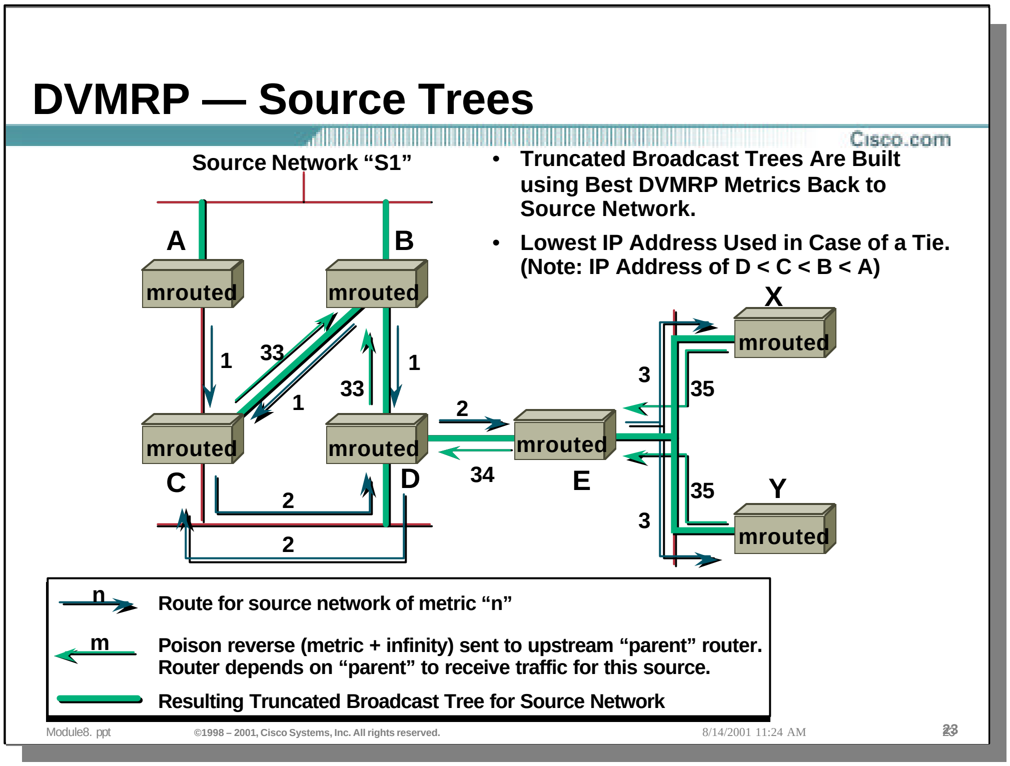
- **DVMRP Route Exchange (cont.)**

5) “Router 2” again sends a *“DVMRP Route Report”* containing its routes to “Router 1”. However, since “Router 1” has a better metric for network 198.14.32.0/24, it Poison Reverses this route by adding 32 to the metric. This informs “Router 1” that “Router 2” expects to receive multicast traffic for sources in network 198.14.32 from “Router 1” (I.e “Router 2” is a Child of “Router 1” for this network).

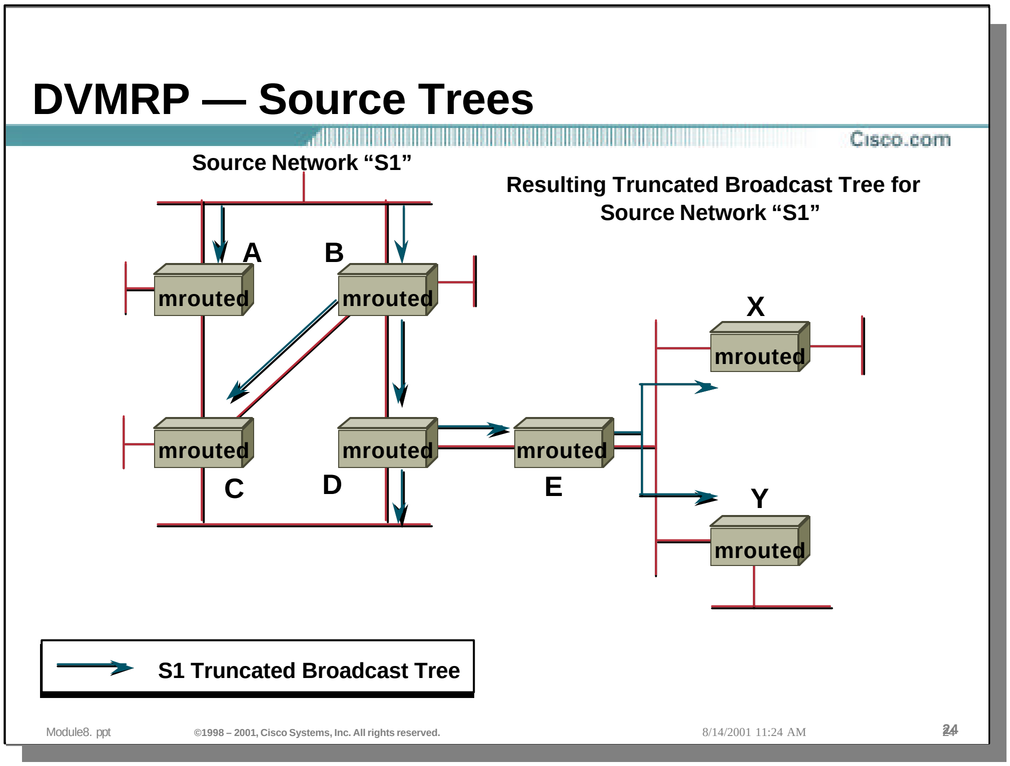
DVMRP—Basic Concepts

Cisco.com

- Neighbor discovery
- Route exchange
- Source trees
- Multicast forwarding
- Pruning
- Grafting
- Tunnels

