CCNA Discovery 4.0 Designing and Supporting Computer Networks

Prototyping the WAN– Chapter 8

Cisco Networking Academy®
Mind Wide Open™

Objectives

- Describe the components and technologies used for WAN connectivity.
- Explain the components of a Frame Relay network.
- Configure a Frame Relay connection between two Cisco routers.
- Describe the VPN technologies available to connect remote sites and workers.
- Configure a VPN client to connect to a VPN server.
- Perform proof-of-concept tests of WAN and remote worker connectivity.

Describe Remote Connectivity Testing Methods

- The results of the prototype testing of the LAN validate the design choices made by the NetworkingCompany designer. The new design elements that provide WAN connectivity to remote sites and workers need to be tested. Testing remote connectivity options may be more difficult than testing the LAN design.

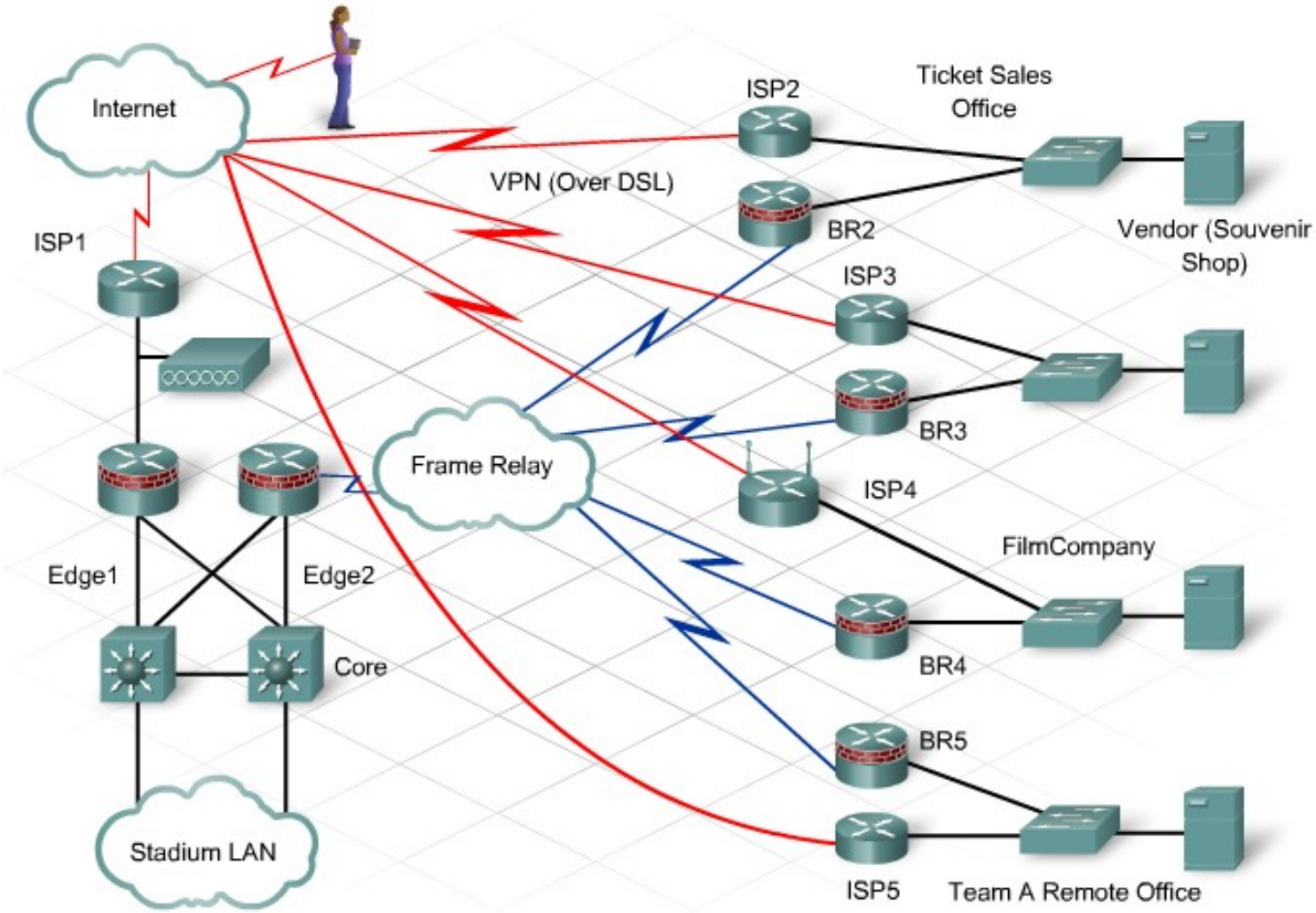
Describe Remote Connectivity Testing Methods

- Remote connectivity usually requires the use of transmission facilities that are not owned or managed by the customer. These facilities, Frame Relay networks, T1 connections, or even DSL links, are usually not available to the designer for testing purposes.

Describe Remote Connectivity Testing Methods

- As a result, the designer must consider ways to test the proposed design without having access to the actual transmission facilities.
- The designer can use three different methods to test remote connectivity designs:
- Simulation software
- Prototype testing using simulated links
- Pilot testing in the actual environment

Describe Remote Connectivity Testing Methods



Testing WAN Connectivity with Simulation Software

- Simulated environments can provide a way to test device configuration and operation. After the design is verified in the simulated environment, remote connectivity can be further tested in a pilot installation.
- **Network Simulation Software**
- Computer software programs offer the designer a tool to test configurations before implementing them on actual equipment.

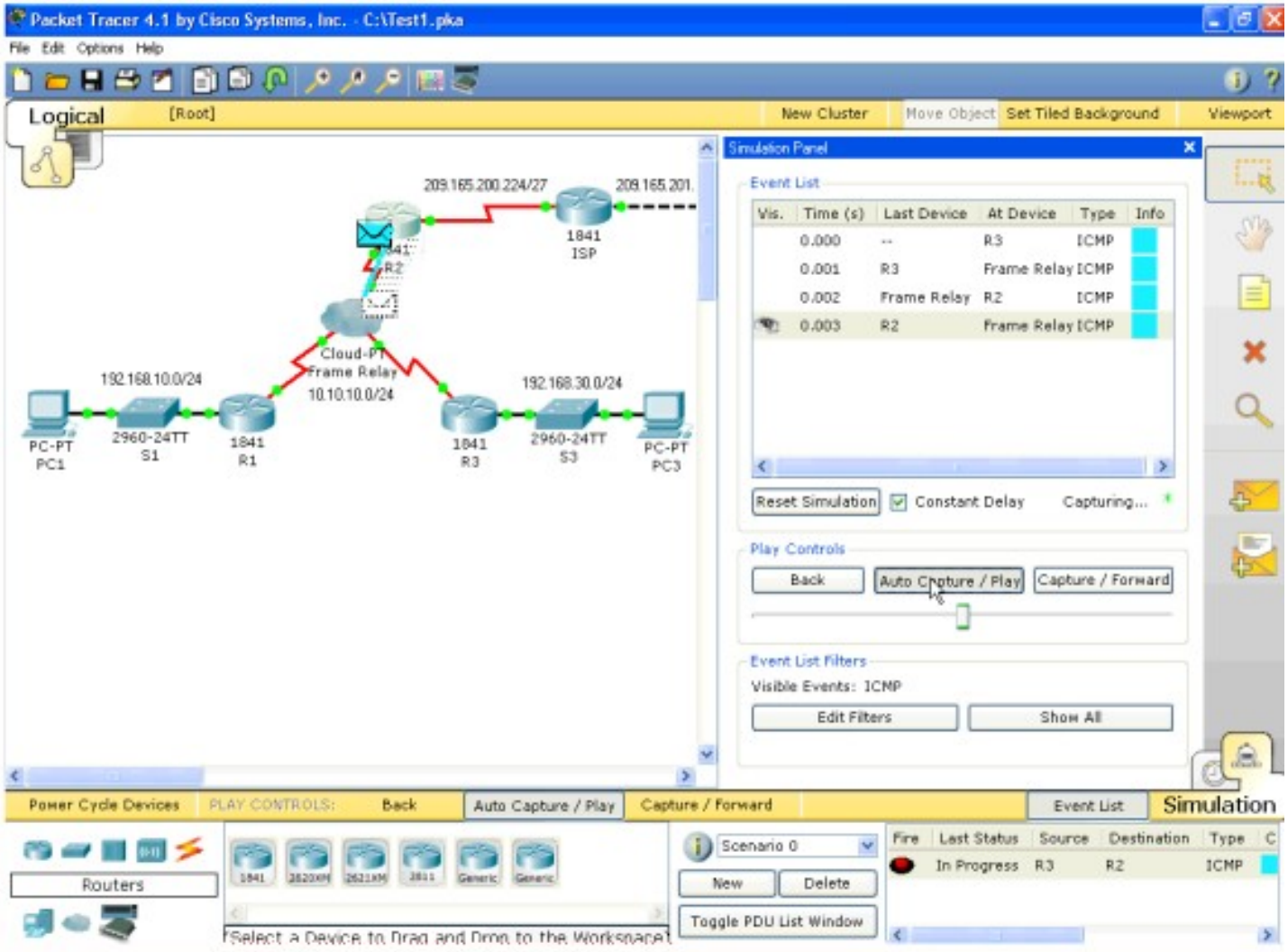
Testing WAN Connectivity with Simulation Software

- The benefits of using a simulation software package are:
- Lower overall cost - Test networks are expensive to build and maintain. Networking device capabilities and configuration options change frequently.
- Flexibility - Simulation software can support many different types of devices and connectivity options. Changing configurations and topologies is usually much quicker and easier in a simulation than when using actual equipment.

Testing WAN Connectivity with Simulation Software

- Scalability - Building a large or complex network in a lab environment is time-consuming and error-prone. Using a simulation program permits testing of large networks in a reduced amount of time.
- Control -Using simulation software allows the designer to control the entire network operation at once. The network designer can determine the types of traffic to send across the network and the rate at which the traffic is sent.

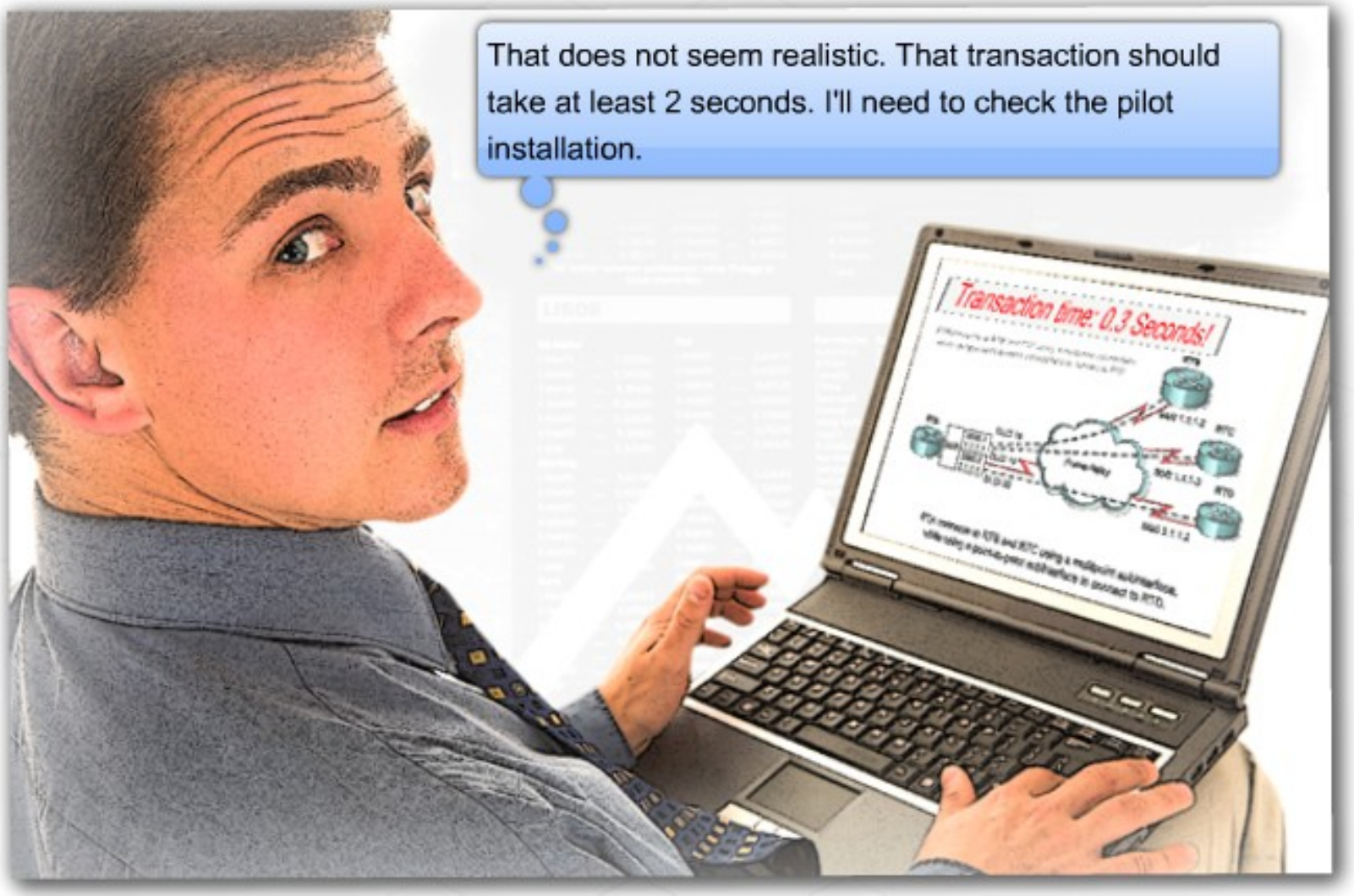
Testing WAN Connectivity with Simulation Software



Testing WAN Connectivity with Simulation Software

- Software Limitations
- Using simulation software programs to validate the network designs has a few disadvantages:
- Limited functionality - Software programs are designed and written long before they are available to the public and can quickly become out-of-date.
- Unrealistic performance - It is difficult, if not impossible, for the software programmers to anticipate and simulate all of the conditions that can occur in an actual network.

Testing WAN Connectivity with Simulation Software



Simulating WAN connectivity in a lab environment

- Almost all WAN technologies require an intermediary device to convert the WAN signals to either serial or Ethernet signals at the customer premise. These devices include various types of modems and CSU/DSUs. An exception to this is Metro Ethernet, which does not require the intermediary device.

Simulating WAN connectivity in a lab environment

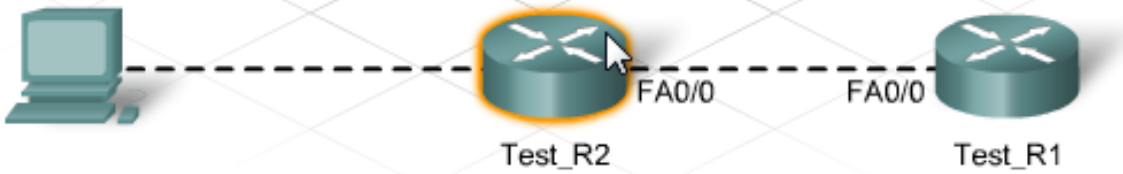
- Simulating a DSL or Cable Connection
- To simulate a DSL or cable WAN connection, an Ethernet connection can be used. Most Ethernet interfaces can be set to provide a 10-Mb connection, which is similar to the type of connectivity provided over DSL or cable. The routers are connected using an Ethernet crossover cable. Routing protocol metrics can be adjusted to simulate the metrics of a lower-speed link.

Simulating WAN connectivity in a lab environment

Routing protocol metrics can be adjusted to simulate the metrics of a lower-speed link by using the bandwidth command on the interface. Static route preference can be manually configured by adjusting the administrative distance assigned to the route.

```
version 12.3
no service password-encryption
!
hostname Test_R2
!
!
interface FastEthernet0/0
  description Remote site souvenir shop WAN Connection
  bandwidth 3000
  no ip address
  duplex full
  speed 10

interface FastEthernet0/1
  no ip address
  duplex auto
--More--
```



Simulating WAN connectivity in a lab environment

Simulating Serial Connectivity

There are two common methods used to simulate serial connectivity:

CSU/DSUs or serial modems V.35 cables

T1 Cross-over Cable

Cable End A RJ45 PIN	Cable End B RJ45 Pin
1	4
2	5
4	1
5	2

A T1 loop-back connector will have these connections all on the same jack or plug:

T1 Loop-back connector

RJ45 Pins
1-4
2-5

Simulating WAN connectivity in a lab environment

- Using CSU/DSUs or Modems
- If CSU/DSUs or modems are available, the documentation included with the device usually includes the wiring diagram necessary to create a crossover cable. If the diagram is not included, a search of the Internet can usually uncover the correct pinouts to use. This crossover cable can be used to connect two like devices to simulate the link provided by the telecommunications service provider (TSP).

