

WinTeam6

Members:

1. Johnson, Anton
2. Sharma, Avinash
3. Pruden, Tyrin
4. Tran, Duc Long
5. Rupinder Singh
6. Marcus-Johnson, Marian

Advanced Network Documentation

Contents

1. Network Design Overview	3
1.1 Core Layer	3
1.2 Distribution Layer.....	3
1.3 Access Layer	3
2. Executive Summary.....	3
3. Network Overview	3
3.1 Purpose	3
3.2 Scope.....	4
3.3 Objectives.....	4
3.4 Audience	4
4. Network Topology.....	5
4.1 Network Overview	6
4.2 Devices and Descriptions	6
4.3 IP Addressing Scheme For Intemediary devices	7
5. VLAN Segmentation	9
5.1 VLAN Definitions	9
5.2 VLAN Descriptions.....	9
6. Advanced Networking Technologies.....	11
6.1 OSPF (Open Shortest Path First)	11

6.2 GLBP (Gateway Load Balancing Protocol).....	12
6.3 EtherChannel's	13
6.4 NAT (Network Address Translation) Translations.....	14
6.5 InterVLAN Routing	14
7. Security Measures.....	14
7.1 Perimeter Security (ASA Firewalls)	14
7.2 Internal Security (ACLs).....	15
7.3 DMZ (Demilitarized Zone)	15
7.4 Switchport Security	15
7.5 Active Directory Policies and Permissions	15
8. Active Directory and Services	16
8.1 Active Directory.....	16
8.2 DHCP (Dynamic Host Configuration Protocol)	16
8.3 DNS (Domain Name System).....	17
8.4 Windows Server Update Services	17
8.5 Email Server (Microsoft Exchange)	17
8.6 Web Server (Red Hat Linux)	20
8.7 Server Redundancy for VMs	20
9. Vulnerability Scan	21
10. Future Cloud Integration and VPN Implementation.....	21
10.1 Cloud Integration:	21
10.2 VPN Implementation:	21
11. Password	22
12. Conclusion.....	23

1. Network Design Overview

The network design of WinTeam6 is structured into three fundamental layers: Core, Distribution, and Access. Each layer plays a crucial role in ensuring efficient data flow, scalability, redundancy, and security.

1.1 Core Layer

The Core Layer forms the backbone of the network, responsible for high-speed data aggregation and routing. It serves as the central hub for interconnecting different parts of the organization, providing fast and reliable communication between departments and data centers. Redundant links and protocols like OSPF (Open Shortest Path First) ensure optimal routing and fault tolerance at this layer.

1.2 Distribution Layer

The Distribution Layer acts as an intermediary between the Core and Access Layers. It manages traffic distribution, policy enforcement, and VLAN segmentation. Distribution switches facilitate communication between different departments and ensure that network traffic flows efficiently to its destination.

1.3 Access Layer

The Access Layer provides connectivity to end-user devices, such as computers, printers, and IP phones. This layer enforces security policies, VLAN assignment, and Quality of Service (QoS) settings. Access layer switches play a vital role in maintaining network integrity and optimizing performance for individual users.

By designing our network with these distinct layers, WinTeam6 achieves a robust, scalable, and efficient infrastructure that meets the diverse needs of our organization.

2. Executive Summary

This advanced network documentation report provides an extensive insight into the intricate network architecture and cutting-edge technologies implemented by WinTeam6. The network is designed to meet the communication needs of a medium to large-sized enterprise, prioritizing scalability, redundancy, robust security, and advanced networking protocols. The document outlines the purpose, scope, objectives, and intended audience of the advanced network documentation.

3. Network Overview

3.1 Purpose

The purpose of this advanced network documentation is to provide a comprehensive understanding of the sophisticated network infrastructure, configuration, and advanced technologies adopted by

WinTeam6. It aims to ensure seamless communication, efficient data transfer, heightened security, and optimized network performance.

3.2 Scope

This advanced documentation encompasses the network topology, device descriptions, IP addressing scheme, VLAN segmentation, advanced networking technologies (OSPF, GLBP, EtherChannel's, NAT Translations, and InterVLAN Routing), security measures, Active Directory policies, permissions, Exchange Email Server, Red Hat Linux Web Server, and plans for future Cloud Integration and VPN Implementation.

3.3 Objectives

The primary objectives of this advanced documentation are:

Provide a detailed overview of the advanced network architecture.

Describe the role and configuration of each advanced network technology.

Explain the integration of advanced networking protocols to enhance network efficiency.

Highlight the security measures and protocols implemented to safeguard the network.

Detail the role of Active Directory, including policies and permissions.

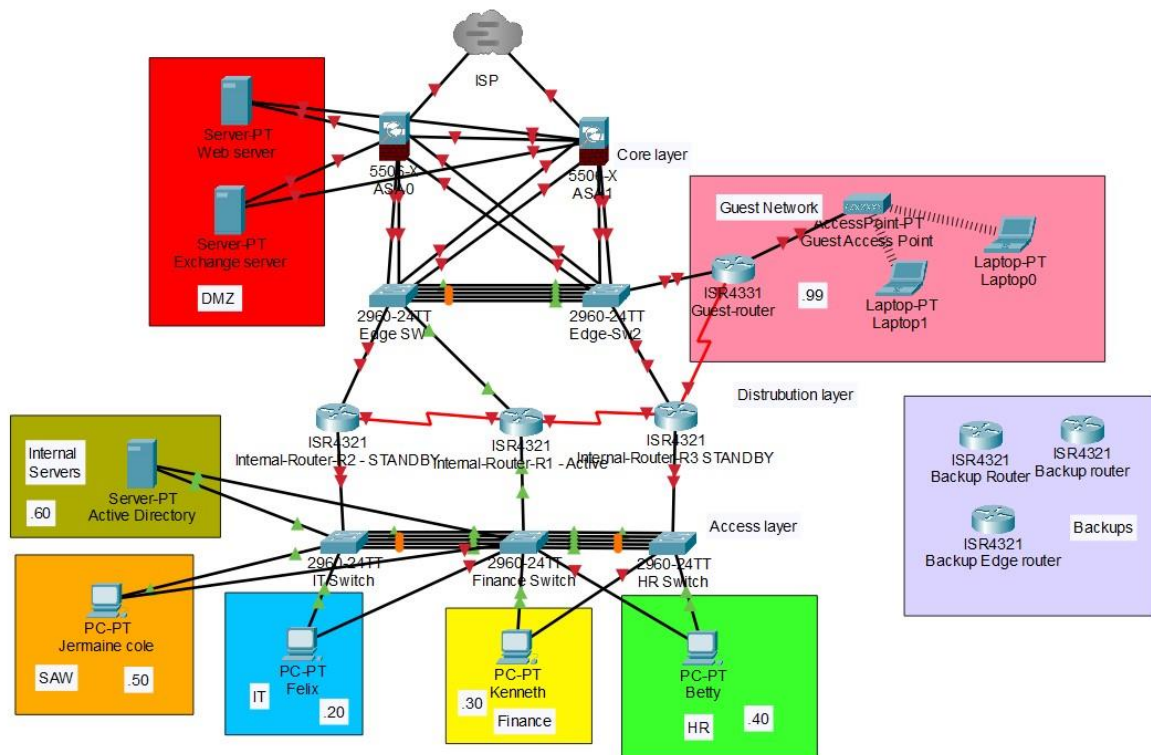
Present plans for future Cloud Integration and VPN Implementation.

