NETWORK OPERATIONS

Network Operations Security Center (NOSC) functions

- Manage Network Infrastructure
  - Network assemblages and appliances
  - Setup and teardown of network
  - Infrastructure change management

- Monitor Network Infrastructure
  - Provision monitoring tools and systems
  - Track status of network systems
  - Track network connectivity and traffic

NETWORK OPERATIONS

- Upper Tier
  - Theater / Regional
  - Corps
  - Division
- Middle Tier
  - Brigade (Lowest level of NETOPS acknowledged by doctrine)
  - Battalion
- Lower Tier
  - Company
  - Platoon

NETWORK OPERATIONS

Network Operations Security Center (NOSC) functions

- Manage Network Services
  - Provisioning, access, maintenance, etc…
- Monitor Network Services
  - Track availability, performance, and distribution
- Direct Network Priorities
  - Set priorities for problem handling
  - Priorities of service provisioning
  - Priorities of network changes

NETWORK OPERATIONS

Network Operations Security Center (NOSC) functions

- Manage Network Support Assets
  - CECOM (IT Switch LAR, LHT LAR, P&E LAR, DSE)
  - FSR contract personnel (GD, Rockwell Collins, Raytheon, etc.)
  - Support request to ESB

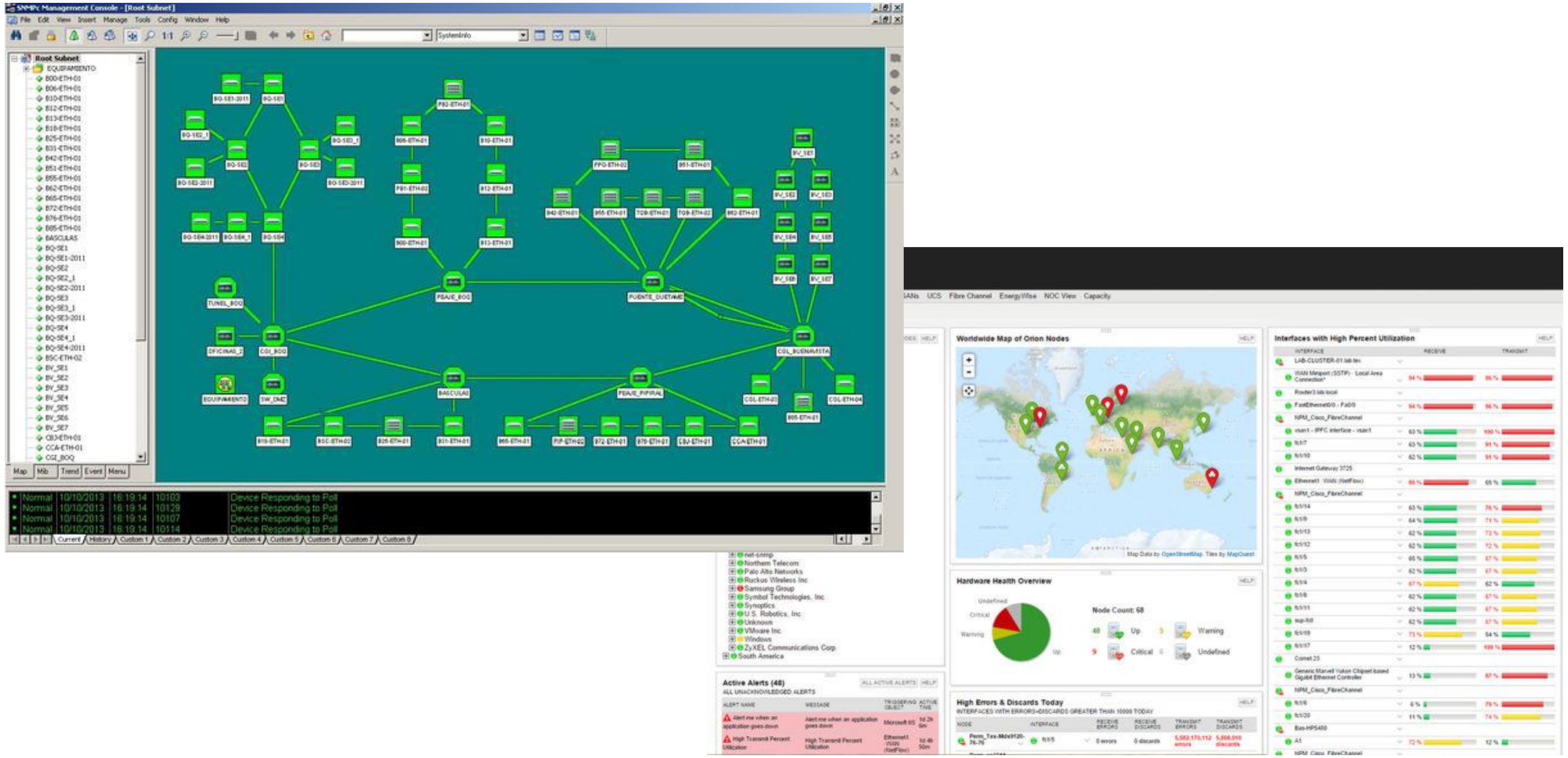
- Manage Cyber Security
  - Policy Enforcement
  - Security Appliance management
  - Threat handling and reporting

NETWORK OPERATIONS

Network Operations Security Center (NOSC) functions

<u>NMS SYSTEMS</u>

- Castle Rock SNMPc
- Solar Winds Orion NPM
- SYSLOG
- HBSS
- ACAS
- Mcafee ESM



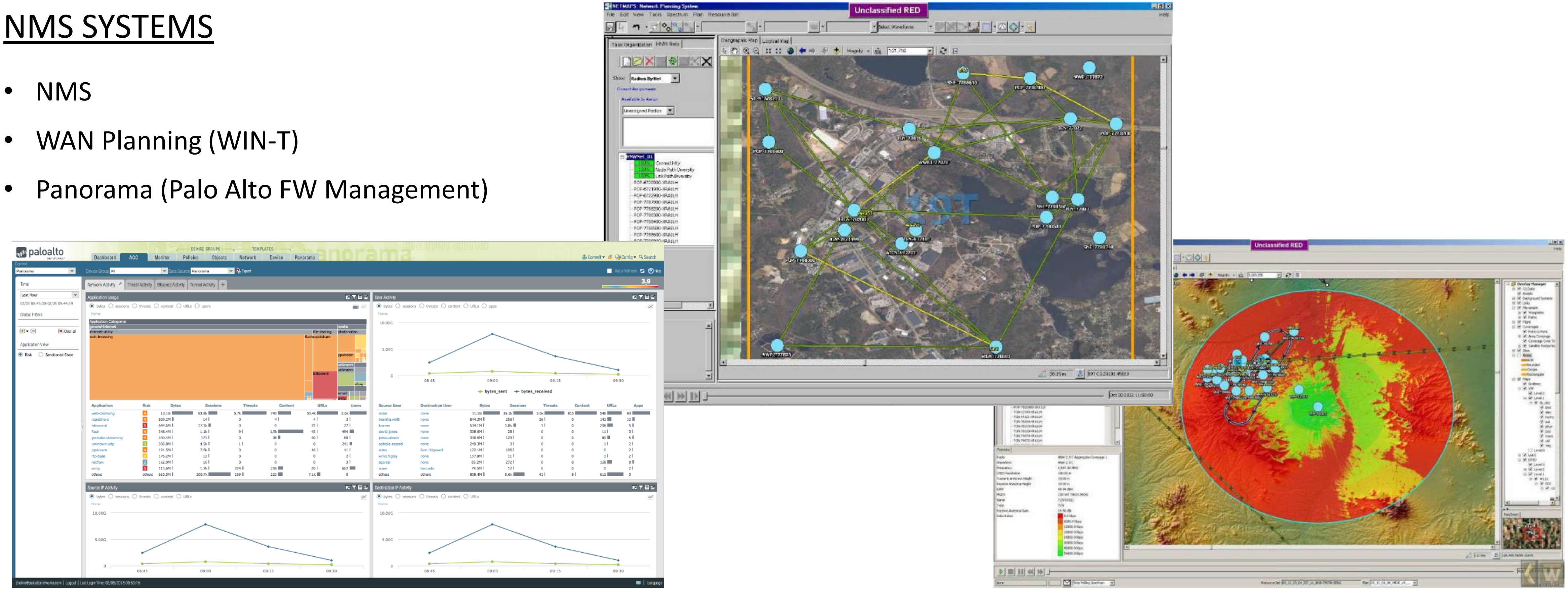
```
● Normal 10/10/2013 16:19:14 10103   Device Responding to Poll
● Normal 10/10/2013 16:19:14 10129   Device Responding to Poll
● Normal 10/10/2013 16:19:14 10107   Device Responding to Poll
● Normal 10/10/2013 16:19:14 10114   Device Responding to Poll
```

NETWORK OPERATIONS

Network Operations Security Center (NOSC) functions

NMS SYSTEMS

- NMS
- WAN Planning (WIN-T)
- Panorama (Palo Alto FW Management)



NETWORK OPERATIONS

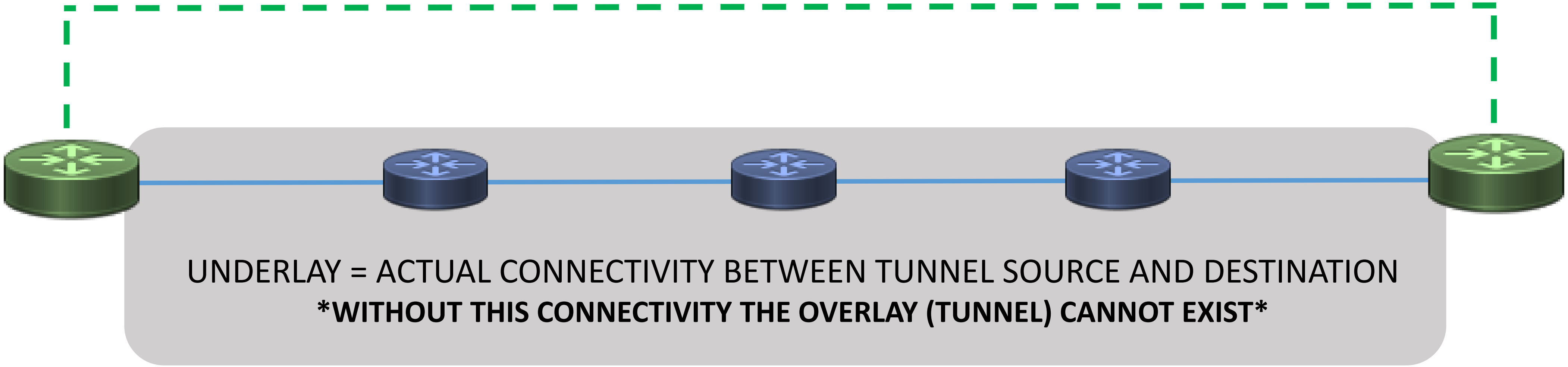
Network Operations Security Center (NOSC) functions

- Information Dissemination Management (IDM)
  - Subordinate NETOPS
  - Higher NETOPS
  - Battle Staff
  - Tactical Nodes

NETWORK OPERATIONAL ISSUES

- The Training Deficit
- Lack of Procedures – (Cyber security, COMSEC, etc…)
- Disengaged S6 – (unprepared, uniformed, lack of interest)
- Disregarded Assets and Resources
- Unauthorized Actions
  - SATCOM
  - NODE Operations
- Failure to Plan

OVERLAY = “LOGICAL” POINT-TO-POINT TUNNEL CONNECTIVITY BASED ON EXISTENCE OF THE UNDERLAY



UNDERLAY = ACTUAL CONNECTIVITY BETWEEN TUNNEL SOURCE AND DESTINATION

WITHOUT THIS CONNECTIVITY THE OVERLAY (TUNNEL) CANNOT EXIST

TUNNEL INTERFACE IP ADDRESSES: OVERLAY

TUNNEL SOURCE: LOCAL UNDERLAY
TUNNEL DESTINATION: DISTAND-END UNDERLAY

THE TUNNEL SOURCE AND DESTINATION MUST BE ABLE TO REACH EACHOTHER BEFORE THE TUNNEL CAN COME UP
(TUNNEL WILL SHOW “UP” AS LONG AS THERE IS A ROUTE TO DESTINATON BUT WILL NOT FUNCTION UNLESS THE CONNECTION IS BI-DIRECTIONAL)

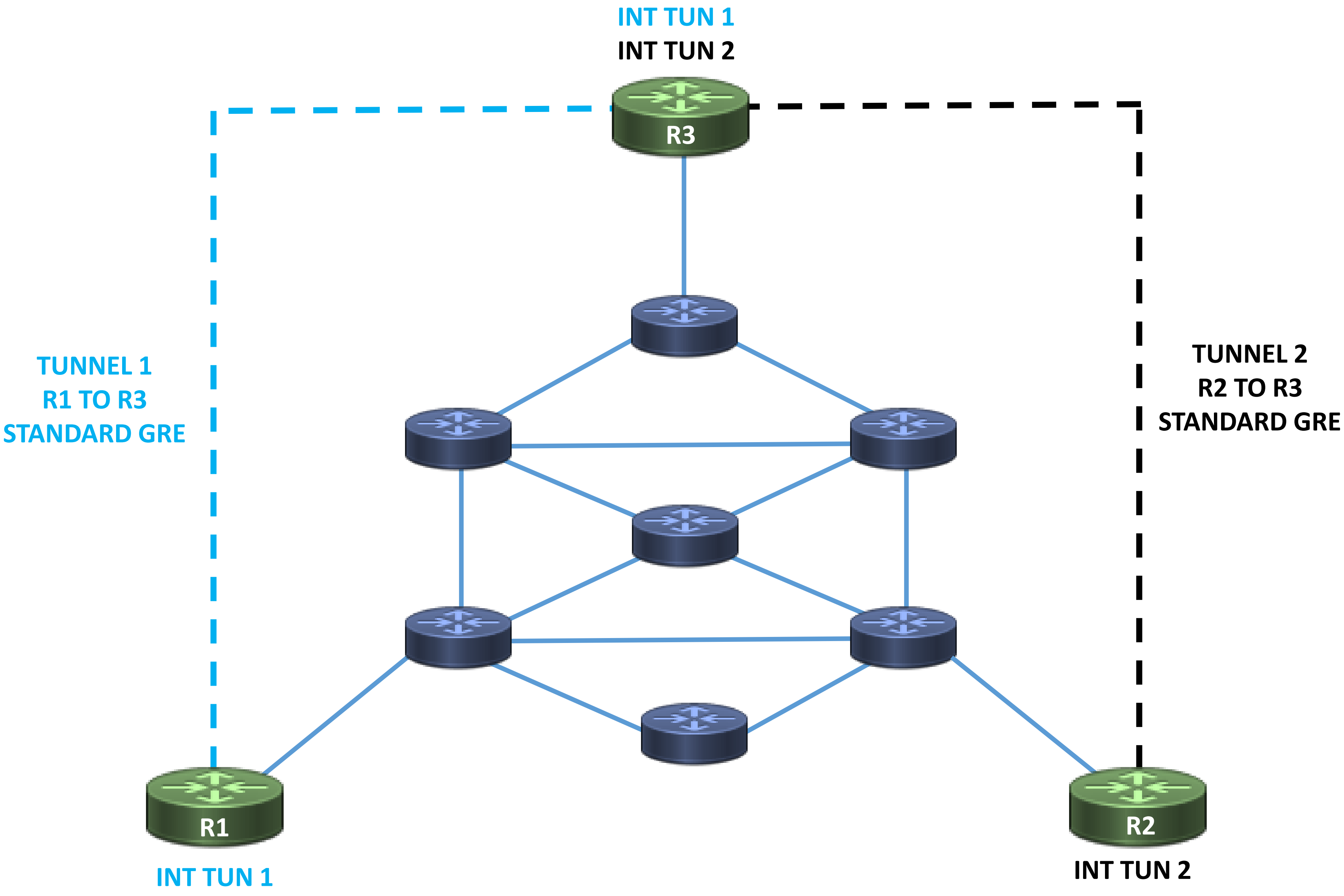
THE UNDERLAY CAN BE IPV4 WITH AN IPV6 OVERLAY, OR VICE VERSA.