Simulating WAN connectivity in a lab environment

- One CSU/DSU or modem is configured to provide the DCE function. The other device is configured as a DTE device. The routers are then connected and configured just as they would be in the actual WAN environment. The CSU/DSU or modem provides the clocking for the link.

Simulating WAN connectivity in a lab environment

- Using V.35 Cables
- In the NetworkingCompany prototype lab environment, it is possible to simulate a point-to-point WAN connection using two serial V.35 cables. One cable must be a V.35 DCE cable, and the other cable must be a V.35 DTE cable. By connecting the two cables, a V.35 crossover cable is created. Interconnecting the routers with these two cables creates a circuit.

Simulating WAN connectivity in a lab environment

- Interconnecting the routers with these two cables creates a circuit. Eliminating the CSU/DSU or modem from the connection removes the clocking function on the circuit. As a result, one of the routers must be configured as a DCE device, using the clock rate command on the interface. In actual implementations, routers and other CPE devices rarely, if ever, provide the DCE function on a circuit.

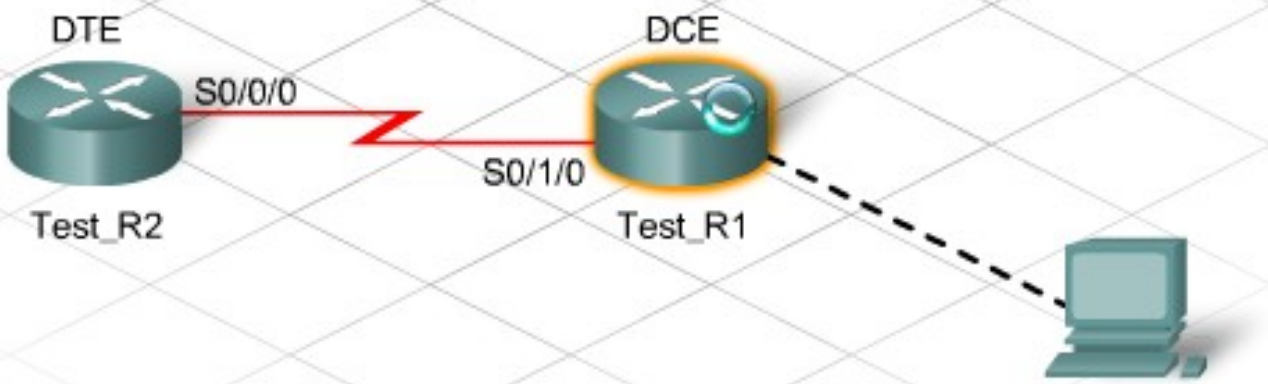
Simulating WAN connectivity in a lab environment

- Setting various clock rates enables the network designer and the NetworkingCompany staff doing the testing to simulate different connection speeds.
- The advantage of using simulated serial WAN connections is that the configuration of the serial interfaces can be tested and verified. The disadvantage of doing this type of simulated testing is that the actual network factors of the telecommunications provider cannot be evaluated.