3.4 Audience

This documentation is intended for network administrators, IT personnel, and relevant stakeholders within WinTeam6. It serves as a comprehensive reference for understanding the advanced network infrastructure, design, and configuration.

4. Network Topology

DEVICE	PORT
IR1 TO EDGE SW1	G0/0 -F0/1
IR1 TO FINANCE SWITCH	G0/1-F0/1
IR2 TO EDGE SW 1	G0/0-F0/2
IR2 TO IT SWITCH	G0/1-F0/1
ASA 2 TO INTERNET	5 -T4.2
ASA 1 TO INTERNET	5 -T4.1
IR1 TO IR3	S/1 TO S/0
IR1 TO IR2	S/0 TO S/0
IR3 TO GUEST ROUTER	S/1 TO S/0
IR3 TO HR SWITCH	G0/1 -F0/1
IR3 TO EDGE SW1	G0/1 -F0/1
GUEST RTR TO AP	G0/1
GUEST RTR TO EDGE SW 2	G0/1 -F0/5



4.1 Network Overview

The network topology of WinTeam6 has been meticulously crafted to seamlessly incorporate advanced networking technologies, ensuring optimal communication, redundancy, and security. Key devices have been strategically positioned to create a resilient and high-performance network infrastructure. This section provides an in-depth overview of the network topology, highlighting the essential components and their roles.

4.2 Devices and Descriptions

The network consists of a diverse range of devices, each playing a crucial role in maintaining the network's functionality and security. These devices are thoughtfully positioned to maximize efficiency and effectiveness:

ASA Firewalls (ASA1 and ASA2): ASA Firewalls serve as the first line of defense, providing perimeter security and segregation of internal VLANs from external threats. ASA1 and ASA2 are strategically placed at the network's edge, ensuring all incoming and outgoing traffic is thoroughly inspected and filtered to prevent unauthorized access and potential security breaches.

Internal Routers: Internal Routers, represented by IR1 ACT, IR2 ST, and IR3 ST, are responsible for efficient data routing and communication between various segments of the network. These routers facilitate seamless and fast data exchange, ensuring that information reaches its intended destination accurately and without delay.

Guest Router (GUEST R): The Guest Router, known as GUEST R, serves a specialized purpose by offering an isolated network for guest users. This isolation ensures that guest traffic remains separate from the internal network, enhancing security and minimizing potential risks associated with guest access.

Switches: Switches are integral to the network's operation, facilitating data transfer within VLANs and advanced networking protocols while maintaining security. The following switches are strategically positioned:

IT SW: This switch is dedicated to the IT department, enabling efficient communication and management of network infrastructure and devices within the IT VLAN.

FIN SW: The Finance switch is responsible for handling financial data and communication within the Finance VLAN, ensuring the security and integrity of financial operations.

HR SW: The HR switch provides a secure environment for Human Resources activities and confidential information within the HR VLAN.

Edge-Sw and Edge-S2: These switches are positioned at the network's edge, connecting various segments and providing access to the internal network. They contribute to the efficient flow of data between VLANs.

DMZ SW: The DMZ switch is directly connected to the ASA Firewalls, creating an isolated Demilitarized Zone for critical servers that need to be accessible from the internet. This separation ensures that external access to DMZ resources does not compromise the internal network's security.

A guest Wi-Fi was also implemented, SSID WINTEAM6 password is the default factory one

The strategic placement and configuration of these devices emphasize WinTeam6's commitment to building a robust and secure network topology that effectively caters to communication needs, security requirements, and scalability.

4.3 IP Addressing Scheme For Intemediary devices

Major Network: 10.0.5.0/24
Available IP addresses in major network: 254
Number of IP addresses needed: 34
Available IP addresses in allocated subnets: 44
About 22% of available major network address space is used
About 77% of subnetted network address space is used

Subnet Name	Needed Size	Allocated Size	Address	Mask	Dec Mask	Assignable Range	Broadcast
A	14	14	10.0.5.0	/28	255.255.255.240	10.0.5.1 - 10.0.5.14	10.0.5.15
B	4	6	10.0.5.16	/29	255.255.255.248	10.0.5.17 - 10.0.5.22	10.0.5.23
C	4	6	10.0.5.24	/29	255.255.255.248	10.0.5.25 - 10.0.5.30	10.0.5.31
D	4	6	10.0.5.32	/29	255.255.255.248	10.0.5.33 - 10.0.5.38	10.0.5.39
E	4	6	10.0.5.40	/29	255.255.255.248	10.0.5.41 - 10.0.5.46	10.0.5.47
F	4	6	10.0.5.48	/29	255.255.255.248	10.0.5.49 - 10.0.5.54	10.0.5.55

The IP addressing scheme is thoughtfully designed to allocate IP addresses efficiently while accommodating advanced networking technologies.