IN A DMVPN, THE UNDERLAY IS THE NBMA ADDRESS AND THE OVERLAY (TUNNEL INTERFACE IP ADDRESS) IS THE NEXT HOP SERVER.

```
INTERFACE TUNNEL 1
IP ADDRESS 10.1.1.1 255.255.255.0
IP MTU XXX
IP NHRP AUTHENTICATION XXXXXXXX
IP NHRP NETWORK-ID XXXX
IP NHRP NHS X.X.X.X NBMA X.X.X.X
TUNNEL SOURCE 2001:ABCD:ABCD:ABCD::1
TUNNEL MODE GRE MULTIPOINT IPV6
```

```
INTERFACE TUNNEL 100
IPV6 ADDRESS 2001:ABCD:ABDC:ABCD::1
IPV6 ENABLE
IPV6 MTU XXX
IPV6 NHRP AUTHENTICATION XXXXXXXX
IPV6 NHRP NETWORK-ID XXXX
IPV6 NHRP NHS X.X.X.X NBMA X.X.X.X
TUNNEL SOURCE 192.168.100.1
TUNNEL MODE GRE MULTIPOINT
```

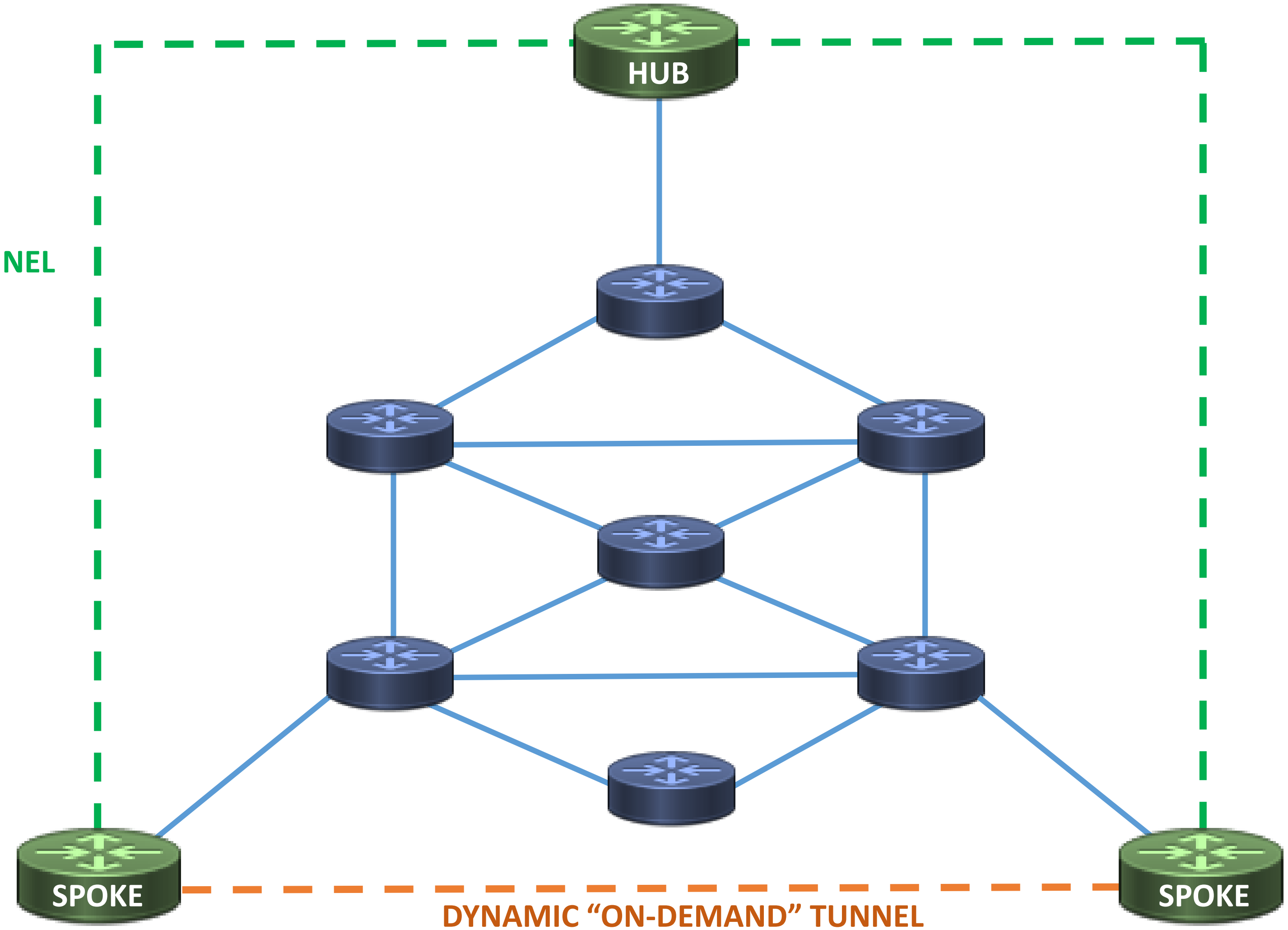
SEPARATE GRE TUNNELS TERMINATING ON R3



A SINGLE DMVPN HOSTING MULTIPLE SPOKES ON R3

DMVPNs use Next Hop Resolution Protocol (NHRP) to improve the efficiency of routing over non-broadcast multiple access networks

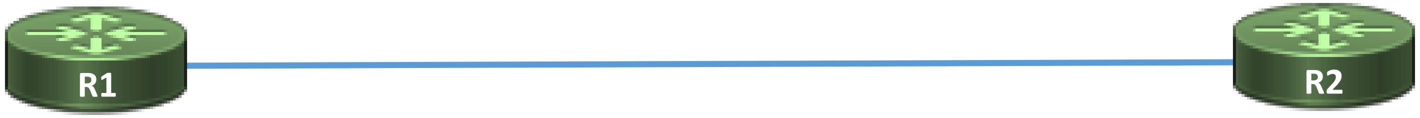
```
INTERFACE TUNNEL 20
DESCRIPTION HUB
IP ADDRESS 20.20.20.1 255.255.255.0
TUNNEL SOURCE 192.168.2.254
IP NHRP NETWORK-ID 12345
IP NHRP NETWORK AUTHENTICATION  cisco123
IP NHRP MAP MULTICAST DYNAMIC
TUNNEL KEY 5555
TUNNEL MODE GRE MULTIPOINT
IP MTU 1400
IP NHRP REDIRECT
```



DYNAMIC “ALWAYS-ON” TUNNEL
SPOKE-TO-HUB

DYNAMIC “ON-DEMAND” TUNNEL
SPOKE-TO-SPOKE

```
INTERFACE TUNNEL 20
DESCRIPTION SPOKE
IP ADDRESS 20.20.20.3 255.255.255.0
TUNNEL SOURCE 192.168.1.1
IP NHRP NETWORK-ID 12345
IP NHRP NETWORK AUTHENTICATION  cisco123
IP NHRP NHS 20.20.20.1 NBMA 192.168.2.254 MULTICAST
TUNNEL KEY 5555
TUNNEL MODE GRE MULTIPOINT
IP MTU 1400
IP NHRP SHORTCUT
```



```
ROUTER EIGRP 1
NETWORK 10.0.0.0 0.0.0.255
NO PASSIVE-INTERFACE G0/0/0
```

```
ROUTER EIGRP TEST
 ADDRESS-FAM IPV4 UNICAST AUTONOMOUS-SYSTEM 1
  NETWORK 10.0.0.0 0.0.0.255
 AF-INTERFACE G0/0/0
  NO PASSIVE-INTERFACE
```

Named EIGRP Configuration

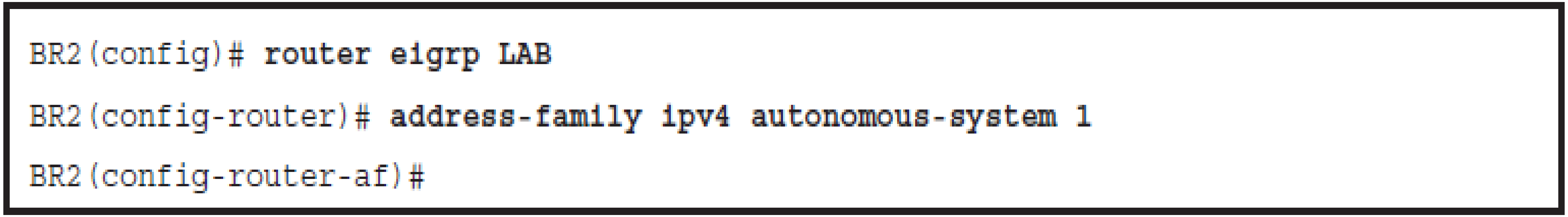
Named EIGRP Configuration

- Configuring EIGRP for both IPv4 and IPv6 on the same router can become a complex task because configuration takes place using different router configuration modes
- A newer configuration enables the configuration of EIGRP for both IPv4 and IPv6 under a single configuration mode.
- EIGRP named configuration helps eliminate configuration complexity that occurs when configuring EIGRP for both IPv4 and IPv6
- EIGRP named configuration is available in Cisco IOS Release 15.0(1)M and later releases.

Address Families

- EIGRP named configuration mode uses the global configuration command **router eigrp** *virtual-instance-name*.
- Both EIGRP for IPv4 and IPv6 can be configured within this same mode.
- EIGRP supports multiple protocols and can carry information about many different route types.
- Named EIGRP configuration organizes specific route types under the same address family.
- IPv4 unicast and IPv6 unicast are two of the most commonly used address families.

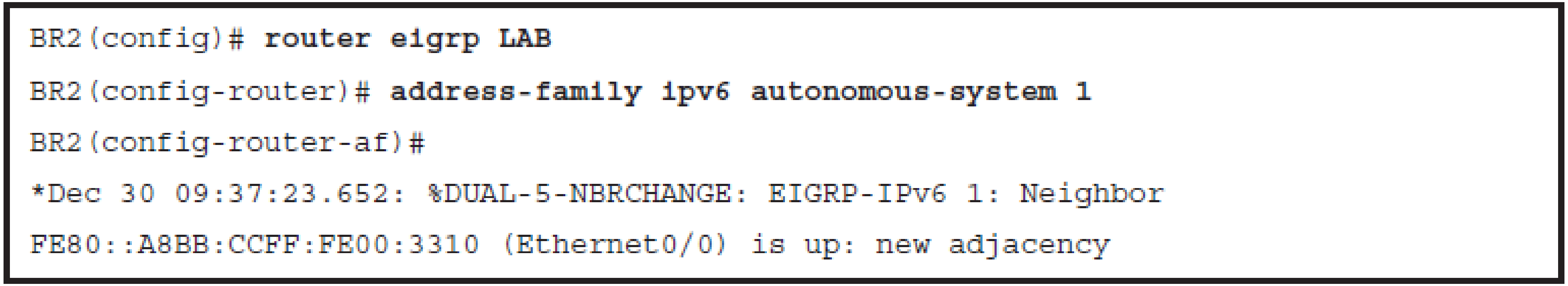
EIGRP for IPv4 Address Family



```
BR2(config)# router eigrp LAB
BR2(config-router)# address-family ipv4 autonomous-system 1
BR2(config-router-af)#
```

address-family ipv4 [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *as-number*

EIGRP for IPv4 Address Family



```
BR2(config)# router eigrp LAB
BR2(config-router)# address-family ipv6 autonomous-system 1
BR2(config-router-af)#
*Dec 30 09:37:23.652: %DUAL-5-NBRCHANGE: EIGRP-IPv6 1: Neighbor
FE80::A8BB:CCFF:FE00:3310 (Ethernet0/0) is up: new adjacency
```

address-family ipv6 [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *as-number*

EIGRP for IPv4 Address Family

- The **address-family** command enables the IPv4 address family and starts EIGRP for the defined autonomous system.
- In IPv4 address family configuration mode, you can enable EIGRP for specific interfaces by using the **network** command, and you can define some other general parameters such as **router-id** or **eigrp stub**.
- Unless specified otherwise, address family is by default defined as unicast address family used the exchange unicast routes.

EIGRP for IPv6 Address Family

- IPv6 EIGRP neighbor relationship gets established as soon as you define the IPv6 address family.
- All IPv6-enabled interfaces are **automatically** included in the EIGRP for IPv6 process.
- The IPv6 address family configuration will show up in the running configuration as a unicast address family by default.
- You can configure or remove individual interfaces from the EIGRP for IPv6 process by using the **af-interface** *interface-type interface number* command in address family configuration mode

NAMED MODE EIGRP for Address Family

```
router eigpr LAB
address-family ipv4 unicast autonomous-system 20
!
network 10.0.0.0 0.0.0.255
network 192.168.1.0 0.0.0.7
!
```

NAMED MODE EIGRP for Address Family

```
router eigpr LAB
address-family ipv4 unicast autonomous-system 20
!
af-interface default
passive-interface
!
af-interface G0/0/1
no passive-interface
authentication mode MD5
```

NAMED MODE EIGRP for Address Family

```
router eigpr LAB
address-family ipv4 unicast autonomous-system 20
!
Topology base
!
redistribute ospf 10 metric 1000000 0 255 1 1500
```

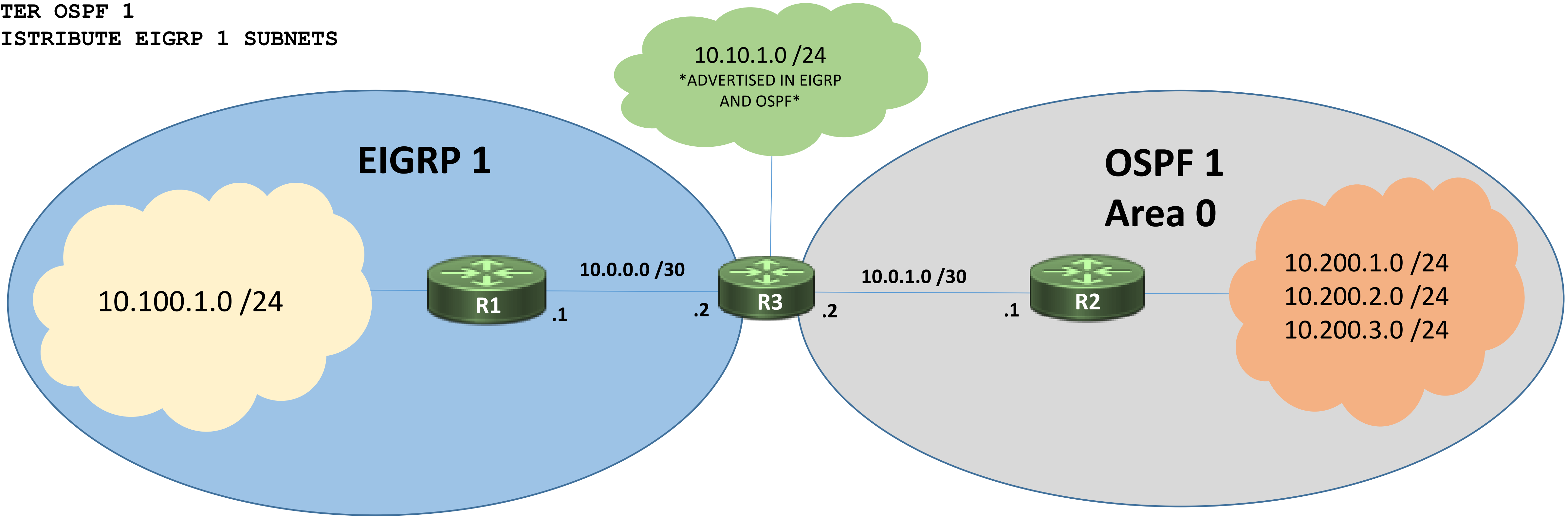
Named EIGRP Configuration Modes

Three different configuration modes:

- **Address family configuration mode**
  - General EIGRP configuration commands for selected address family are entered under address family configuration mode. Here you can configure the router ID and define network statements and also configure router as an EIGRP stub.
  - Address family configuration mode gives you access to two additional configuration modes: address family interface configuration mode and address family topology configuration mode.
- **Address family interface configuration mode**
  - You should use address family interface configuration mode for all those commands that you have previously configured directly under interfaces. Most common options are setting summarization with the **summary-address** command or marking interfaces as passive using **passive-interface** command. You can also modify default hello and hold-time timers.
- **Address family topology configuration mode**
  - Address family topology configuration mode gathers all configuration options that directly impact the EIGRP topology table. Here you can set load-balancing parameters such as **variance** and **maximum-paths,** or you can redistribute static routes using the **redistribute** command.

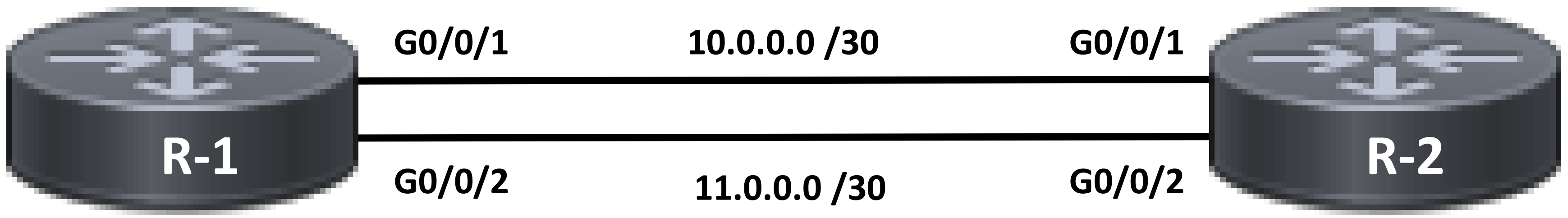
MUTUAL REDISTRIBUTION

```
R3#

ROUTER EIGRP NET-ENG
ADDRESS-FAMILY IPV4 UNICAST AUTONOMOUS-SYSTEM 1
REDISTRIBUTE OSPF 1 METRIC 1000000 10 255 1 1500

ROUTER OSPF 1
REDISTRIBUTE EIGRP 1 SUBNETS
```



```
R1# SHOW IP ROUTE
C         10.0.0.0/30 [CONNECTED]
C         10.100.1.0/24 [CONNECTED]
D         10.10.1.0/24 [90/25618] VIA 10.0.0.2 G0/0/0
D EX      10.200.1.0/24 [170/12679] VIA 10.0.0.2 G0/0/0
D EX      10.200.2.0/24 [170/12629] VIA 10.0.0.2 G0/0/0
D EX      10.200.3.0/24 [170/12679] VIA 10.0.0.2 G0/0/0
```

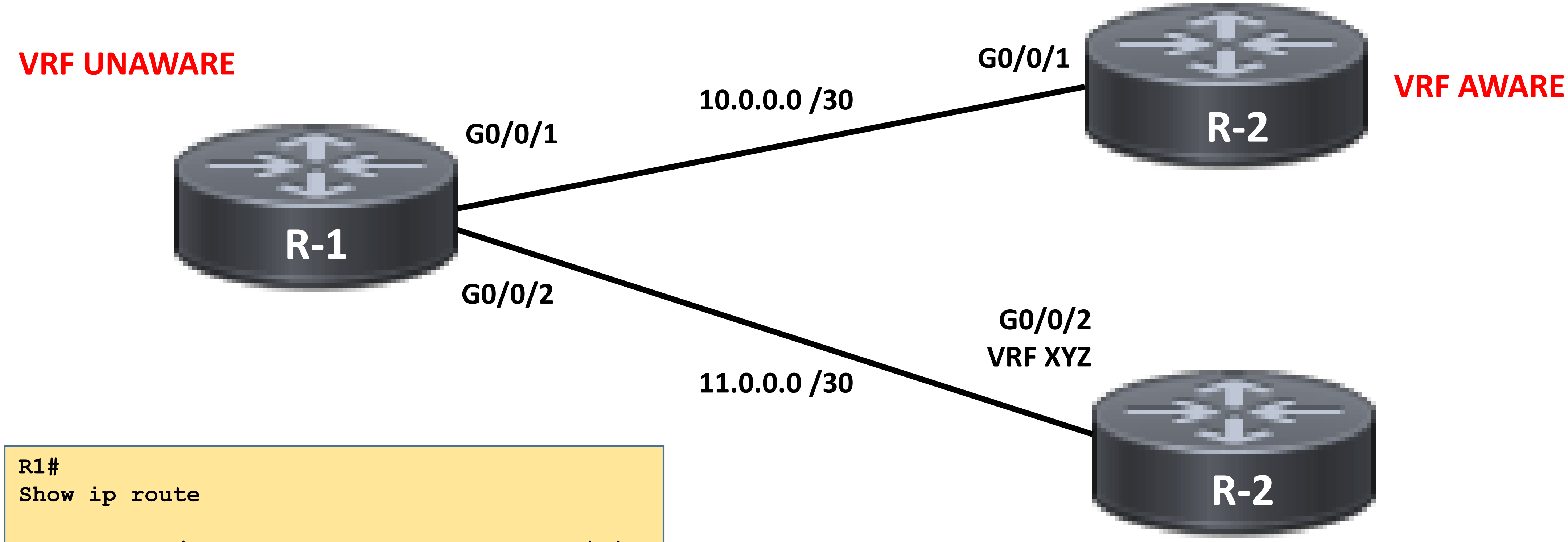
```
R2# SHOW IP ROUTE
C         10.0.1.0/30 [CONNECTED]
C         10.200.1.0/24 [CONNECTED]
C         10.200.2.0/24 [CONNECTED]
C         10.200.3.0/24 [CONNECTED]
O         10.10.1.0/24 [110/25] VIA 10.0.0.2 G0/0/0
O E2      10.100.1.0/24 [110/20] VIA 10.0.0.2 G0/0/0
```



```
R1#
Show ip route

C 10.0.0.0 /30 directly connected via G0/0/1
C 11.0.0.0 /30 directly connected via G0/0/2
```

```
R2#
Show ip route

C 10.0.0.0 /30 directly connected via G0/0/1
C 11.0.0.0 /30 directly connected via G0/0/2
```

```
R2#
Show ip route

C 10.0.0.0 /30 directly connected via G0/0/1
```

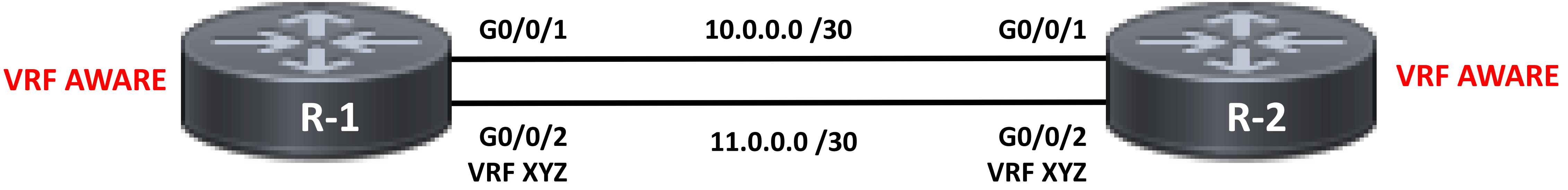


```
R1#
Show ip route

C 10.0.0.0 /30 directly connected via G0/0/1
C 11.0.0.0 /30 directly connected via G0/0/2
```

```
R2#
Show ip route vrf XYZ

C 11.0.0.0 /30 directly connected via G0/0/2
```

```
R1#
Show ip route

C 10.0.0.0 /30 directly connected via G0/0/1
```

```
R2#
Show ip route

C 10.0.0.0 /30 directly connected via G0/0/1
```



```
R1#
Show ip route vrf XYZ

C 11.0.0.0 /30 directly connected via G0/0/2
```

```
R2#
Show ip route vrf XYZ

C 11.0.0.0 /30 directly connected via G0/0/2
```

Why MPLS?