Simulating WAN connectivity in a lab environment

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#interface s0/1/0
Router(config-if)#clock rate 56000
Router(config-if)#no shut
Router(config-if)#
```



Identify WAN Goals and Requirements

- Connectivity to the remote sites is a major issue in the existing stadium network. A high-priority goal for the stadium management is to extend the new IP telephony system and the video surveillance network to current remote sites. These services cannot be supported over the existing WAN.

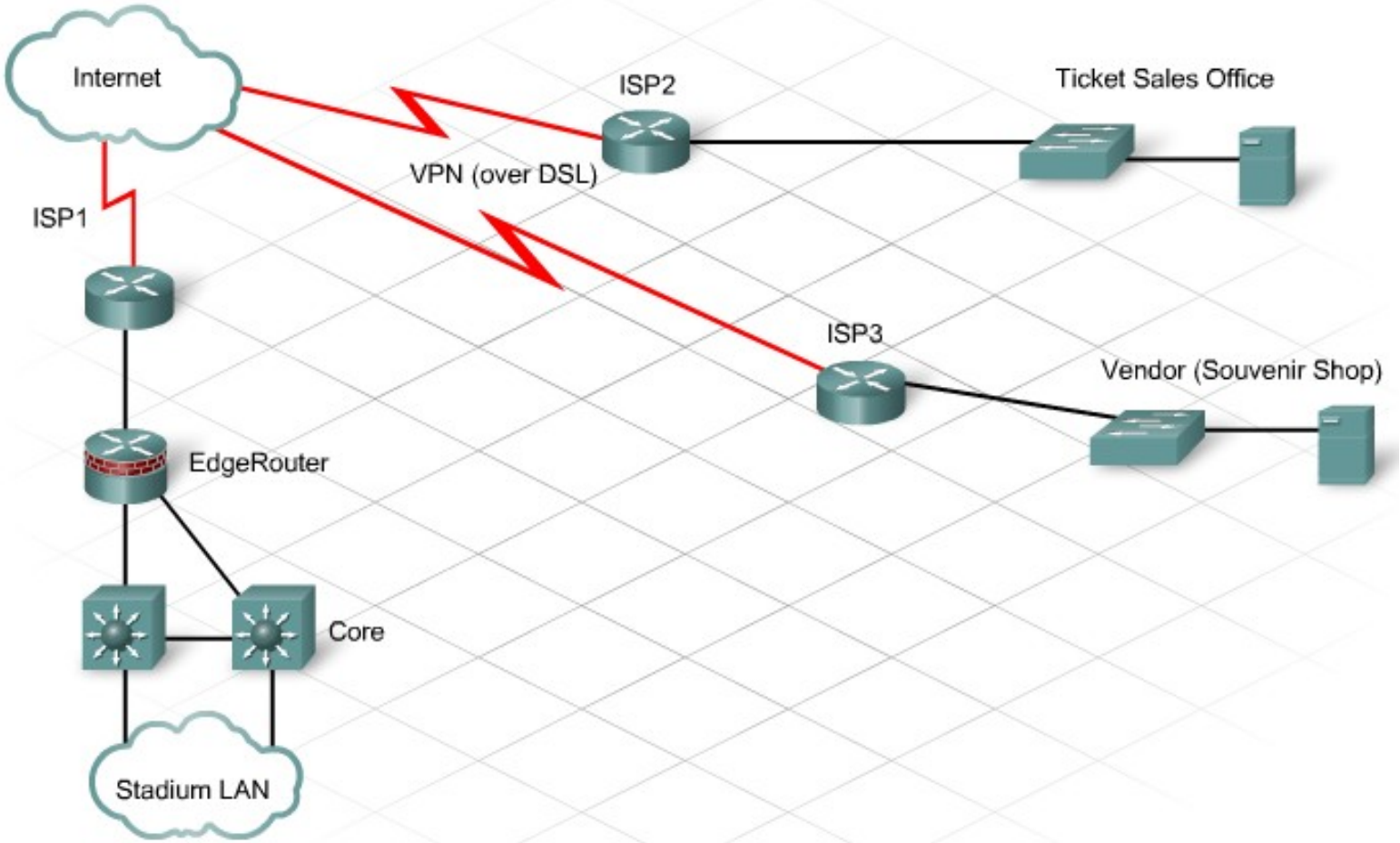
Identify WAN Goals and Requirements

- In the stadium network, the two current remote sites access the main network using virtual private network (VPN) connections across the Internet. These VPN connections use DSL lines. The ISP does not offer a guarantee of bandwidth or QoS. The proposed design includes an upgrade to dedicated Frame Relay WAN connectivity. The network designer recommends using Frame Relay to connect the new remote office for Team A and the FilmCompany office.

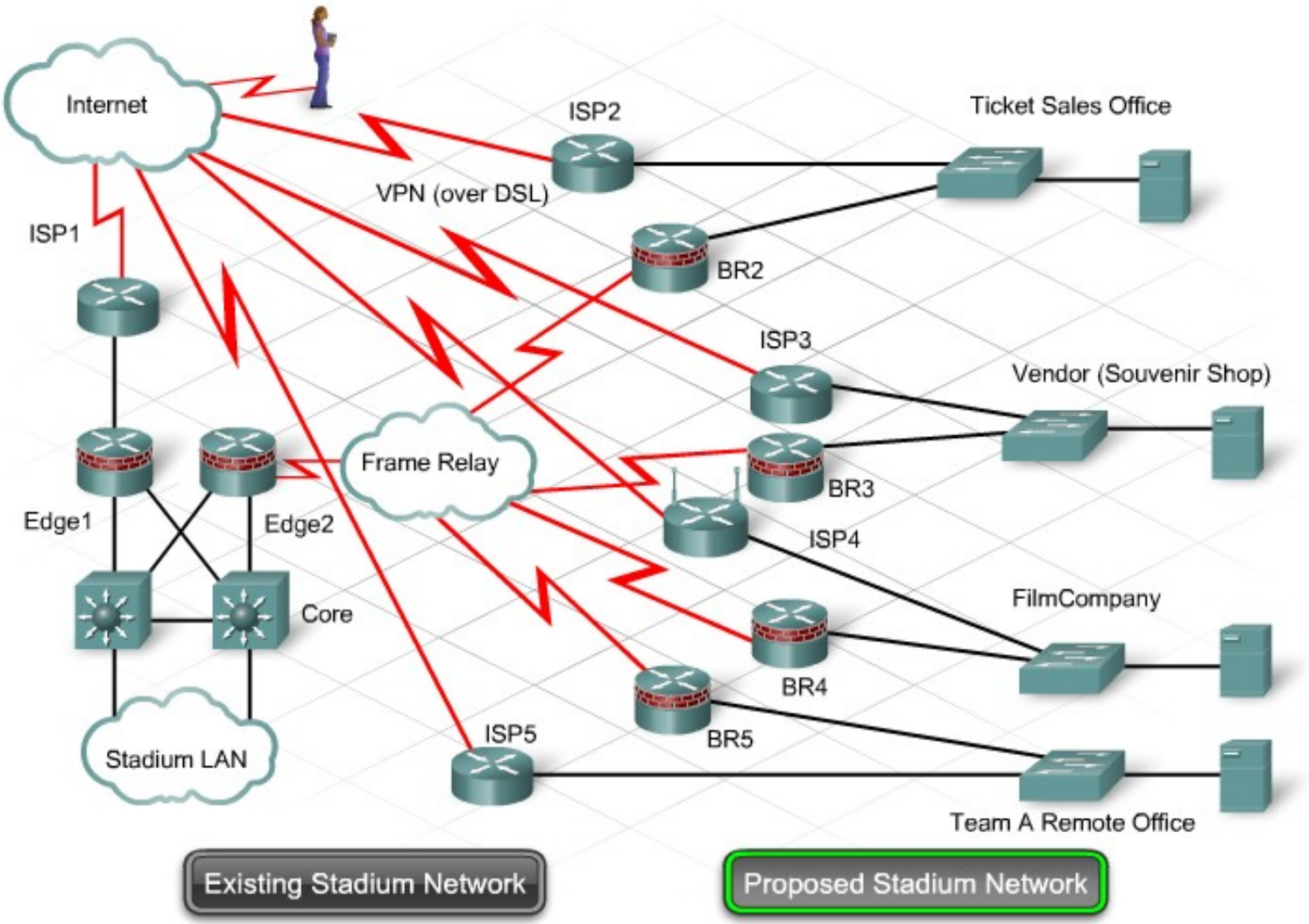
Identify WAN Goals and Requirements

- The designer decides to build a prototype to simulate the WAN connectivity. This prototype tests the configurations and the failover in case of a link failure. It is not possible to simulate the entire TSP packet-switched network using either a prototype or simulation software. The actual Frame Relay connection through the TSP network can only be tested in a pilot. After the prototype is completed and the design accepted, a pilot installation is planned for the souvenir shop.

Identify WAN Goals and Requirements



Identify WAN Goals and Requirements



Creating the Test Plan

- The performance through the TSP network cannot be tested in the prototype. However, other important elements of the design can be tested in the prototype WAN network:
- Frame Relay local loop configuration
- Mechanisms to activate the VPN backup link in the event of a Frame Relay failure
- Static routing configuration
- ACLs that filter traffic to and from the WAN sites
- SSH configuration to enable remote management

Creating the Test Plan

- To prototype the WAN connectivity, the network designer recommends using a Cisco router to simulate a Frame Relay switch. This simulation enables the local loop configurations to be tested without having to physically connect to the TSP network. To build the WAN prototype, the designer needs four routers to test all of the functionality.

Creating the Test Plan

Business Goal	Overall Success Criteria
Provide additional services, such as voice and video, to the remote sites.	Frame Relay links that provide guaranteed bandwidth for delay sensitive traffic, and backup links that operate as expected.
Technical Requirements	Success Criteria
Scalability	
Use of Frame Relay connections to connect the remote sites.	Adding additional sites does not require additional local loop connections
Configuring bandwidth requirements for each virtual circuit	CIR guarantees bandwidth for configured virtual circuits
Availability	
Configuring backup connections using the VPN through the Internet	Connectivity is not lost for major applications if Frame Relay fails
Security	
Applying filters to permit only authorized traffic to and from the WAN sites	Undesirable traffic is blocked
Manageability	
Creating a management network and provision of access to devices through SSH	Management station is able to initiate an SSH session to devices at the WAN sites

Creating the Test Plan

- The topology for the Frame Relay WAN test requires a different type of connectivity than the earlier prototypes. In an actual implementation, a Frame Relay local loop usually connects to a CSU/DSU at the customer premise. From the CSU/DSU, a serial connection is made to the customer premise equipment (CPE) router.

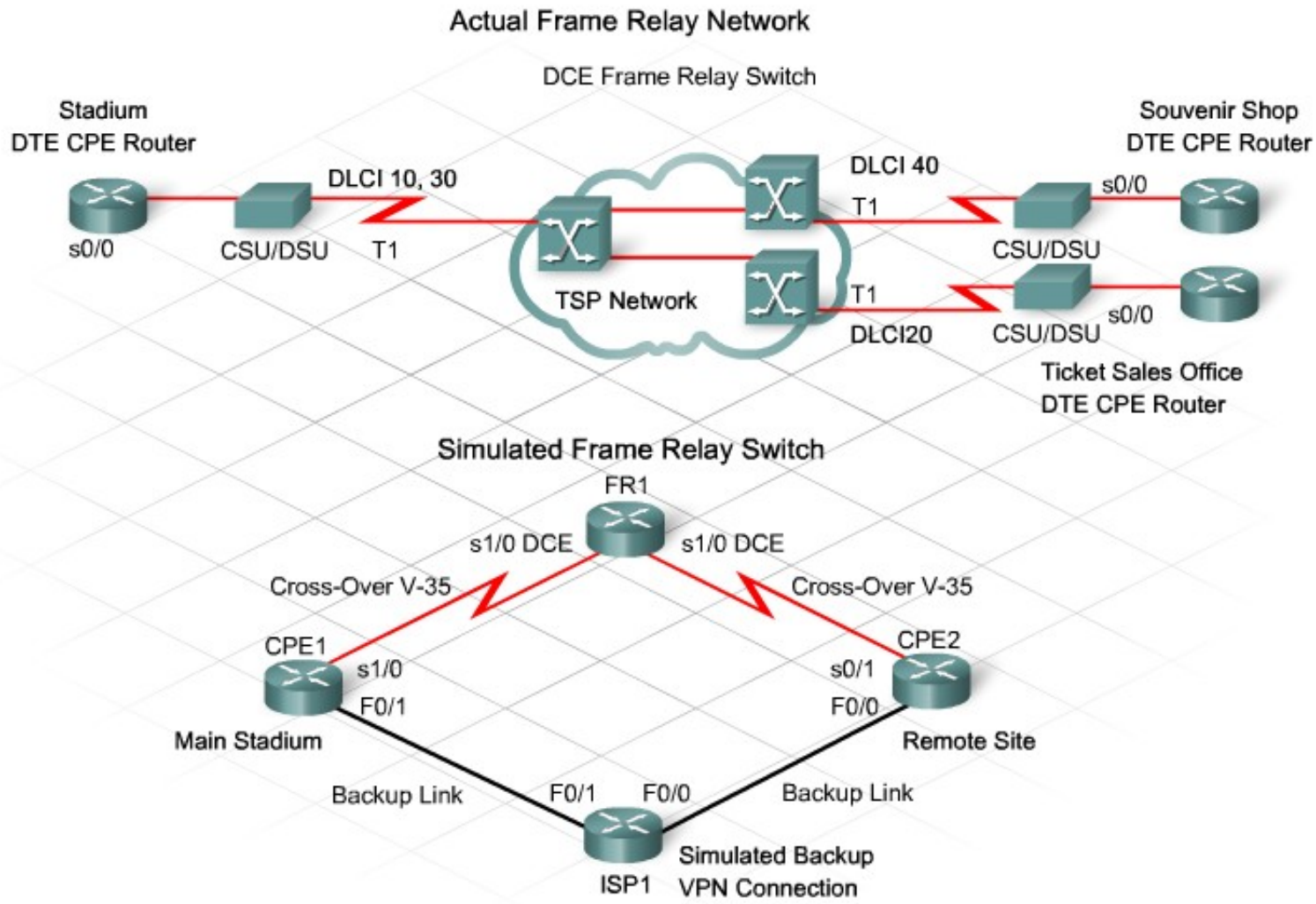
Creating the Test Plan

- The DCE function on the local loop is provided by either the TSP or the CSU/DSU. The clocking for the serial connection between the CSU/DSU and the CPE router is provided by the CSU/DSU. All of the connections at the router are DTE connections and use DTE cable.

Creating the Test Plan

- In the prototype test network, a true T1 or E1 connection to a Frame Relay switch does not exist. It has to be simulated using a Cisco router acting as the Frame Relay switch. This router is identified as FR1. It connects to the other routers in the topology using a crossover connection. At the NetworkingCompany, this crossover function is created by connecting one V.35 DTE cable directly to a V.35 DCE cable.

Creating the Test Plan



Validating the choice of devices and topologies

- The Frame Relay topology recommended in the proposed WAN design is radically different from the existing VPN connectivity managed by the ISP. There are many options available when using Frame Relay. It is a recommended practice for the network designer to review the design and operation of the WAN with the NetworkingCompany staff before they set up the prototype.

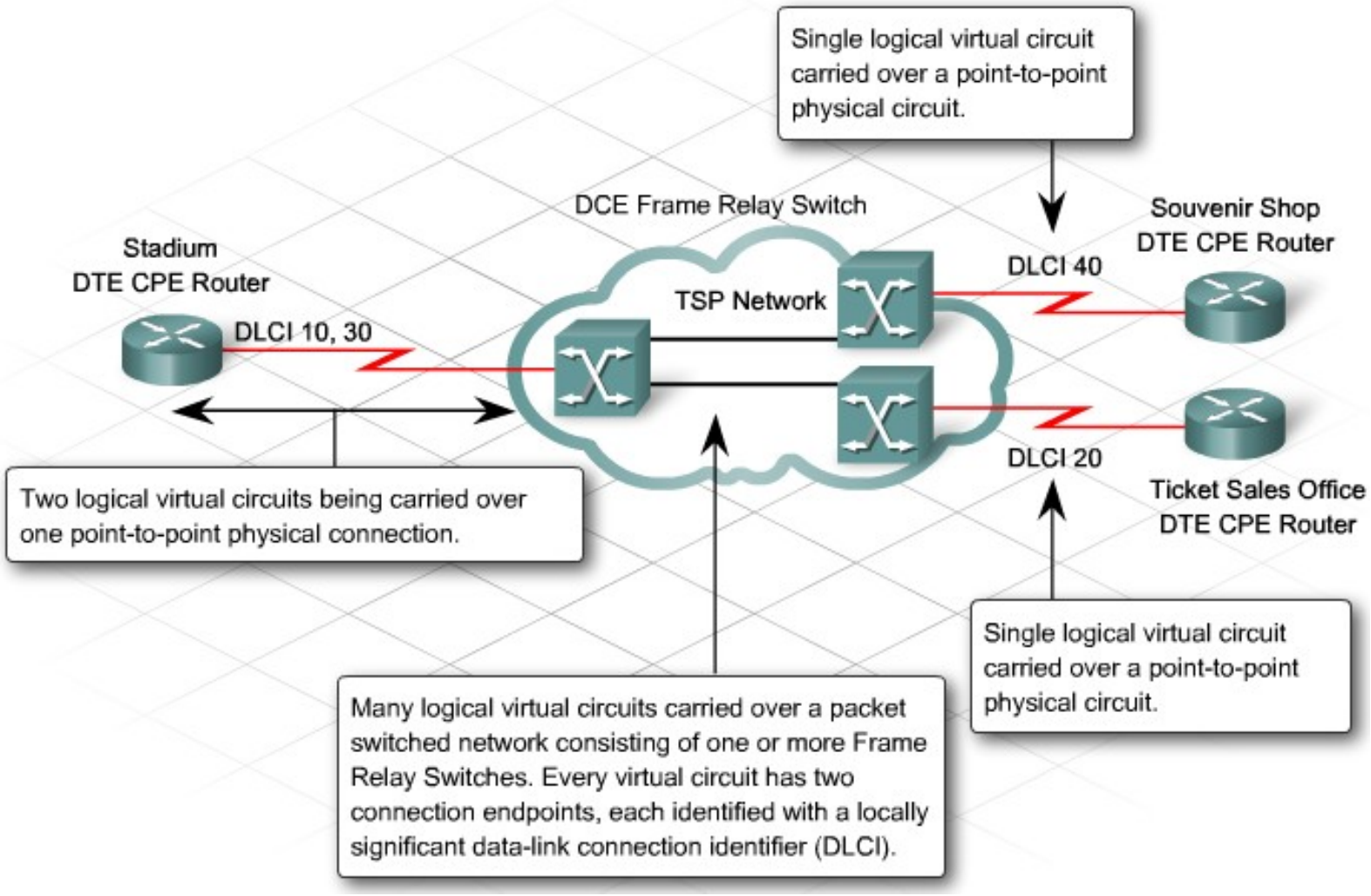
Validating the choice of devices and topologies

- Frame Relay
- Frame Relay is a high-performance WAN protocol that was standardized by the International Telecommunication Union ITU-T. It is widely used in the United States. Many people think of a Frame Relay link as a physical connection between two sites. In reality, a Frame Relay link is a virtual circuit that spans a series of connections.

Validating the choice of devices and topologies

- Every Frame Relay link has at least three components:
- The local point-to-point circuit that connects the local CPE router to the TSP Frame Relay switch
- The TSP packet-switched network
- The remote point-to-point circuit that connects the remote site into the TSP network
- Configuring Frame Relay on the CPE router consists of configuring only the settings for the point-to-point link with the TSP Frame Relay switch. These point-to-point links are usually T1/E1 or fractional T1/E1 circuits. The TSP configures the virtual circuit through the packet-switched network.

Validating the choice of devices and topologies



Validating the choice of devices and topologies

- Frame Relay terminology and configuration can easily become confusing. To explain the configuration options to the NetworkingCompany staff, the network designer starts with the link between the planned new stadium CPE router and a TSP Frame Relay switch.

Validating the choice of devices and topologies

- The Local Loop
- The proposed connection between the stadium CPE router and the Frame Relay switch at the TSP is a T1 circuit. This connection is referred to as a local loop. The local loop connects the provider Frame Relay switch to the CSU/DSU on the stadium premises. The connection then terminates on the serial port of the CPE router.

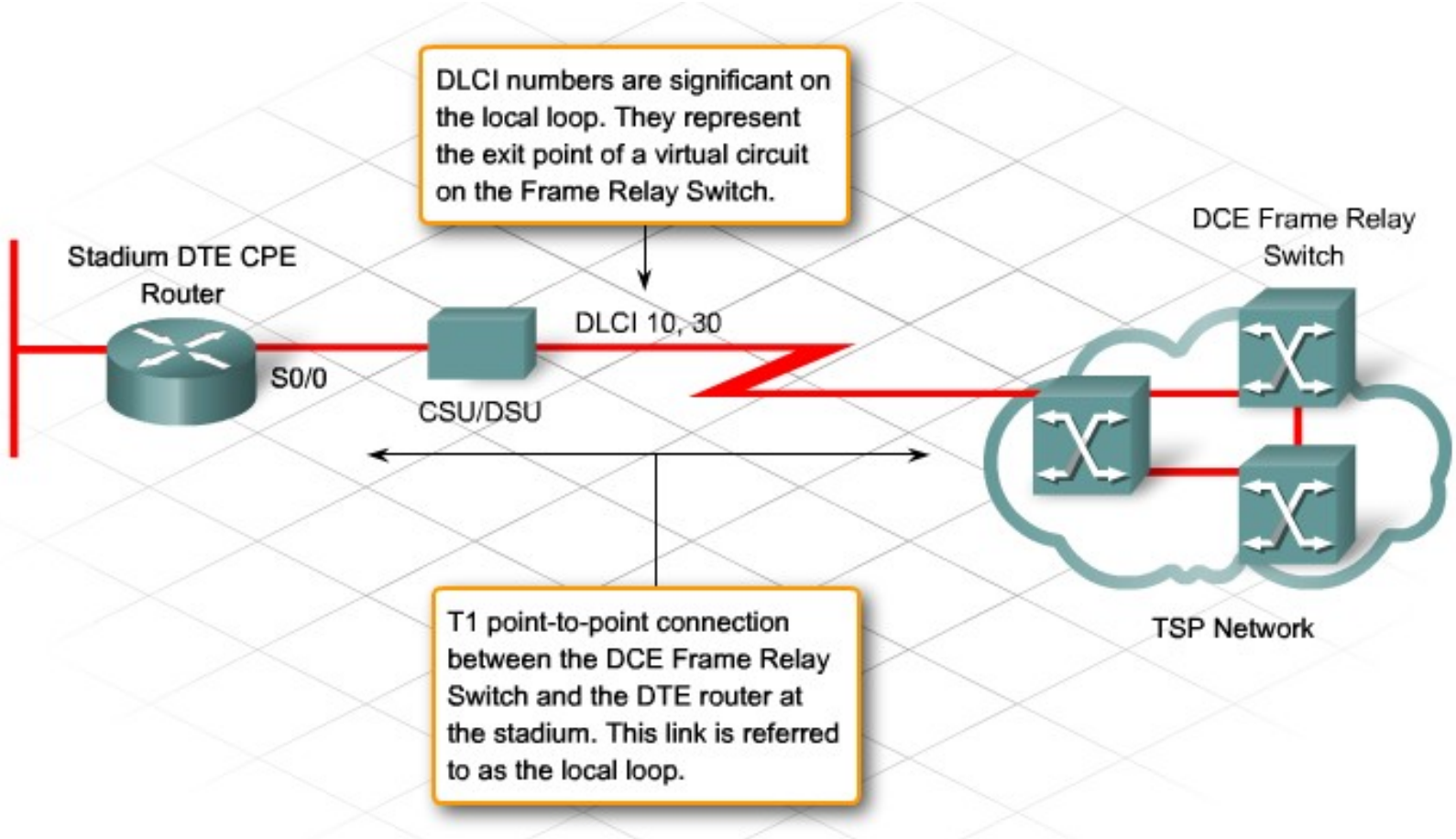
Validating the choice of devices and topologies

- The clock speed (port speed) of the local loop connection to the Frame Relay cloud is known as the local access rate. The local access rate defines the rate at which data can travel into or out of the provider packet-switched network, regardless of other settings.

Validating the choice of devices and topologies

- Data-link Connection Identifier
- More than one virtual circuit can be carried on a single physical local loop circuit. Each virtual circuit endpoint is identified by a data-link connection identifier (DLCI). A DLCI is usually significant only on the local loop. In other words, DLCI numbers are unique within a single Frame Relay switch. However, because there can be many Frame Relay switches within the network, DLCI numbers can be duplicated on other switches.

Validating the choice of devices and topologies



Validating the choice of devices and topologies

- Some of the services offered by the Frame Relay switch impact the quality of the data transmissions through the telecommunications provider network.
- Guaranteed Data Rates
- Frame Relay providers offer services with guaranteed average data transfer rates through the provider packet-switched network. This committed information rate (CIR) specifies the maximum average data rate that the network delivers under normal conditions.

Validating the choice of devices and topologies

- The CIR is less than or equal to the local access rate. A CIR is assigned to each DLCI that is carried on the local loop. If the stadium attempts to send data at a faster rate than the CIR, the provider network flags some frames with a discard eligible (DE) bit in the frame address header. The network attempts to deliver all frames. However, if there is congestion, it discards any frames marked with the DE bit.

Validating the choice of devices and topologies

- Zero CIR
- Many inexpensive Frame Relay services are based on a CIR of zero. A zero CIR means that every frame is a DE frame, and the network can throw any frame away when there is congestion. There is no guarantee of service with a CIR set to zero, so these services are not good choices for mission critical data.

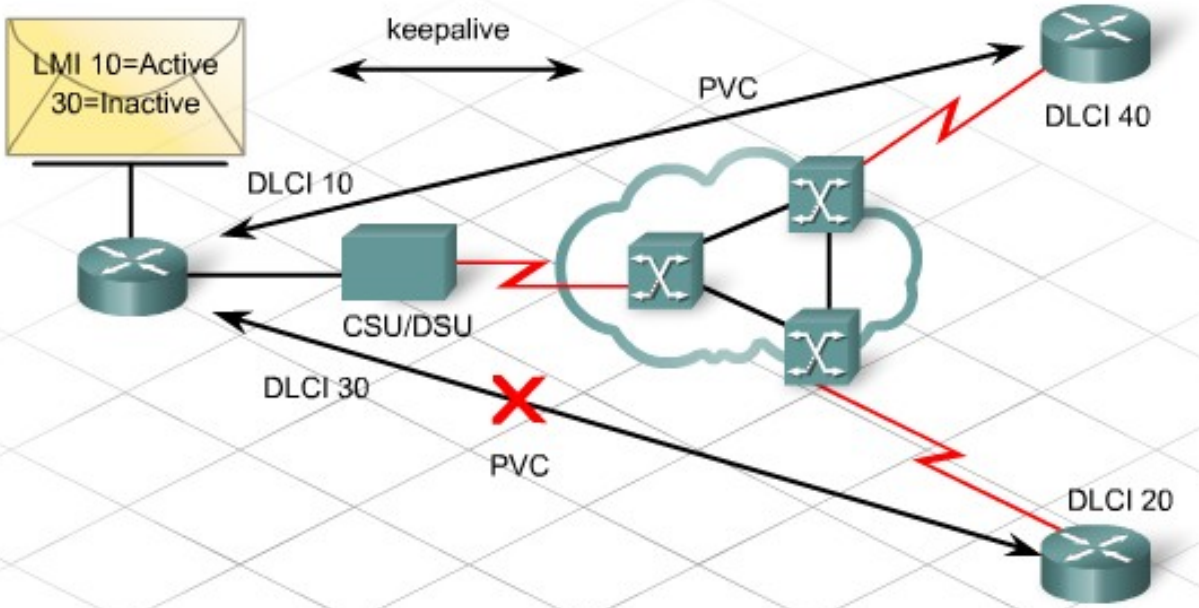
Validating the choice of devices and topologies

- Local Management Interface
- Local Management Interface (LMI) is a signaling standard between the router (DTE device) and the local Frame Relay switch (DCE device). LMI is responsible for managing the connection and maintaining status between the router and the Frame Relay switch. For example, LMI uses keepalive messages to monitor the status of network connections.

Validating the choice of devices and topologies

- LMI Frame Relay adds a set of enhancements, referred to as extensions, to basic Frame Relay. One important LMI extension is the ability to report the status of the virtual circuit as well as the status of the physical connection. LMI standards can differ between networks. Cisco routers support three LMI types: Cisco, ANSI Annex D, and ITU-T Q.933 Annex A.

Validating the choice of devices and topologies



Cisco IOS Keyword	Description
ansi	Annex D defined by American National Standards Institute (ANSI) standards T1.617.
cisco	LMI type defined jointly by Cisco and three other companies.
q933a	ITU-T Q.933 Annex A.

Validating the choice of devices and topologies

- Congestion Control
- To help manage traffic flows in the network, Frame Relay implements two mechanisms:
- Forward-explicit congestion notification (FECN)
- Backward-explicit congestion notification (BECN)
- FECNs and BECNs are controlled by a single bit contained in the Frame Relay frame header.

Validating the choice of devices and topologies

- FECN
- FECN informs the destination device about congestion on the network path. The FECN bit is part of the Address field in the Frame Relay frame header. The FECN mechanism works in the following way:
- 1. A DTE device sends Frame Relay frames into the network.

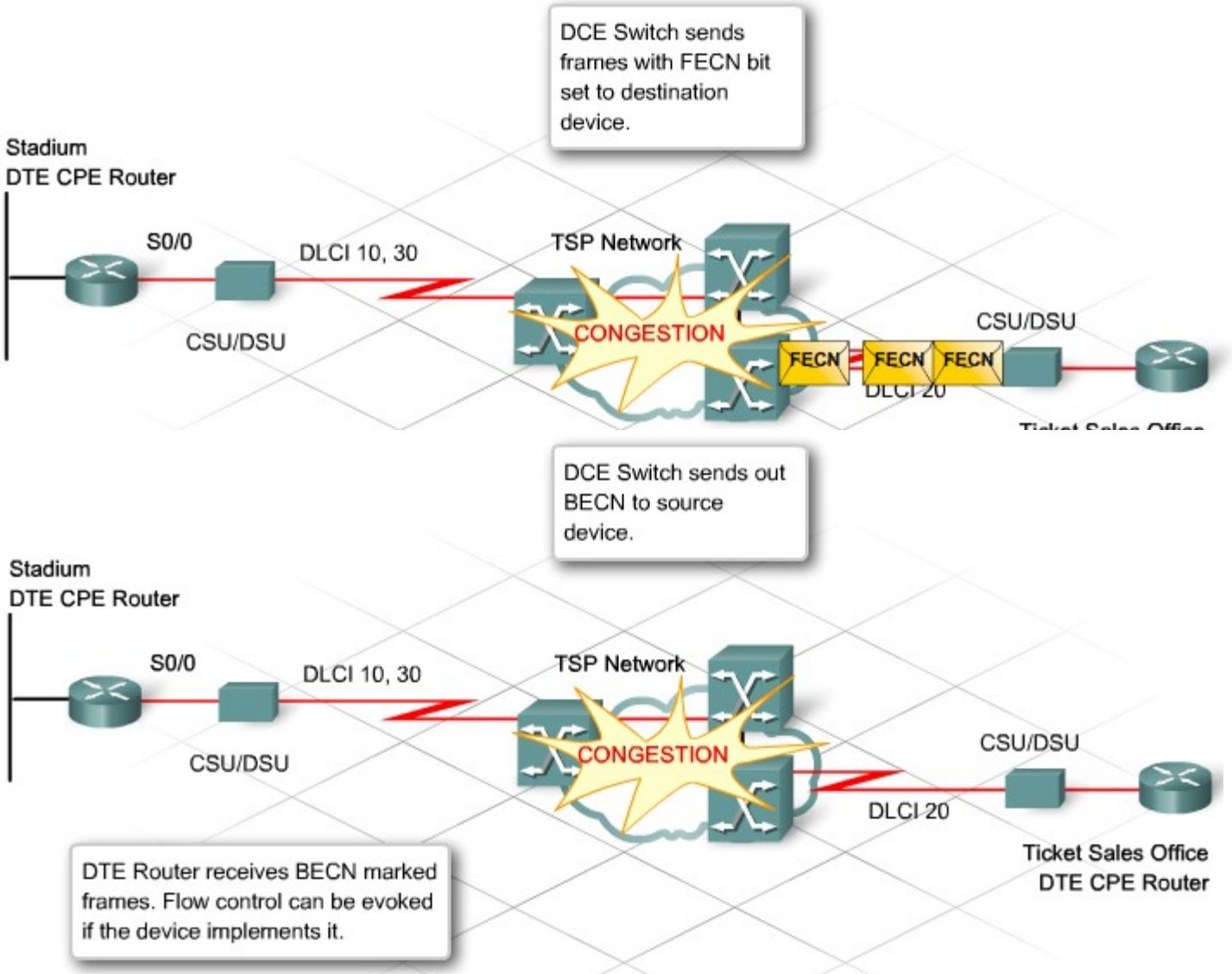
Validating the choice of devices and topologies

- 2. If the network is congested, the DCE devices (switches) set the value of the FECN bit to 1.
- 3. The frames reach the remote destination DTE device.
- 4. The DTE device reads the Address field with the FECN bit set to 1.
- 5. This setting indicates that the frame experienced congestion in the path from source to destination.

Validating the choice of devices and topologies

- BECN
- BECN informs the source device about congestion on the network path. The BECN bit is also part of the Address field in the Frame Relay frame header. A BECN works in the following way:
- 1. A Frame Relay switch detects congestion in the network.
- 2. It sets the BECN bit to 1 in frames headed in the opposite direction from the frames marked with the FECN bit.
- 3. This setting informs the source DTE device that a particular path through the network is congested.

Validating the choice of devices and topologies



Prototype the WAN

- To configure the Frame Relay WAN prototype, the NetworkingCompany staff first configures the router FR1 to act as the Frame Relay switch. The staff uses the command frame-relay switching to begin the configuration. This command tells the router to act as the DCE device and to emulate a Frame Relay switch. Additional frame-relay route configuration commands are applied to the router to enable it to switch the DLCIs from each interface.

Prototype the WAN

- The two serial interfaces on FR1 can now be configured as the Frame Relay DCE devices. Frame Relay encapsulation must be specified on each interface. The two possible Frame Relay encapsulations are ietf and cisco. The default encapsulation is cisco. The cisco method is proprietary and should not be used if the router is connected to a non-Cisco router across a Frame Relay WAN.

Prototype the WAN

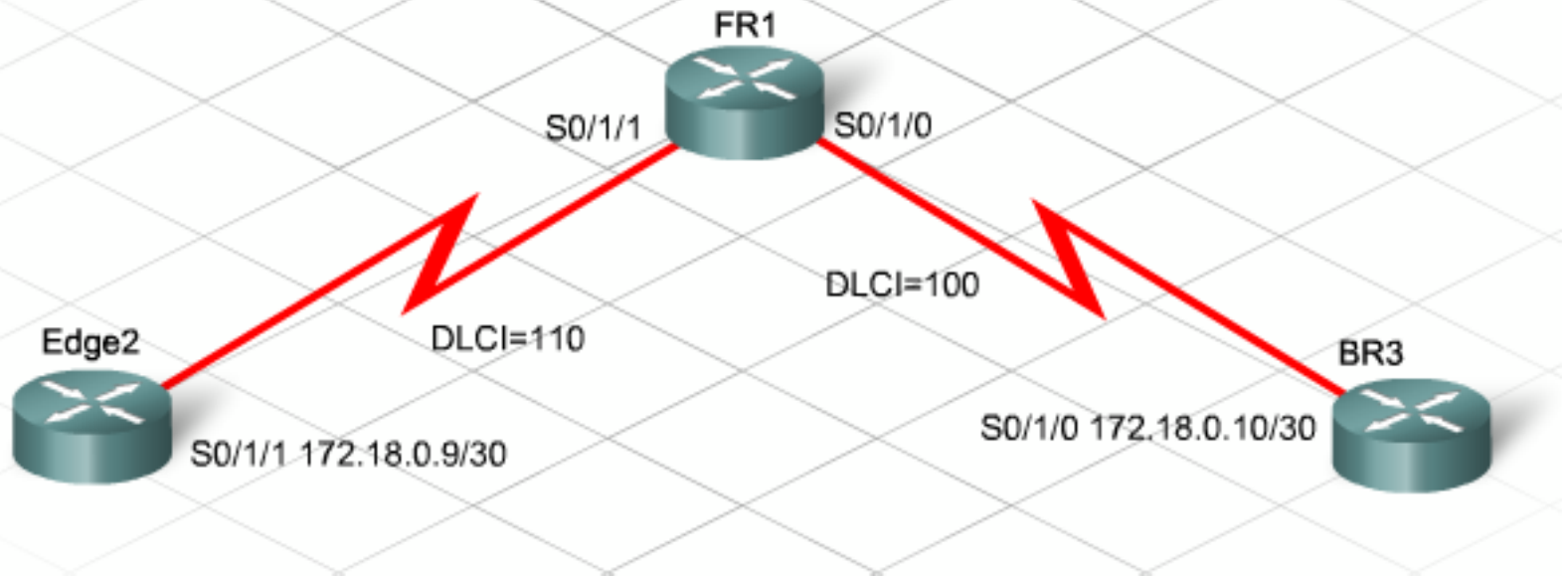
- The network designer configures Frame Relay by configuring the Layer 3 IP address on the interface and setting the encapsulation type to Frame Relay. Encapsulation is set using the following command:
- Router(config-if)#encapsulation frame-relay {cisco | ietf}

Prototype the WAN

- The CPE routers do not need to be configured as Frame Relay switches. However, the CPE router serial interface needs to be configured with Frame Relay encapsulation and an IP address. The designer uses the names of the planned devices and their addresses during the test.
- In the prototype network, there is no CSU/DSU device to provide the clocking. Therefore, it is important to configure a clock rate on the serial interfaces of FR1.

Prototype the WAN