Device	Interface	IP	Mask	DFG	VLAN	DESCRIPTION
EDG-RTR	G0/0/0	ISP		ISP		Link to ISP1
	G0/0/1	10.0.5.17	255.255.255.248		B	Link to DMZ SW
	Loopback	10.0.15.11				
ASA	G1/1	10.0.5.1	255.255.255.240		A	
	G1/5	10.0.5.18	255.255.255.248		B	
	M1/1	10.0.5.69	255.255.255.0			MANAGEMENT PURPOSES ONLY
IR1 ACT	G0/0	10.0.5.2	255.255.255.240		A	Link to Edge SW
	G0/1		255.255.255.0			Link to Finance switch
	G0/1.20	10.0.20.2	255.255.255.0		IT	Interface VLAN 20 IT
	G0/1.30	10.0.30.2	255.255.255.0		FINANCE	Interface VLAN30 FINANCE
	G0/1.40	10.0.40.2	255.255.255.0		HR	Interface VLAN40 HR
	G0/1.50	10.0.50.1	255.255.255.0			MANAGEMENT PURPOSES ONLY

	G0/1.60	10.0.60.2	255.255.255.0			Interface VLAN60 SERVERS
	G0/1.1000	NATIVE				NATIVE VLAN
	S0/1/0	10.0.5.25	255.255.255.248		C	Link to Internal-R2
	S0/1/1	10.0.5.33	255.255.255.248		D	Link to Internal-R3
IR2 ST	G0/0/0	10.0.5.3	255.255.255.240		A	Link to Main Router SW
	G0/0/1	MAIN INT	255.255.255.0			Link to IT SW
	G0/1.20	10.0.20.3	255.255.255.0		IT	Interface VLAN 20 IT
	G0/1.30	10.0.30.3	255.255.255.0		FINANCE	Interface VLAN30 FINANCE
	G0/1.40	10.0.40.3	255.255.255.0		HR	Interface VLAN40 HR
	G0/1.50	10.0.50.2	255.255.255.0			MANAGEMENT PURPOSES ONLY
	G0/1.60	10.0.60.3	255.255.255.0			Interface VLAN60 SERVERS
	G0/1.1000	NATIVE				NATIVE VLAN
	S0/1/0	10.0.5.26	255.255.255.248		C	Link to Internal-R1
IR3 ST	G0/0/0	10.0.5.4	255.255.255.240		A	Link to Main Router SW
	G0/0/1	MAIN INT	255.255.255.0			Link to HR SW
	G0/0/1.20	10.0.20.4	255.255.255.0		IT	Interface VLAN 20 IT
	G0/0/1.30	10.0.30.4	255.255.255.0		FINANCE	Interface VLAN 30 FINANCE
	G0/1.40	10.0.40.4	255.255.255.0		HR	Interface VLAN 40 HR
	G0/1.50	10.0.50.3	255.255.255.0			MANAGEMENT PURPOSES ONLY
	G0/1.60	10.0.60.4	255.255.255.0			Interface VLAN 60 SERVERS
	G0/1.1000	NATIVE				NATIVE VLAN
	S0/1/0	10.0.5.34	255.255.255.248		D	Link to Internal-R1
GUEST R	G0/0/0	10.0.5.5	255.255.255.240		A	Link to Access point
	G0/0/1	10.0.99.1	255.255.255.0		Guest	Link to VLAN99 GUEST
IT SW	SVI VL50	10.0.50.4	255.255.255.0	10.0.20.1		MANAGEMENT PURPOSES ONLY
FIN SW	SVI VL50	10.0.50.5	255.255.255.0	10.0.30.1		MANAGEMENT PURPOSES ONLY
HR SW	SVI VL50	10.0.50.6	255.255.255.0	10.0.40.1		MANAGEMENT PURPOSES ONLY
Edge-Sw	SVI VL50	10.0.5.7	255.255.255.0	10.0.50.17		MANAGEMENT PURPOSES ONLY
DMZ-Sw	SVI VL50	10.0.5.19	255.255.255.248			
EXCH SVR	NIC	PUBLIC				Link to DMZ SW
WEB SVR	NIC	PUBLIC				Link to DMZ SW
AD	NIC	10.0.60.51	255.255.255.248			
SAW	NIC	10.0.60.6				
IT PC	NIC	DHCP				
FIN PC	NIC	DHCP				
SAW	NIC	10.0.4.20	255.255.255.			

HR PC	NIC	DHCP				
-------	-----	------	--	--	--	--

5. VLAN Segmentation

5.1 VLAN Definitions

- VLAN 20 (IT): Managed by the IT department.
- VLAN 30 (Finance): Dedicated to financial data and communication.
- VLAN 40 (HR): Reserved for HR-related activities.
- VLAN 50 (Management): For network administrators and management.
- VLAN 60 (Servers): Houses critical servers and services.
- VLAN 99 (Guest): Isolated VLAN for guest users.
- VLAN 1000 (Native): Native

5.2 VLAN Descriptions

VLAN 20 - IT:

Purpose: Dedicated to the IT department for managing network infrastructure and devices.

IP Range: 10.0.20.0/24

Description: This VLAN is used for IT personnel to access and manage networking equipment, including switches, routers, and servers. It ensures a secure and isolated environment for network administrators to perform configuration, troubleshooting, and maintenance tasks.

VLAN 30 - Finance:

Purpose: Reserved for financial operations and secure data communication.

IP Range: 10.0.30.0/24

Description: The Finance VLAN is designed to handle sensitive financial transactions, data, and communications. It ensures that financial operations are isolated from other departments for security and compliance purposes.

VLAN 40 - HR:

Purpose: Dedicated to Human Resources activities and confidential information.

IP Range: 10.0.40.0/24

Description: The HR VLAN provides a secure environment for HR personnel to manage employee data, payroll, and other confidential HR functions. It prevents unauthorized access to sensitive HR-related information.

VLAN 50 - Management:

Purpose: Reserved for network administrators and management personnel.

IP Range: 10.0.50.0/24

Description: The Management VLAN is intended for network administrators, IT managers, and other authorized personnel. It allows for centralized management, monitoring, and control of network devices and services. The SAW computer is on this vlan to configure intermediary devices

VLAN 60 - Servers:

Purpose: Hosts critical servers and services for the organization.

IP Range: 10.0.60.0/24

Description: The Servers VLAN houses essential servers such as domain controllers, email servers, and application servers. It ensures efficient communication between servers while providing a secure environment for hosting critical services.

VLAN 99 - Guest:

Purpose: Provides internet access for guest users while ensuring network separation.