- Logical separation of traffic can be imposed at the PE, and maintained through the Service Provider Core
  - VRF’s, Multi-protocol BGP
- The use of one unified network infrastructure
  - Hybrid systems of IP / ATM / Frame-Relay are unnecessary
  - MPLS encapsulation can contain a variety of payloads, IP, IPv6, Ethernet, HDLC, PPP
    - L3VPN, VPLS, Pseudowire, etc.
- Optimal / Flexible traffic flow
  - SP Core network IGP will dynamically determine best path vs. static assignments (Frame-Relay / ATM)
  - SP networks can implement static LSP determination (Traffic Engineering)

Benefits of MPLS

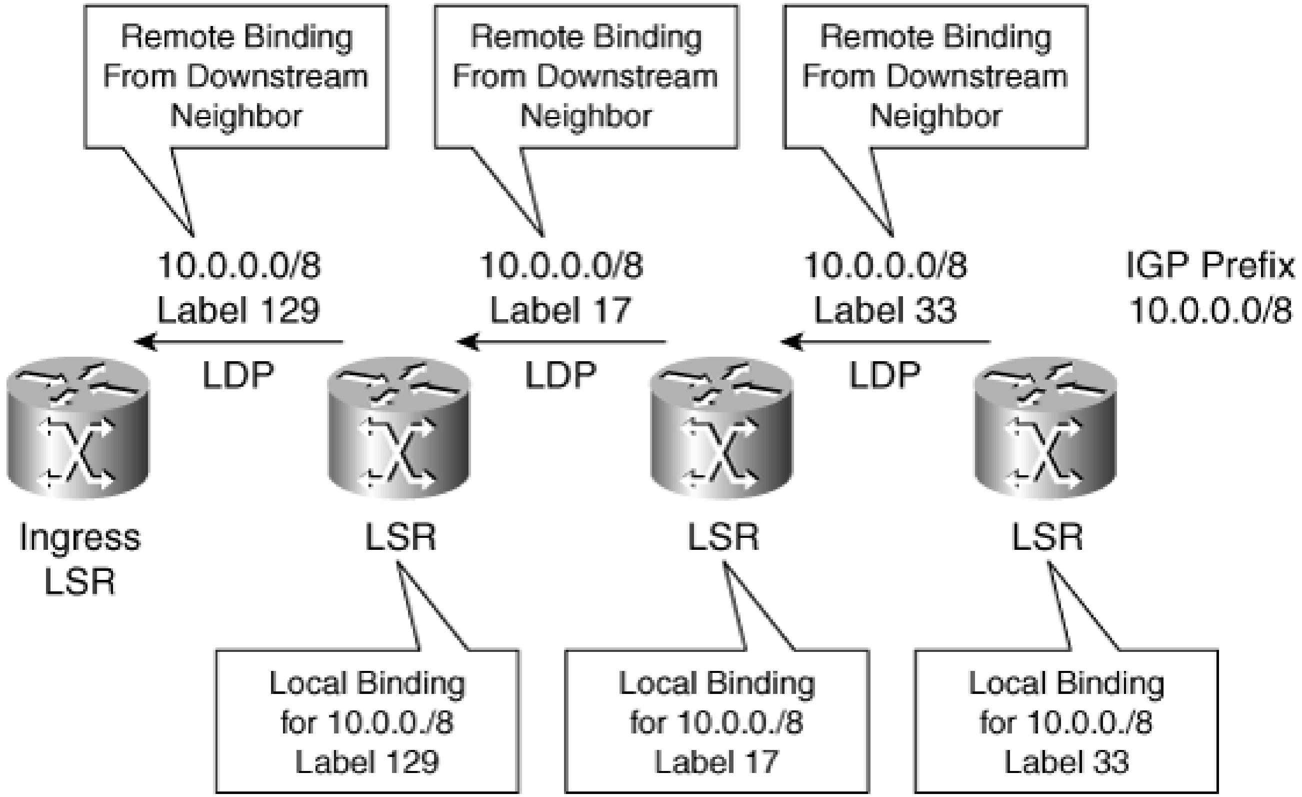
- Dynamic traffic flow
  - the provider’s IGP will chose the best path across the core, without having to configure virtual circuits for every connection
- Traffic Engineering – RSVP-TE
  - The ability to assign traffic to links that not the “best path” to make usage of all the links in the core
  - Gives us the ability to map one FEC (LSP) traffic over SATCOM and another FEC over LOS
  - Adds the ability to do source routing
  - MPLS-TE Fast Reroute (FRR)
  - Attribute flag tunneling

LDP

- Label Distribution Protocol
- Open Standard per RFC 3036, 5036
- Two LSRs adjacent and exchanging label information are “LDP Peers”
- Stages of LDP operation:
  - IGP Convergence
  - Assign an LDP local binding to all IGP learned prefixes
  - Assign a default LFIB action = POP
  - Form LDP Neighbor (based on LDP router-id learned in first hello packet)
    - Neighbor discovery via link-local multicast (224.0.0.2 – UDP port 646)
    - Session built via TCP port 646
  - Exchange local-bindings
  - Modify the LFIB default actions per LDP peer exchanged binding
- All label entries are stored in the LIB (Label Information Base)

Label Distribution Operation

- MPLS PHB – Per Hop Behavior



Remote Binding From Downstream Neighbor
Remote Binding From Downstream Neighbor
Remote Binding From Downstream Neighbor
10.0.0.0/8 Label 129
10.0.0.0/8 Label 17
10.0.0.0/8 Label 33
IGP Prefix 10.0.0.0/8
LDP
LDP
LDP
Ingress LSR
LSR
LSR
LSR
Local Binding for 10.0.0./8 Label 129
Local Binding for 10.0.0./8 Label 17
Local Binding for 10.0.0./8 Label 33

Label Operations

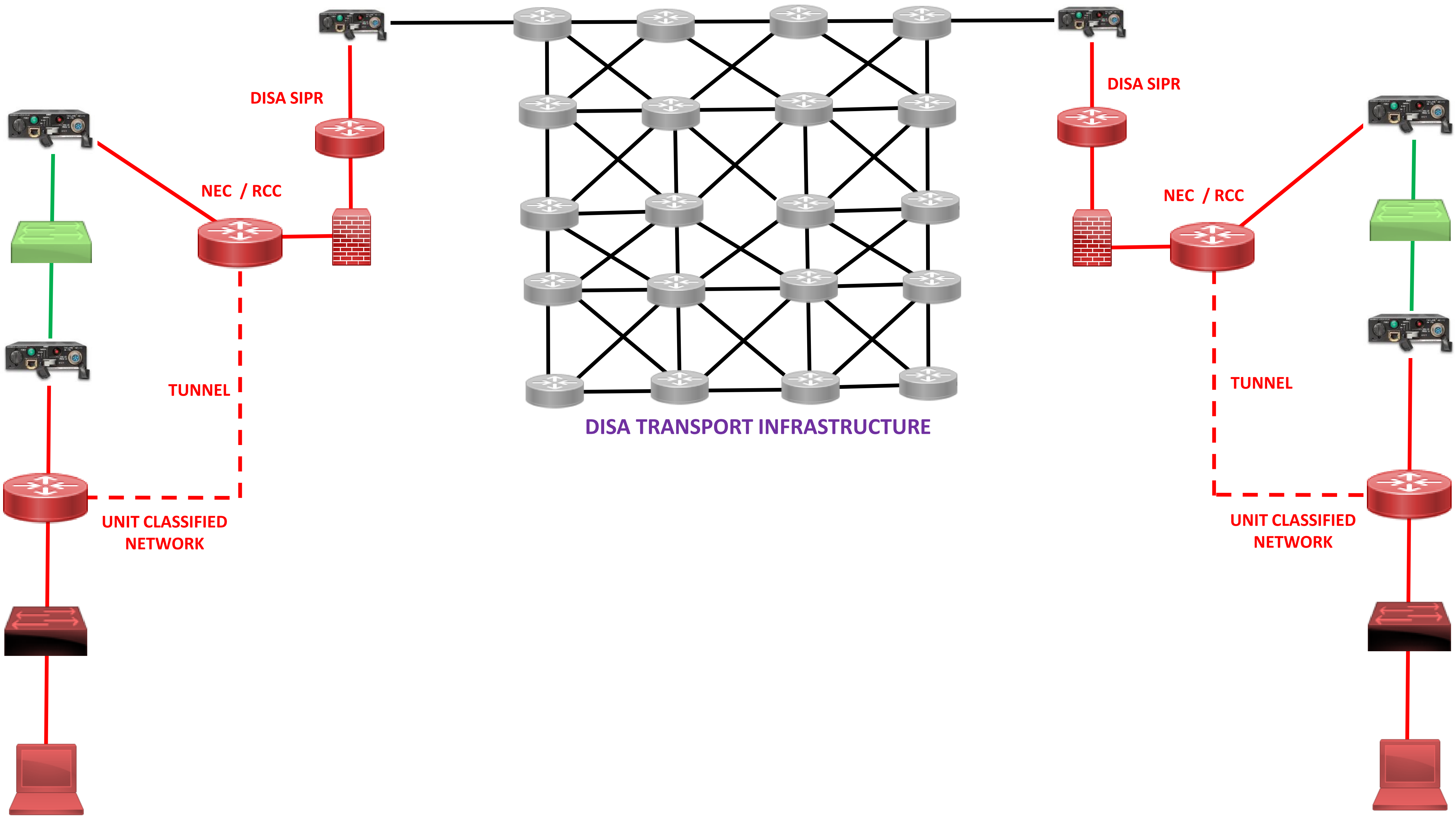
- PE and P devices perform 3 main label operations
  - Label push (Label Imposition)
    - Add a label to an incoming packet, happens at Ingress LER
  - Label swap (Label Replacement)
    - Replaces a label on an incoming packet, happens as LSR
  - Label pop (Label Disposition)
    - Remove a label from an outgoing packet, happens at Egress LER
- Labels are advertised for:
  - Connected IGP interfaces
  - IGP learned routes (OSPF or IS-IS)

MPLS Commands

- Configuration

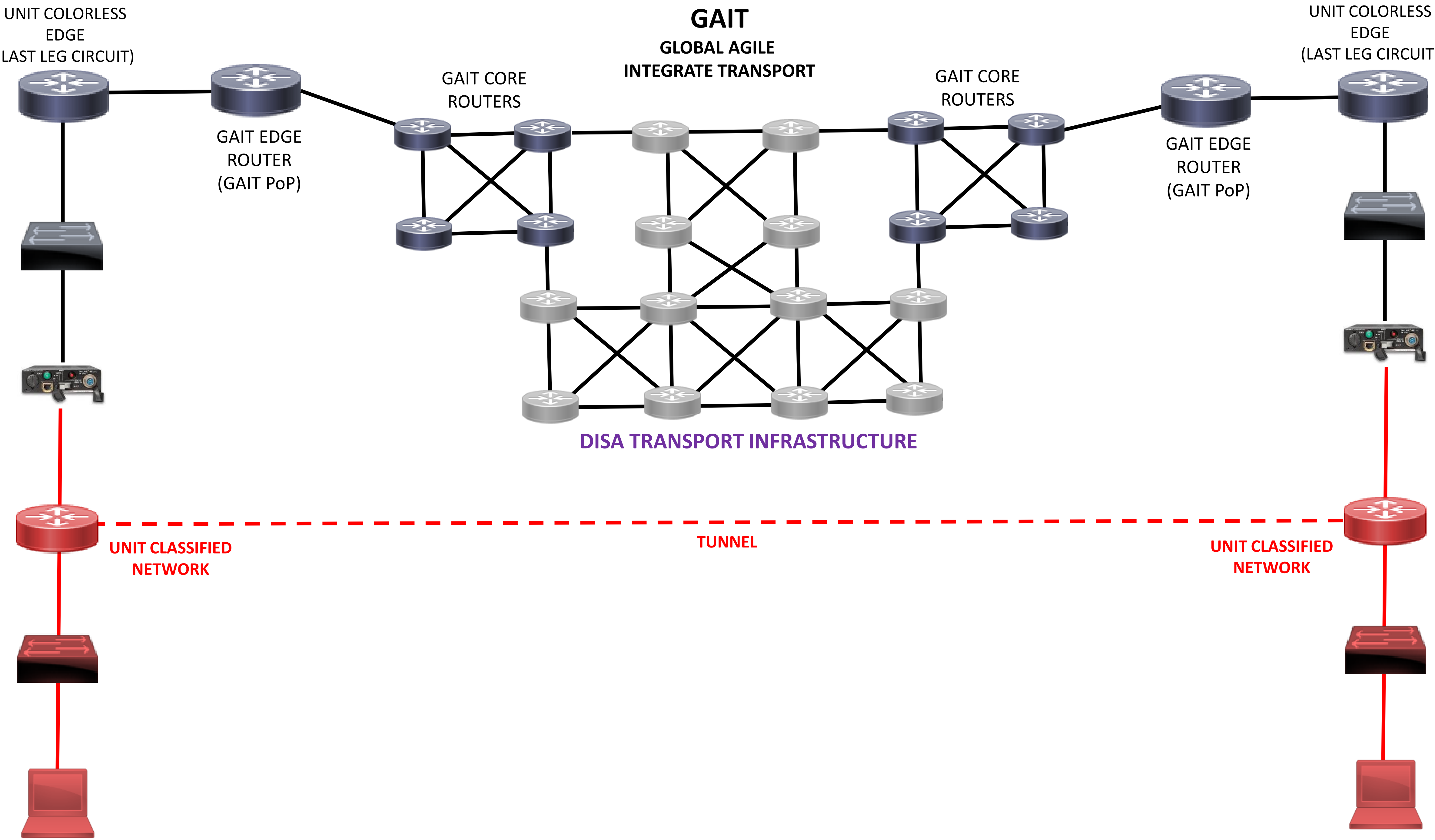
```
R20(config)#ip cef
R20(config)#mpls label protocol ldp
R20(config)#mpls ldp router-id loopback0 force
R20(config)#mpls label range 20000 20999
R20(config)#mpls ip
R20(config)#int g0/0
R20(config-if)#mpls ip
```

- Verification:
  - Show mpls interface
  - Show mpls ldp discovery
  - Show mpls ldp neighbor
  - Show mpls ldp bindings
  - Show mpls forwarding-table
  - Show mpls ip binding
  - Show ip cef x.x.x.x
  - Traceroute x.x.x.x (notice MPLS: Label XX in output)


DISA SIPR
NEC / RCC
TUNNEL
UNIT CLASSIFIED NETWORK
DISA TRANSPORT INFRASTRUCTURE
DISA SIPR
NEC / RCC
TUNNEL
UNIT CLASSIFIED NETWORK

GAIT

GLOBAL AGILE INTEGRATE TRANSPORT



UNIT COLORLESS EDGE (LAST LEG CIRCUIT)

GAIT EDGE ROUTER (GAIT PoP)

GAIT CORE ROUTERS

GAIT CORE ROUTERS

GAIT EDGE ROUTER (GAIT PoP)

UNIT COLORLESS EDGE (LAST LEG CIRCUIT)

DISA TRANSPORT INFRASTRUCTURE

UNIT CLASSIFIED NETWORK

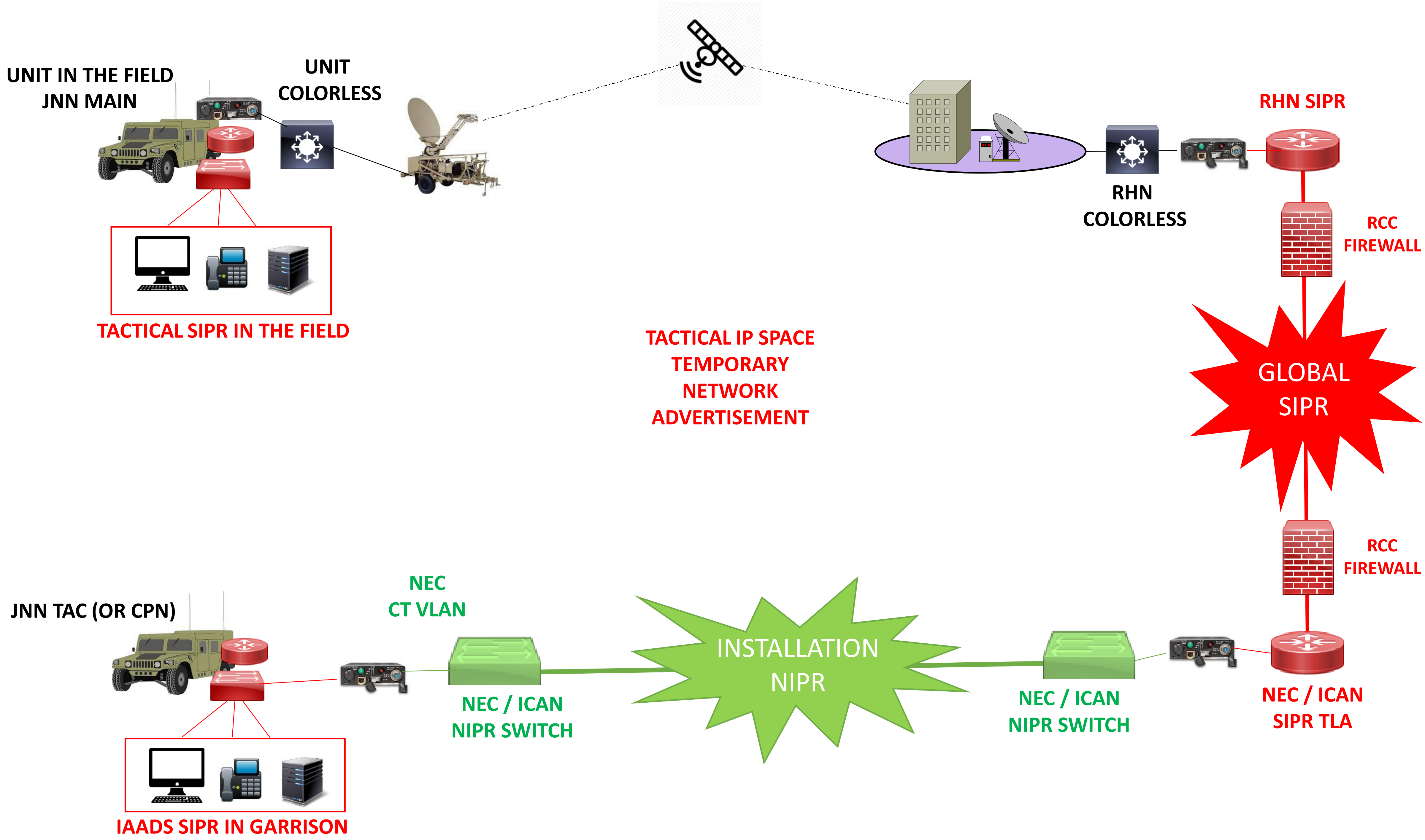
TUNNEL

UNIT CLASSIFIED NETWORK

Installation As A Docking Station (IAADS)

What does IaaDS include?