```
Edge2(config)#interface serial 0/1/1
Edge2(config-if)#ip address 172.18.0.9 255.255.255.252
Edge2(config-if)#encapsulation frame-relay
```



Prototyping the WAN

- During the prototype test, the router FR1 acts as the Frame Relay switch at the service provider. This simulates the connectivity through the Frame Relay cloud. A virtual circuit is created between the Edge2 and BR3 routers. This circuit behaves the same as a directly connected link.

Prototyping the WAN

- Inverse ARP and Frame Relay Maps
- Inverse Address Resolution Protocol (Inverse ARP) provides a mechanism to create dynamic DLCI-to-Layer 3 address maps. Inverse ARP works similarly to ARP on an Ethernet local network. With ARP, the sending device knows the Layer 3 IP address. It sends broadcasts to learn the remote data link MAC address.

Prototyping the WAN

- With Inverse ARP, the router learns the Layer 2 address, which is the DLCI. It sends requests for the remote Layer 3 IP address.
- When an interface on a Cisco router is configured to use Frame Relay encapsulation, Inverse ARP is on by default. It is possible to manually configure a static mapping for a specific DLCI. Static mapping is used if the router at the other end does not support Inverse ARP.

Prototyping the WAN

- An advantage of Frame Relay connectivity is that one physical interface can support multiple virtual circuits. Frame Relay enables one connection into the provider packet-switched network to provide connectivity to multiple remote sites. This type of multi-access WAN is less expensive than one that requires dedicated point-to-point links between sites.

Prototyping the WAN

- Multiple links sharing a single interface can cause problems for distance vector routing protocol updates. Frame Relay is a nonbroadcast multi-access (NBMA) protocol. This means that each virtual circuit on an interface is treated as a separate local network. Split horizon stops routing table updates from going out of the same interface on which they were received.

Prototyping the WAN

- To avoid the problems caused by split horizon, the physical interface is divided into logical subinterfaces. The two types of Frame Relay subinterfaces are point to-point and multipoint.

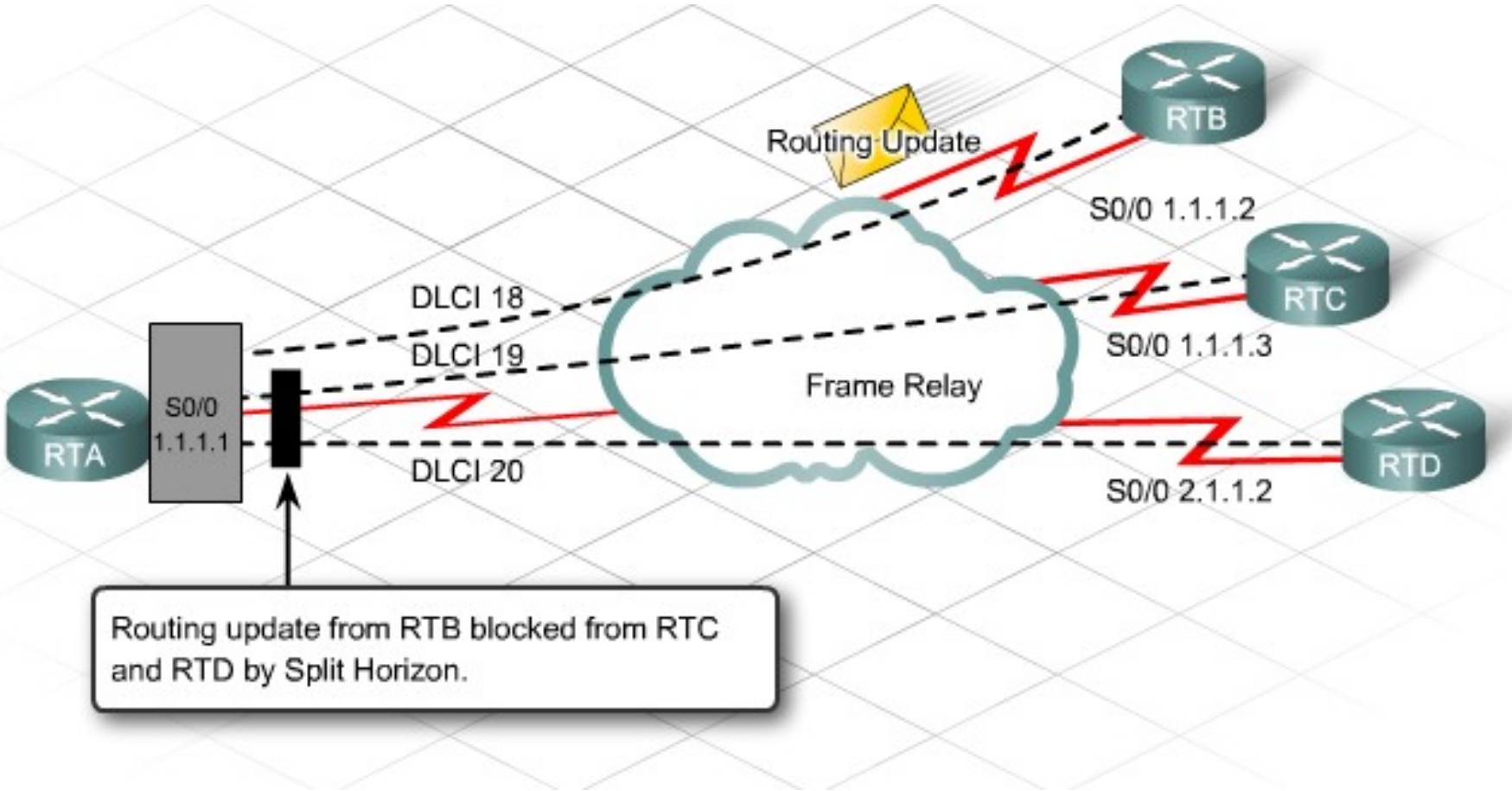
Prototyping the WAN

- Point-to-point
- With point-to-point subinterfaces, a single subinterface is used to establish one permanent virtual circuit (PVC) connection to another physical interface or subinterface on a remote router. Each pair of interfaces is in its own subnet, and each interface has a single DLCI. Broadcasts are not a problem in this environment because the routers are connected in a point-to-point manner and act like leased lines.

Prototyping the WAN

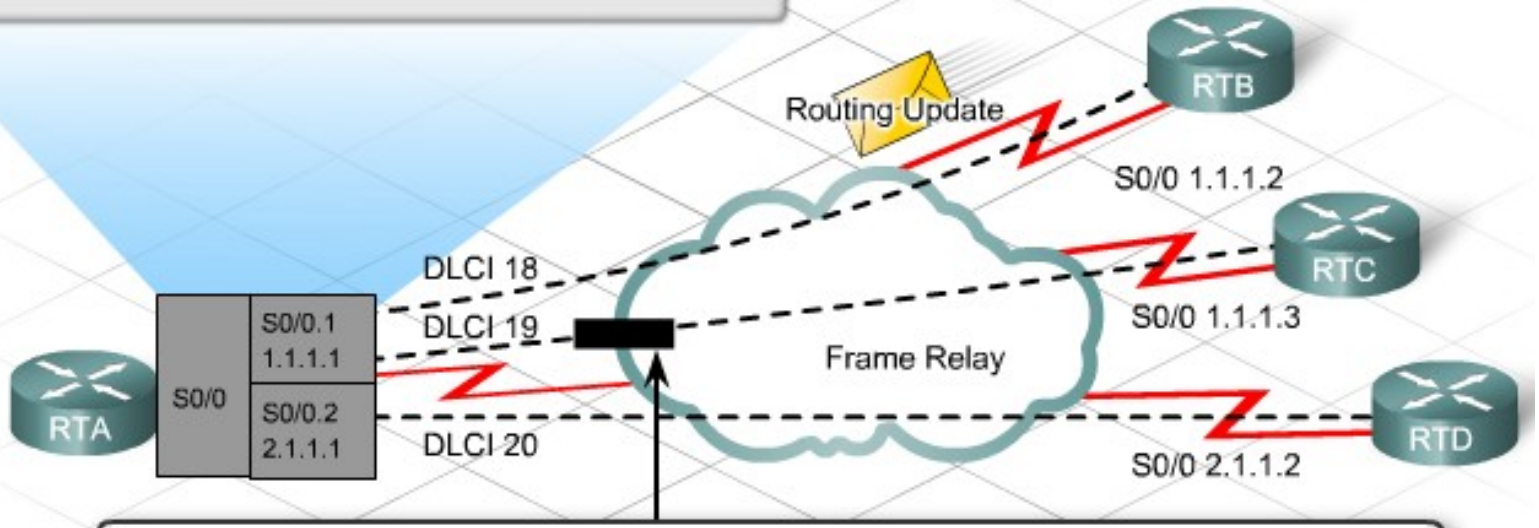
- Multipoint
- With multipoint subinterfaces, a single subinterface is used to establish multiple PVC connections to multiple physical interfaces or subinterfaces on remote routers. This configuration does not solve the problems with split horizon. Split horizon must be turned off for distance vector routing protocols to work with multipoint links.

Prototyping the WAN



Prototyping the WAN