IP Range: 10.0.99.0/24

Description: The Guest VLAN offers isolated internet access for visitors or guest users. It prevents guest traffic from interfering with internal network traffic, enhancing security and network performance.

VLAN 1000 - Native:

Purpose: Reserved for native VLAN traffic on trunks.

IP Range: Not applicable (reserved for layer 2 traffic)

Description: The Native VLAN is used for trunking purposes and carries untagged traffic. It allows compatibility with devices that do not support VLAN tagging.

VLAN 666 - Blackhole:

Purpose: Assigned to unused ports as a security measure.

IP Range: Not applicable (reserved for layer 2 traffic)

Description: The Blackhole VLAN is designated for unused ports. It prevents unauthorized devices from connecting to the network, enhancing security by isolating potential threats.

These VLAN descriptions illustrate how each VLAN is carefully designed and configured to meet specific organizational needs, enhance security, and optimize network performance.

6. Advanced Networking Technologies

6.1 OSPF (Open Shortest Path First)

OSPF, or Open Shortest Path First, is a dynamic routing protocol that significantly enhances network efficiency. By dynamically calculating the shortest path for data transmission, OSPF ensures optimal traffic flow across the network. This intelligent routing mechanism adapts to changes in network topology, facilitating faster data transmission and reducing latency. OSPF's ability to quickly reroute traffic in case of link failures or changes makes it a vital component for maintaining a robust and responsive network infrastructure.

```

Internal-R3#show ip ospf interface brief
Interface      PID  Area  IP Address/Mask  Cost  State  Nbrs  F/C
Se0/1/1        10   0      10.0.66.2/24     50    P2P    1/1
Gi0/0/1.60     10   0      10.0.60.4/24     1     DR     0/0
Gi0/0/1.50     10   0      10.0.50.3/24     1     DR     0/0
Gi0/0/1.40     10   0      10.0.40.4/24     1     DR     0/0
Gi0/0/1.30     10   0      10.0.30.4/24     1     DR     0/0
Gi0/0/1.20     10   0      10.0.20.4/24     1     DR     0/0
Se0/1/0        10   0      10.0.5.34/29     49    P2P    1/1
Gi0/0/0        10   0      10.0.5.4/28      1     DR     0/0
Internal-R3#

```

6.2 GLBP (Gateway Load Balancing Protocol)

GLBP NET	IP
20	10.0.20.1
30	10.0.30.1
40	10.0.40.1
50	10.0.50.1
60	10.0.60.1

GLBP, the Gateway Load Balancing Protocol, serves as a pivotal component in enhancing redundancy and load balancing within EtherChannel's. By intelligently distributing traffic across multiple physical links, GLBP ensures seamless connectivity and maximizes network performance. This protocol optimizes the utilization of available bandwidth, prevents link congestion, and provides fault tolerance, resulting in a more stable and efficient network environment.

6.3 EtherChannel's

EtherChannel's provide a mechanism to aggregate multiple physical links into a single logical link, effectively increasing bandwidth and enhancing fault tolerance. By bundling these links, EtherChannel's optimize network throughput and improve data transmission reliability. This technology is particularly valuable in high-demand environments where data-intensive tasks require robust and efficient communication channels.

ETHERCHANNEL		
FINANCE TO IT SWITCH	PORT CHANNEL 1	F0/10-16
FINANCE TO HR	PORT CHANNEL 2	F0/17-23
EDGE SW 1 TO EGDE SW 2	PORT CHANNEL 1	F0/13-18
ASA 2 TO EDGE SW 2	PORT CHANNEL 6	6-7 ,F0/9-10
ASA 1 TO EDGE SW 1	PORT CHANNEL 5	1-3 ,F0/5-7
ASA 1 TO EDGE SW 1	PORT CHANNEL 3	6-7 ,F0/2-3
ASA2 TO EDGE SW 1	PORT CHANNEL 2	6-7 ,F0/9-10

```
COM1 - Tera Term VT
File Edit Setup Control Window Help
Flags: D - down          P/bndl - bundled in port-channel
       I - stand-alone  s/susp - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator

       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 0
Number of aggregators: 0

Group  Port-channel Protocol  Ports
-----+-----+-----+-----
RU - L3 port-channel UP State
SU - L2 port-channel UP state
P/bndl - Bundled
S/susp - Suspended
Internal-R3#
```

6.4 NAT (Network Address Translation) Translations

NAT translations are a cornerstone of secure network communication. They enable seamless and secure data exchange between internal and external networks by mapping private IP addresses to a public IP. This translation process ensures that internal network resources remain hidden from the public internet, adding an extra layer of security to the network infrastructure.

6.5 InterVLAN Routing

InterVLAN Routing is a fundamental mechanism that facilitates efficient data exchange between different VLANs. By allowing communication between distinct virtual LANs, InterVLAN Routing ensures that information flows smoothly and quickly across the network. This technology is essential for optimizing network performance while maintaining strict segregation between different segments of the network.

```
IT-Switch#show vlan
```

VLAN	Name	Status	Ports
1	default	active	
20	IT	active	Fa0/24
30	Finance	active	
40	HR	active	
50	Management	active	
60	Servers	active	Fa0/23
666	Blackhole	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Gi0/1, Gi0/2
1000	Native	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0

These advanced networking technologies, including OSPF, GLBP, EtherChannel's, NAT translations, and InterVLAN Routing, collectively contribute to WinTeam6's goal of achieving a high-performance, resilient, and secure network environment. Their implementation underscores our dedication to leveraging cutting-edge solutions to meet the demands of a dynamic and growing enterprise.

7. Security Measures

7.1 Perimeter Security (ASA Firewalls)

Perimeter security is fortified by ASA Firewalls, which serve as robust sentinels, meticulously inspecting incoming and outgoing traffic. These firewalls employ sophisticated rule sets and deep packet inspection to filter and scrutinize data packets. By establishing a strong perimeter defense, ASA Firewalls shield the

network from external threats, thwarting unauthorized access attempts, and safeguarding sensitive information.

7.2 Internal Security (ACLs)

Access Control Lists (ACLs) play a pivotal role in enhancing internal security by governing the flow of traffic between VLANs. These finely tuned rules dictate which devices or users can communicate across different segments of the network. ACLs provide a powerful tool for preventing unauthorized access, minimizing lateral movement within the network, and ensuring that only authorized communication pathways are established.