- Installation connection for voice, data, and video pass through (i.e. a docking station)
- All mission command systems (i.e. CPOF, BCCS, WIN-T, DCGS-A, IFS, Chat, VTC, VoIP, JNN, TCN, CPN, etc…)
- Support for Enterprise Identity, Authentication, and Collaborative Services
- Minimum SIPRNET and NIPRNET Transport
- Objective JWICS and Coalition Transport
- Allows units at the home station to connect to their tactical assets in the field without dedicating an assemblage (JNN, CPN, TCN) to providing transport in garrison.



UNIT IN THE FIELD
JNN MAIN

UNIT
COLORLESS

TACTICAL SIPR IN THE FIELD

RHN SIPR

RHN
COLORLESS

RCC
FIREWALL

GLOBAL
SIPR

TACTICAL IP SPACE
TEMPORARY
NETWORK
ADVERTISEMENT

RCC
FIREWALL

JNN TAC (OR CPN)

NEC
CT VLAN

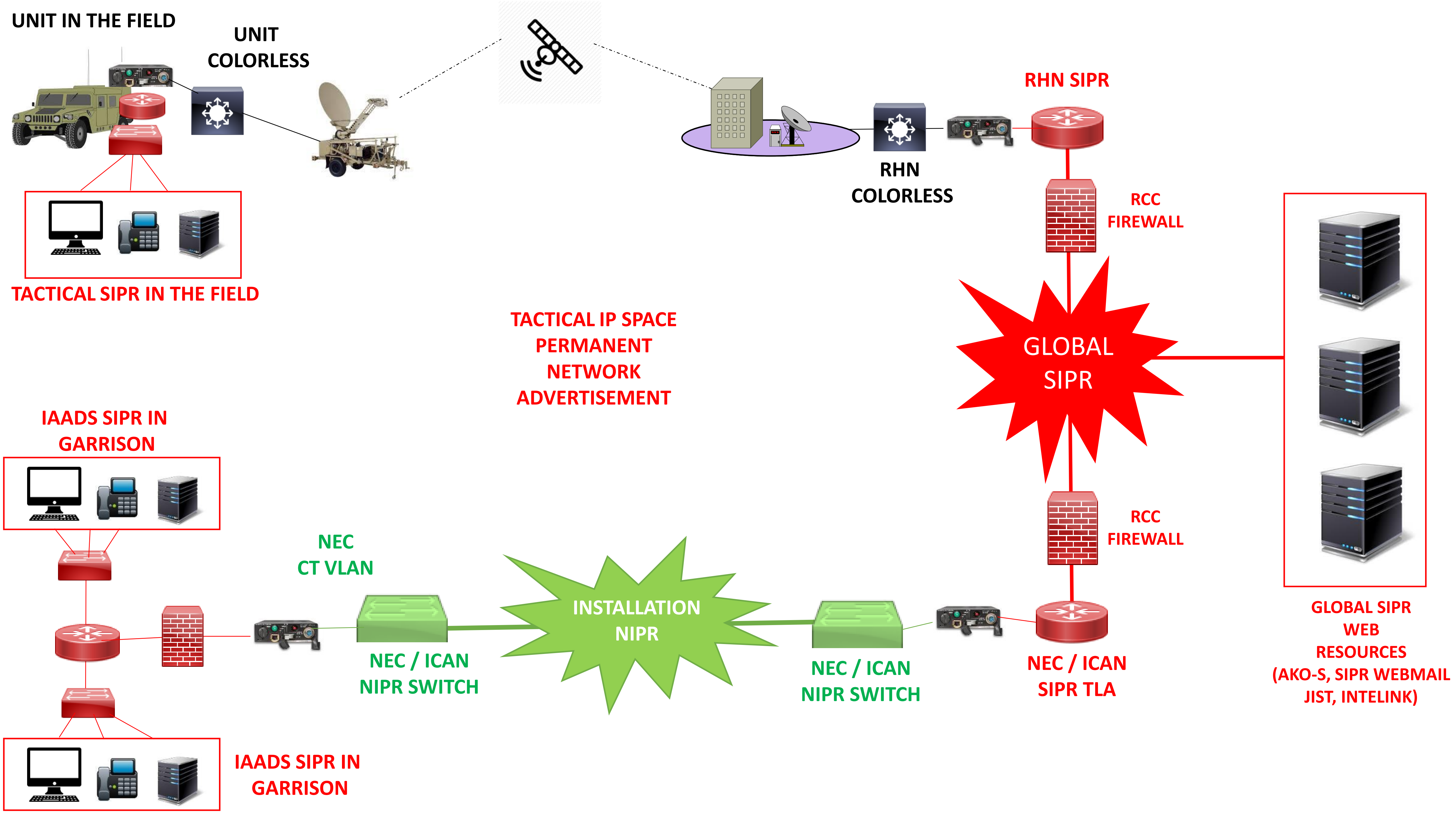
INSTALLATION
NIPR

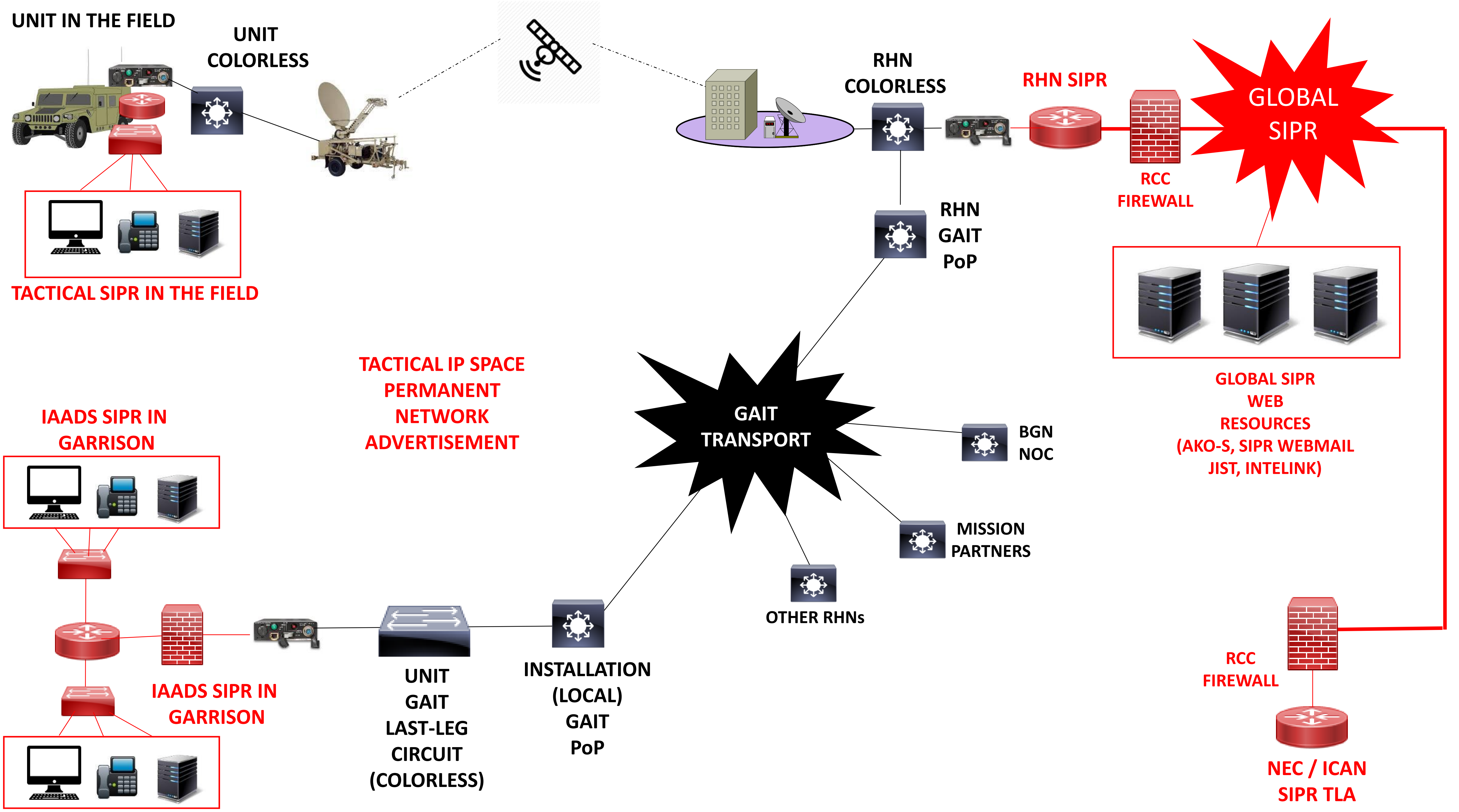
NEC / ICAN
NIPR SWITCH

NEC / ICAN
NIPR SWITCH

NEC / ICAN
SIPR TLA

IAADS SIPR IN GARRISON


UNIT IN THE FIELD
UNIT COLORLESS
TACTICAL SIPR IN THE FIELD
RHN SIPR
RHN COLORLESS
RCC FIREWALL
GLOBAL SIPR
TACTICAL IP SPACE PERMANENT NETWORK ADVERTISEMENT
IAADS SIPR IN GARRISON
NEC CT VLAN
INSTALLATION NIPR
RCC FIREWALL
NEC / ICAN NIPR SWITCH
NEC / ICAN NIPR SWITCH
NEC / ICAN SIPR TLA
GLOBAL SIPR WEB RESOURCES (AKO-S, SIPR WEBMAIL JIST, INTELINK)
IAADS SIPR IN GARRISON



UNIT IN THE FIELD

UNIT COLORLESS

TACTICAL SIPR IN THE FIELD

RHN COLORLESS

RHN SIPR

RCC FIREWALL

GLOBAL SIPR

RHN GAIT PoP

GLOBAL SIPR WEB RESOURCES (AKO-S, SIPR WEBMAIL JIST, INTELINK)

TACTICAL IP SPACE PERMANENT NETWORK ADVERTISEMENT

IAADS SIPR IN GARRISON

GAIT TRANSPORT

BGN NOC

MISSION PARTNERS

OTHER RHNs

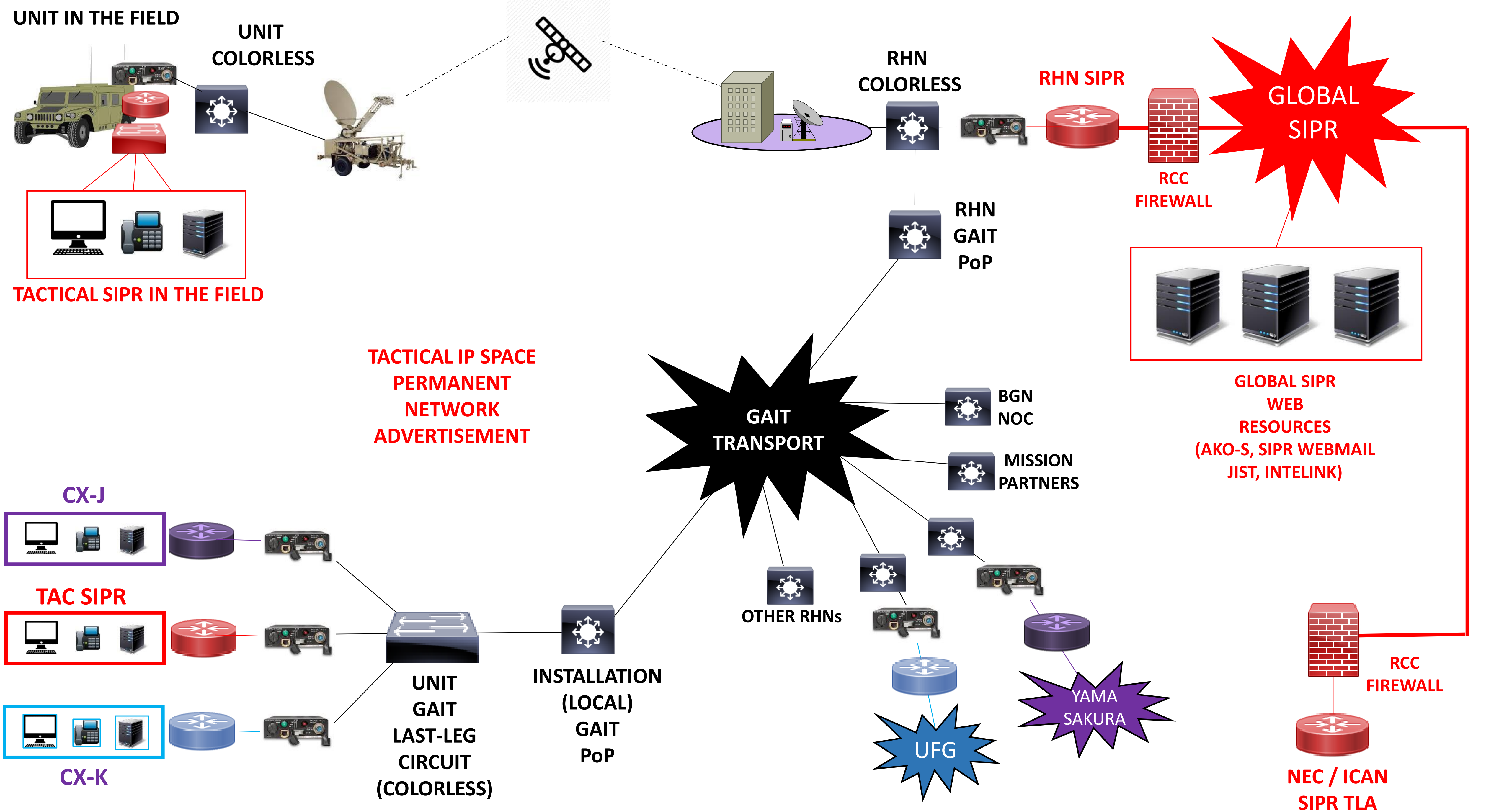
IAADS SIPR IN GARRISON

UNIT GAIT LAST-LEG CIRCUIT (COLORLESS)

INSTALLATION (LOCAL) GAIT PoP

RCC FIREWALL

NEC / ICAN SIPR TLA



UNIT IN THE FIELD

UNIT COLORLESS

TACTICAL SIPR IN THE FIELD

RHN COLORLESS

RHN SIPR

GLOBAL SIPR

RCC FIREWALL

RHN GAIT PoP

GLOBAL SIPR WEB RESOURCES (AKO-S, SIPR WEBMAIL JIST, INTELINK)

TACTICAL IP SPACE PERMANENT NETWORK ADVERTISEMENT

GAIT TRANSPORT

BGN NOC

MISSION PARTNERS

CX-J

TAC SIPR

CX-K

UNIT GAIT LAST-LEG CIRCUIT (COLORLESS)