```
interface Serial0/0.1 multipoint
 ip address 1.1.1.1 255.255.255.0
 frame-relay interface-dlci 18
 frame-relay interface-dlci 19
```



Routing update from RTB blocked from RTC by Split Horizon, but allowed to RTD across point-to-point interface.

RTA connects to RTB and RTC using a multipoint subinterface, while using a point-to-point subinterface to connect to RTD.

Prototyping the WAN

- Once the Frame Relay WAN is configured, it is necessary to verify that it is operating as expected. On the CPE router, there are a number of show commands that display information about the status of the Frame Relay local loop and the PVC circuit.

Prototyping the WAN

Verifying Frame Relay Operation: Look at the Interfaces

```
R1#show interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  LMI enq sent  59, LMI stat recvd 59, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 11/0, interface broadcasts 0
  Last input 00:00:05, output 00:00:05, output hang never
  Last clearing of "show interface" counters 00:09:55
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

Prototyping the WAN

Verifying Frame Relay Operation: LMI Statistics

```
R1#show frame-relay lmi
LMI Statistics for interface Serial0/0/1 (Frame Relay DTE) LMI TYPE = CISCO
  Invalid Unnumbered info 0              Invalid Prot Disc 0
  Invalid dummy Call Ref 0               Invalid Msg Type 0
  Invalid Status Message 0               Invalid Lock Shift 0
  Invalid Information ID 0               Invalid Report IE Len 0
  Invalid Report Request 0               Invalid Keep IE Len 0
  Num Status Enq. Sent 76                Num Status msgs Rcvd 76
  Num Update Status Rcvd 0               Num Status Timeouts 0
  Last Full Status Req 00:00:48          Last Full Status Rcvd 00:00:48
----------------------------------------------------------------------
```

Prototyping the WAN

Verifying Frame Relay Operation: PVC Status

```
R1#show frame-relay pvc 102
PVC Statistics for interface Serial0/0/1 (Frame Relay DTE)
DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/1.102
  input pkts 12             output pkts 20            in bytes 2816
  out bytes 5455            dropped pkts 0            in pkts dropped 0
  out pkts dropped 0                  out bytes dropped 0
  in FECN pkts 0            in BECN pkts 0            out FECN pkts 0
  out BECN pkts 0           in DE pkts 0              out DE pkts 0
  out bcast pkts 15         out bcast bytes 4935
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:13:27, last time pvc status changed 00:07:47
------------------------------------------------------------------
```

Prototyping the WAN

```
R1#show frame-relay map

Serial0/0/0 (up): ip 10.1.2.2 dlci 100(0x64,0x1840), dynamic,
              broadcast, CISCO, status defined, active
Serial0/0/1.102 (up): point-to-point dlci, dlci 102 (0x66, 0x1860),
              broadcast, status defined, active
```

```
R1#clear frame-relay inarp
R1#show frame-relay map
Serial0/0/1.102 (up): point-to-point dlci, dlci 102(0x66,0x1860), broadcast
          status defined, active
```

Troubleshooting Frame Relay Operations

After testing the basic Frame Relay connectivity, the network designer and NetworkingCompany staff decide to test the backup capabilities. They set up Ethernet connections between the routers. These Ethernet connections are intended to simulate the existing VPNs between the remote sites and the main stadium network. Another router, called ISPX, is added to the topology to simulate the ISP connectivity.

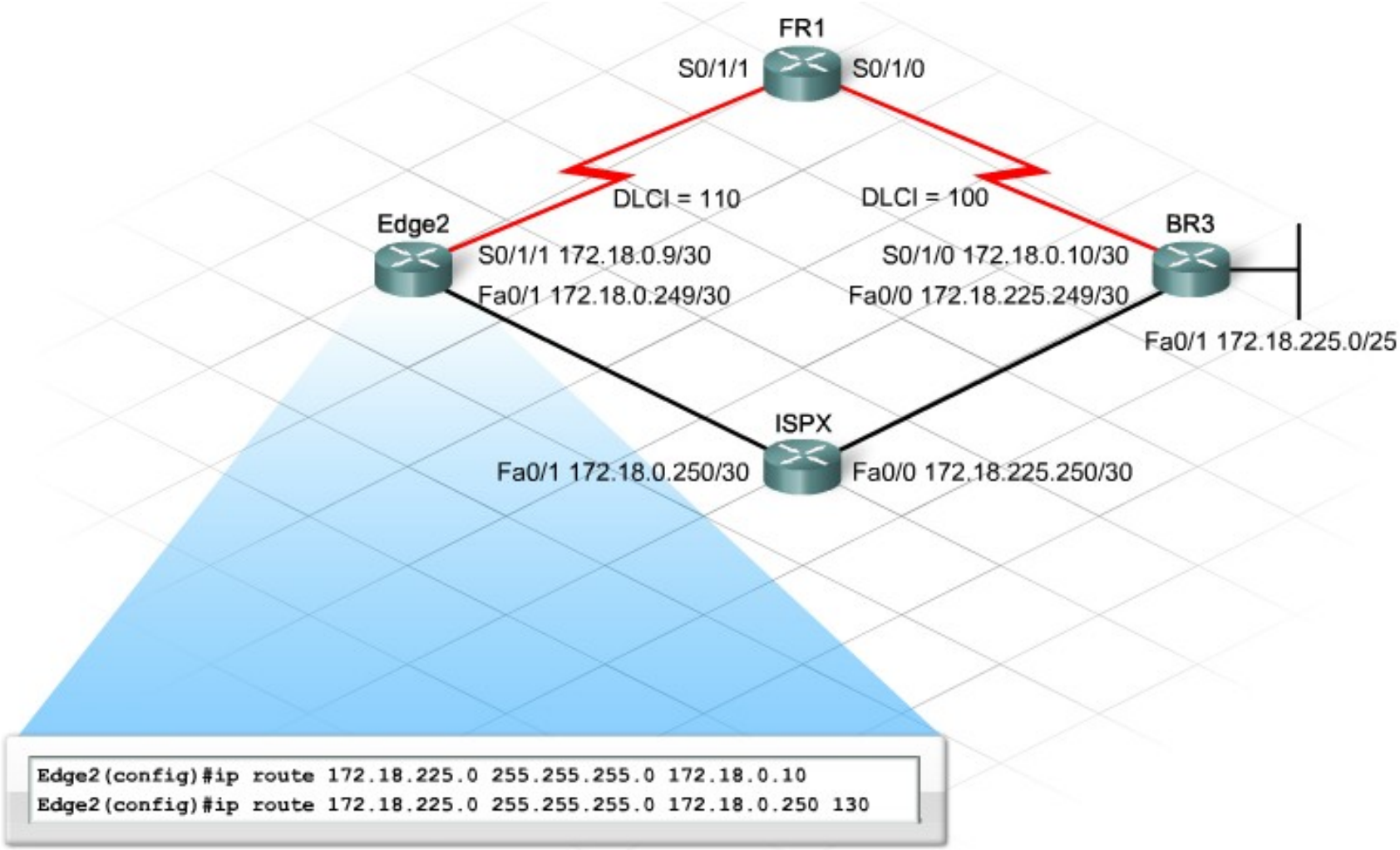
Troubleshooting Frame Relay Operations

- Configuring the Backup Link
- Routing on the two CPE routers must be configured so that the backup link is used if the Frame Relay link fails. One way to configure the routers to use the backup is to create floating static routes.

Troubleshooting Frame Relay Operations

- A floating static route is a static route that has an administrative distance greater than the administrative distance of the corresponding dynamic routes. The staff can configure a static route using the Fast Ethernet interfaces. The configuration specifies a higher administrative distance than the Frame Relay route, using the following command:
- Edge2(config)#ip route 172.18.225.0 255.255.255.0 172.18.0.250 130

Troubleshooting Frame Relay Operations



Troubleshooting Frame Relay Operations

- Troubleshooting a Primary Link Failure
- In a WAN design, the network designer must ensure that there are backup links, and that they function correctly in the event of a primary link failure. Frame Relay and other WAN technologies are generally very reliable services. There are times however, when the WAN network may perform at less than expected levels, or the circuit may be down. A backup link can carry traffic during these times, as well as during the time it takes to troubleshoot and repair the primary connection failure.

Troubleshooting Frame Relay Operations

- Checking Frame Relay Interface Status
- The first step in verifying or troubleshooting Frame Relay configuration issues is to use the show interface serial command. If the output of the show interface serial command indicates that both the interface and the line protocol are down, it typically indicates a problem at Layer 1. There may be a problem with the cable or CSU/DSU that needs to be corrected.

Troubleshooting Frame Relay Operations

- Verify LMI Operation
- When the output of a show interface serial command indicates that the interface is up, but the line protocol is down, there can be problem at Layer 2. The serial interface may not be receiving the LMI keep alive messages from the Frame Relay switch. The next step in troubleshooting the Frame Relay circuit is to verify that LMI messages are being sent and received correctly. Use the show frame-relay lmi command and look for a non-zero value in any of the Invalid counters. Also make sure that the LMI type is correct for the circuit.

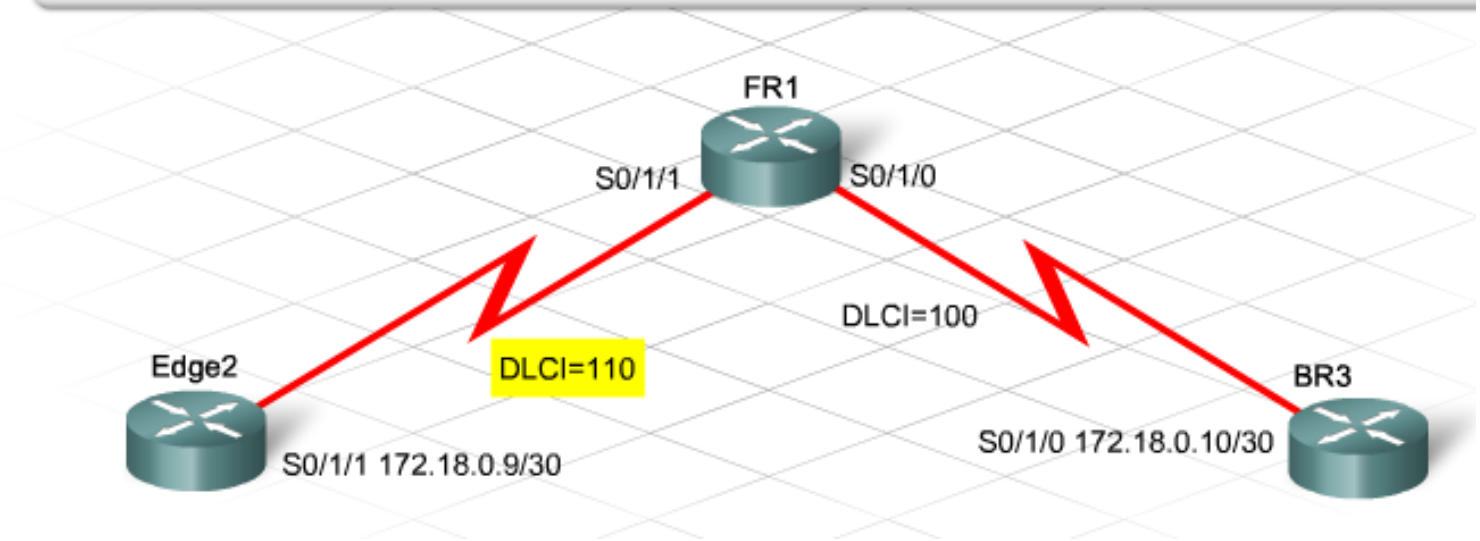
Troubleshooting Frame Relay Operations

```
Edge2#sh frame-relay pvc

PVC Statistics for interface Serial0/1/1 (Frame Relay DTE)

                Active      Inactive      Deleted      Static
  Local            0             0            1           0
  Switched         0             0            0           0
  Unused           0             0            0           0

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = DELETED, INTERFACE = Serial0/1/1
```



Troubleshooting Frame Relay Operations

- Debugging the LMI Exchange
- If the LMI type is correct for the circuit, but invalid messages are indicated, the debug frame-relay lmi command can provide more information. The debug command output shows the LMI messages as they are being sent and received between the Frame Relay switch and the CPE router in real time.

Troubleshooting Frame Relay Operations

- A type 0 message is a full LMI status message. Within the status message, the dlci 110, status 0x2 output indicates that DLCI 110 is active. The common values of the DLCI status field are:
- 0x0: Added and inactive - the switch has this DLCI programmed but it is not usable.
- 0x2: Added and active - the Frame Relay switch has the DLCI and everything is operational.

Troubleshooting Frame Relay Operations

- LMI status messages sent by the router are indicated by the (out) output. The (in) output indicates a message received from the Frame Relay switch.
- A type 0 message is a full LMI status message. Within the status message, the dlci 110, status 0x2 output indicates that DLCI 110 is active. The common values of the DLCI status field are:

Troubleshooting Frame Relay Operations

- 0x4: Deleted - the Frame Relay switch does not have this DLCI programmed for the router. This status can happen if the DLCIs are reversed on the router or if the PVC was deleted in the Frame Relay cloud.
- A type 1 message indicates a keepalive LMI exchange.

Troubleshooting Frame Relay Operations

- Checking Layer 3 Functionality
- At times, the Layer 1 and 2 functions are operational, but IP communication is not occurring over the PVC. For a router to reach a remote router across the Frame Relay network, it must map the IP address of the remote router with the correct local DLCI. If the IP address of the remote router does not appear in the Frame Relay mapping table, it may not support Inverse ARP.

Troubleshooting Frame Relay Operations

- It may require the IP address-to-DLCI mapping to be configured using the frame-relay map ip{ip address} {dlci} [broadcast] command.
- In addition, it is necessary to verify that no access control lists or IP routing table issues exist, as well. Although these types of issues are not directly related to the WAN circuit operation, they can make it appear as though the circuit is not functioning correctly.

Troubleshooting Frame Relay Operations

Troubleshooting Frame Relay Operation

```
Edge2# debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
Edge2#
1w2d: Serial0/1/1(out): StEnq, myseq 140, yourseen 139, DTE up
1w2d: datagramstart = 0xE008EC, datagramsize = 13
1w2d: FR encap = 0xFCF10309
1w2d: 00 75 01 01 01 03 02 8C 8B
1w2d:
1w2d: Serial0/1/1(in): Status, myseq 140
1w2d: RT IE 1, length 1, type 1
1w2d: KA IE 3, length 2, yourseq 140, myseq 140
1w2d: Serial0/1/1(out): StEnq, myseq 141, yourseen 140, DTE up
1w2d: datagramstart = 0xE008EC, datagramsize = 13
1w2d: FR encap = 0xFCF10309
1w2d: 00 75 01 01 01 03 02 8D 8C
1w2d:
1w2d: Serial0/1/1(in): Status, myseq 142
1w2d: RT IE 1, length 1, type 0
1w2d: KA IE 3, length 2, yourseq 142, myseq 142
1w2d: PVC IE 0x7 , length 0x6 , dlci 110, status 0x2 , bw 0
```

Identifying Risks and Weaknesses

- After completing the prototype testing of the WAN, the network designer and the NetworkingCompany staff discuss the results of the testing. The Frame Relay configuration performs as expected and the backup links protect the WAN connectivity in the event the Frame Relay link fails.
- However, there are a couple of risks involved with the Frame Relay configuration that must be communicated to the stadium management.