7.3 DMZ (Demilitarized Zone)

The DMZ serves as an isolated enclave, housing critical servers that interact with external networks, such as web servers or email servers. By physically segregating these servers from the internal network, WinTeam6 adds an extra layer of protection. This isolation mitigates the potential impact of a security breach by limiting the exposure of internal assets, making it significantly more challenging for malicious actors to infiltrate deeper into the network. The Exchange server and webserver are in the DMZ.

7.4 Switchport Security

Switchport security is an essential component of our defense strategy, preventing unauthorized devices from connecting to the network through various mechanisms. MAC address filtering allows only approved devices to communicate, while port security limits the number of MAC addresses that can be associated with a single port. Dynamic ARP inspection safeguards against ARP spoofing attacks, maintaining the integrity of ARP resolution. Furthermore, DHCP snooping counters potential DHCP-based threats by ensuring that only authorized DHCP servers can assign IP addresses, minimizing the risk of unauthorized network access. To enhance security, we disable CDP and LLDP protocols, minimizing information exposure. Collectively, these measures fortify our network, ensuring its integrity and confidentiality.

```
IT-Switch#show port-security address
Secure Mac Address Table
```

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
60	000c.29d4.2514	SecureSticky	Fa0/23	-
60	001b.216a.b1ad	SecureSticky	Fa0/23	-
20	001b.216a.b0ef	SecureSticky	Fa0/24	-

```
Total Addresses in System (excluding one mac per port) : 1
Max Addresses limit in System (excluding one mac per port) : 8192
```

7.5 Active Directory Policies and Permissions

Active Directory emerges as a central pillar of user management and access control. Through granular policies and meticulously crafted permissions, WinTeam6 governs who can access specific resources, applications, and data. This robust authentication and authorization mechanism prevents unauthorized access attempts, enforces data protection, and maintains the overall security posture of the network.

By harmoniously integrating these comprehensive security measures, WinTeam6 embraces a multi-faceted approach to network security. The synergy of perimeter defense, internal segmentation, DMZ

isolation, switchport security, DHCP snooping, and Active Directory policies collectively forms a resilient shield, preserving the confidentiality, integrity, and availability of critical network assets.

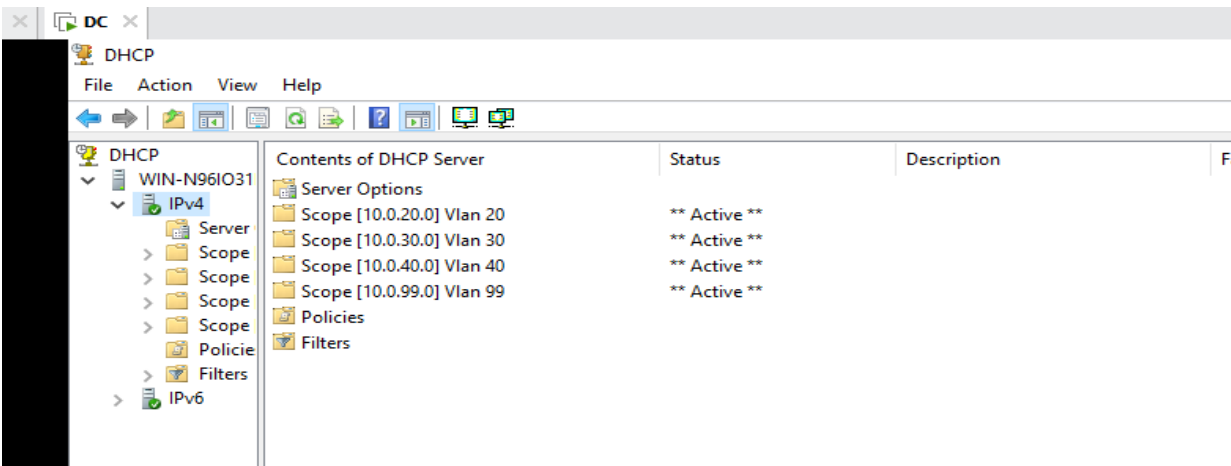
8. Active Directory and Services

8.1 Active Directory

Active Directory serves as the centralized platform for user management, authentication, and authorization, enhancing network security and control. It provides a robust directory service that enables centralized user authentication and access control across the network. Through Active Directory, WinTeam6 can efficiently manage user accounts, assign permissions, and enforce security policies, ensuring that only authorized personnel have access to network resources. This centralized approach streamlines user management, simplifies access control, and contributes to a more secure and organized network environment.

OU	Group	Users
Finance	GFinanace	Avi Sharma
		Marian Marcus
HR	GHR	Rupinder Singh
		Tyrin Pruden
IT	GIT	Duc Long
		Anthony Johnson
Guest	GGuest	Arun Khach
		Jeavi Putt

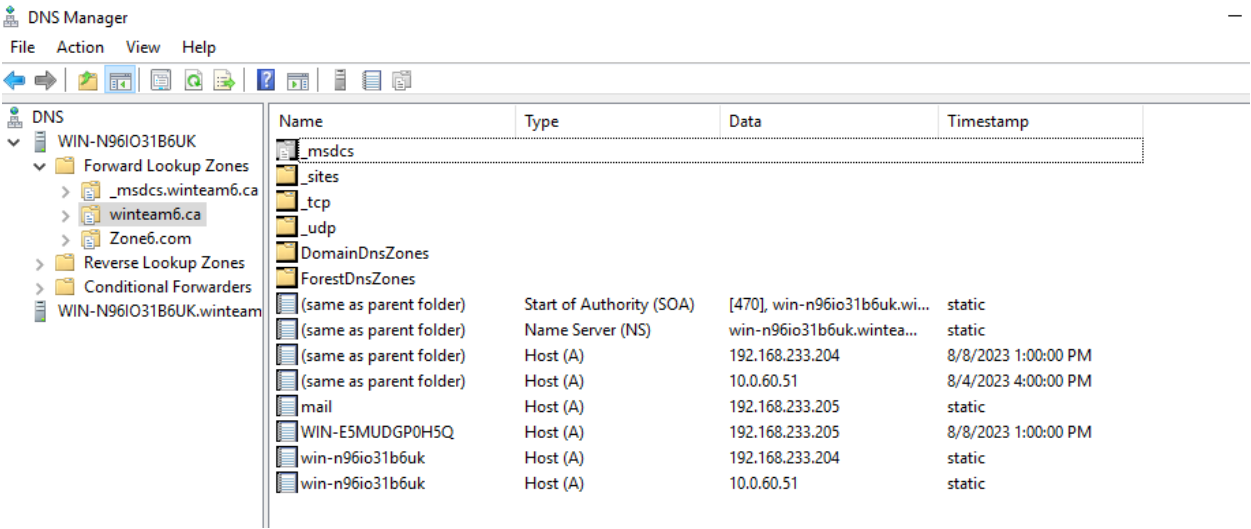
8.2 DHCP (Dynamic Host Configuration Protocol)