INSTALLATION (LOCAL) GAIT PoP

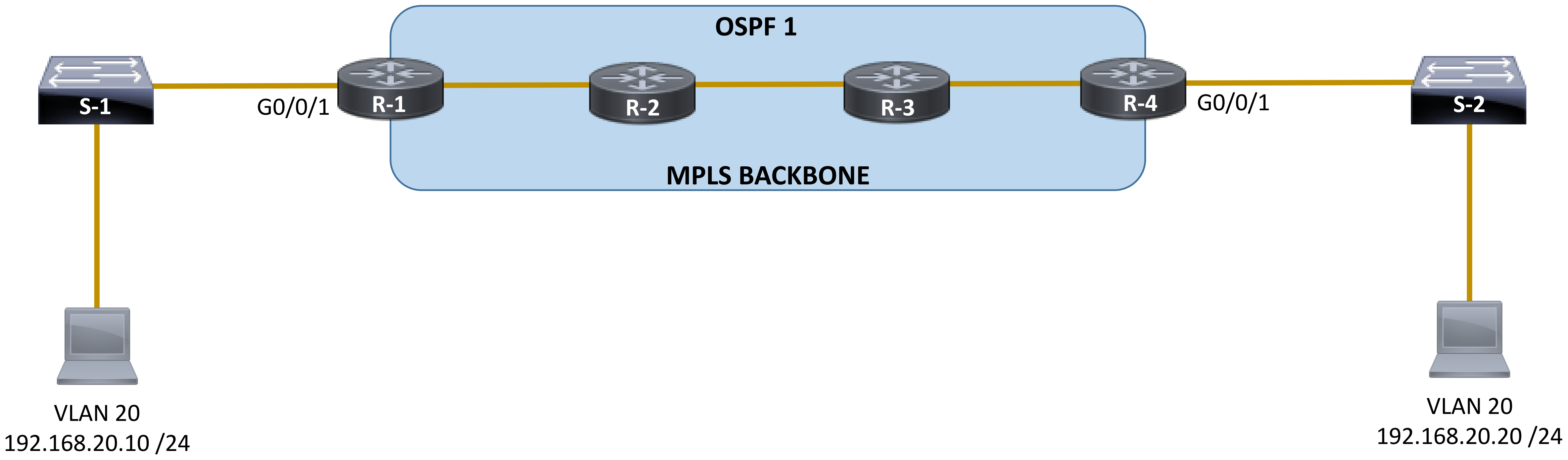
OTHER RHNs

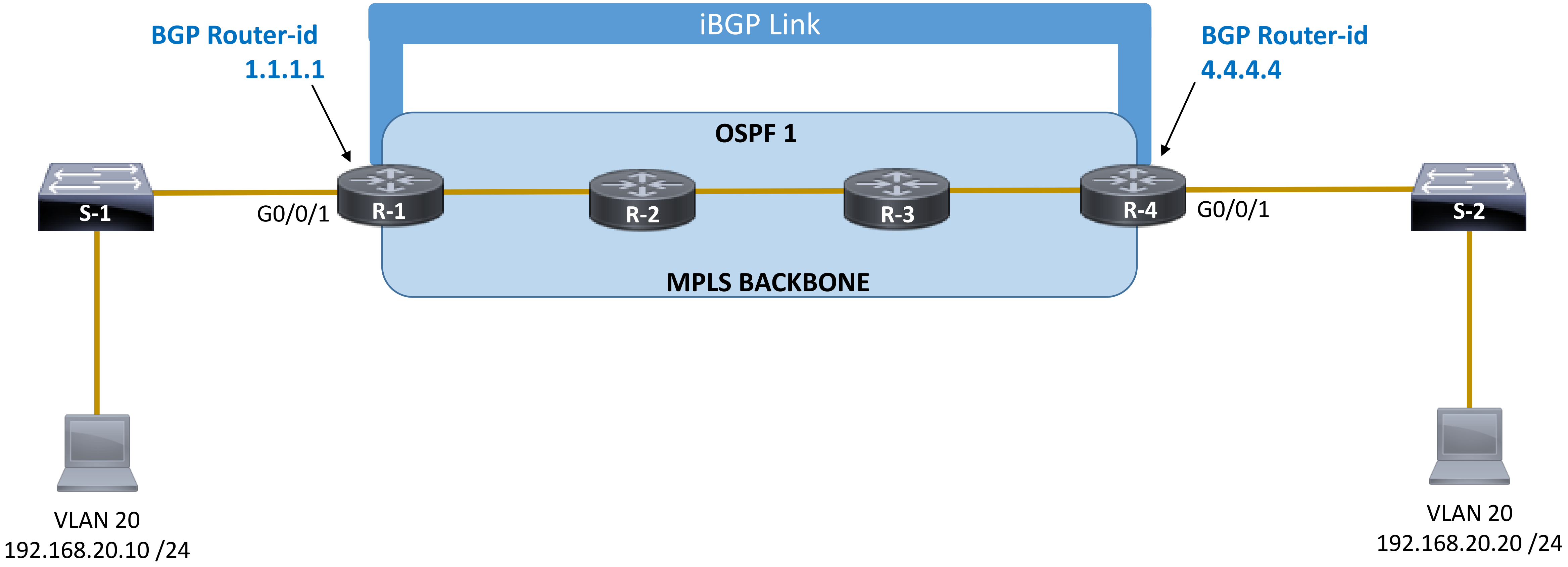
UFG

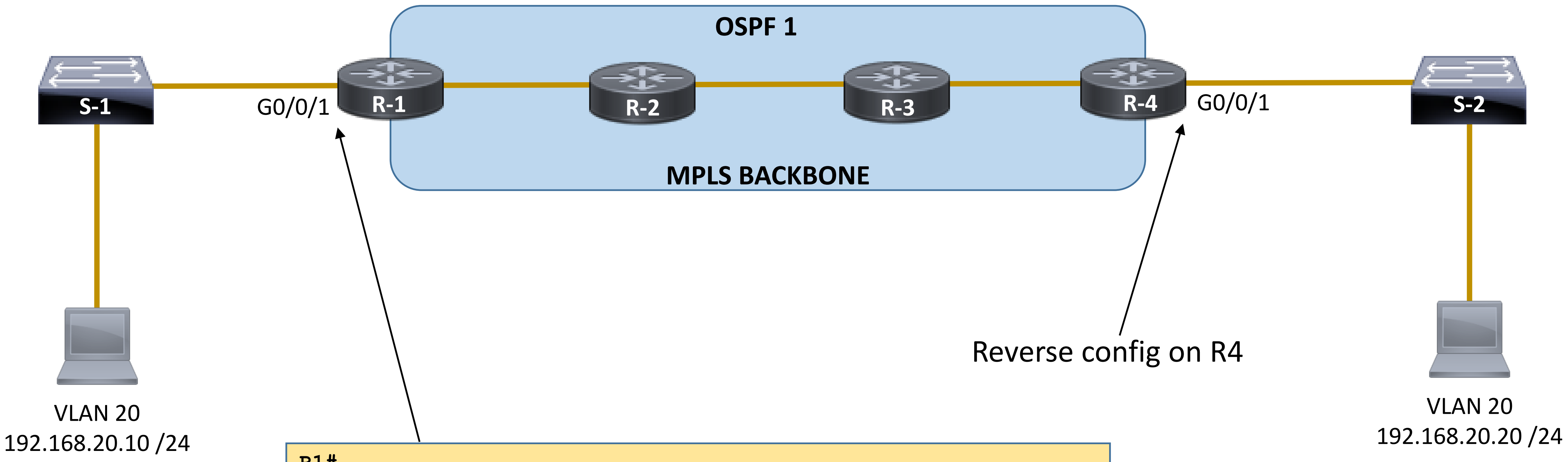
YAMA SAKURA

RCC FIREWALL

NEC / ICAN SIPR TLA

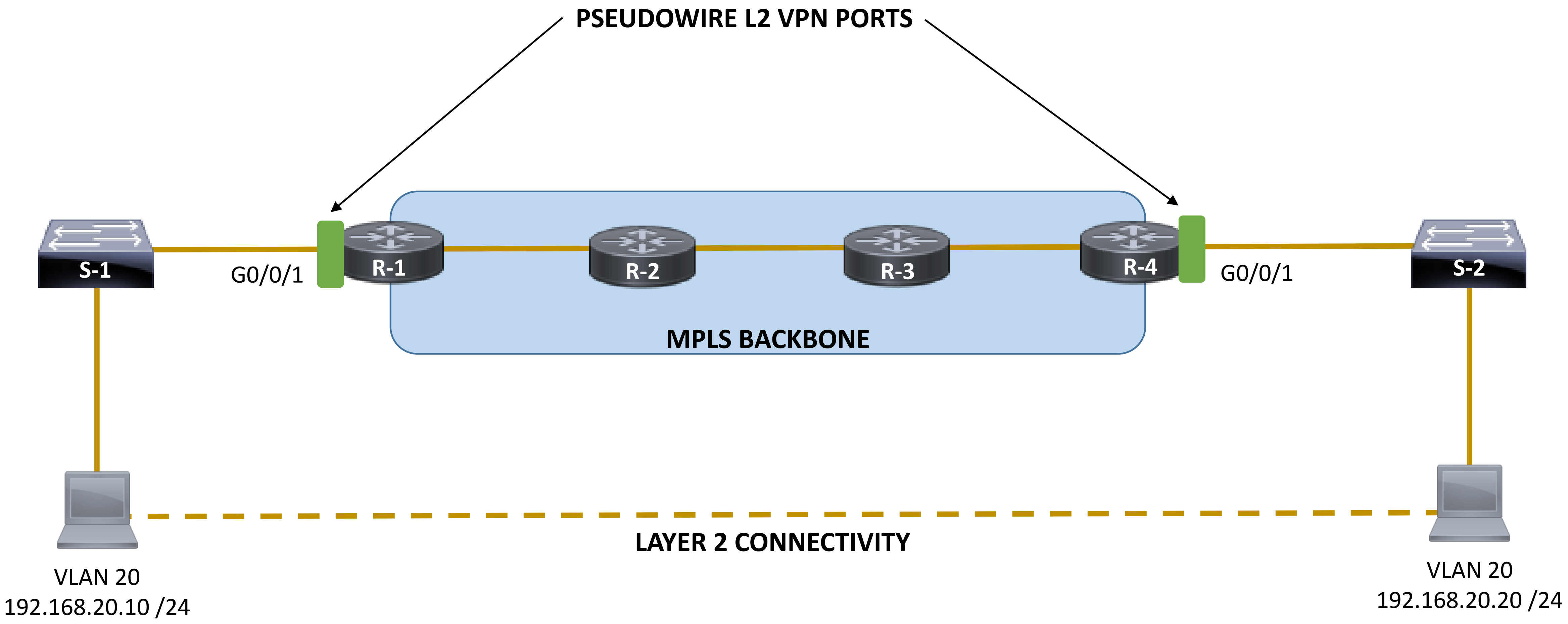

OSPF 1
S-1
G0/0/1
R-1
R-2
R-3
R-4
G0/0/1
S-2
MPLS BACKBONE
VLAN 20
192.168.20.10 /24
VLAN 20
192.168.20.20 /24

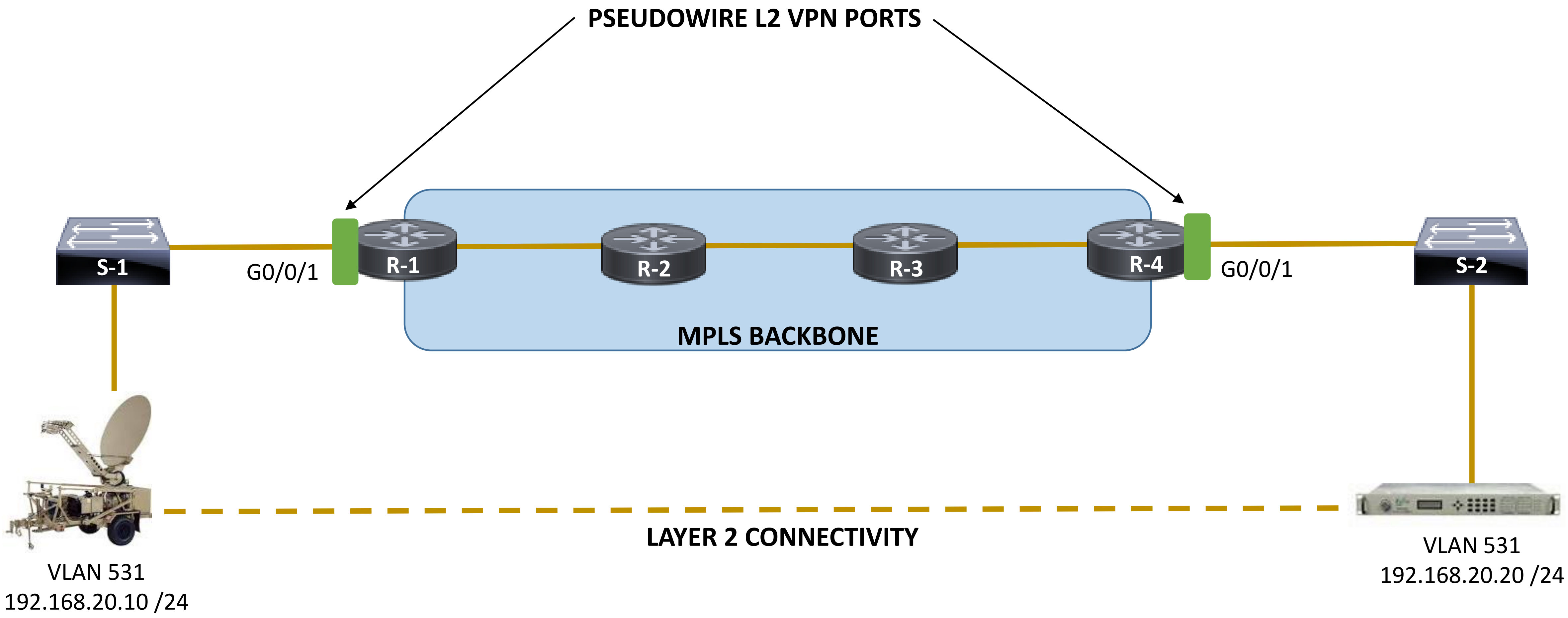

iBGP Link
BGP Router-id
1.1.1.1
BGP Router-id
4.4.4.4
OSPF 1
MPLS BACKBONE
S-1
G0/0/1
R-1
R-2
R-3
R-4
G0/0/1
S-2
VLAN 20
192.168.20.10 /24
VLAN 20
192.168.20.20 /24



Reverse config on R4

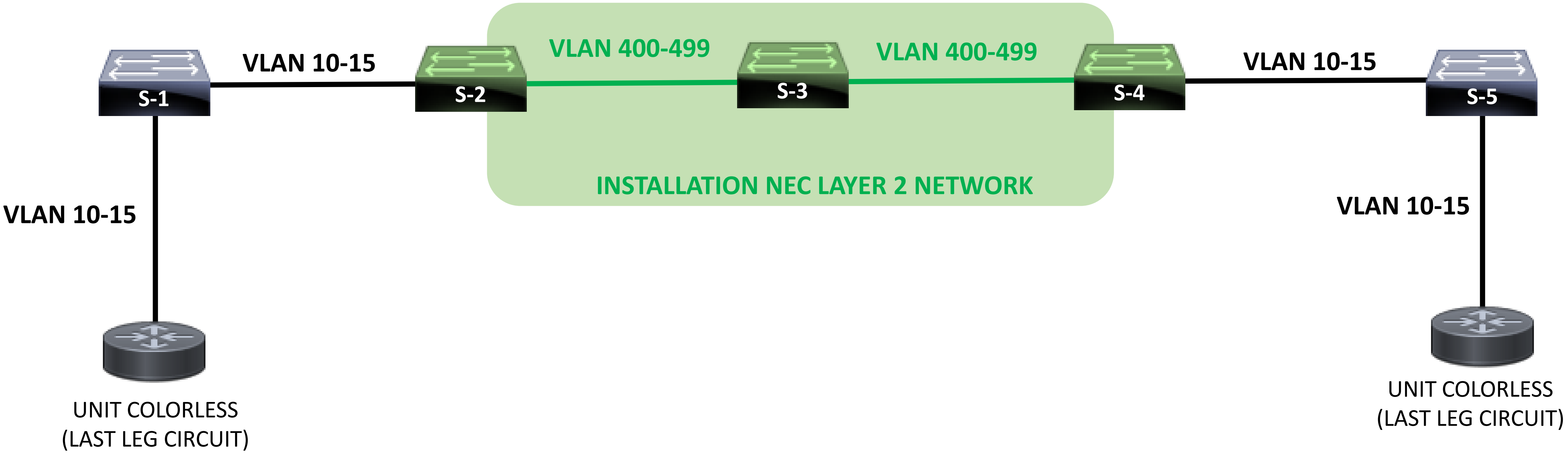
```
R1#
!
Pseudowire-class L2_CKT
Encapsulation mpls
!
Int g0/0/1
No ip address
xconnect 4.4.4.4 100 encapsulation mpls pw-class L2_CKT
```


PSEUDOWIRE L2 VPN PORTS
S-1
G0/0/1
R-1
R-2
R-3
R-4
G0/0/1
S-2
MPLS BACKBONE
LAYER 2 CONNECTIVITY
VLAN 20
192.168.20.10 /24
VLAN 20
192.168.20.20 /24


PSEUDOWIRE L2 VPN PORTS

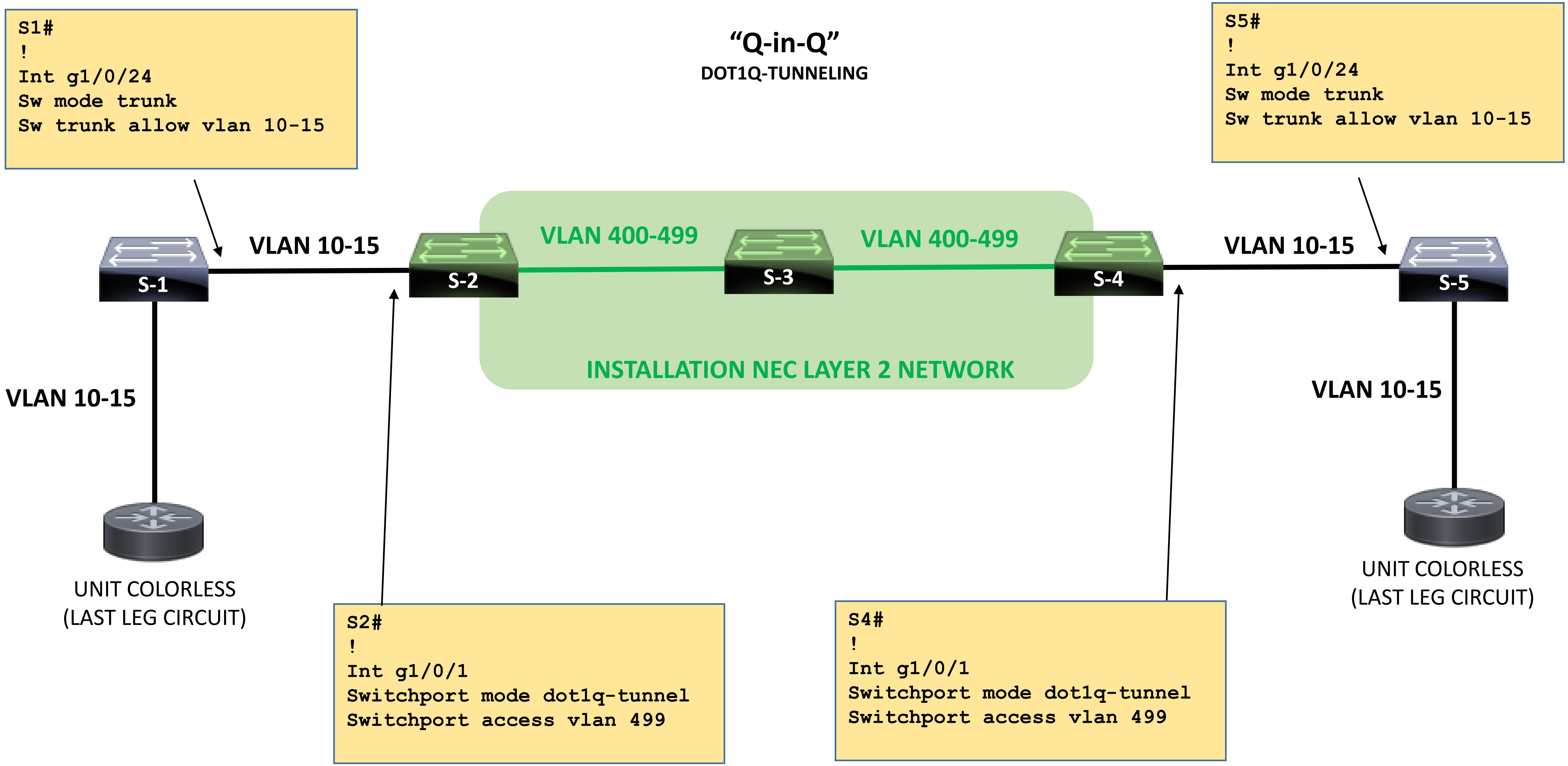
MPLS BACKBONE

LAYER 2 CONNECTIVITY


S-1
VLAN 10-15
S-2
VLAN 400-499
S-3
VLAN 400-499
S-4
VLAN 10-15
S-5
INSTALLATION NEC LAYER 2 NETWORK
VLAN 10-15
VLAN 10-15
UNIT COLORLESS
(LAST LEG CIRCUIT)
UNIT COLORLESS
(LAST LEG CIRCUIT)