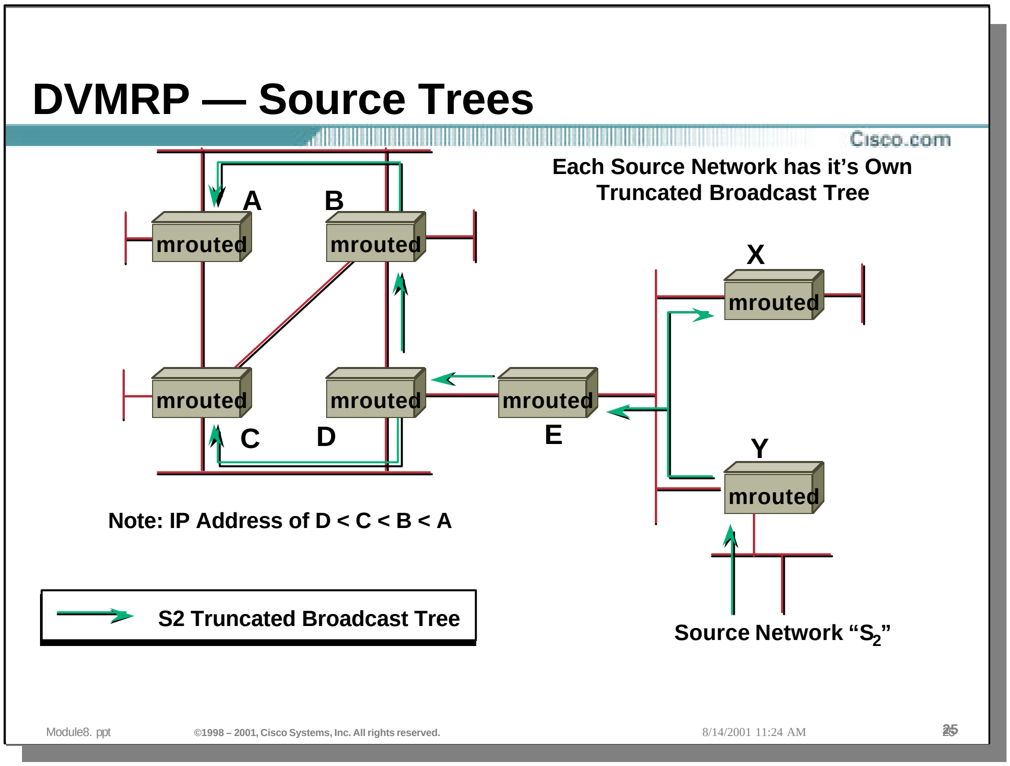


- **DVMRP Source Trees**
  - DVMRP builds its Source Trees utilising the concept of "Truncated Broadcast Trees". The basic definition of a Truncated Broadcast Tree (TBT) is as follows:
    - A Truncated Broadcast Tree (TBT) for source subnet "S1", represent a shortest path spanning tree rooted at subnet "S1" to all other routers in the network.
  - In DVMRP, the abstract notion of the TBT's for all sub-networks are built by the exchange of periodic DVMRP routing updates between all DVMRP routers in the network. Just like its unicast cousin, RIPv2, DVMRP updates contain network prefixes/masks along with route metrics (in hop-counts) that describe the cost of reaching a particular subnets in the network.
  - Unlike RIPv2, a downstream DVMRP router makes use of a special Poison-Reverse advertisement to signal an upstream router that this link is on the TBT for source subnet S1. This Poison-Reverse (PR) is created by adding 32 to the advertised metric and sending back to the upstream router.
- **Example DVMRP TBT for network "S1":**
  - In the above example, DVMRP updates are being exchanged for source network "S1". Routers A and B both advertise a metric of 1 (hop) to reach network S1 to routers C and D. In the case of router D, the advertisement from B is the best (only) route to source network S1 which causes router D to send back a PR advertisement (metric = 33) to B. This tells router B that router D is on the TBT *for source network S1*. In the case or router C, it received an advertisement form both A and B with the same metric. It breaks the tie using the lowest IP address and therefore sends a PR advertisement to router B. B now knows it has two branches of the TBT, one to router C and one to router D. These DVMRP updates flow throughout the entire network causing each router to send PR advertisements to its upstream DVMRP neighbor on the TBT for source network S1.



- **Example DVMRP TBT for network "S1" (cont.)**
  - Once the DVMRP network has converged and all PR advertisements have been sent up the TBT toward source network "S1", the S1 TBT has been built.
  - The drawing above shows the S1 TBT that resulted in the DVMRP route update exchanges from the previous page. Notice that this is a minimum spanning tree that is rooted at source network "S1" and "spans" all routers in the network.
  - If a multicast source were to now go active in network "S1", the DVMRP routers in the network will initially "flood" this sources traffic down the S1 TBT.