DHCP automates IP address allocation, simplifying network configuration and management. DHCP is configured on the Active Directory server, dynamically assigning IP addresses to devices on the network. This eliminates the need for manual IP address configuration, reduces the risk of IP conflicts, and eases the administrative burden. DHCP ensures efficient IP address utilization, optimizes network resource

allocation, and supports the seamless integration of new devices, enhancing network scalability and flexibility.

8.3 DNS (Domain Name System)



DNS resolves domain names to IP addresses, facilitating efficient access to internal and external resources. DNS is also configured on the Active Directory server, providing domain name resolution for the network. It acts as a critical component of network infrastructure, enabling users to access websites, applications, and services using user-friendly domain names instead of numerical IP addresses. DNS caching enhances browsing speed and efficiency by storing previously resolved domain name-to-IP mappings. By maintaining a reliable and responsive DNS infrastructure, WinTeam6 ensures smooth and consistent access to online resources, both within the organization and on the wider internet.

8.4 Windows Server Update Services

Windows Server Update Services (WSUS) enables information technology administrators to deploy the latest Microsoft product updates. You can use WSUS to fully manage the distribution of updates that are released through Microsoft Update to computers on your network.

8.5 Email Server (Microsoft Exchange)

The Microsoft Exchange email server facilitates efficient and secure email communication across WinTeam6. It enables reliable email delivery, advanced calendaring, and seamless collaboration among employees. Microsoft Exchange ensures data integrity and confidentiality through robust email encryption and authentication mechanisms. By managing email traffic, scheduling, and contact information, Microsoft Exchange enhances productivity and communication within the organization, offering integration with other Microsoft Office applications.