"Q-in-Q"

DOT1Q-TUNNELING

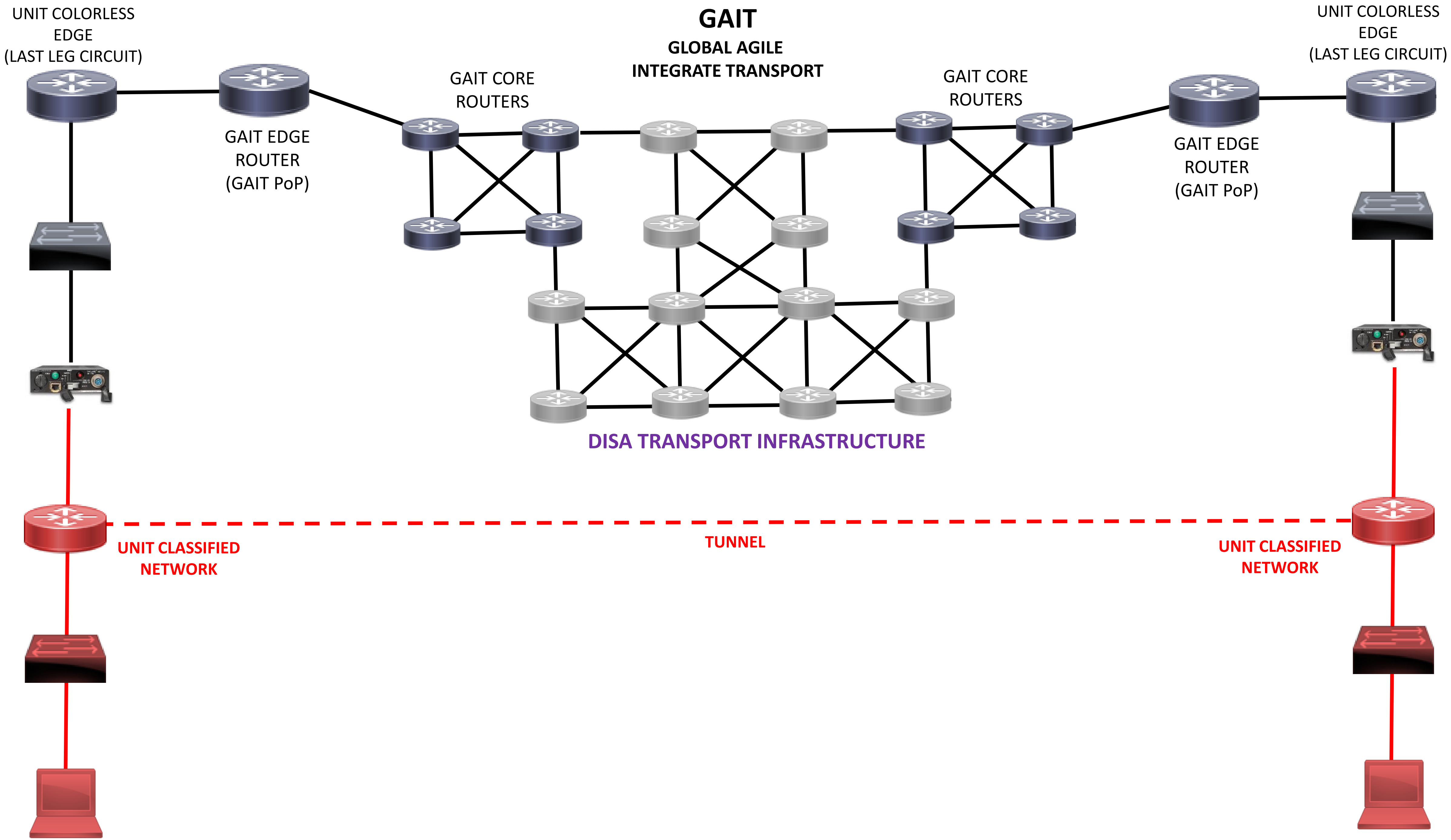


```
S1#
!
Int g1/0/24
Sw mode trunk
Sw trunk allow vlan 10-15
```

```
S5#
!
Int g1/0/24
Sw mode trunk
Sw trunk allow vlan 10-15
```

```
S2#
!
Int g1/0/1
Switchport mode dot1q-tunnel
Switchport access vlan 499
```

```
S4#
!
Int g1/0/1
Switchport mode dot1q-tunnel
Switchport access vlan 499
```



GAIT

GLOBAL AGILE INTEGRATE TRANSPORT

UNIT COLORLESS EDGE (LAST LEG CIRCUIT)

GAIT EDGE ROUTER (GAIT PoP)

GAIT CORE ROUTERS

GAIT CORE ROUTERS

GAIT EDGE ROUTER (GAIT PoP)

UNIT COLORLESS EDGE (LAST LEG CIRCUIT)

DISA TRANSPORT INFRASTRUCTURE

UNIT CLASSIFIED NETWORK

TUNNEL

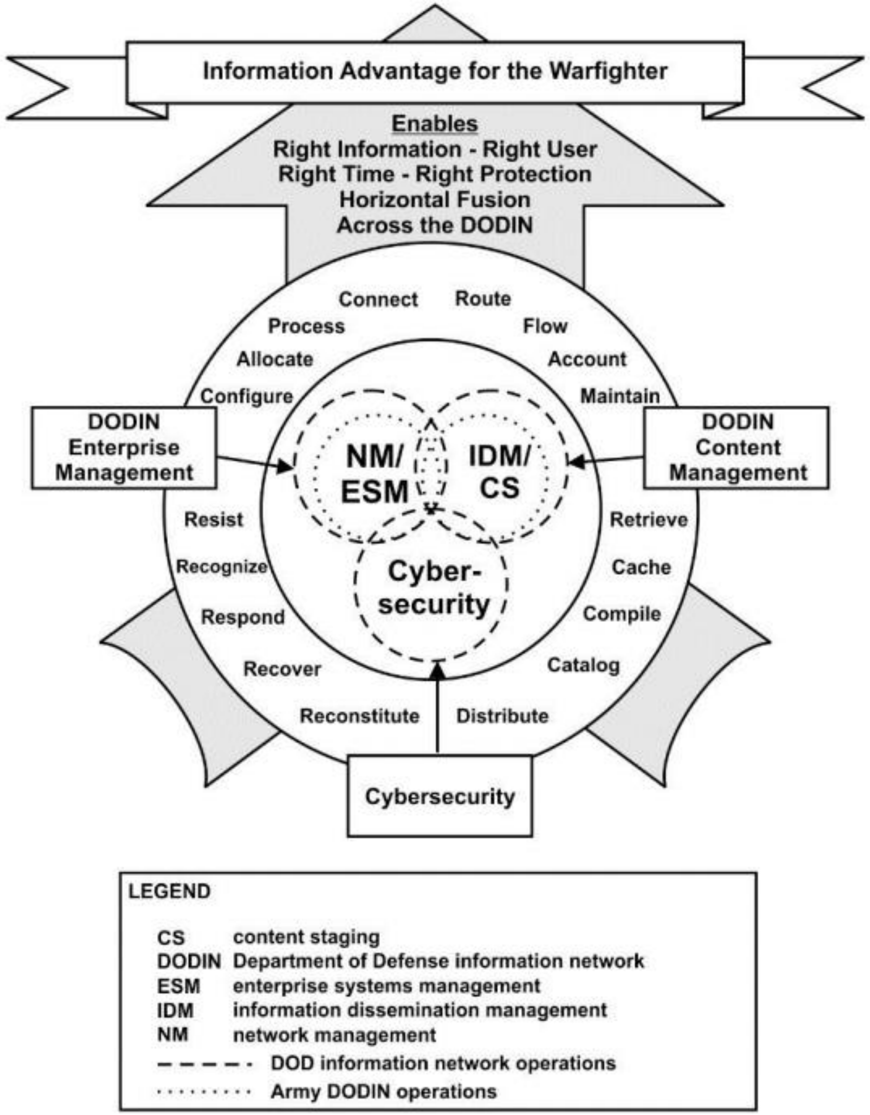
UNIT CLASSIFIED NETWORK

NETWORK OPERATIONS

ATP 6-02.71
TECHNIQUES FOR DEPARTMENT OF
DEFENSE INFORMATION
NETWORK OPERATIONS

<u>DoDIN Operations Operational Construct</u>

Replaces FMI 6-02.71 (2009)
**Expected to be published June 2016



Information Advantage for the Warfighter

Enables
Right Information - Right User
Right Time - Right Protection
Horizontal Fusion
Across the DODIN

Connect, Route, Process, Flow, Allocate, Account, Configure, Maintain

DODIN Enterprise Management

NM/ESM

IDM/CS

Cyber-security

DODIN Content Management

Resist, Recognize, Respond, Recover, Reconstitute

Retrieve, Cache, Compile, Catalog, Distribute

Cybersecurity

LEGEND

CS	content staging
DODIN	Department of Defense information network
ESM	enterprise systems management
IDM	information dissemination management
NM	network management
– – – –	DOD information network operations
· · · · · · · ·	Army DODIN operations

NETWORK OPERATIONS

ATP 6-02.60
TECHNIQUES FOR WARFIGHTER INFORMATION NETWORK-TACTICAL (WIN-T)

- INC1 & 2 Overview
- System Descriptions
- Management
- Interoperability
- Employment
- Architecture
- Definitions

NETWORK OPERATIONS

Network Governance

- Risk Management Framework (RMF)
- Security Technical Implementation Guide (STIG)
- Interim Approval to Connect (IATC)
- Interim Authorization to Operate (IATO)
- Interim Authorization to Test (IATT)
- Approval to Connect (ATC)
- Approval to Operate (ATO)
- Joint Interoperability Test Command (JITC)
- Security Requirements Guide (SRG)
- Telecommunications Service Order (TSO)
- Telecommunications Service Request (TSR)
- Designated Accrediting Authority (DAA)
- Information Assurance Vulnerability Management (IAVM)

NETWORK OPERATIONS

FCAPS

Fault

- Accurate fault localization leads to rapid resolution minimizing service outage

Configuration

- Through automated configuration functions, elements are provisioned in bulk, immediately ready for service

Accounting

- Usage account details are collected and stored for each subscriber, each business and each application

Performance

- Remotely monitor vital statistics of thousands of elements receiving alarms at critical performance and Capability thresholds

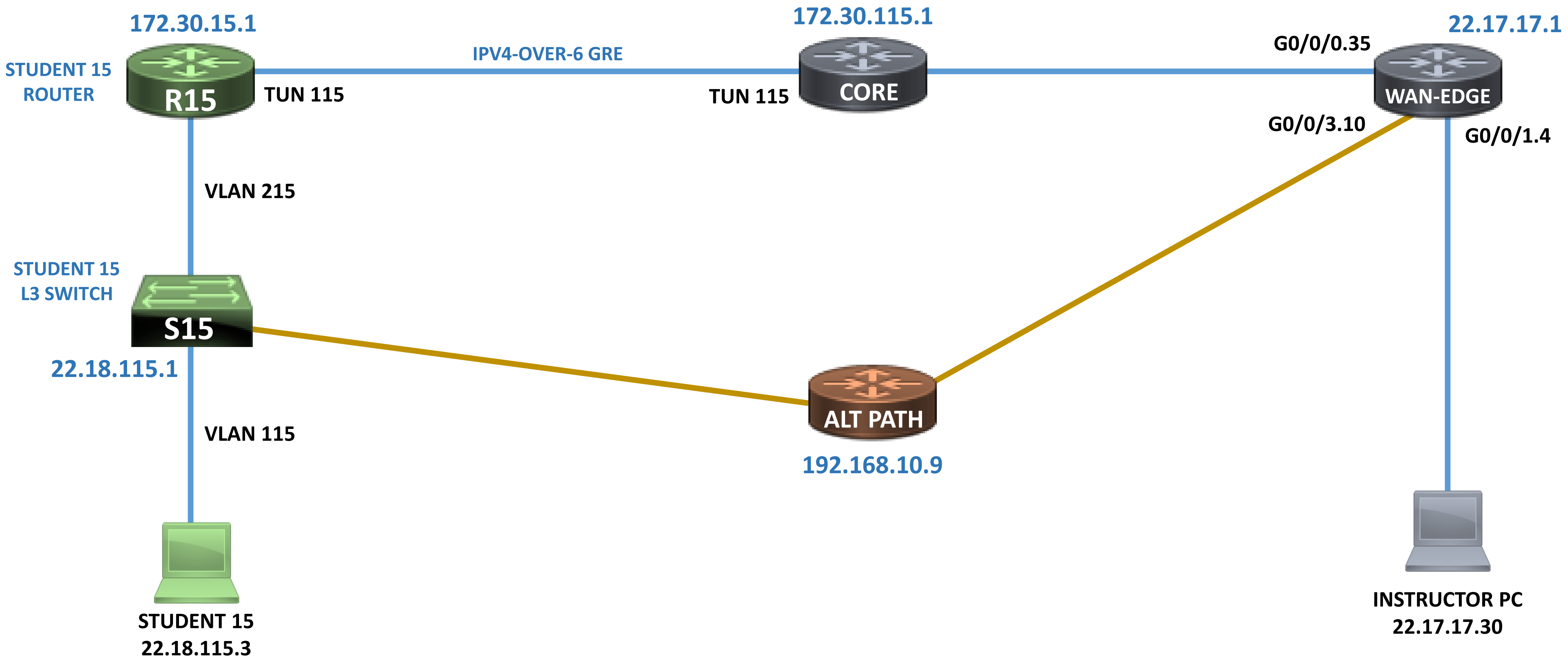
Security

- Subscriber and device identity is authenticated before network admission; security breaches are logged and alarmed

🟦 NORMAL ROUTED PATH

🟨 SECONDARY PATH

Policy-based routing allows an administrator to control traffic in accordance with specific configurations rather than let the path be determined by the routing table.



```
Ip access-list extended TRAFFIC
Permit ip host 22.17.17.30 host 22.18.115.1
Deny ip any
```

```
Route-map CONTROL-1
Match ip address TRAFFIC
Set ip next-hop 192.168.10.9
```

```
Int g0/0/1.4
Ip policy route-map CONTROL-1
```

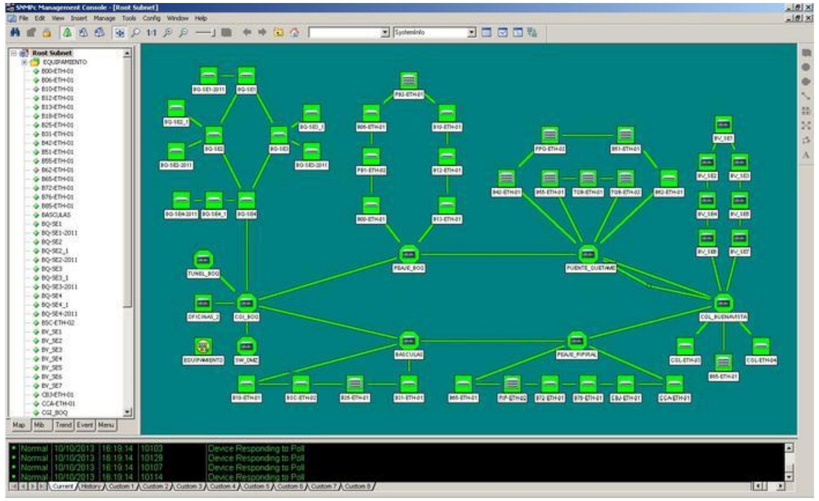
PERFORMANCE MANAGEMENT

Performance Management Knowledge Areas

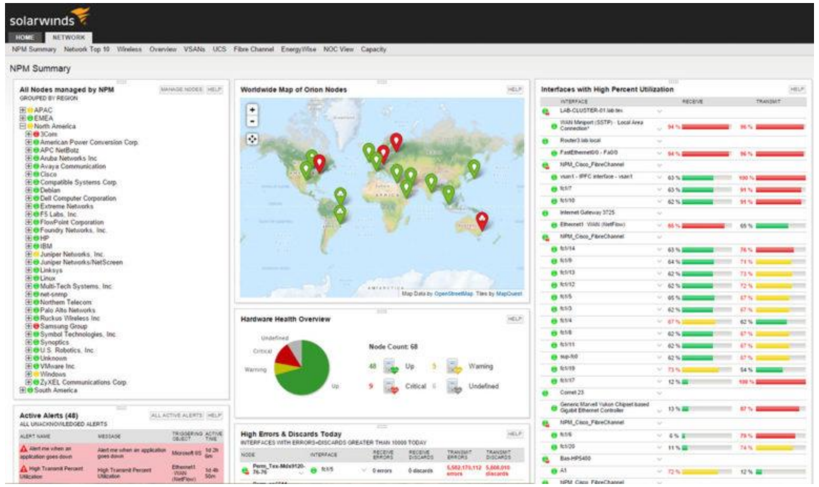
- Capacity Planning
- Availability
- Utilization
- Latency

Performance Management Tools

- ICMP and SNMP
- NetFlow



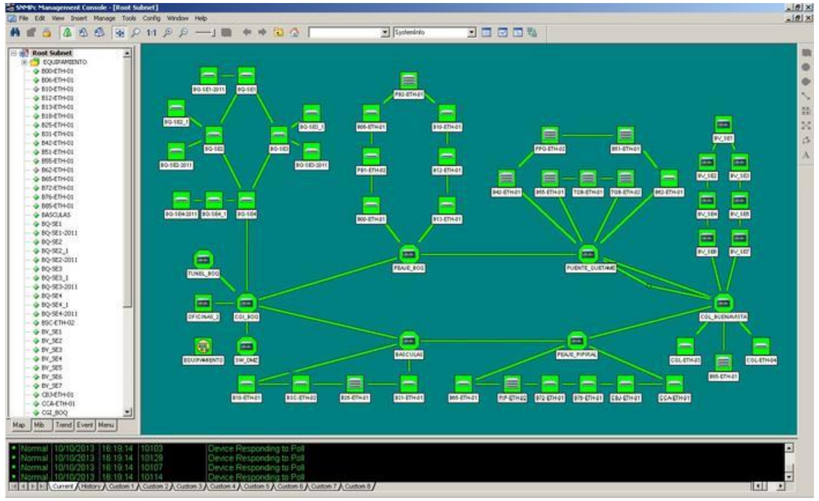
```
Normal  10/10/2013  16:19:14  10103  Device Responding to Poll
Normal  10/10/2013  16:19:14  10129  Device Responding to Poll
Normal  10/10/2013  16:19:14  10107  Device Responding to Poll
Normal  10/10/2013  16:19:14  10114  Device Responding to Poll
```



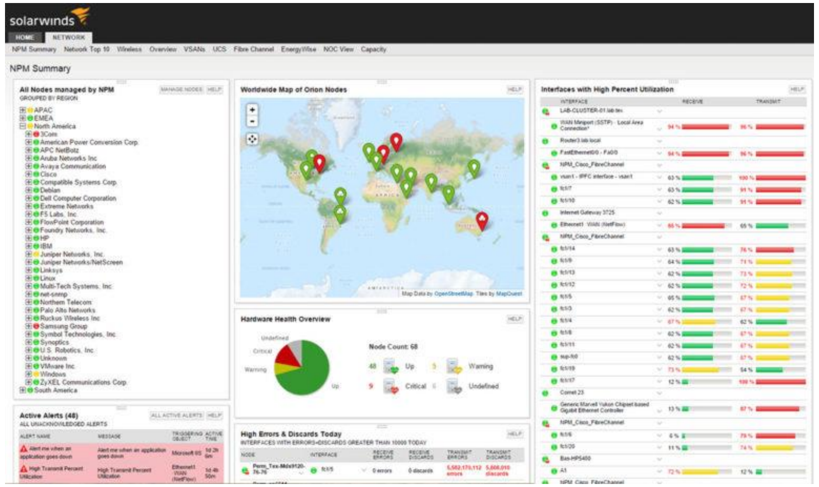
PERFORMANCE MANAGEMENT

Capacity Planning

- What is the capacity of the network?
  - Network Boundary Interfaces
  - Interior Network Segments
  - Provisioned Network Services
  - External & Internal sourcing
- Legitimate Traffic – traffic that is related to operations
- Inappropriate Traffic – traffic that is not related to operations
- Unwise Traffic – poorly managed traffic
- Oversubscription?