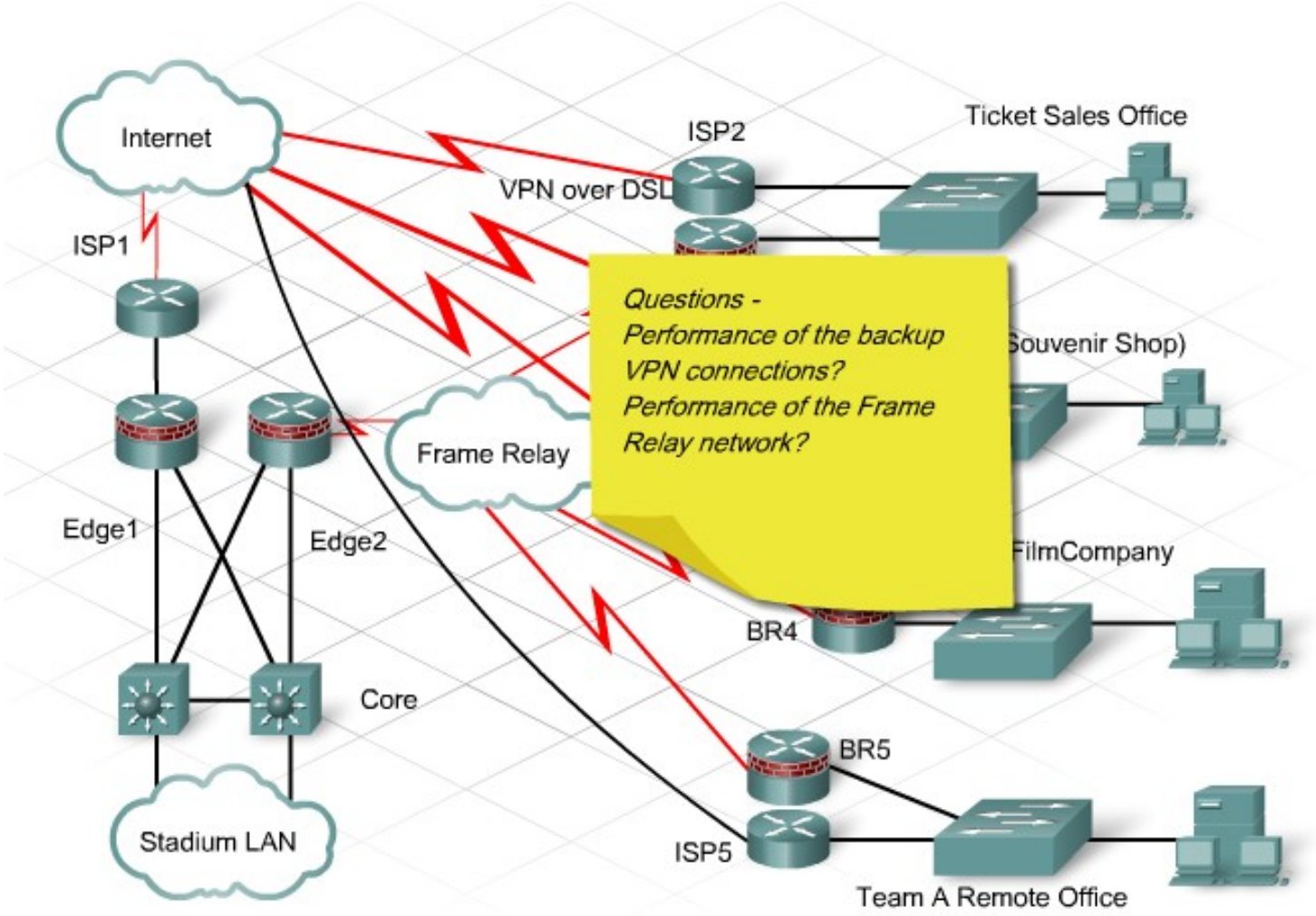
Identifying Risks and Weaknesses

- Areas of Risk
- The most critical area of risk is the performance of the VPN links functioning correctly when used as backups. When the voice and video components of the network are added to the existing WAN traffic, there may be a quality of service issue if the VPN connection must be used. The current VPN through the ISP does not have a guaranteed level of service

Identifying Risks and Weaknesses

- Furthermore, it does not have mechanisms to provide QoS. As a result, the backup links can only provide limited connectivity in the event of a failure.
- It is not possible to test the performance through the actual TSP Frame Relay network; therefore, there is a risk associated with the design. The final acceptance of the design cannot be done until the results of the pilot installation are known.

Identifying Risks and Weaknesses



Identifying VPN goals and Requirements

- A high-priority business goal of the stadium network design is to offer additional services to stadium vendors and customers to improve the stadium experience.
- Team Office Requirements
- The team offices are requesting a secure method for their scouts to connect to the team servers. The scouts need to transmit prospect information to the team servers when they are away from the stadium.

Identifying VPN goals and Requirements

- Because this information is extremely confidential, the team wants the scouts to be able to connect remotely via a VPN. A VPN is an extension of the internal private network. VPNs transmit information securely across shared or public networks, like the Internet. The network designer needs to consider the network impact of providing this service.

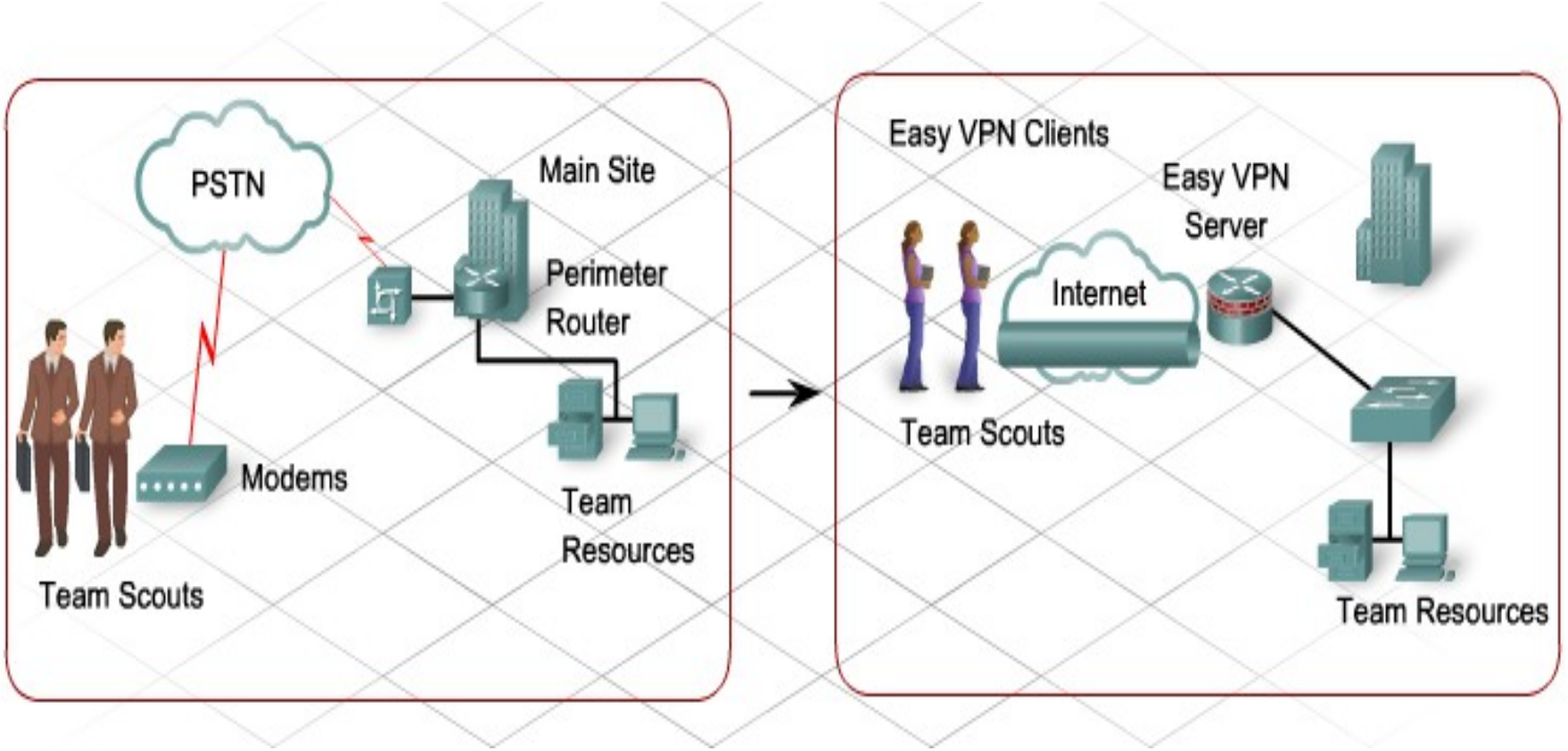
Identifying VPN goals and Requirements

- How a VPN Works
- A VPN emulates a point-to-point link. The VPN encapsulates the data with a header that provides routing information. This format enables the data to traverse the public network to reach its destination. To emulate a private link, the encapsulated data is encrypted for confidentiality. Encryption algorithms ensure that if packets are intercepted on the public network, they cannot be read without the encryption keys.

Identifying VPN goals and Requirements

- The team scouts, as well as others working at home or on the road, can use VPN connections to establish remote access to servers located at the stadium. From the perspective of the users, the VPN is a point-to-point connection between their computer (the VPN client) and a VPN endpoint (the VPN server or VPN concentrator) at the stadium.

Identifying VPN goals and Requirements



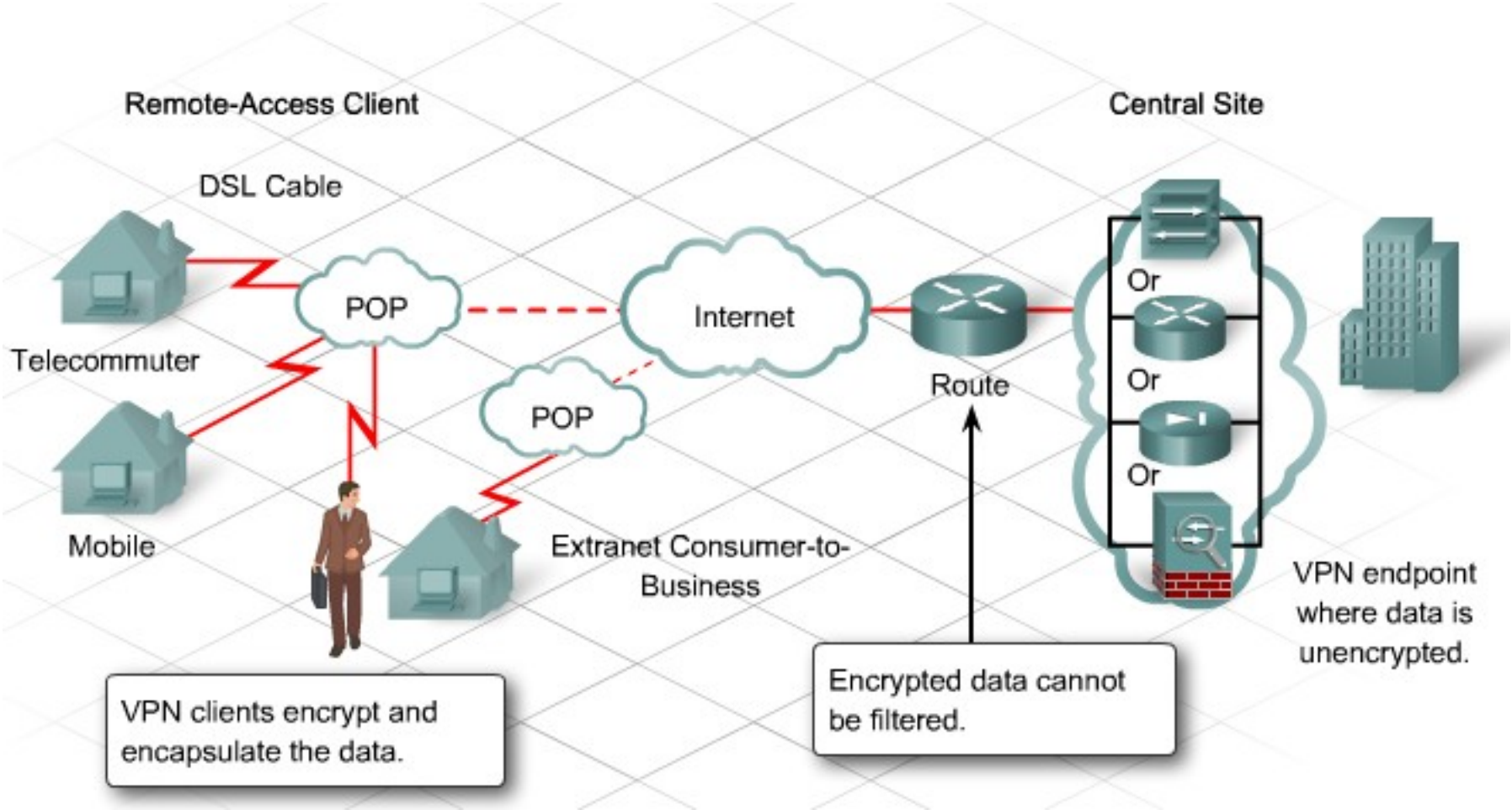
Identifying VPN goals and Requirements

- VPN Security
- In many businesses, remote workers accessing resources at the central site through a VPN are considered "trusted" users, just like those workers who actually work on site. Unlike the on-site workers, VPN users may be accessing the network from devices that are not fully secured or from insecure locations in public areas. Extra care needs to be taken to ensure that these remote workers do not have access to resources or areas of the network that they do not need to do their jobs.

Identifying VPN goals and Requirements

- VPN Server Location
- The network designer knows that encrypted data cannot be filtered until it is unencrypted at the VPN server endpoint. For that reason, the location of the VPN server in the network is very important. It must be located at a point where incoming packets can be examined and filtered before being delivered to the internal network resources.

Identifying VPN goals and Requirements



Creating the Test Plan

- What Needs to Be Tested?
- The stadium uses VPN networks to connect to the souvenir shop and the ticket outlet. These VPNs are site-to-site VPNs managed by the ISP and do not need to be tested.
- Team Scout Support
- Two options are available to support the team scout VPN requirements for the remote clients:
- Option 1: The stadium management can request additional VPN services from the current ISP.
- Option 2: The VPN server can be installed on the stadium network.

Creating the Test Plan

- VPN Server Management
- The designer suggests using split tunneling to allow users to send traffic that is destined for the corporate network across the VPN tunnel, while allowing all other traffic to be sent out to the Internet through the local LAN of the VPN client. The designer must determine if a VPN server can be configured and managed by the existing stadium personnel. To do this, the designer decides to test the ease of configuring and installing the VPN server and client software. After configuring the VPN, the designer tests the ACLs for filtering traffic coming through the VPN and the placement of the VPN server in the network.

Creating the Test Plan

- Cisco EasyVPN
- The designer decides that Cisco EasyVPN is the best option to use for configuring and managing remote user VPN connectivity. EasyVPN is a Cisco IOS software tool. It facilitates the configuration of a Cisco security appliance or router as a VPN server or endpoint.
- For the prototype, the designer selects the IP Advanced Security feature set for the 1841 router. The Cisco SDM interface on the 1841 can be used to configure the EasyVPN Server for the remote clients.

Creating the Test Plan

Business Goal	Overall Success Criteria
Improve the customer experience by offering additional services to customers and vendors.	Sports team personnel using VPN clients can successfully connect to team resources located on the stadium network.

Technical Requirements	Success Criteria
Scalability	
Configure split tunneling to permit only the traffic destined for the stadium resources access via the VPN.	VPN clients can be added without impacting the performance of the LAN.
Availability	
Configure redundant VPN servers to provide failover.	Connectivity is not lost if one VPN server goes down.
Security	
Configure IPSec VPNs.	EasyVPN client configuration supports a high level of security.
Manageability	
Use Cisco EasyVPN to configure the VPN settings.	It is easy to perform and manage configurations.
Use SDM to configure and manage VPN server.	It is easy to perform and manage configurations.

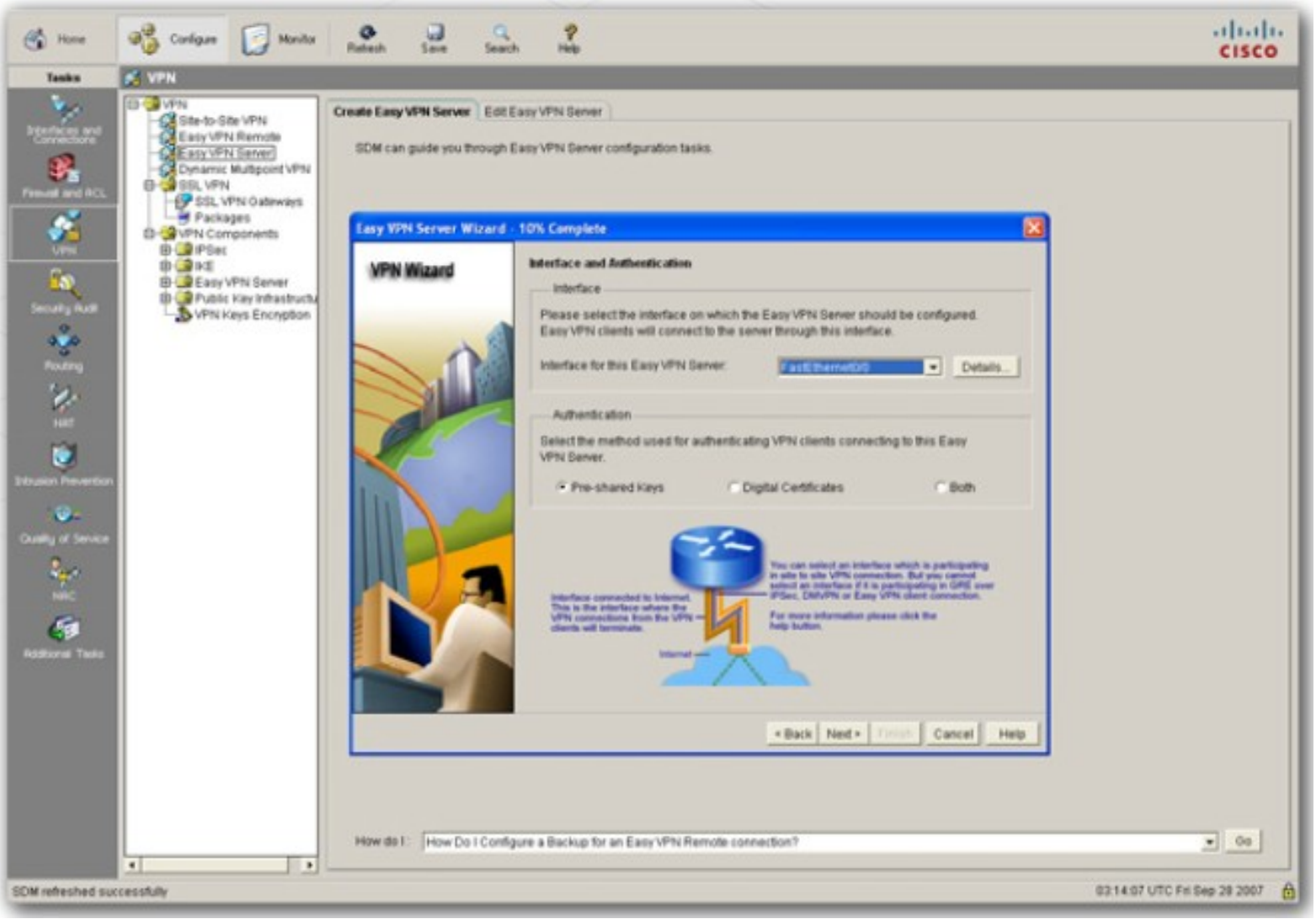
Creating the Test Plan

- The Cisco EasyVPN Solution
- To ensure that the VPN can support the mobile team scouts, ease of deployment is important. There are two components of Cisco EasyVPN:
- Cisco EasyVPN Server - This server can be a router or a dedicated VPN gateway, such as a PIX firewall or a VPN concentrator. A VPN gateway using Cisco EasyVPN Server software can terminate remote access VPNs and site-to-site VPN connections.