mailboxes - Microsoft Exchange

Mail - avi@winteam6.ca

← → ↺

Not secure | https://mail.winteam6.ca/owa/#path=/mail/sentitems

🔍 ☆ 🏠 👤 ⋮

Mail

🔔 ⚙️ ? 👤

Search Mail and People 🔍


➕ New | ▾ Empty folder 📁 Mark all as read


^ Favorites
Inbox
Sent Items
Drafts
^ Avi Sharma
Inbox
Drafts
Sent Items

Sent Items

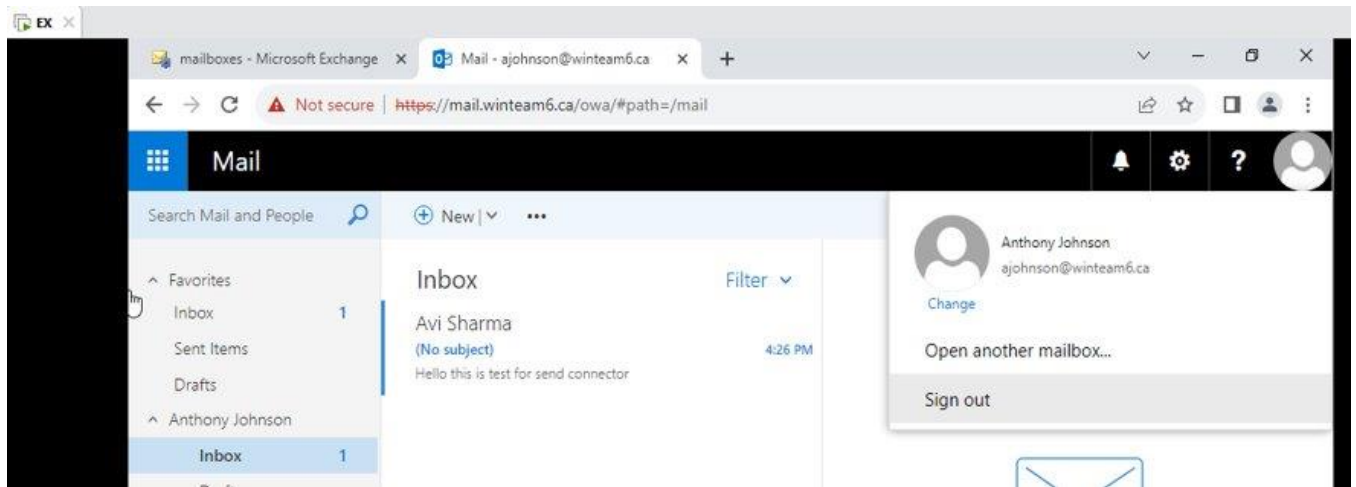
Filter ▾

Anthony Johnson
(No subject)
Hello this is test for send connector
4:26 PM

 **Avi Sharma**
avi@winteam6.ca
[Change](#)
Open another mailbox...
Sign out



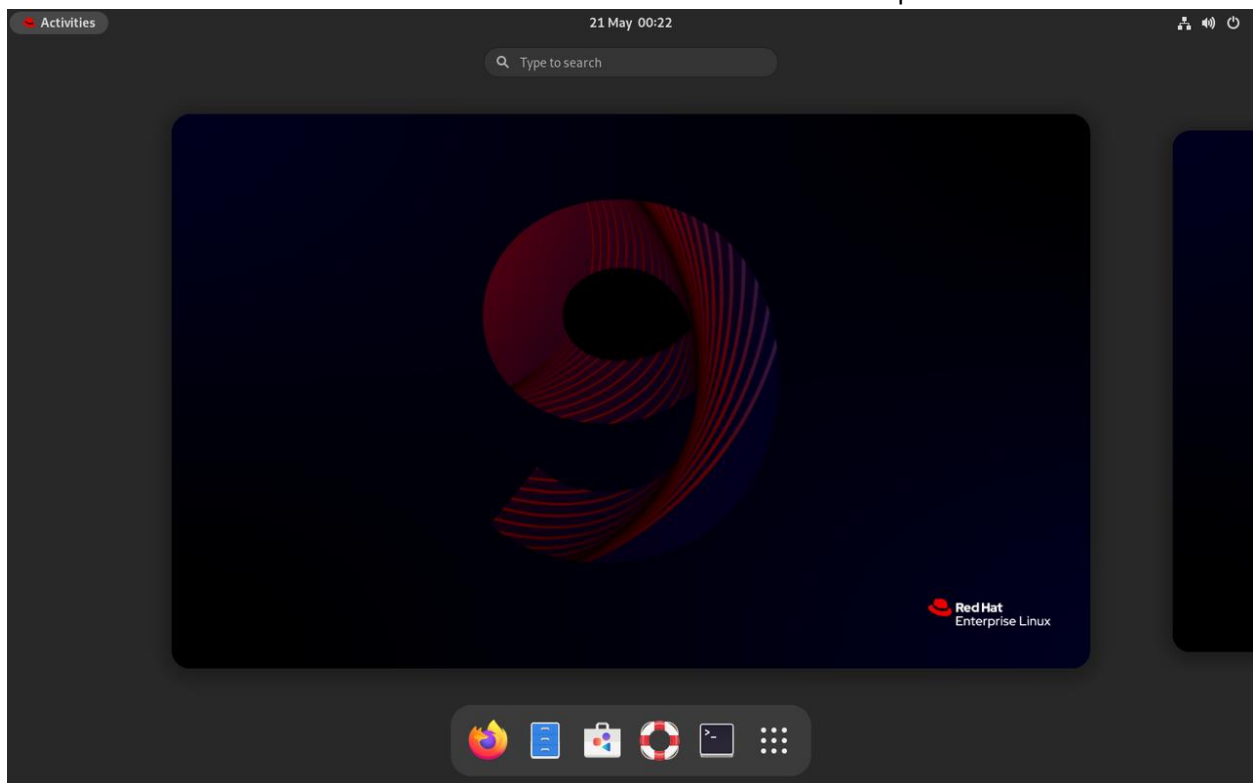
EMAIL RECEIVE



8.6 Web Server (Red Hat Linux)

The Red Hat Linux web server plays a pivotal role in hosting and delivering web-based applications and content. It provides a secure and high-performance platform for serving web pages, applications, and multimedia content to users within and outside the organization. Leveraging the power of open-source technology, the Red Hat Linux web server ensures seamless and efficient distribution of online resources, contributing to an enhanced user experience and promoting the organization's online presence.

The deployment of these services, along with the separate configuration of DHCP and DNS on the Active Directory server, exemplifies WinTeam6's commitment to providing a comprehensive and versatile suite of network and communication tools to meet the needs of a modern enterprise.



8.7 Server Redundancy for VMs

Implementing redundancy for critical components like Active Directory, Exchange Server, and web servers is essential to ensure high availability and minimize downtime. Virtualization can play a significant role in achieving this goal.

Active Directory:

Active Directory (AD) redundancy is crucial for maintaining proper user authentication, authorization, and domain services.

Exchange Server:

Redundancy for Exchange Server is crucial to maintain email communication without interruptions.

Web Server:

Redundancy for web servers is essential to maintain the availability of your website or web application. Additionally, consider backup and disaster recovery plans to complement your redundancy strategy.

9. Vulnerability Scan

A Vulnerability Scan is a systematic process of identifying security weaknesses and vulnerabilities within a computer system, network, application, or any other computing environment. Winteam6 will conduct vulnerability scans to proactively identify potential points of exploitation that malicious actors could leverage to compromise the confidentiality, integrity, or availability of the system or data.

10. Future Cloud Integration and VPN Implementation

As part of our commitment to staying at the forefront of technological advancements and ensuring continued scalability, WinTeam6 has strategic plans for both cloud integration and VPN implementation. While our current network infrastructure is designed to meet our present communication and data management needs, we recognize the potential benefits that these technologies can bring to our organization in terms of growth, flexibility, security, and ease of management.

10.1 Cloud Integration

Cloud integration offers several advantages, including:

Scalability: Cloud platforms provide the ability to easily scale up or down based on the organization's evolving requirements. This agility ensures that resources are allocated efficiently and cost-effectively, accommodating changes in demand without the need for extensive hardware investments.

Resource Optimization: Cloud services enable us to optimize resource allocation and utilization. This includes the dynamic allocation of computing resources, storage, and bandwidth, ensuring that we only pay for what we use.

Ease of Management: Cloud-based solutions simplify network and infrastructure management. Tasks such as software updates, security patches, and hardware maintenance can be managed centrally, reducing the administrative burden on our IT team.

Remote Accessibility: Cloud technology provides the flexibility for authorized personnel to access critical applications, data, and services remotely. This capability enhances collaboration and productivity, allowing employees to work from various locations.

Disaster Recovery and Redundancy: Cloud platforms offer robust disaster recovery options, ensuring data integrity and business continuity in the event of unforeseen disruptions. Redundancy measures provided by cloud providers enhance overall system reliability.

10.2 VPN Implementation

Virtual Private Network (VPN) technology enhances network security and enables secure remote access. A VPN provides encrypted communication over public networks, ensuring that data remains confidential and protected from unauthorized access. Our plans for VPN implementation include:

Secure Remote Access: VPNs will allow authorized users to securely access our internal network from remote locations, ensuring that sensitive data remains protected during transmission.

Data Encryption: VPNs encrypt data traffic, preventing eavesdropping and unauthorized interception of information. This ensures the confidentiality and integrity of data as it traverses public networks.

Enhanced Security: By implementing VPNs, we strengthen our network's overall security posture, mitigating the risks associated with remote access and ensuring that only authorized users can connect to our network.

Geographical Flexibility: VPN technology will enable employees working from different geographical locations to connect to our network securely, facilitating seamless collaboration and communication.

As WinTeam6 continues to experience growth and explore new avenues, we are actively evaluating opportunities for both cloud integration and VPN implementation. Our IT department is closely monitoring developments in these technologies and assessing how they align with our organizational goals. We envision a strategic and integrated approach that leverages cloud services and VPNs to complement and enhance our existing network infrastructure.