DVMRP — Source Trees

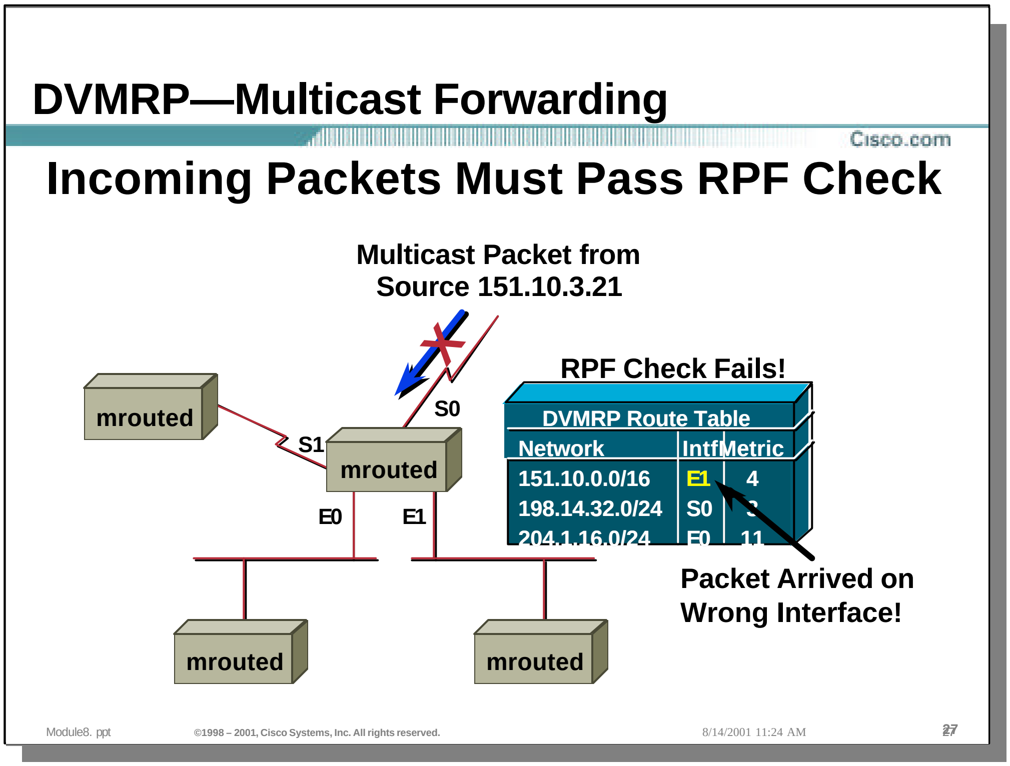


- **Every source network has its own TBT**
  - In the drawing above, the TBT for network S2 is shown. This TBT would also be created by the exchange of DVMRP route updates and by PR advertisements sent by all routers in the network toward network S2.
  - It is important to remember that these TBT's simply exist in the form of PR advertisements in the DVMRP routing tables of the routers in the network and as such, there is one TBT for every source network in the DVMRP network.
- **Advantages of TBT's**
  - The advantage of TBT's is that the initial flooding of multicast traffic throughout the DVMRP network is limited to flowing down the branches of the TBT. This insures that there are no duplicate packets sent as a result of parallel paths in the network.
- **Disadvantages of TBT's**
  - The disadvantage of using TBT's is that it requires separate DVMRP routing information to be exchanged throughout the entire network. (Unlike other multicast protocols such as PIM that make use of the existing unicast routing table and do not have to exchange additional multicast routing data.
  - Additionally, because DVMRP is based on a RIP model, it has all of the problems associated with a Distance-Vector protocol including, count-to-infinity, holddown, periodic updates.
    - One has to ask oneself, "Would I recommend someone build a unicast network based on RIP today?" The answer is of course not, protocols like OSPF, IS-IS, and EIGRP have long since superseded RIP in robustness and scalability. The same is true of DVMRP.

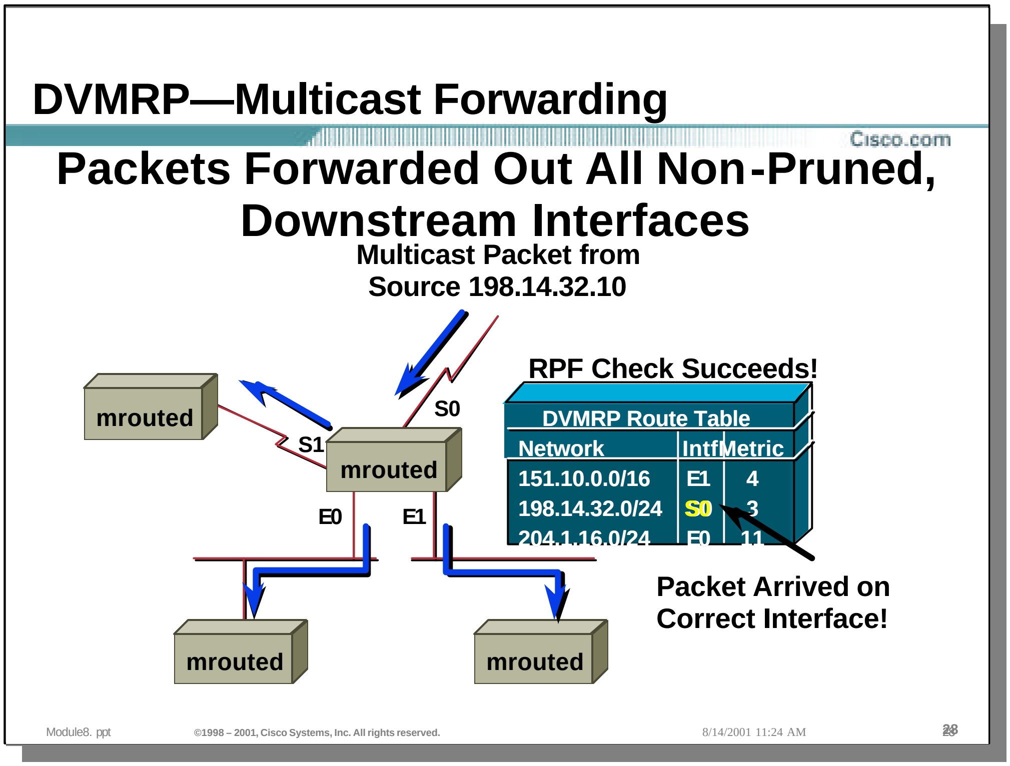
DVMRP—Basic Concepts

Cisco.com

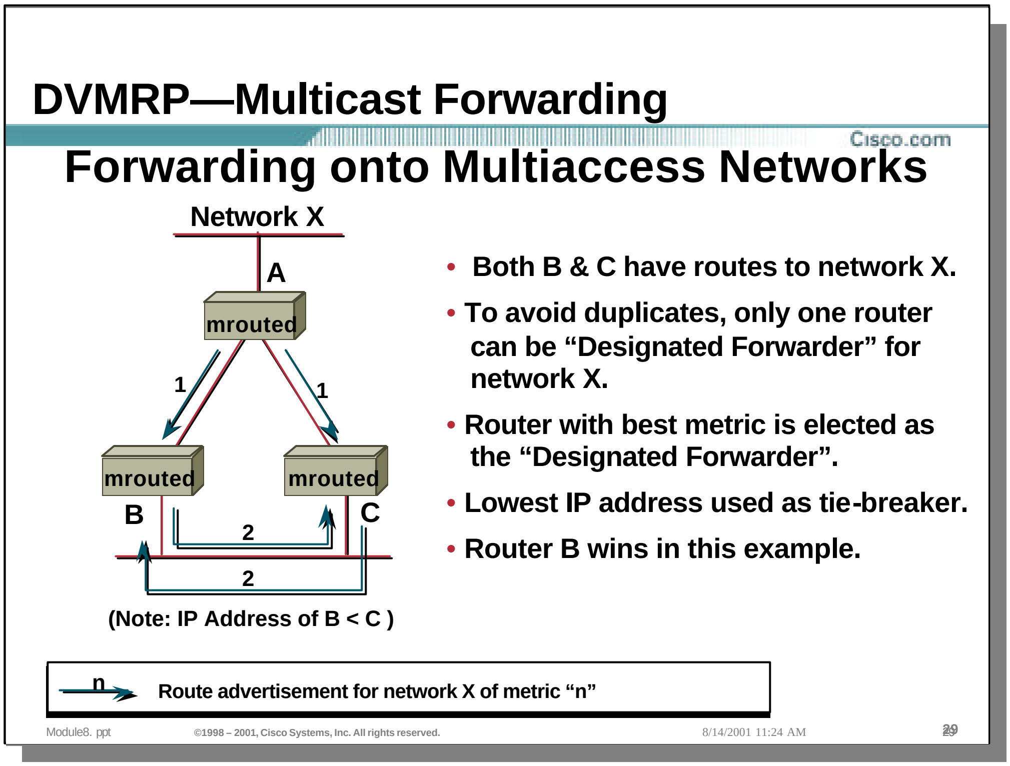
- Neighbor discovery
- Route exchange
- Source trees
- **Multicast forwarding**
- Pruning
- Grafting
- Tunnels