Creating the Test Plan

- Cisco EasyVPN Remote - Cisco EasyVPN Remote enables remote devices to receive security policies from a Cisco EasyVPN Server. This minimizes configuration requirements at the remote VPN location. Cisco EasyVPN Remote allows the VPN parameters to be pushed from the server to the remote device. VPN parameters include internal IP addresses, internal subnet masks, and DHCP server addresses.

Creating the Test Plan



Validating Choice of VPN Topology, Devices and Topologies

- Before testing the VPN prototype configuration, the network designer needs to consider many different protocols, algorithms, and options.
- VPN Components
  - VPNs have two important components:
    - Tunneling to create the virtual network
    - Encryption to enable privacy and security

Validating Choice of VPN Topology, Devices and Topologies

- Virtual Network
- To build a virtual network, a tunnel is created between the two endpoints. In a site-to-site VPN, hosts send and receive normal TCP/IP traffic through a VPN gateway. A gateway can be a router, firewall, VPN concentrator, or security appliance. The gateway is responsible for encapsulating outbound traffic from one site and sending it through a tunnel over a network to a peer gateway at the remote site.

Validating Choice of VPN Topology, Devices and Topologies

- A tunnel by itself may not guarantee security. The tunnel simply creates an extension of the local network across the WAN or public network. Tunnels can carry either encrypted or unencrypted content. Upon receipt, the remote peer gateway strips the headers, decrypts the packet, and relays it toward the target host inside its private network. In a remote-access VPN, the VPN client on the user computer contacts the gateway to set up the tunnel.

Validating Choice of VPN Topology, Devices and Topologies

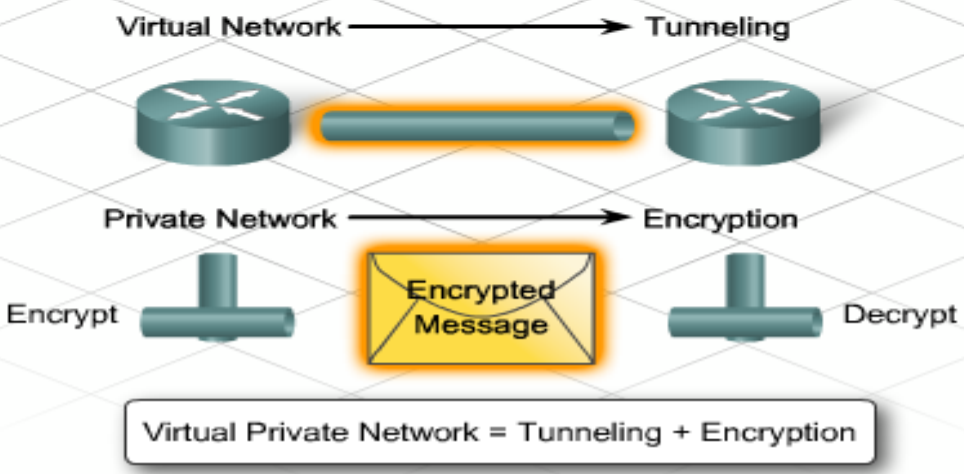
- VPN Tunnel Protocols
- VPN tunnels are created using a number of different encapsulation protocols. These protocols include:
- Generic routing encapsulation (GRE)
- IP Security (IPSec)
- Layer 2 Forwarding (L2F) Protocol
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)

Validating Choice of VPN Topology, Devices and Topologies

Encryption algorithms

Data Encryption Standard (DES) algorithm- DES was developed by IBM. DES uses a 56-bit key, ensuring high-performance encryption. 3DES is a symmetric key cryptosystem.

Generic Routing Encapsulation (GRE) tunnels provide a specific pathway across the shared WAN. They encapsulate traffic with new packet headers to ensure delivery to specific destinations. The network is private. This is because traffic can enter a tunnel only at an endpoint and can leave only at the other endpoint. Tunnels do not provide



Validating Choice of VPN Topology, Devices and Topologies

- VPN technologies use encryption algorithms that prevent data from being read if it is intercepted. An encryption algorithm is a mathematical function that combines the message with a string of digits called a key. The output is an unreadable cipher string. Decryption is extremely difficult or impossible without the correct key. The most common encryption methods used for VPNs are Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES), and Rivest, Shamir, and Adleman (RSA).

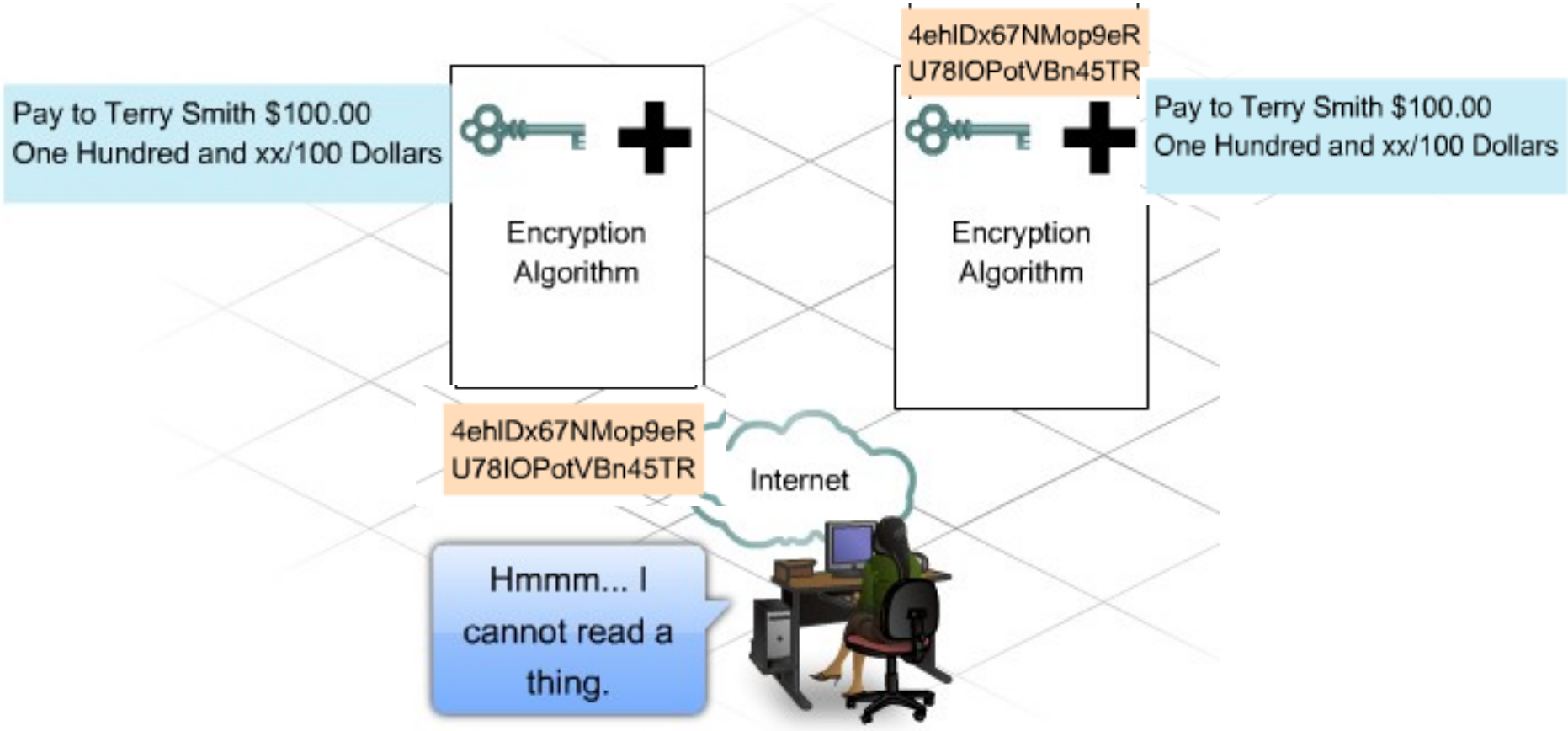
Validating Choice of VPN Topology, Devices and Topologies

- Encryption Algorithms
- Encryption algorithms, such as DES and 3DES, require a symmetric, shared secret key to perform encryption and decryption. The network administrator can manually configure keys.
- Alternatively, keys can be configured through the use of a key exchange method. The Diffie-Hellman (DH) key agreement is a public key exchange method. It provides a way for two peers to establish a shared secret key, which only they recognize, while communicating over an unsecured channel.

Validating Choice of VPN Topology, Devices and Topologies

- Diffie-Hellman groups specify the type of cryptography to be used:
- DH GROUP 1 - Uses 768-bit cryptography.
- DH GROUP 2 - Cisco IOS, PIX Firewall, and Cisco Adaptive Security Appliances (ASA) devices only. Specifies to use 1024-bit cryptography.
- DH GROUP 5 - Supported if the software system requirements are met. Specifies to use 1536-bit cryptography.

Validating Choice of VPN Topology, Devices and Topologies



Validating Choice of VPN Topology, Devices and Topologies

- To guard against the interception and modification of VPN data, a data integrity algorithm can be used. A data integrity algorithm adds a hash to the message. If the transmitted hash matches the received hash, the received message is accepted as an exact copy of the transmitted message. Keyed Hashed Message Authentication Code (HMAC) is a data integrity algorithm that guarantees the integrity of the message. There are two common HMAC algorithms:

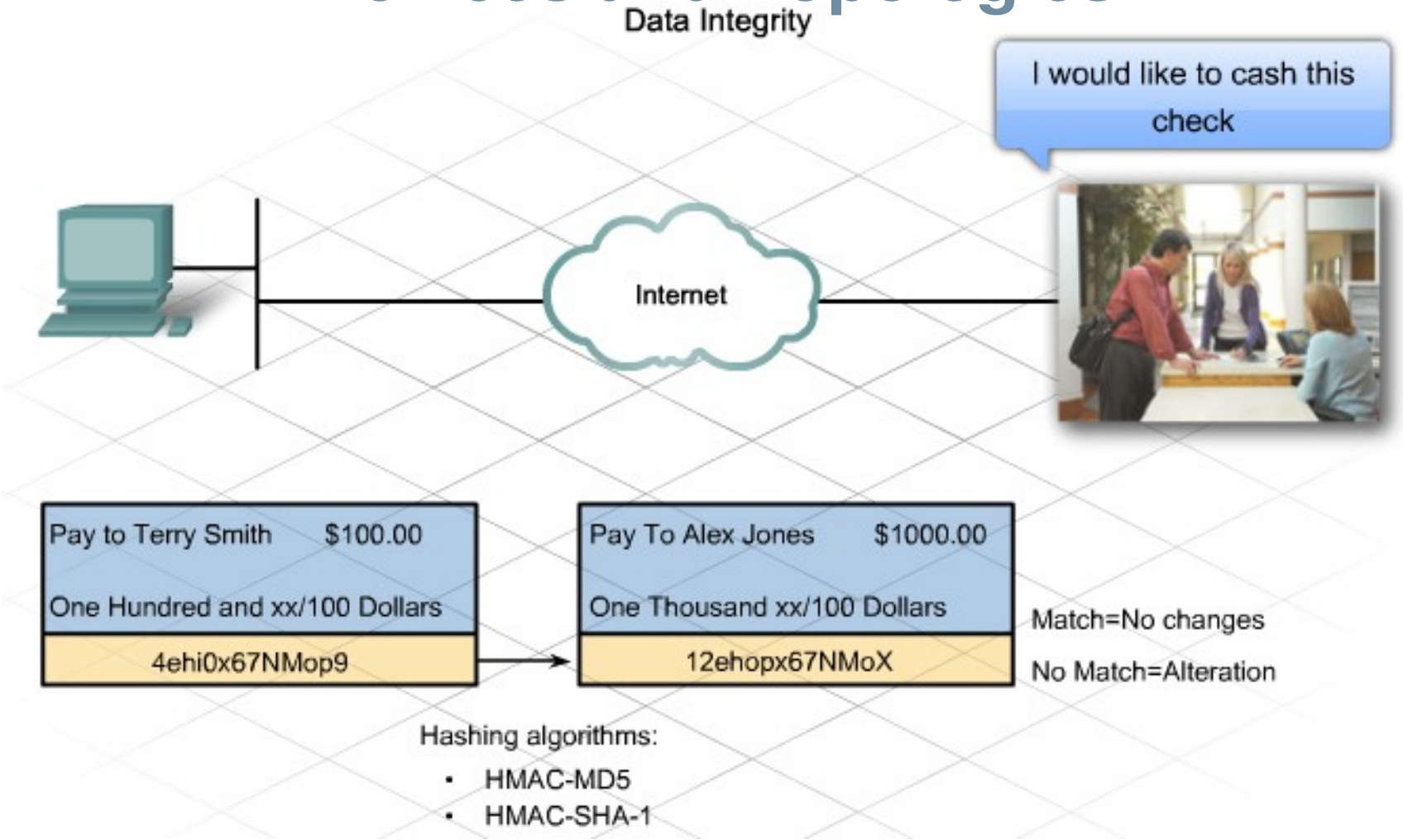
Validating Choice of VPN Topology, Devices and Topologies

- HMAC-Message Digest 5 (MD5) - This algorithm uses a 128-bit shared secret key. The variable length message and 128-bit shared secret key are combined and run through the HMAC-MD5 hash algorithm. The output is a 128-bit hash. The hash is appended to the original message and forwarded to the remote end.

Validating Choice of VPN Topology, Devices and Topologies

- HMAC-Secure Hash Algorithm 1 (HMAC-SHA-1) - This algorithm uses a 160-bit secret key. The variable length message and the 160-bit shared secret key are combined and run through the HMAC-SHA-1 hash algorithm. The output is a 160-bit hash. The hash is appended to the original message and forwarded to the remote end.