While our current focus remains on optimizing our internal network, we are committed to adapting and embracing cloud solutions and VPN technology when the time is right. By incorporating these advanced technologies into our network strategy, we aim to further elevate our network's capabilities, ensuring that WinTeam6 remains agile, competitive, and well-prepared for the future.

11. Password

All cisco routers and switches password is **cisco**.

ASA password is **Seahorse!Exfoliate@Tower#**

SSH Password-**Plug!Ball@Eggplant#**

12. Conclusion

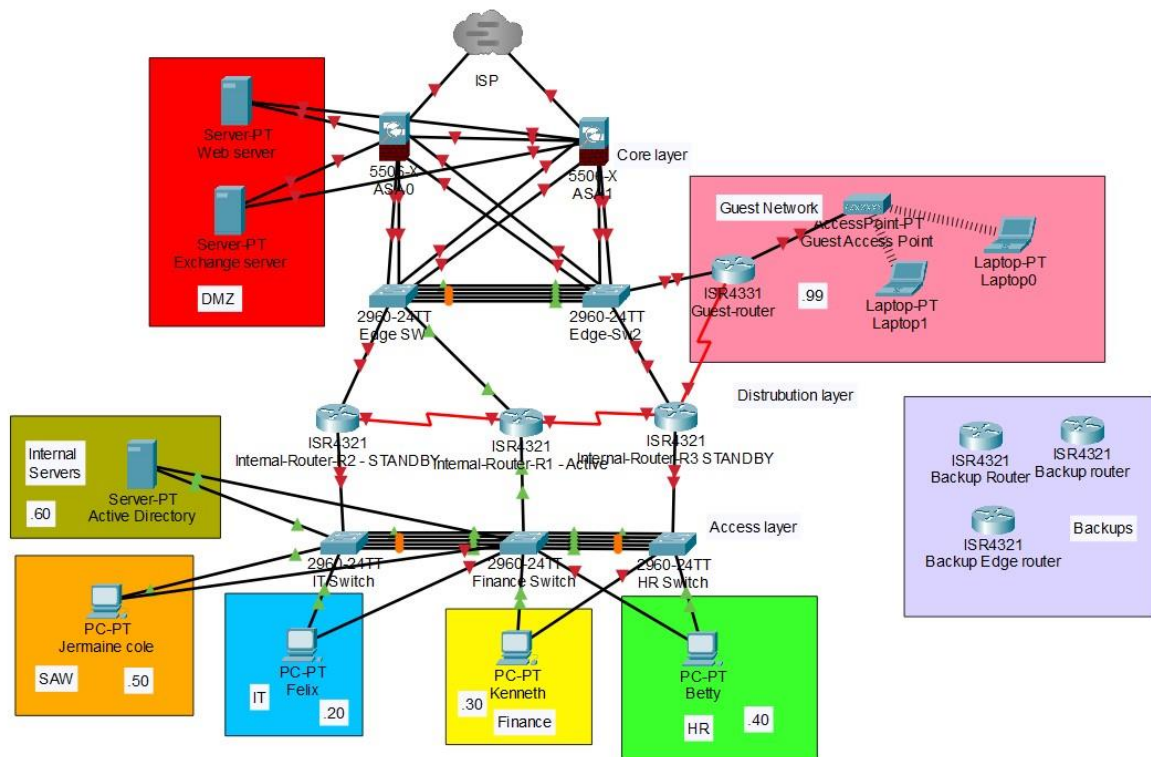
In conclusion, this advanced network documentation demonstrates WinTeam6's commitment to leveraging advanced networking technologies, protocols, and security measures to create a robust, efficient, and secure network infrastructure. The integration of OSPF, GLBP, EtherChannel's, NAT Translations, and InterVLAN Routing showcases our dedication to optimizing network performance and resilience. By implementing stringent security measures, including perimeter and internal security, switchport security, and Active Directory policies and permissions, WinTeam6 ensures data confidentiality, integrity, and controlled access. Through meticulous VLAN segmentation and the incorporation of specialized servers, seamless communication is achieved, catering to the unique needs of each department. Our strategic plans for cloud integration and VPN implementation further highlight our forward-looking approach, ensuring that WinTeam6 remains adaptable, competitive, and well-prepared for the future.

This advanced network documentation serves as a testament to WinTeam6's commitment to technological excellence and dedication to providing a secure, scalable, and future-ready network environment. The carefully designed network architecture, advanced networking technologies, robust security measures, and plans for cloud integration and VPN implementation collectively reflect our organization's proactive stance towards optimizing network performance, enhancing security, and facilitating efficient communication.

As WinTeam6 continues to grow and adapt to evolving technological landscapes, this documentation will serve as a valuable resource for network administrators, IT personnel, and stakeholders, providing comprehensive insights into the intricate design, configuration, and management of our advanced network infrastructure.

We remain diligent in our pursuit of excellence, driven by the goal of delivering a network environment that not only meets the current needs of our organization but also lays the foundation for continued innovation and success.

Thank you for your commitment to WinTeam6's technological vision.



Major Network: **10.0.5.0/24**

Available IP addresses in major network: **254**

Number of IP addresses needed: **34**

Available IP addresses in allocated subnets: **44**

About **22%** of available major network address space is used

About **77%** of subnetted network address space is used

Subnet Name	Needed Size	Allocated Size	Address	Mask	Dec Mask	Assignable Range	Broadcast
A	14	14	10.0.5.0	/28	255.255.255.240	10.0.5.1 - 10.0.5.14	10.0.5.15
B	4	6	10.0.5.16	/29	255.255.255.248	10.0.5.17 - 10.0.5.22	10.0.5.23
C	4	6	10.0.5.24	/29	255.255.255.248	10.0.5.25 - 10.0.5.30	10.0.5.31
D	4	6	10.0.5.32	/29	255.255.255.248	10.0.5.33 - 10.0.5.38	10.0.5.39
E	4	6	10.0.5.40	/29	255.255.255.248	10.0.5.41 - 10.0.5.46	10.0.5.47
F	4	6	10.0.5.48	/29	255.255.255.248	10.0.5.49 - 10.0.5.54	10.0.5.55