- **DVMRP Multicast Forwarding**
  - Just as in PIM, incoming packets must pass a "Reverse Path Forwarding" (RPF) check before they are accepted. However, DVMRP has its own DVMRP Route Table that is used for performing the RPF check.
  - In the above example, a multicast packet from a source in the 151.10.0.0/16 network was received via interface S0. However, the DVMRP Route Table shows that the correct interface should be E1, not S0. Therefore, the RPF check for this packet fails and the packet is discarded.



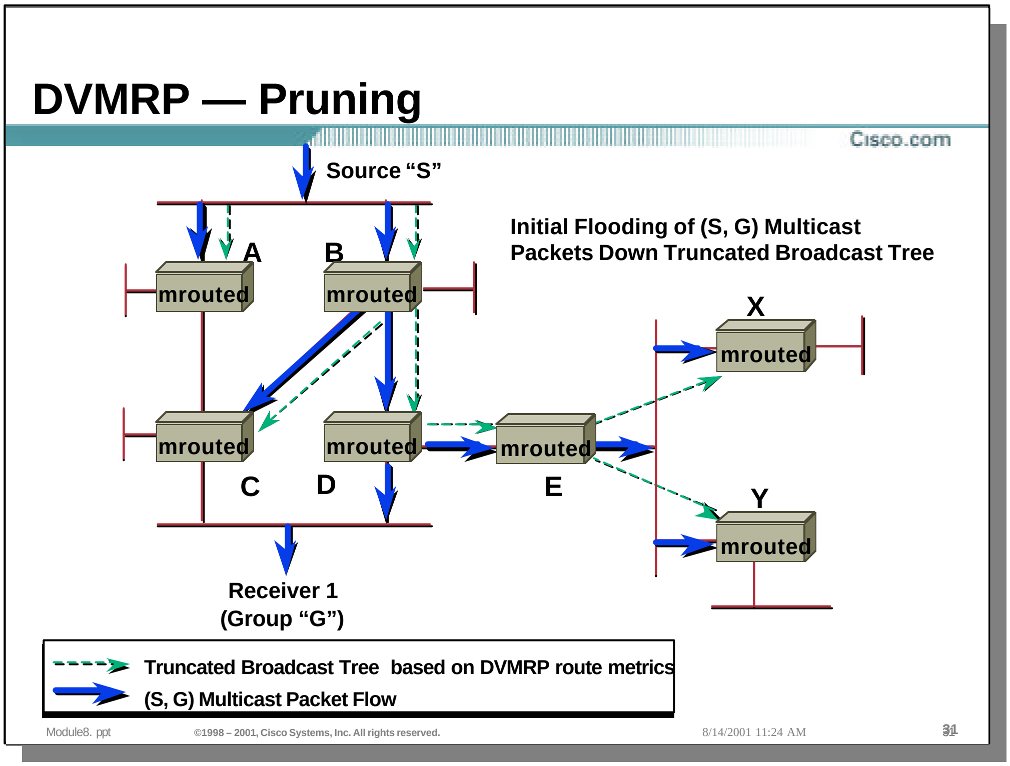
- **DVMRP Multicast Forwarding (cont.)**
  - In the above example, a multicast packet from a source in the 198.14.32.0/24 network was received via interface S0. In this case the DVMRP Route Table shows that the correct interface is S0. Therefore, the RPF check for this packet succeeds and the packet is forwarded out all unpruned interfaces on the source tree.



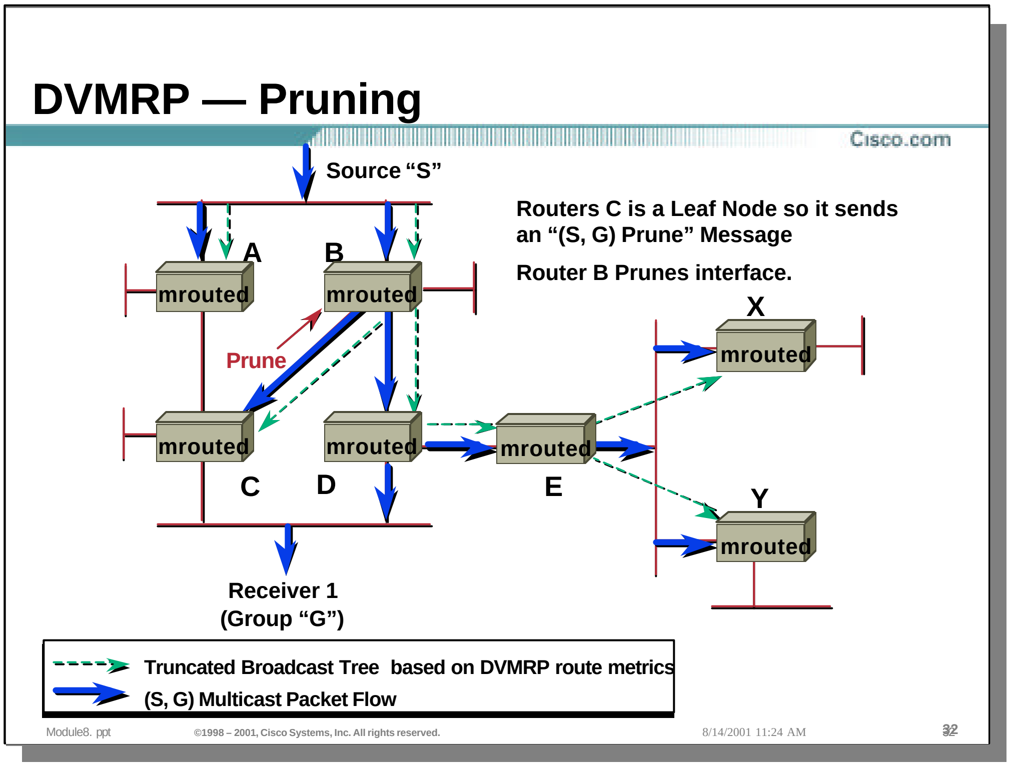
- **DVMRP Multicast Forwarding (cont.)**
  - When two or more routers share a common multi-access network, only one can be the "Designated Router" which is responsible for forwarding a source network's traffic onto the multi-access network; otherwise duplicate packets will be generated.
  - The "Designated Forwarder" is selected based on the best route metric back to the source network (with the Lowest IP Address used as a tie-breaker).
  - In the example above, both Router B and C share a common multi-access network and each have routes to network X. Since both have the same metric to network X, the lowest IP address is used to break the tie (in this case, Router B wins).