SNMPc Management Console - [Root Subnet]
File Edit View Insert Manage Tools Config Window Help
SystemInfo
Root Subnet
EQUIPAMIENTO
Map Mib Trend Event Menu
Current History Custom 1 Custom 2 Custom 3 Custom 4 Custom 5 Custom 6 Custom 7 Custom 8

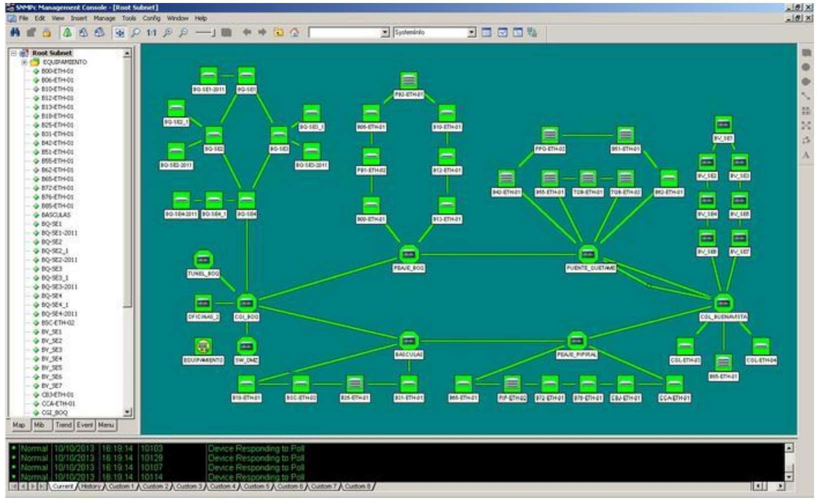
```
Normal  10/10/2013  16:19:14  10103   Device Responding to Poll
Normal  10/10/2013  16:19:14  10129   Device Responding to Poll
Normal  10/10/2013  16:19:14  10107   Device Responding to Poll
Normal  10/10/2013  16:19:14  10114   Device Responding to Poll
```


solarwinds
HOME NETWORK
NPM Summary Network Top 10 Wireless Overview VSANs UCS Fibre Channel EnergyWise NOC View Capacity
NPM Summary
All Nodes managed by NPM
GROUPED BY REGION
Worldwide Map of Orion Nodes
Interfaces with High Percent Utilization
INTERFACE RECEIVE TRANSMIT
Hardware Health Overview
Node Count: 68
Up Warning Critical Undefined
Active Alerts (48)
High Errors & Discards Today

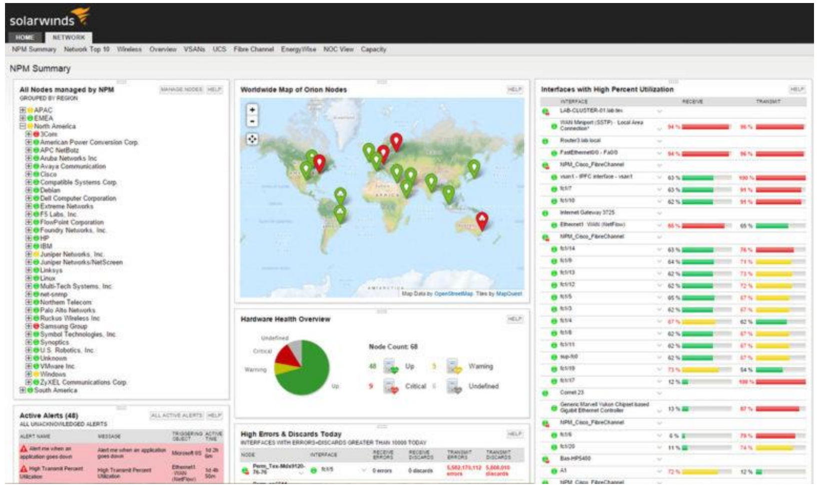
PERFORMANCE MANAGEMENT

Availability

- Network resources are available for utilization
  - Services
  - Bandwidth
- Primary paths
- Alternate paths
  - Backup
  - Load balance/load share
- Reliability
- What can effect availability?



```
Normal  10/10/2013  16:19:14  10103   Device Responding to Poll
Normal  10/10/2013  16:19:14  10129   Device Responding to Poll
Normal  10/10/2013  16:19:14  10107   Device Responding to Poll
Normal  10/10/2013  16:19:14  10114   Device Responding to Poll
```

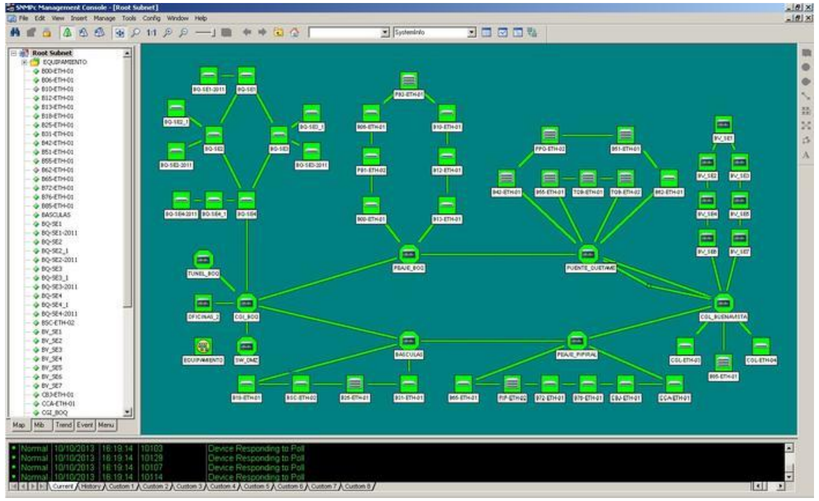


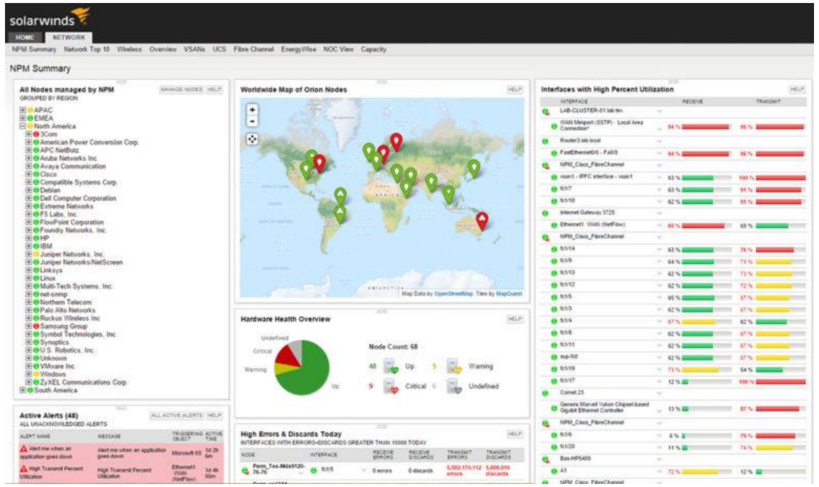
PERFORMANCE MANAGEMENT

Utilization

- Load placed on network resources
- Use of services
- Network segment traversal
- Bandwidth consumption
- What are some concerns with utilization?

LEGITIMATE / INAPPROPRIATE / UNWISE


SNMPc Management Console - [Root Subnet]
Root Subnet
EQUIPAMIENTO
Map
Mib
Trend
Event
Menu
Normal 10/10/2013 16:19:14 10103 Device Responding to Poll
Normal 10/10/2013 16:19:14 10128 Device Responding to Poll
Normal 10/10/2013 16:19:14 10107 Device Responding to Poll
Normal 10/10/2013 16:19:14 10114 Device Responding to Poll
Current
History
Custom 1
Custom 2
Custom 3
Custom 4
Custom 5
Custom 6
Custom 7
Custom 8

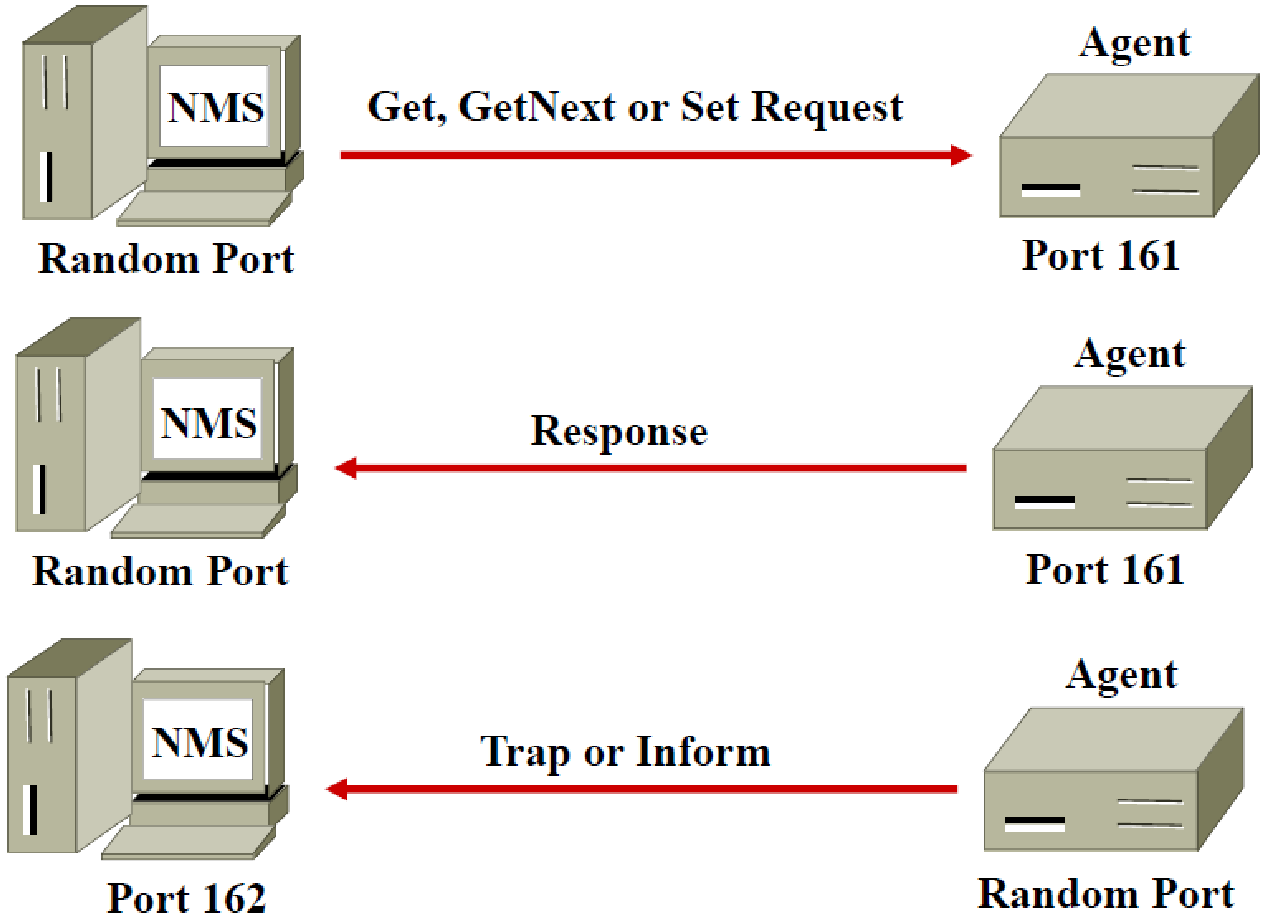


SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

- SNMP is an application layer protocol. It is designed to be platform independent
- Typically SNMP agents listen on UDP port 161
- Asynchronous traps are typically received by NMS on UDP port 162
- Default ports and behavior can be modified on both NMS and Agents
- RFC 3430 Defines methods for implementing SNMP over TCP
  - Intent of being to support large size data

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

SNMP Traffic



SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

SNMP Versions

- SNMPv1
  - Not secure
  - Poor performance
- SNMPv2c
  - Not secure
  - Better performance (getBulk)
- SNMPv3
  - Secure
  - High Performance

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

SNMPv2c

- Includes the basic functions of SNMPv1 & can co-exist with SNMPv1
- It is defined by the standards: RFCs 2578, 2579, 2580, 3416, 3417, 3418, Standard 58 & 62.
- Includes four new message types
- Allows retrieval of large amounts of management information using fewer network resources (GetBulk)
- The “C” stands for community-based security
- SNMPv2c Protocol Data Unit Messages include:
    - SNMPv1 PDUs: Get, GetNext, Set, GetResponse, Traps
    - Four new PDUs: GetBulk, Notification, Inform, and Reports.

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

SNMPv3 Security Features:

- Message Integrity
  - Checks against message tampering that could have occurred during transit
- Authentication
  - Checks and verifies message is from a valid source
- Encryption
  - Protects message from being viewed by an unauthorized source if intercepted

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

SNMPv3 Security Features:

Level	**Authentication Mechanism**	**Encryption Support**	**Process**
noAuthNoPriv	Username	No	Checks username match for authentication
authNoPriv	MD5 or SHA	No	Authenticates through Hashed Message Authentication Code (HMAC-MD5 or HMAC-SHA)
authPriv	MD5 or SHA	DES, 3DES AES	Authenticates the same as authNoPriv and encrypts using 56 bit DES encryption

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

Configuration Example:

Version 2c

```
snmp-server community n3tm@n RO
snmp-server community n@mt3n RW
```

Version 3

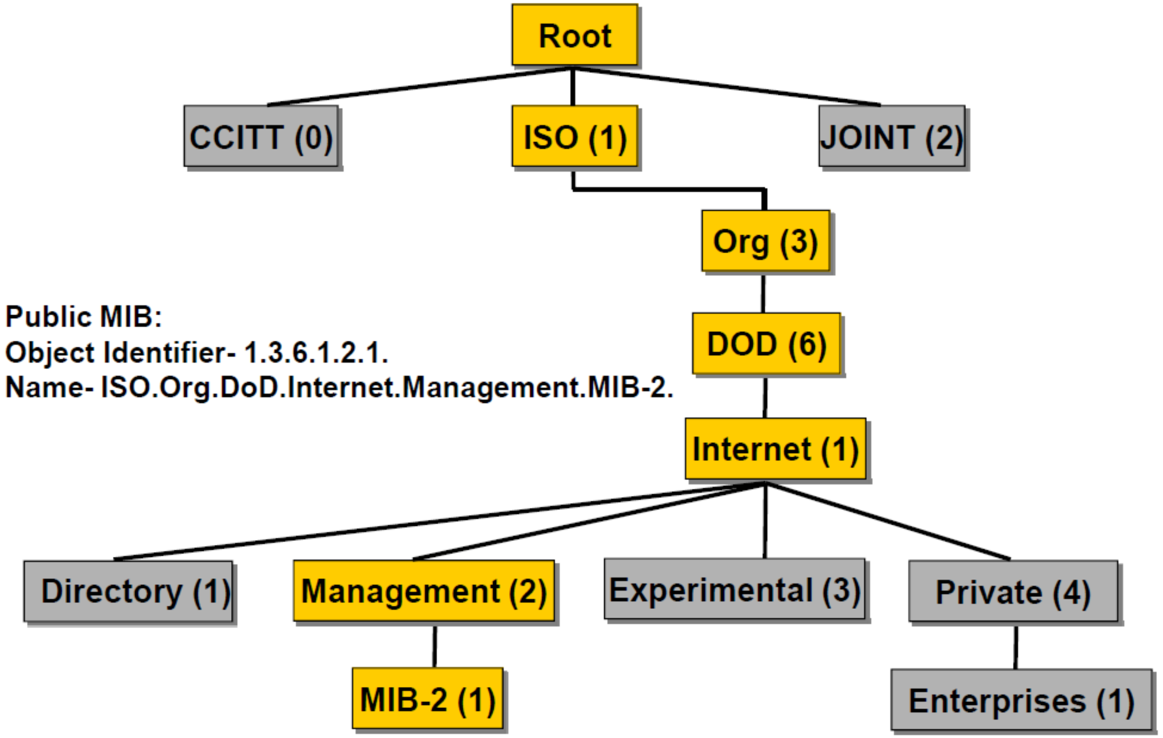
```
snmp-server engineID local 1234567890 (must be configured first)
snmp-server group NETOPS v3 priv write NETMAN
snmp-server user NETADMIN NETOPS v3 auth sha a-pass123 priv aes 128 e-pass123
snmp-server view NETMAN iso included
snmp-server host 22.227.38.2 version 3 priv NETOPS
```

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

Management Information Base (MIB)

- Structured Hierarchy of Information
  - Uses <u>Structure of Management Information</u>
  - Defines the structure and definition of Object Identifiers (OID)
  - Collection of OIDs supported by a vendor

1.3.6.1.2 (ISO, Org, DoD, Internet, Mgmt)



Public MIB:
Object Identifier- 1.3.6.1.2.1.
Name- ISO.Org.DoD.Internet.Management.MIB-2.