Validating Choice of VPN Topology, Devices and Topologies



Prototype VPN Connectivity for remote workers

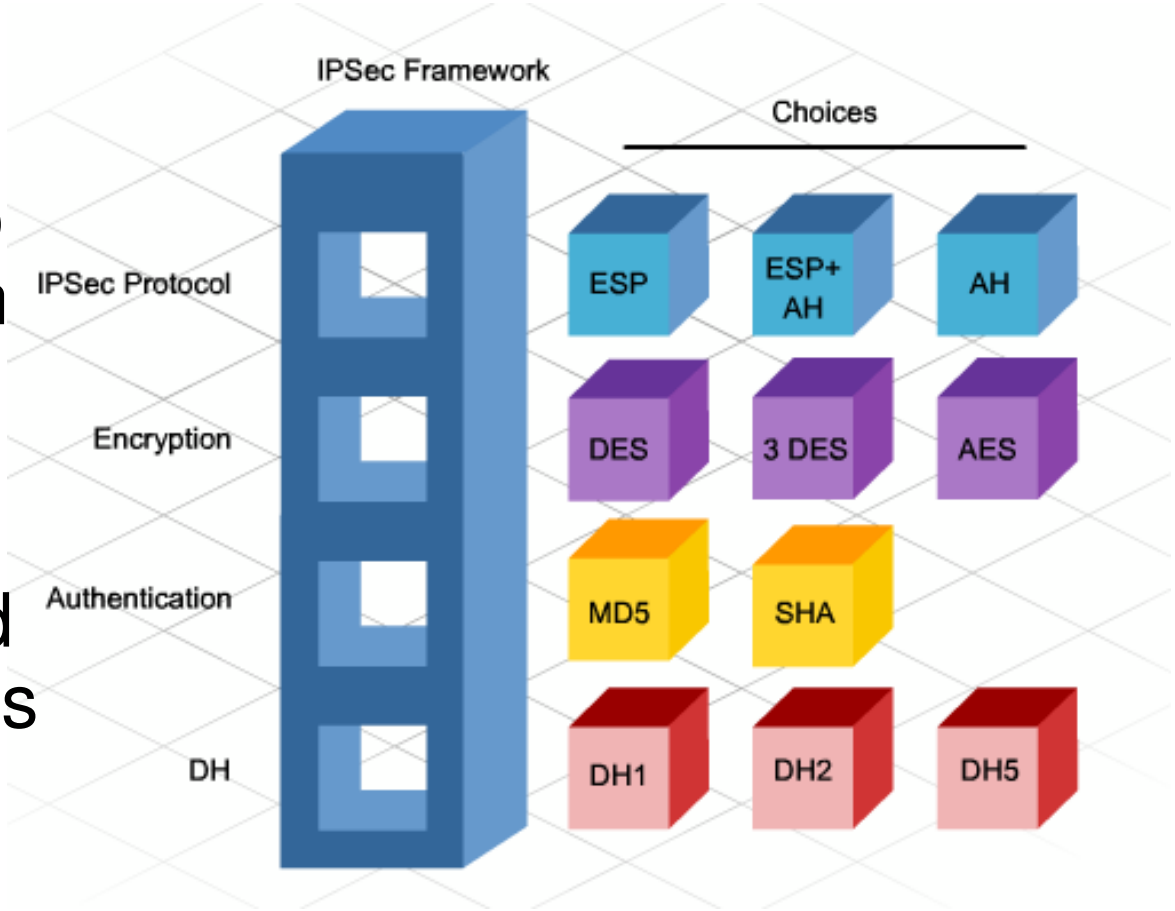
- In the proposed stadium network, the network designer chooses IPSec technology for the remote access VPNs.
- IPSec
- IPSec is a framework of open standards. It provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at Layer 3.

Prototype VPN Connectivity for remote workers

- IPSec relies on existing algorithms to implement the encryption, authentication, and key exchange. When configuring the VPN server, the following settings must be configured:
- An IPSec protocol - The choices are Encapsulating Security Payload (ESP), Authentication Header (AH), or ESP with AH.
- An encryption algorithm that is appropriate for the desired level of security - The choices are DES, 3DES, or AES.
- An authentication algorithm to provide data integrity - The choices are MD5 or SHA.
- A Diffie-Hellman group - The choices are DH1, DH2, and DH5, if supported.

Prototype VPN Connectivity for remote workers

IPSec can use Internet Key Exchange (IKE) to handle negotiation of protocols and algorithms. IKE can also generate the encryption and authentication keys that IPSec uses.



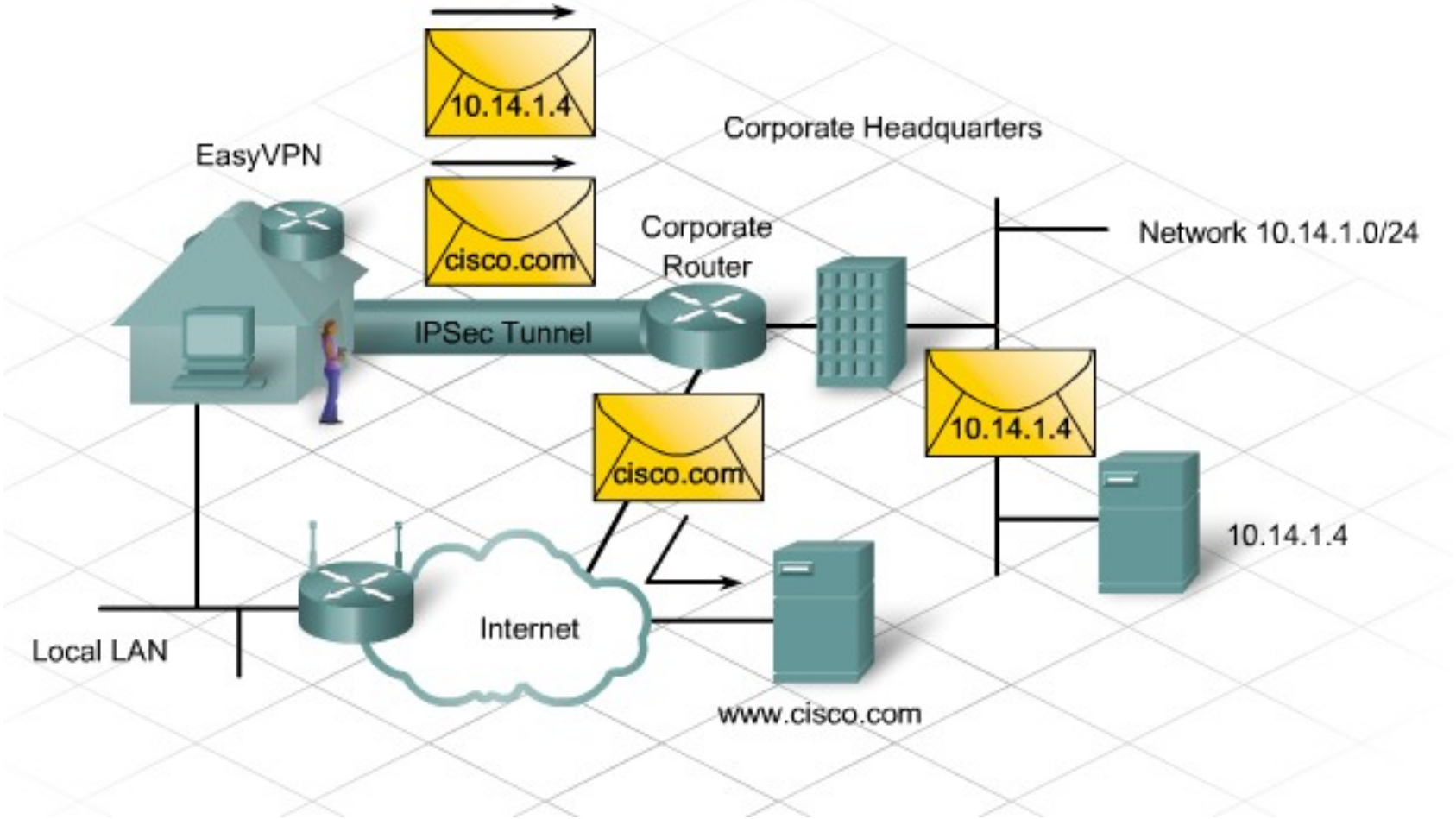
Prototype VPN Connectivity for remote workers

- Split tunneling allows users to send only the traffic that is destined for the corporate network across the tunnel. All other traffic is sent out to the Internet via the local LAN of the VPN client. Examples of other traffic include instant messaging, email, and casual web browsing. Cisco VPN client software can be configured for split tunnels by enabling the Allow Local LAN Access option. Split tunneling increases security risks, because an attack can come from the Internet side of the client into the secured network.

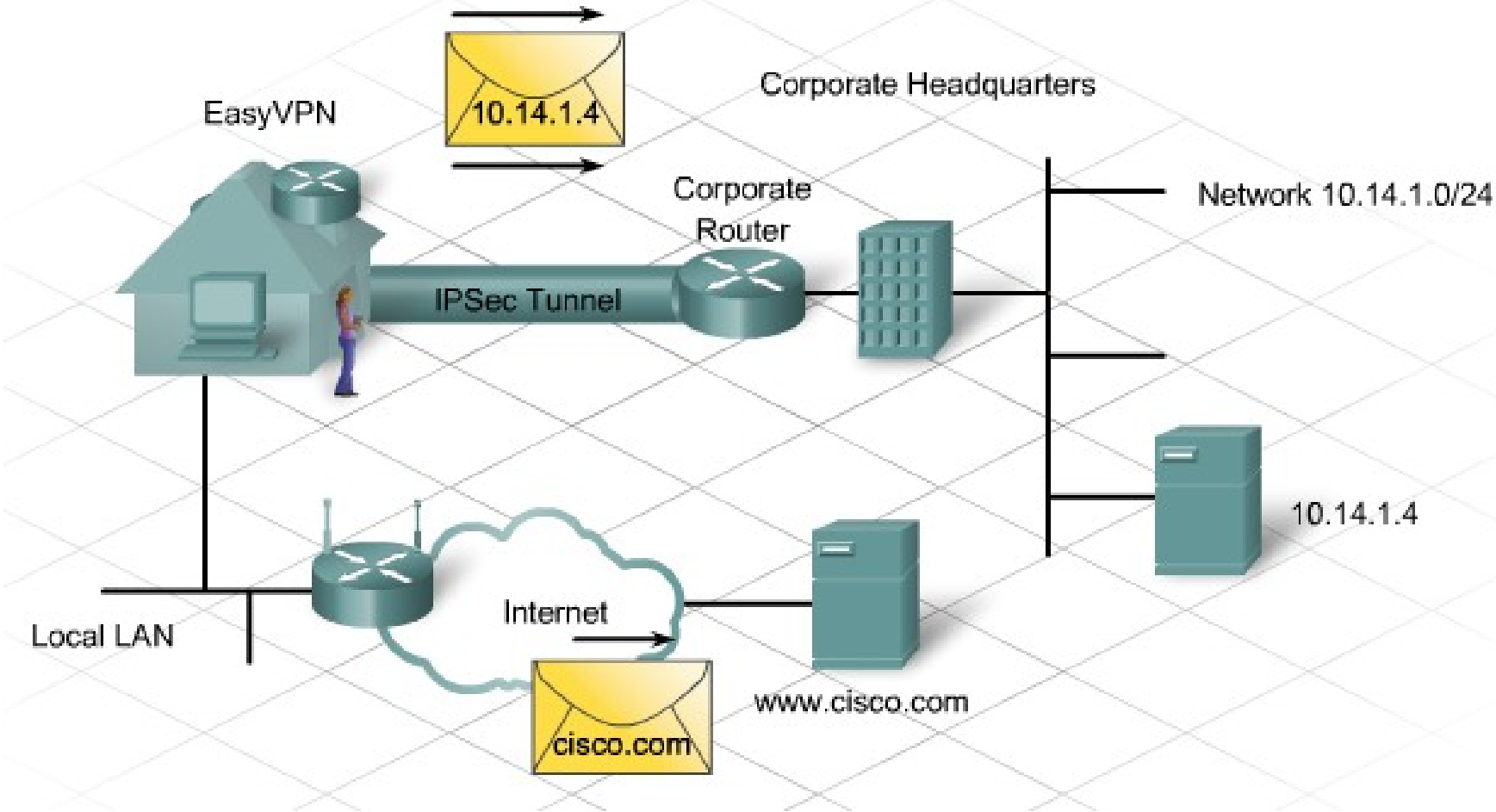
Prototype VPN Connectivity for remote workers

- VPN clients receive a logical network interface with an IPv4 address that is significant on the central site internal network. This IPv4 address typically comes from a private IP address range. As a result, VPN users may not be able to access their local resources, such as printers and servers.
- Split Tunnels
- In a basic VPN client scenario, all traffic from the VPN client is encrypted using the logical network interface. It is then sent to the VPN server, regardless of where the traffic is destined to go.

Prototype VPN Connectivity for remote workers



Prototype VPN Connectivity for remote workers



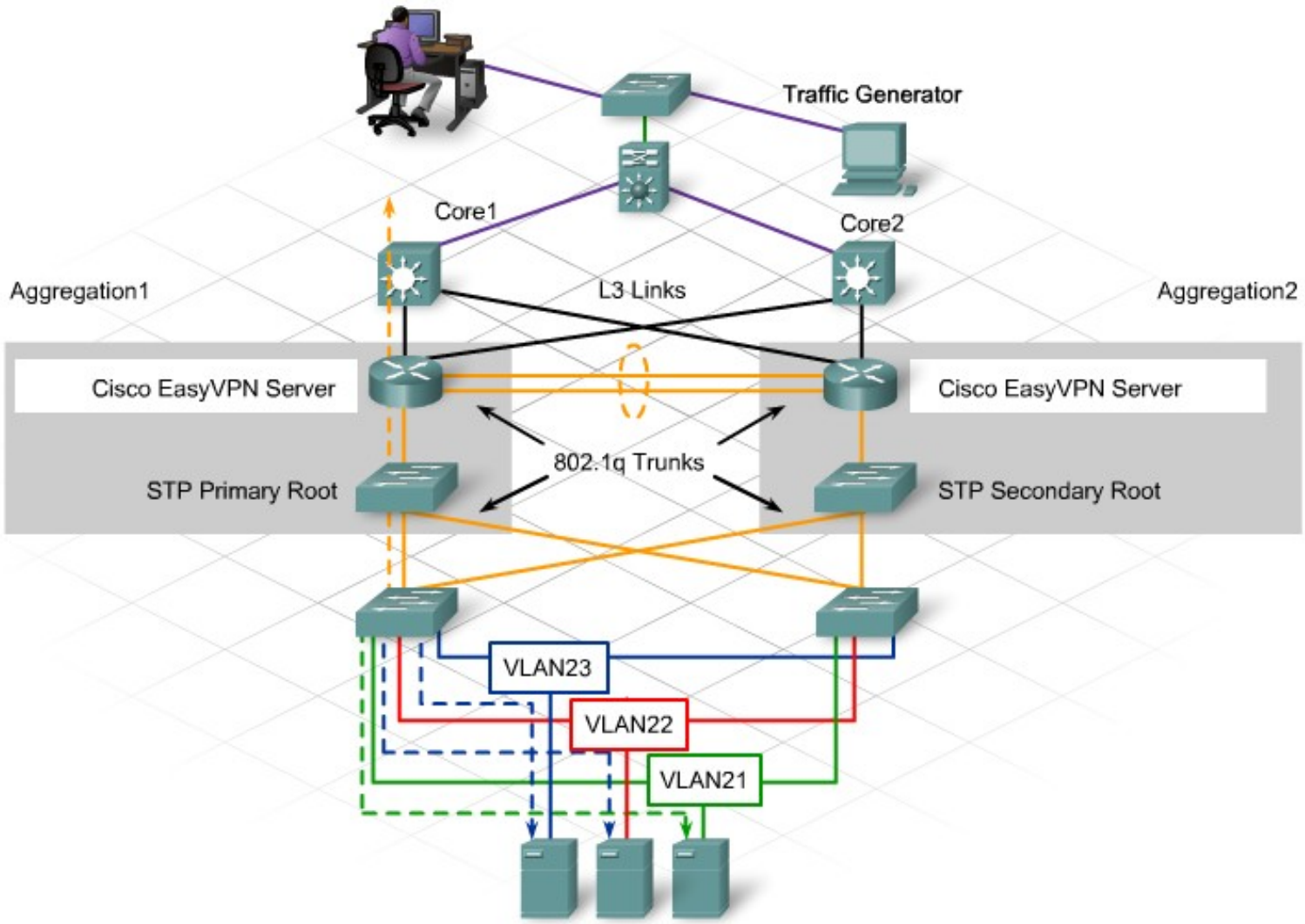
Validate Placement of VPN Servers

- The network designer must decide where to place the VPN server before determining how and where to filter and control traffic.
- VPN Server Placement
- Often, VPN servers are placed at the WAN edge of a network. In these cases, firewalls or ACLs are used to ensure that VPN users have access only to appropriate network resources.

Validate Placement of VPN Servers

- If the stadium management chooses to install a local VPN server, the designer recommends placing the VPN server on the same device that is providing firewall filtering for servers. The remote user traffic can be decrypted and filtered before being sent to the server.
- The designer creates a test topology that is similar to the topology used in the server farm prototype testing. The designer then creates an installation checklist and a test plan to test the operation of the VPN and the ACL filtering.

Validate Placement of VPN Servers



Validate Placement of VPN Servers

- Upon completion of the testing, the network designer analyzes the results to determine the level of risk in the design.
- VPN Design Risks
- In the VPN design to support the remote team personnel, the main risk relates to the ability of the current IT support staff to configure and maintain the VPN server. Configuring clients as the need arises is also a risk.

Validate Placement of VPN Servers

- Using Cisco EasyVPN and SDM proves to be the correct choice for configuring and maintaining the remote access VPN for the stadium network. It is relatively easy to create secure connectivity for the remote workers.
- With the entire prototype testing complete, the designer can work with the rest of the NetworkingCompany staff to prepare the final design presentation for the stadium network upgrade.