DVMRP—Basic Concepts

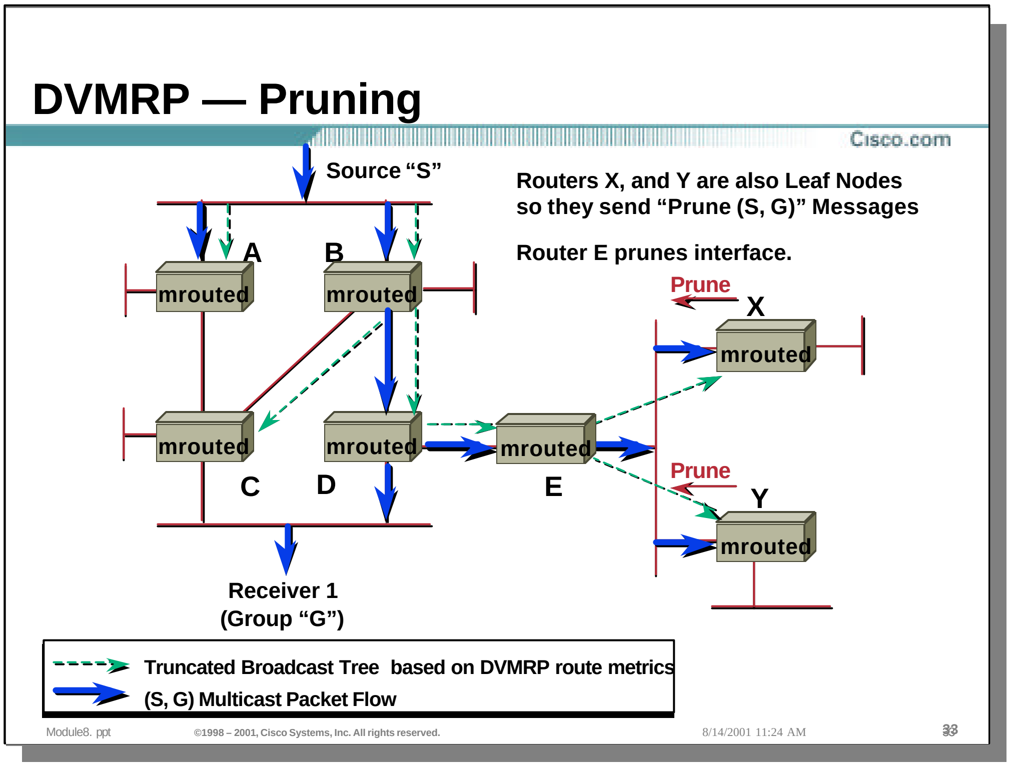
- Neighbor discovery
- Route exchange
- Source trees
- Multicast forwarding
- Pruning
- Grafting
- Tunnels



- **DVMRP Pruning**
  - In this example we see source "S" has begun to transmit multicast traffic to group "G".
  - Initially, the traffic (shown by the solid arrows) is flooded to all routers in the network down the Truncated Broadcast Tree (indicated by the dashed arrows) and is reaching Receiver 1.

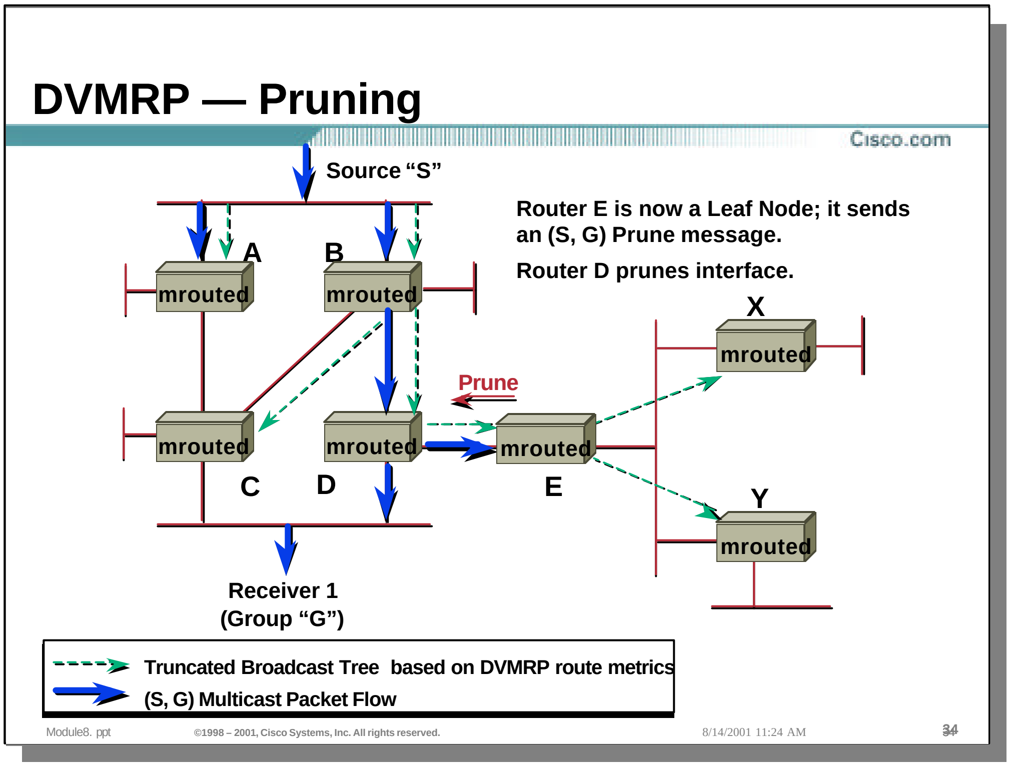


- **DVMRP Pruning (cont.)**
  - At this point, we see that router C is a leaf node on the TBT and has no need for the traffic. Therefore, it sends a DVMRP (S, G) Prune message up the TBT to router B to shutoff the unwanted flow of traffic.
  - Router B receives this (S, G) Prune message and shuts off the flow of (S, G) traffic to router C.