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

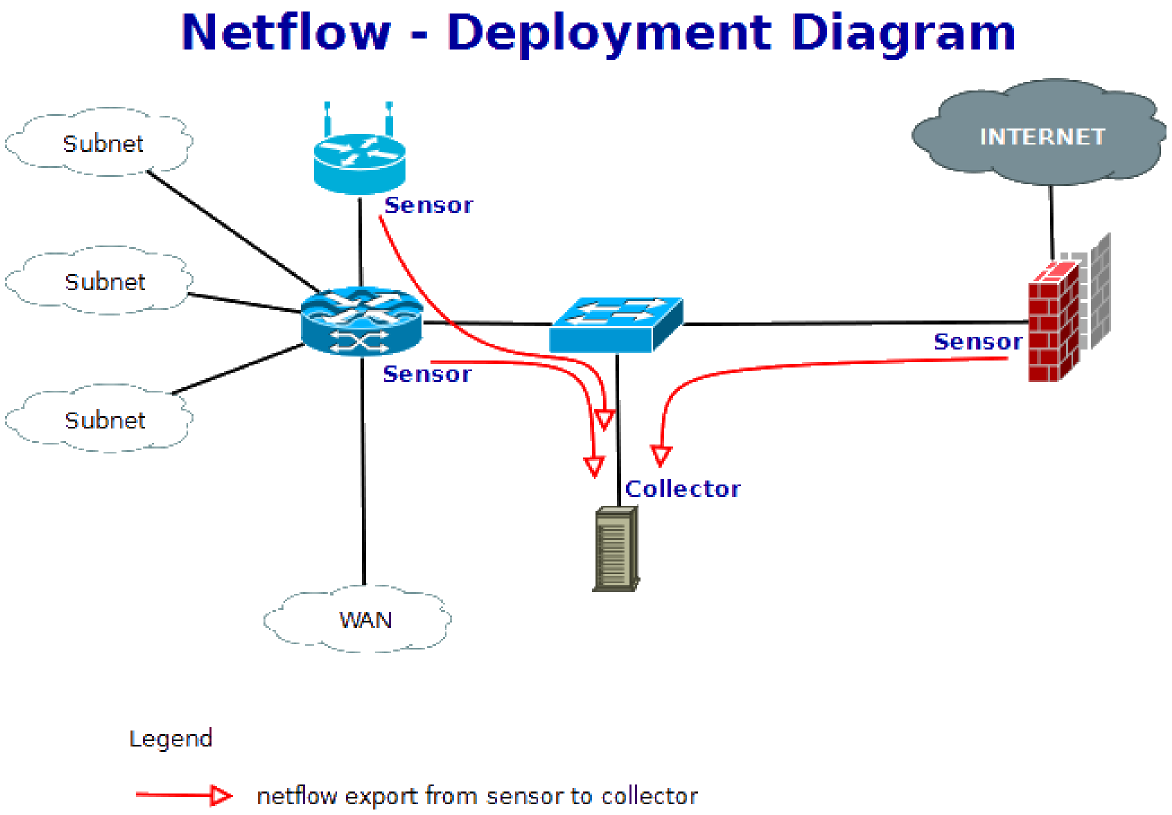
OBJECT IDENTIFIER (OID) Data Types:

- **INTEGER** – 32 bit number, provides status (up/down, full, critical)
- **OCTET STRING** – bytes used to represent string of text/information
- **COUNTER** – 32 bit number, 0 - 4,294,967,295, counts up and rolls over
- **OBJECT IDENTIFIER** – OID string, *1.3.6.1.4.1.9 (What OID is this?)*
- **GAUGE** – 0 - 4,294,967,295, counts up and down
- **TIME TICKS** – measures time in one hundredths of a second
- **IP ADDRESS** – represents an IP address
- **NETWORK ADDRESS** – represents a network address

PERFORMANCE MANAGEMENT

NetFlow Performance

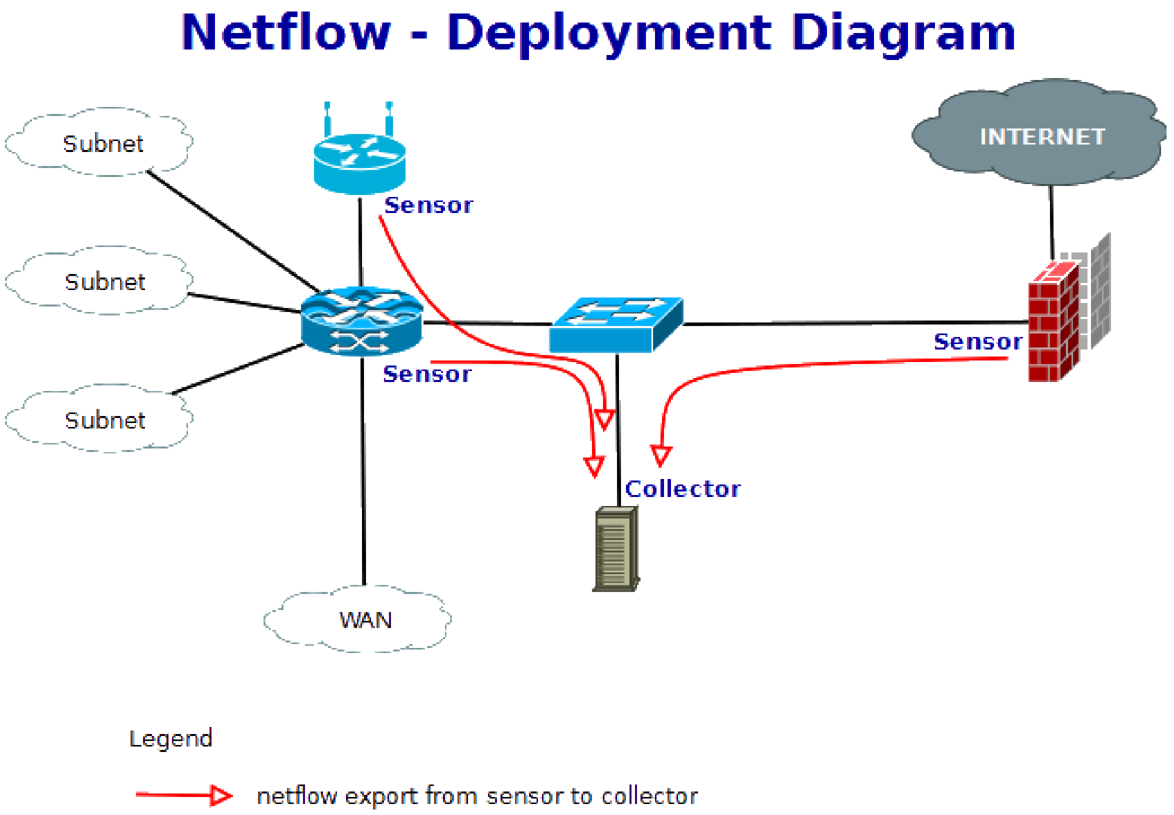
- How traffic is moving through a network
- Aggregate flows
  - Per segment (Distribution, Core)
  - Network Boundary Interfaces
- End to End flows
  - Application specific
  - System specific
  - Full path
- Identity of traffic types
  - (http, smtp, snmp, dns, etc…)
- Points of congestion


Netflow - Deployment Diagram
Subnet
Subnet
Subnet
Sensor
Sensor
INTERNET
Sensor
Collector
WAN
Legend
netflow export from sensor to collector

PERFORMANCE MANAGEMENT

NetFlow Capabilities

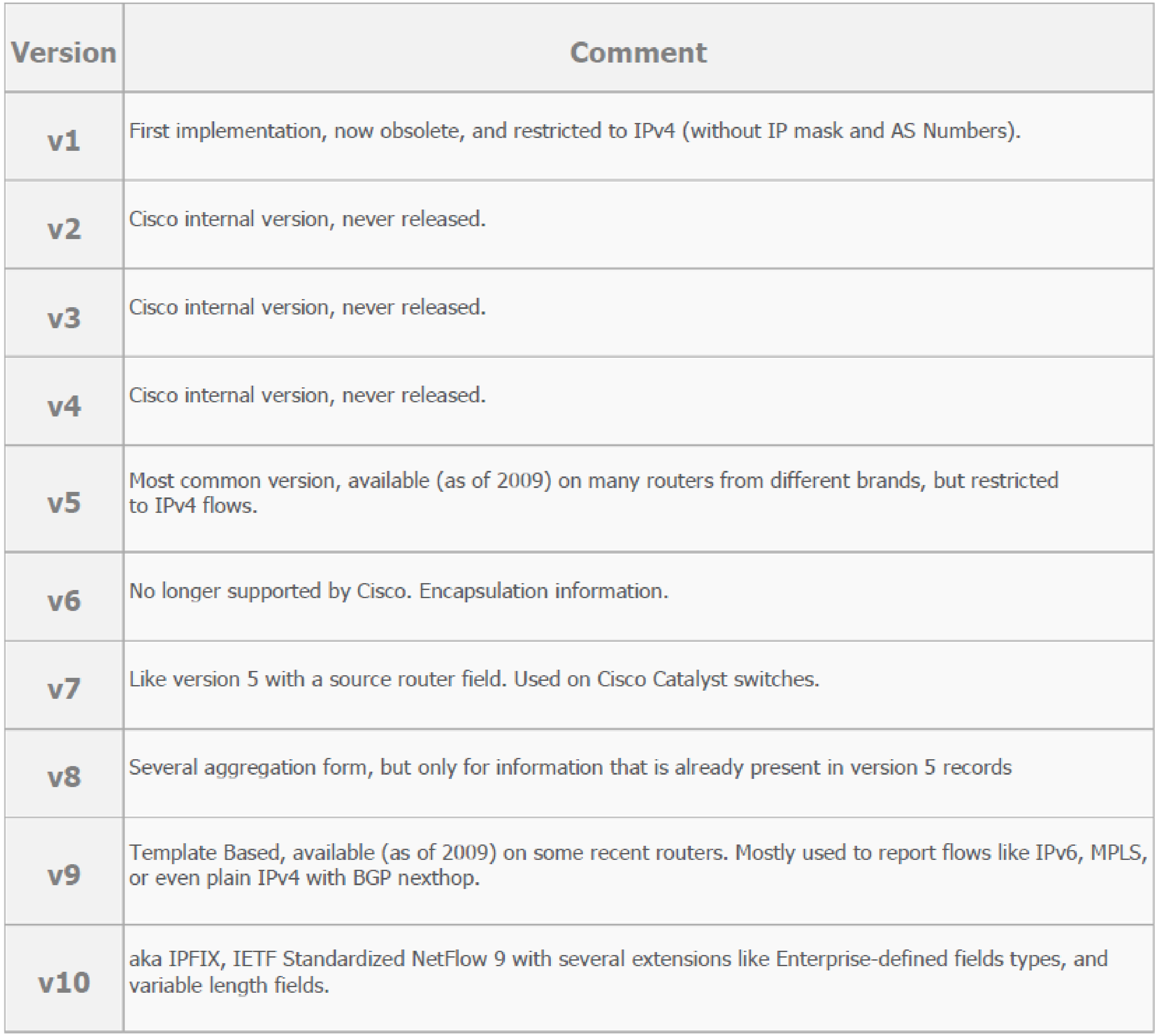
- Ability to characterize traffic from applications and users
- Understand the traffic patterns
- Provide a holistic view into bandwidth utilization and WAN traffic
- Support CBQoS validation and performance monitoring
- Network traffic forensics
- Aid in compliance reporting


Netflow - Deployment Diagram
Subnet
Subnet
Subnet
Sensor
INTERNET
Sensor
Sensor
Collector
WAN
Legend
netflow export from sensor to collector

PERFORMANCE MANAGEMENT

NetFlow Versions

- NetFlow v1 was originally introduced in 1990 and has since evolved to NetFlow version 9.
- Today, the most common versions are v5 and v9.
- UDP Ports
  - 2055
  - 2056
  - 4432
  - 4739
  - 9995
  - 9996
  - 6343



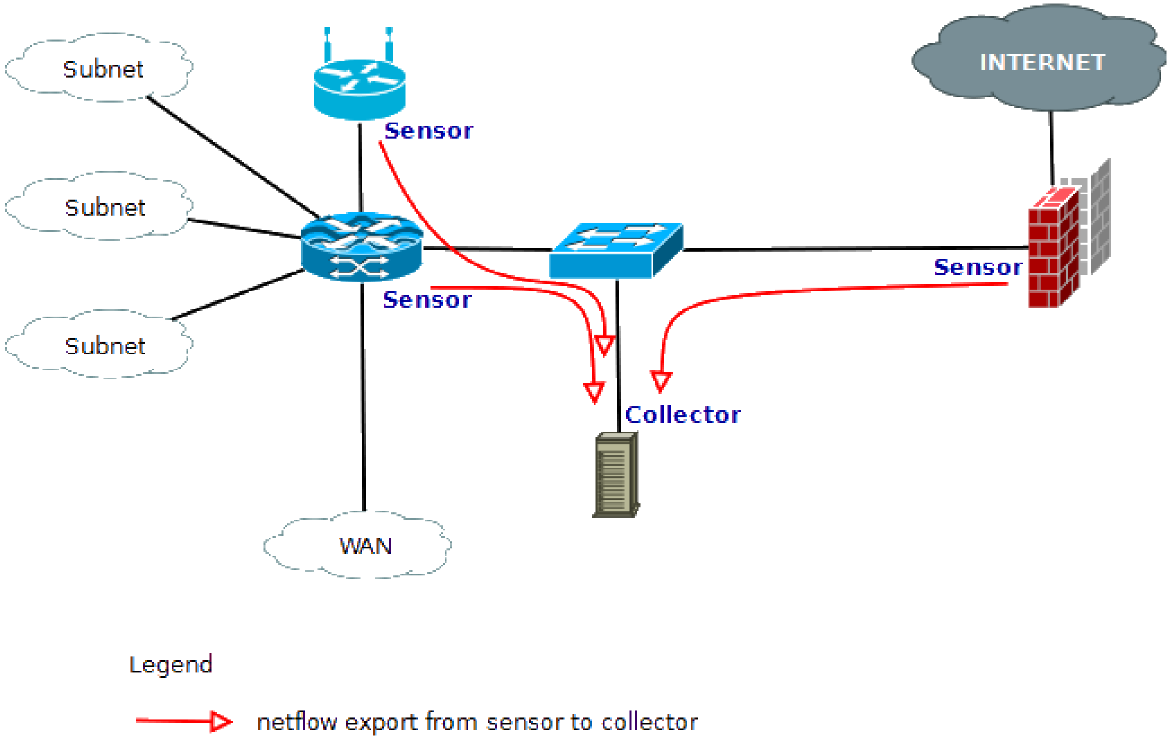
Version	Comment
v1	First implementation, now obsolete, and restricted to IPv4 (without IP mask and AS Numbers).
v2	Cisco internal version, never released.
v3	Cisco internal version, never released.
v4	Cisco internal version, never released.
v5	Most common version, available (as of 2009) on many routers from different brands, but restricted to IPv4 flows.
v6	No longer supported by Cisco. Encapsulation information.
v7	Like version 5 with a source router field. Used on Cisco Catalyst switches.
v8	Several aggregation form, but only for information that is already present in version 5 records
v9	Template Based, available (as of 2009) on some recent routers. Mostly used to report flows like IPv6, MPLS, or even plain IPv4 with BGP nexthop.
v10	aka IPFIX, IETF Standardized NetFlow 9 with several extensions like Enterprise-defined fields types, and variable length fields.

PERFORMANCE MANAGEMENT

Network flow application to CBQoS

- Identify bottle necks
- View of traffic performance
- Identify network segments for QoS treatment
- Validation of QoS implementation

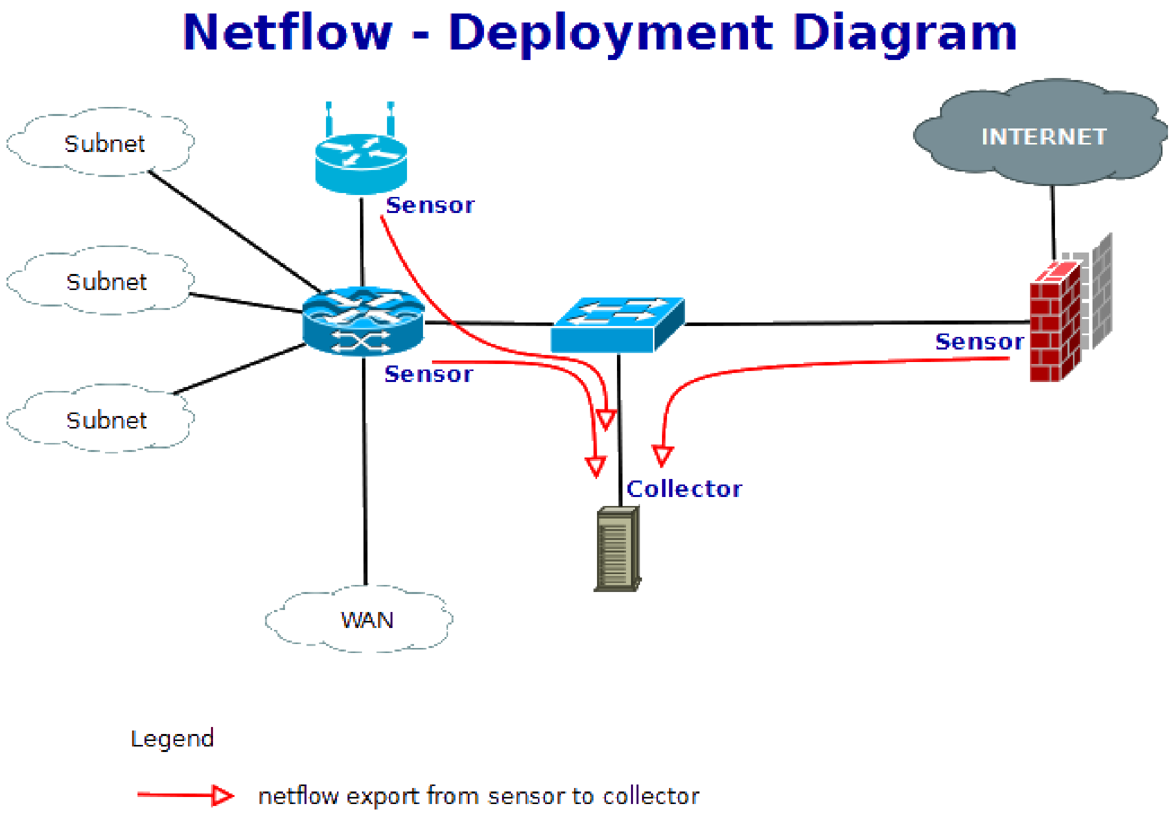
Netflow - Deployment Diagram



PERFORMANCE MANAGEMENT

Network flow application to Security and Troubleshooting

- Provides accounting of network activity 24x7
- Reduction of Mean Time To Know (MTTK)
- Provides "What is happening now" perspective
- Provides interior network picture
- Detection of attacks that have no signature
- Provides Isolation of network communications end to end


Netflow - Deployment Diagram
Subnet
Subnet
Subnet
Sensor
INTERNET
Sensor
Sensor
Collector
WAN
Legend
netflow export from sensor to collector