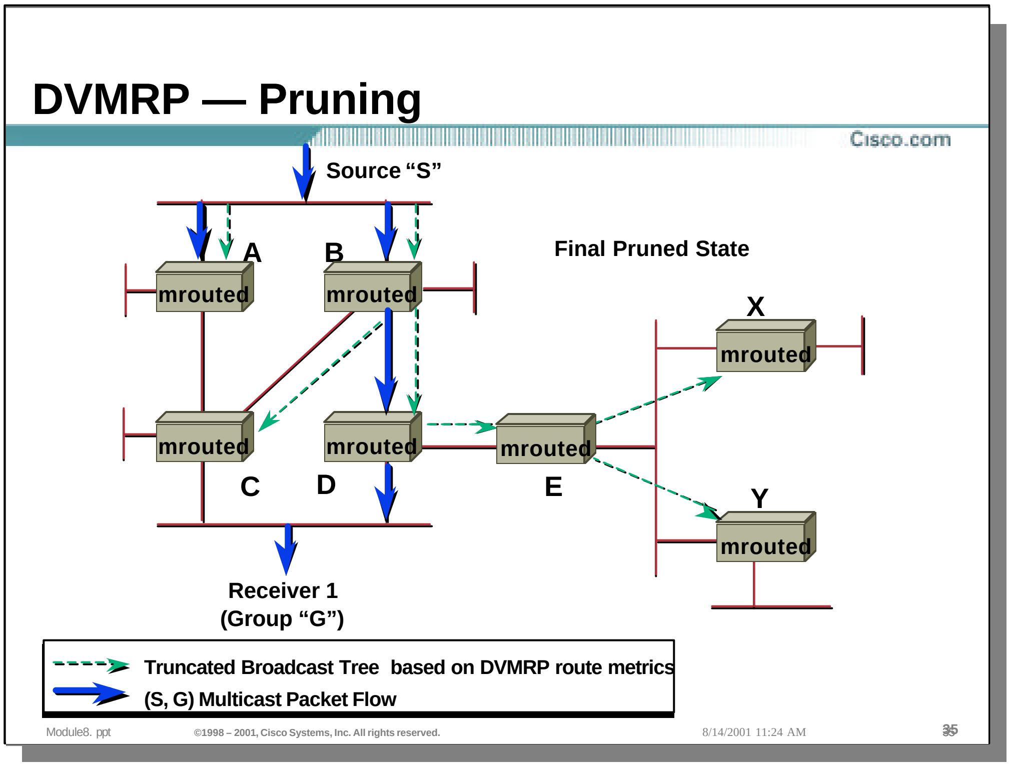


- **DVMRP Pruning (cont.)**
  - Both routers X and Y are also leaf nodes that have no need for the (S, G) traffic (i.e. they have no directly connected receivers) and therefore send (S, G) Prunes up the TBT to router E.
  - Once router E has received (S, G) Prunes messages *from all DVMRP neighbours on the subnet* it prunes the Ethernet interface connecting to router X and Y.

DVMRP — Pruning



- **DVMRP Pruning (cont.)**
  - At this point, all of router E's downstream interfaces on the TBT have been pruned and it no longer has any need for the (S, G) traffic. As a result, it too sends an (S,G) Prune up the TBT to router D.
  - When router D receives this (S, G) Prune, it prunes the interface and shuts off the flow of (S, G) traffic to router E.

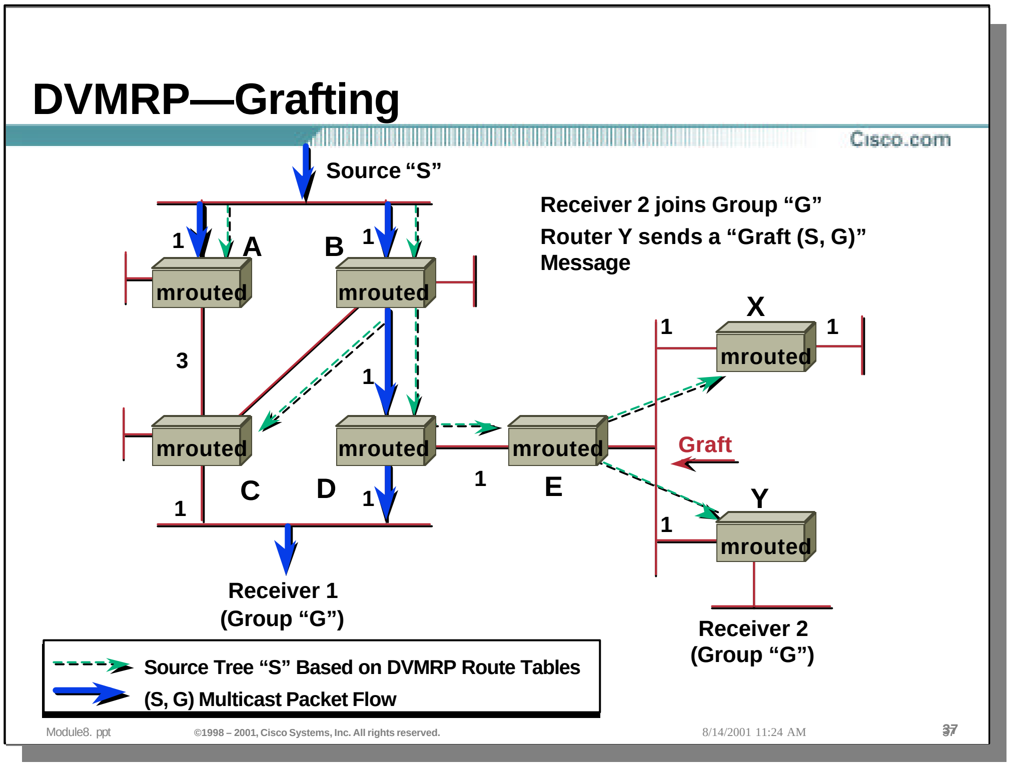


- **DVMRP Pruning (cont.)**
  - In the drawing above, we see the final pruned state of the TBT which leaves traffic flowing to the receiver.
  - However, because DVMRP is a "flood and prune" protocol, these pruned branches of the TBT will time out (typically after 2 minutes) and (S, G) traffic will once again flood down all branches of the TBT. This will again trigger the sending (S, G) Prune messages up the TBT to prune of unwanted traffic.

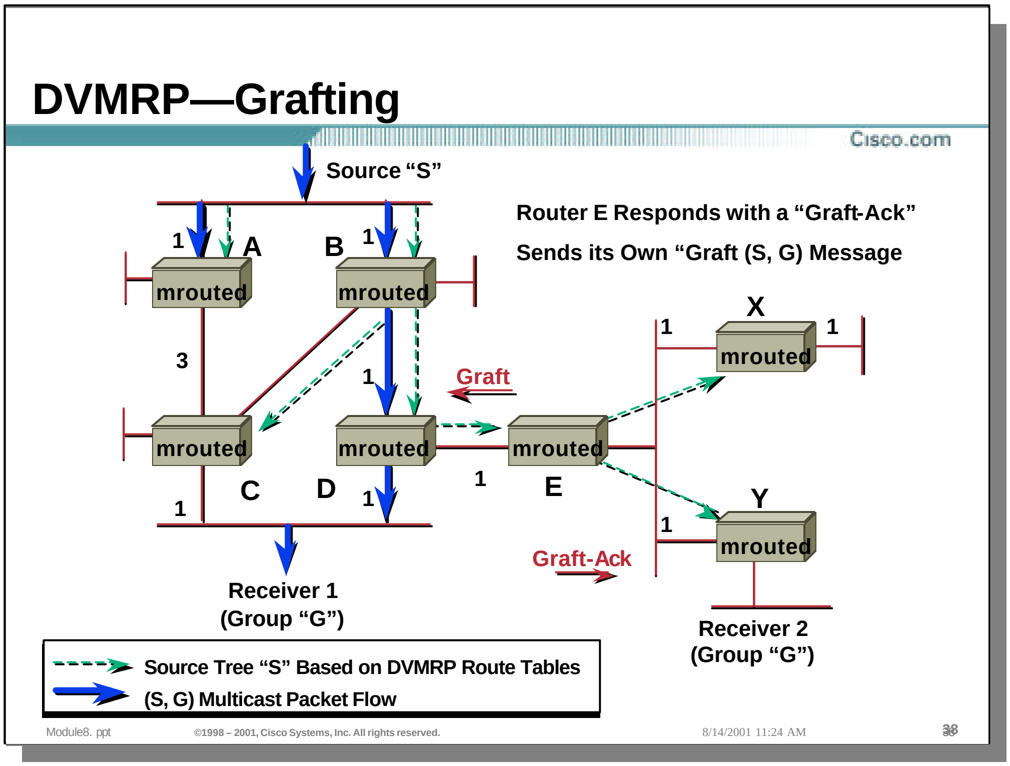
DVMRP—Basic Concepts

Cisco.com

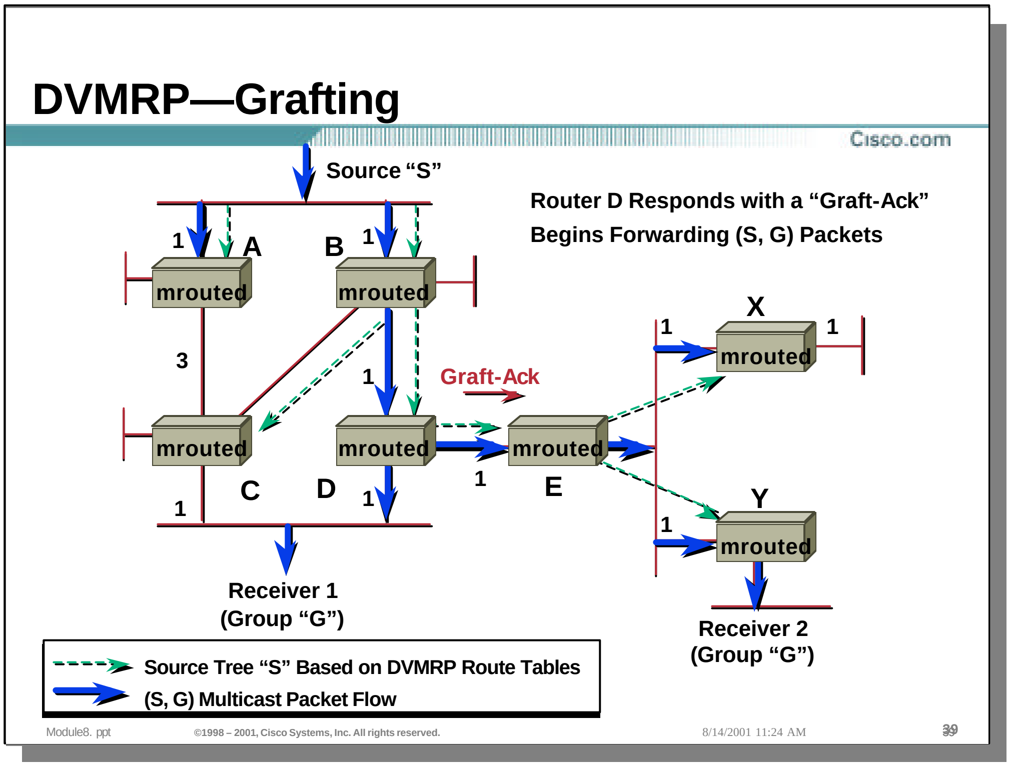
- Neighbor discovery
- Route exchange
- Source trees
- Multicast forwarding
- Pruning
- Grafting
- Tunnels



- **DVMRP Grafting**
  - Let’s now assume that “Receiver 2” now joins Group “G” by sending an IGMP Host Membership report for group “G” to Router Y.
  - Router Y finds that it has state for source (S, G) and that it has previously pruned the source from the Source Tree (show with dashed green arrows). As a result, Router Y sends a “Graft” message to its upstream neighbor, Router E, for source S.



- **DVMRP Grafting**
  - Router E receives the Graft for (S, G) from Router Y and first responds by sending a Graft-Ack message to acknowledge the receipt of Router Y's Graft message.
  - Router E now finds that it too has previously pruned (S, G) from the Source Tree and must therefore send an (S, G) Graft to its upstream neighbor Router D.

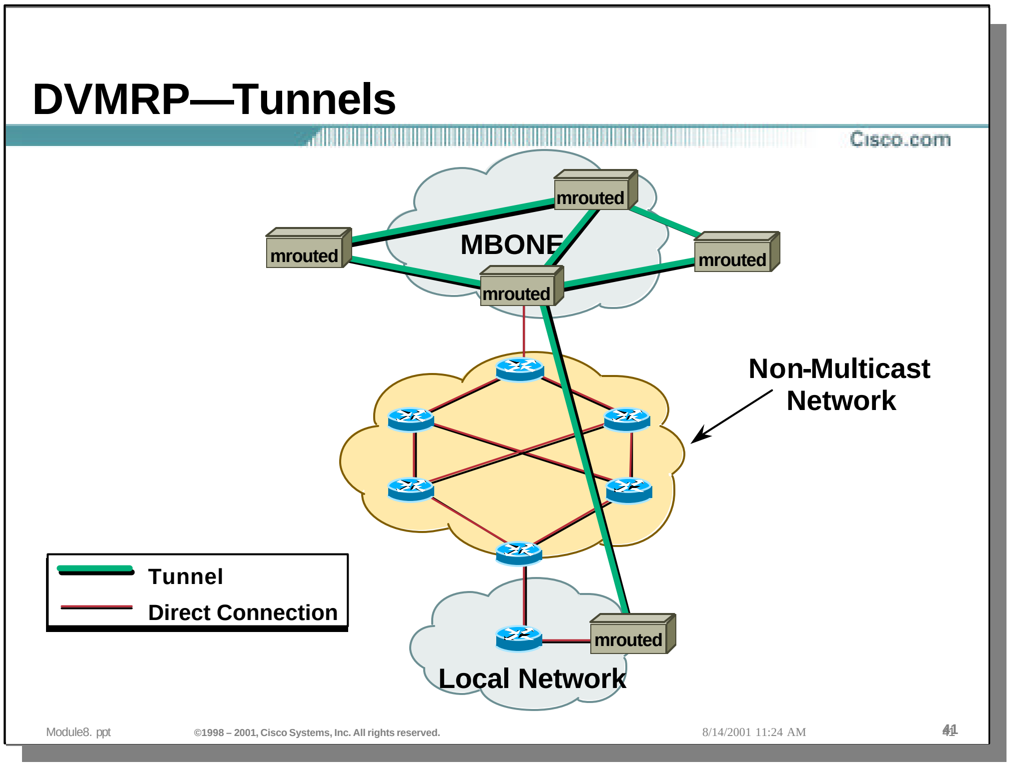


- **DVMRP Grafting**
  - Router D receives the Graft for (S, G) from Router E and first responds by sending a Graft-Ack message to acknowledge the receipt of Router E's Graft message.
  - Router D has not pruned (S, G) traffic from the Source Tree and therefore simply adds the interface towards Router E to its outgoing interface list. This restarts the flow of (S, G) traffic down to Receiver 2.

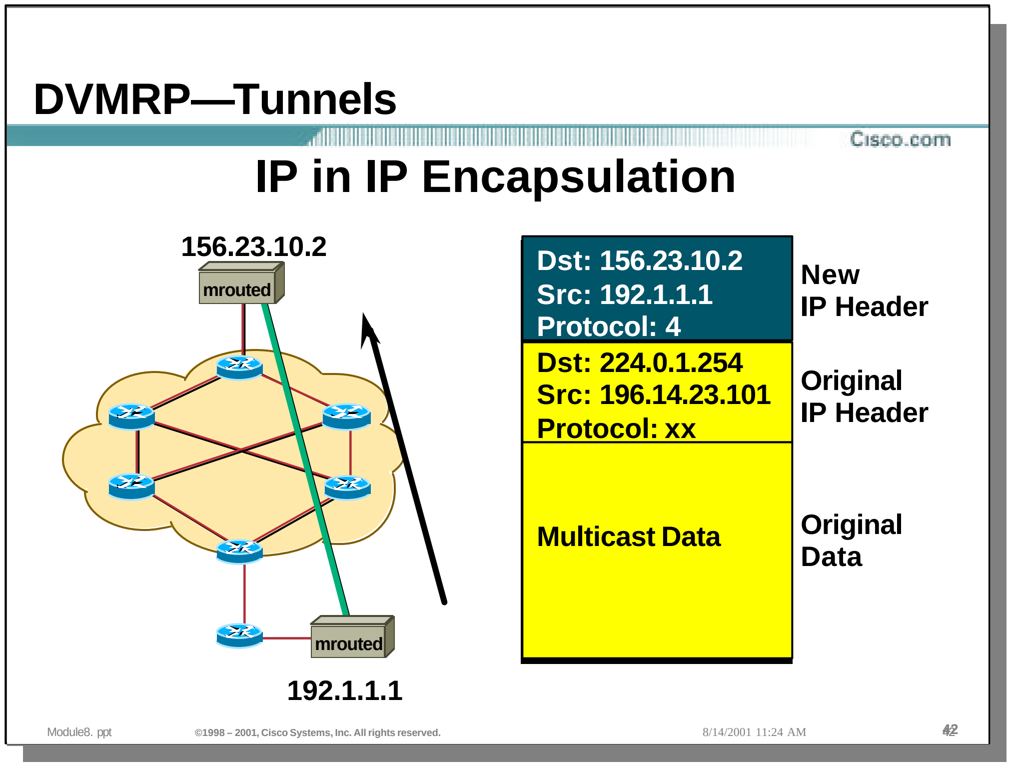
DVMRP—Basic Concepts

Cisco.com

- Neighbor discovery
- Route exchange
- Source trees
- Multicast forwarding
- Pruning
- Grafting
- Tunnels



- **DVMRP Tunnels**
  - DVMRP Tunnels are primarily used to "tunnel" through non-Multicast capable networks.
  - DVMRP Tunnels also have the added benefit of reducing the hop count across non-Multicast enabled networks to 1 hop. This is important when one considers that "infinity" is 32 hops in DVMRP. Since the Internet is considerably more than 32 hops in diameter, DVMRP Tunnels are a necessity in the Internet.



- **DVMRP Tunnels**
  - DVMRP Tunnels are implemented using "IP-in-IP" Encapsulation. This encapsulation method uses an additional IP wrapper header with a protocol number of 4. The IP wrapper header uses the IP addresses of the end points of the tunnel as the Source and Destination addresses.

CISCO SYSTEMS

EMPOWERING THE INTERNET GENERATION℠